



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

A security engineer is reviewing event logs because an employee successfully connected a personal Windows laptop to the corporate network, which is against company policy. Company policy allows all Windows 10 and 11 laptops to connect to the system as long as the MDM agent installed by IT is running. Only compliant devices can connect, and the logic in the system to evaluate compliant laptops is as follows: Which of the following most likely occurred when the employee connected a personally owned Windows laptop and was allowed on the network?

```
if laptop['OsVersion'] >= 10:
    if laptop['agentRunning']:
        return COMPLIANT
    else:
        return NON_COMPLIANT
else:
    return COMPLIANT
```



- A. The agent was not running on the laptop, which triggered a false positive.
- B. The OS was a valid version, but the MDM agent was not installed, triggering a true positive.
- C. The OS was running a Windows version below 10 and triggered a false negative.
- D. The OS version was higher than 11, and the MDM agent was running, triggering a true negative.

**Correct Answer:** C

Community vote distribution

C (50%)

B (50%)

  **Learner213** 5 days, 8 hours ago

**Selected Answer: C**

I'm changing my answer to C. MDM is not installed, so the personal laptop should not be able to connect. A false negative is the only thing that makes sense.

upvoted 1 times

  **Learner213** 6 days, 10 hours ago

**Selected Answer: B**

The MDM is not running on the personal laptop. There is no indication of the version of Windows running on the laptop. Why would anyone assume the version is not 10 or 11?

B is the correct answer.

upvoted 1 times

An organization is working to secure its development process to ensure developers cannot deploy artifacts directly into the production environment. Which of the following security practice recommendations would be the best to accomplish this objective?

- A. Implement least privilege access to all systems.
- B. Roll out security awareness training for all users.
- C. Set up policies and systems with separation of duties.
- D. Enforce job rotations for all developers and administrators.
- E. Utilize mandatory vacations for all developers.
- F. Review all access to production systems on a quarterly basis.

**Correct Answer:** C

*Community vote distribution*

C (100%)

 **HopHopHipHip** 3 weeks, 2 days ago

**Selected Answer: C**

Separation of duties (SoD) is a foundational security principle that prevents a single individual from having control over all aspects of a critical process. In this case, it ensures that the people who write the code (developers) are not the same ones who deploy or approve it for production.

Job rotations: Useful for avoiding fraud and reducing knowledge silos, but not relevant to deployment control.

upvoted 2 times

A security architect discovers the following while reviewing code for a company's website: `selection = "SELECT Item FROM Catalog WHERE ItemID = " & Request("ItemID")`

Which of the following should the security architect recommend?

- A. Client-side processing
- B. Query parameterization
- C. Data normalization
- D. Escape character blocking
- E. URL encoding

**Correct Answer:** B

*Community vote distribution*

B (100%)


  **HopHopHipHip** 3 weeks, 2 days ago

**Selected Answer: B**

The code shown is vulnerable to SQL injection, as it directly concatenates user input (`Request("ItemID")`) into a SQL query. This allows attackers to manipulate the input to execute arbitrary SQL commands.

Query parameterization (also known as prepared statements) is the best defense against SQL injection. It ensures that user input is treated strictly as data, not executable SQL code.

upvoted 2 times

  **vichersong** 1 month, 1 week ago

**Selected Answer: B**

Query parameterization involves using placeholders in SQL statements, so user input is treated strictly as data, not as executable code. Prevents attackers from injecting malicious SQL code.

upvoted 2 times

A security architect needs to enable a container orchestrator for DevSecOps and SOAR initiatives. The engineer has discovered that several Ansible YAML files used for the automation of configuration management have the following content:

```
$ hostnamectl
COMPTIA001

$ cat /etc/ansible/ansible.cfg
[inventory]
enable_plugins = kubernetes.core.k8s

$ cat /etc/ansible/projects/roles/k8/default/main.yml
---
- Name: Create a Kubernetes Service Objects
  kubernetes.core.k8s:
    state: present
    definition:
      apiVersion: v2
      kind: Service

$ cat /etc/kubernetes/manifests
insecure-bind-address "localhost"
```

Which of the following should the engineer do to correct the security issues presented within this content?

- A. Update the kubernetes.core.k8s module to kubernetes.core.k8s\_service in the main.yml file.
- B. Update the COMPTIA001 hostname to localhost using the hostnamectl command.
- C. Update the state: present module to state: absent in the main.yml file.
- D. Update or remove the ansible.cfg file.
- E. Update the insecure-bind-address from localhost to the COMPTIA001 in the manifests file.

**Correct Answer: D**

Community vote distribution

E (100%)

 **vichersong** 1 month, 1 week ago

**Selected Answer: E**

The main concern in this context is that the API server is explicitly bound using the insecure-bind-address, which:

Is deprecated and discouraged in secure Kubernetes environments.

May allow unauthenticated access to the Kubernetes API if not tightly controlled.

Should be removed altogether or replaced with secure configurations.

Switching insecure-bind-address to a hostname (like COMPTIA001) doesn't solve the underlying issue — instead, removing this flag is the best practice.

So while option E addresses the specific insecure setting shown, the ideal fix is actually:

Remove the insecure-bind-address flag altogether from the manifest.

upvoted 2 times

A CRM company leverages a CSP PaaS service to host and publish its SaaS product. Recently, a large customer requested that all infrastructure components must meet strict regulatory requirements, including configuration management, patch management, and life-cycle management. Which of the following organizations is responsible for ensuring those regulatory requirements are met?

- A. The CRM company
- B. The CRM company's customer
- C. The CSP
- D. The regulatory body

**Correct Answer:** A

*Community vote distribution*

A (100%)

  **vicbersong** 1 month, 1 week ago

**Selected Answer: A**

The CRM company is using a PaaS (like Azure App Service, Google App Engine, or Heroku) to host their SaaS product. So they own the app, and must ensure:

It complies with regulations

It's securely configured

It's patched and maintained

Even though the CSP handles the platform, the CRM company is still responsible for making sure everything above the platform layer meets the requirements.

upvoted 2 times

Company A is merging with Company B. Company A is a small, local company. Company B has a large, global presence. The two companies have a lot of duplication in their IT systems, processes, and procedures. On the new Chief Information Officer's (CIO's) first day, a fire breaks out at Company B's main data center. Which of the following actions should the CIO take first?

- A. Determine whether the incident response plan has been tested at both companies, and use it to respond.
- B. Review the incident response plans, and engage the disaster recovery plan while relying on the IT leaders from both companies.
- C. Ensure hot, warm, and mobile disaster recovery sites are available, and give an update to the companies' leadership teams.
- D. Initiate Company A's IT systems processes and procedures, assess the damage, and perform a BIA.

**Correct Answer:** B

*Community vote distribution*

B (100%)

  **vicbersong** 1 month, 1 week ago

**Selected Answer:** B

When a critical incident like a data center fire occurs, the first step for a newly appointed CIO is to:

Review the existing incident response (IR) plans.

Engage the appropriate disaster recovery (DR) protocols to restore services.

Coordinate with existing IT leaders from both companies who understand the systems and response procedures.

Since Company A and Company B have not yet fully merged and the CIO is new, relying on existing staff familiar with the environments is essential for a quick and informed response.

upvoted 2 times

The results of an internal audit indicate several employees reused passwords that were previously included in a published list of compromised passwords.

The company has the following employee password policy:

Attribute	Requirement
Complexity	Enabled
Character class	Special character, number
Length	10 characters
History	8
Maximum age	60 days
Minimum age	0

Which of the following should be implemented to best address the password reuse issue? (Choose two.)

- A. Increase the minimum age to two days.
- B. Increase the history to 20.
- C. Increase the character length to 12.
- D. Add case-sensitive requirements to character class.
- E. Decrease the maximum age to 30 days.
- F. Remove the complexity requirements.
- G. Increase the maximum age to 120 days.

**Correct Answer:** AB

Currently there are no comments in this discussion, be the first to comment!



A mobile administrator is reviewing the following mobile device DHCP logs to ensure the proper mobile settings are applied to managed devices:

```
10,10/18/2021,17:01:05,Assign,192.168.1.10,UserA-MobileDevice,0236FB12CA0B
23,10/19/2021,07:11:19,Assign,192.168.1.23,UserA-MobileDevice,068ADIFAB109
10,10/20/2021,19:22:56,Assign,192.168.1.96,UserA-MobileDevice,0ABC65E81AB0
10,10/21/2021,22:34:15,Assign,192.168.1.33,UserA-MobileDevice,BAC034EF9451
10,10/22/2021,11:55:41,Assign,192.168.1.12,UserA-MobileDevice,0E938663221B
```

Which of the following mobile configuration settings is the mobile administrator verifying?

- A. Service set identifier authentication
- B. Wireless network auto joining
- C. 802.1X with mutual authentication
- D. Association MAC address randomization

**Correct Answer:** D

Currently there are no comments in this discussion, be the first to comment!

A security analyst is investigating a possible insider threat incident that involves the use of an unauthorized USB from a shared account to exfiltrate data. The event did not create an alert. The analyst has confirmed the USB hardware ID is not on the device allow list, but has not yet confirmed the owner of the USB device. Which of the following actions should the analyst take next?

- A. Classify the incident as a false positive.
- B. Classify the incident as a false negative.
- C. Classify the incident as a true positive.
- D. Classify the incident as a true negative.

**Correct Answer:** B

*Community vote distribution*

B (100%)

🗨️ 👤 **vicbersong** 1 month, 1 week ago

**Selected Answer: B**

A false negative occurs when a real threat is not detected by security systems or does not trigger an alert — exactly what happened here.

The unauthorized USB was not on the allow list, indicating a policy violation (a real threat), yet no alert was generated.

upvoted 2 times

Which of the following security features do email signatures provide?

- A. Non-repudiation
- B. Body encryption
- C. Code signing
- D. Sender authentication
- E. Chain of custody

**Correct Answer:** A

*Community vote distribution*

A (100%)

  **vichersong** 1 month, 1 week ago

**Selected Answer:** A

Non-repudiation: This means the sender cannot deny sending the message, because the digital signature proves the email came from them and was not altered in transit.

upvoted 3 times

A software development company wants to ensure that users can confirm the software is legitimate when installing it. Which of the following is the best way for the company to achieve this security objective?

- A. Code signing
- B. Non-repudiation
- C. Key escrow
- D. Private keys

**Correct Answer:** A

*Community vote distribution*

A (100%)

 **vicbersong** 1 month, 1 week ago

**Selected Answer: A**

Code signing uses a digital signature to verify that software has:

Come from a trusted source (authenticity)

Not been altered since it was signed (integrity)

This allows users to confirm the software is legitimate during installation

upvoted 2 times



While performing mandatory monthly patch updates on a production application server, the security analyst reports an instance of buffer overflow for a new application that was migrated to the cloud and is also publicly exposed. Security policy requires that only internal users have access to the application. Which of the following should the analyst implement to mitigate the issues reported? (Choose two.)

- A. Configure firewall rules to block all external traffic.
- B. Enable input validation for all fields.
- C. Enable automatic updates to be installed on all servers.
- D. Configure the security group to enable external traffic.
- E. Set up a DLP policy to alert for exfiltration on all application servers.
- F. Enable nightly vulnerability scans.

**Correct Answer:** AB

*Community vote distribution*

AB (100%)

  **vicbersong** 1 month, 1 week ago

**Selected Answer:** AB

A. Configure firewall rules to block all external traffic

Restricts access so only internal users can connect, aligning with policy.

B. Enable input validation for all fields

Input validation is critical to prevent buffer overflow and other injection attacks.

upvoted 2 times

PKI can be used to support security requirements in the change management process. Which of the following capabilities does PKI provide for messages?

- A. Non-repudiation
- B. Confidentiality
- C. Delivery receipts
- D. Attestation

**Correct Answer:** A

*Community vote distribution*

A (100%)

 **vichersong** 1 month, 1 week ago

**Selected Answer: A**

PKI (Public Key Infrastructure) supports several security goals, and one of its key features is non-repudiation – ensuring that:

A sender cannot deny having sent a message.

This is achieved through digital signatures, which use a sender's private key to sign messages.

upvoted 2 times

Several unlabeled documents in a cloud document repository contain cardholder information. Which of the following configuration changes should be made to the DLP system to correctly label these documents in the future?

- A. Digital rights management
- B. Network traffic decryption
- C. Regular expressions
- D. Watermarking

**Correct Answer:** C

*Community vote distribution*

C (100%)

  **vicbersong** 1 month, 1 week ago

**Selected Answer: C**

DLP (Data Loss Prevention) systems use pattern matching to identify sensitive information like:

Credit card numbers

Social Security numbers

Bank account details

To detect cardholder information, DLP systems typically rely on:

Regular expressions (regex) to match patterns such as the 16-digit format of credit card numbers.

Additional logic like Luhn checks to validate numbers.

By configuring the DLP system with appropriate regex patterns, it can automatically identify and label documents containing cardholder data in the future.

upvoted 4 times

A systems administrator at a web-hosting provider has been tasked with renewing the public certificates of all customer sites. Which of the following would best support multiple domain names while minimizing the amount of certificates needed?

- A. OCSP
- B. CRL
- C. SAND. CA

**Correct Answer:** C

*Community vote distribution*

C (100%)

🗨️ 👤 **Bright07** 2 weeks ago

**Selected Answer: C**

That is typographical error. The administrator was trying to write C. SAN and D. CA.

upvoted 2 times

🗨️ 👤 **vichersong** 1 month, 1 week ago

**Selected Answer: C**

The Subject Alternative Name (SAN) extension in an SSL/TLS certificate allows multiple domain names to be secured using a single certificate.

This is ideal for a web hosting provider managing many customer sites, such as:

www.customer1.com

mail.customer1.com

customer2.net

Instead of issuing separate certificates for each domain, a SAN certificate consolidates them, minimizing overhead and simplifying management.

C. SAND. CA – This appears to be a typo or incorrect term; the intended answer is SAN.

upvoted 4 times



Which of the following best explain why organizations prefer to utilize code that is digitally signed? (Choose two.)

- A. It provides origin assurance.
- B. It verifies integrity.
- C. It provides increased confidentiality.
- D. It integrates with DRMs.
- E. It verifies the recipient's identity.
- F. It ensures the code is free of malware.

**Correct Answer:** AB

*Community vote distribution*

AB (100%)

  **vichersong** 1 month, 1 week ago

**Selected Answer:** AB

Digitally signed code uses cryptographic techniques to:

- A. Provide origin assurance – Confirms the software came from a trusted, verified publisher.
- B. Verify integrity – Ensures the code has not been modified or tampered with after it was signed.

These are the two main security benefits of digital code signing.

upvoted 2 times

A security engineer receives reports through the organization's bug bounty program about remote code execution in a specific component in a custom application. Management wants to properly secure the component and proactively avoid similar issues. Which of the following is the best approach to uncover additional vulnerable paths in the application?

- A. Leverage an exploitation framework to uncover vulnerabilities.
- B. Use fuzz testing to uncover potential vulnerabilities in the application.
- C. Utilize a software composition analysis tool to report known vulnerabilities.
- D. Reverse engineer the application to look for vulnerable code paths.
- E. Analyze the use of an HTTP intercepting proxy to dynamically uncover issues.

**Correct Answer:** B

*Community vote distribution*

B (100%)

  **vicbersong** 1 month, 1 week ago

**Selected Answer: B**

Fuzz testing (fuzzing) is a proactive dynamic application security testing technique where the system is bombarded with random, malformed, or unexpected inputs to discover:

Buffer overflows

Input validation issues

Memory corruption

Remote code execution flaws

Since the report is about remote code execution, fuzzing is ideal to uncover other vulnerable paths in the same component or similar logic areas.  
upvoted 2 times

A security technician is investigating a system that tracks inventory via a batch update each night. The technician is concerned that the system poses a risk to the business, as errors are occasionally generated and reported inventory appears incorrect. The following output log is provided:

Starting Boxes = 20

Transaction	Operation	Running total
1	+ 10	30
2	+ 30	50
3	+ 10	60
4	- 10	50
5	- 40	(Below zero balance!) -10
6	+ 30	20
7	+ 10	60
8	+ 40	60

The technician reviews the output of the batch job and discovers that the inventory was never less than zero, and the final inventory was 100 rather than 60. Which of the following should the technician do to resolve this issue?

- A. Ensure that the application is using memory-safe functions to prevent integer overflows.
- B. Recommend thread-safe processes in the code to eliminate race conditions.
- C. Require the developers to include exception handlers to accommodate out-of-bounds results.
- D. Move the batch processing from client side to server side to remove client processing inconsistencies.

**Correct Answer:** C

Currently there are no comments in this discussion, be the first to comment!

A programmer is reviewing the following proprietary piece of code that was identified as a vulnerability due to users being authenticated when they provide incorrect credentials:

```
GET USERID
GET PASS
JUMP TO :ALLOWUSER:
    IF USERID == GETDBUSER(USERID) AND HASH(PASS) == GETDBPASS(USERID)
EXIT
:ALLOWUSER:
SET USERACL(USERID)
...
...
...
```

Which of the following should the programmer implement to remediate the code vulnerability?

- A. Salted hashing via the proprietary SHASH function
- B. Input validation in the first two lines of code
- C. Atomic execution of subroutines
- D. TOCTOU remediation in SET USERACL
- E. Database connection over encrypted channels

**Correct Answer:** B

Community vote distribution

B (100%)

 **vichersong** 1 month, 1 week ago

**Selected Answer:** B

- Input validation ensures that user-supplied data (such as USERID and PASS) meets security requirements before being processed.
- Without proper validation, attackers might inject unexpected values to bypass authentication or exploit the system.

upvoted 1 times

A senior cybersecurity engineer is solving a digital certificate issue in which the CA denied certificate issuance due to failed subject identity validation. At which of the following steps within the PKI enrollment process would the denial have occurred?

- A. RAB. OCSP
- C. CA
- D. IdP

**Correct Answer: A**

*Community vote distribution*

A (100%)

  **vichersong** 1 month, 1 week ago

**Selected Answer: A**

RA (✓ Correct Answer): Verifies the subject's identity during enrollment.

CA: Issues or denies certificates, but relies on the RA for identity validation. If the RA fails the subject, the CA doesn't proceed.

OCSP: Checks revocation status of an already issued certificate. Not part of the issuance process.

IdP (Identity Provider): Used in federated identity or SSO systems, not standard PKI enrollment.

upvoted 4 times

An internal user can send encrypted emails successfully to all recipients, except one. at an external organization. When the internal user attempts to send encrypted emails to this external recipient, a security error message appears. The issue does not affect unencrypted emails. The external recipient can send encrypted emails to internal users. Which of the following is the most likely cause of the issue?

- A. The validity dates of the external recipient's private key do not match the SSH keys with which the internal user is accessing the system.
- B. The external recipient has an expired public/private key pair that has not been revoked by the CA.
- C. The internal user's company email servers have an incorrect implementation of OCSP and CRL settings.
- D. The external recipient's email address and the email address associated with the external recipient's public key are mismatched.

**Correct Answer:** D

Currently there are no comments in this discussion, be the first to comment!

A security administrator is setting up a virtualization solution that needs to run services from a single host. Each service should be the only one running in its environment. Each environment needs to have its own operating system as a base but share the kernel version and properties of the running host. Which of the following technologies would best meet these requirements?

- A. Containers
- B. Type 1 hypervisor
- C. Type 2 hypervisor
- D. Virtual desktop infrastructure
- E. Emulation

**Correct Answer:** A

Currently there are no comments in this discussion, be the first to comment!

A company has data it would like to aggregate from its PLCs for data visualization and predictive maintenance purposes. Which of the following is the most likely destination for the tag data from the PLCs?

- A. External drive
- B. Cloud storage
- C. System aggregator
- D. Local historian

**Correct Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!



Which of the following is the best way to protect the website browsing history for an executive who travels to foreign countries where internet usage is closely monitored?

- A. DOH
- B. EAP-TLS
- C. Geofencing
- D. Private browsing mode

**Correct Answer:** A

*Community vote distribution*

A (100%)

🗨️ 👤 **vichersong** 1 month ago

**Selected Answer: A**

✓ Correct Answer: A. DOH (DNS over HTTPS)

Why:

DNS over HTTPS encrypts DNS queries, preventing third parties (like governments or ISPs in foreign countries) from seeing which websites the executive is trying to visit. This helps protect privacy by obscuring the domain names being accessed, which are typically exposed during DNS resolution.

✗ Why the Others Are Less Suitable:

B. EAP-TLS:

This is used for secure authentication on networks (e.g., Wi-Fi), not for protecting website browsing history.

C. Geofencing:

It's used to restrict or allow access based on location — not for encrypting or hiding browsing activity.

D. Private Browsing Mode:

This only prevents local storage of browsing data (e.g., cookies, history) on the device, but does not hide activity from ISPs or network monitors.  
upvoted 4 times

A systems administrator is working with the SOC to identify potential intrusions associated with ransomware. The SOC wants the systems administrator to perform network-level analysis to identify outbound traffic from any infected machines. Which of the following is the most appropriate action for the systems administrator to take?

- A. Monitor for IoCs associated with C&C communications.
- B. Tune alerts to identify changes to administrative groups.
- C. Review NetFlow logs for unexpected increases in egress traffic.
- D. Perform binary hash comparisons to identify infected devices.

**Correct Answer:** C

Community vote distribution

C (100%)

 **vickersong** Highly Voted 1 month ago

**Selected Answer:** C

Explanation:

Ransomware often communicates with Command and Control (C&C) servers or exfiltrates data, resulting in unusual outbound (egress) network traffic.

NetFlow logs capture metadata about traffic flows (such as source/destination IPs, ports, bytes transferred), allowing the systems administrator to:

Detect unusual or high-volume outbound traffic from machines that might be infected.

Spot patterns consistent with data exfiltration or C&C communication.

▮ Why the Others Are Less Suitable:

A. Monitor for IoCs associated with C&C communications:

This is a SOC-level activity, more about signature-based or behavioral monitoring – not direct network-level analysis by a systems admin.

B. Tune alerts to identify changes to administrative groups:

Useful for detecting privilege escalation, but not directly related to identifying ransomware's outbound traffic.

D. Perform binary hash comparisons to identify infected devices:

This is host-level analysis, not network-level. Also requires known malicious file hashes.

upvoted 5 times

A retail organization wants to properly test and verify its capabilities to detect and/or prevent specific TTPs as mapped to the MITRE ATTACK framework specific to APTs. Which of the following should be used by the organization to accomplish this goal?

- A. Tabletop exercise
- B. Penetration test
- C. Sandbox detonation
- D. Honeypot

**Correct Answer:** B

Community vote distribution

B (100%)

🗳️ 👤 **vicbersong** 1 month ago

**Selected Answer: B**

❓ Why the Others Are Less Appropriate:

A. Tabletop exercise

Simulates incident response in a discussion-based format — no real testing of controls or detection capabilities.

C. Sandbox detonation

Tests how malware behaves in a safe environment — useful for analyzing malicious files, not TTP-based detection across the network.

D. Honeypot

Lures attackers for monitoring, but passive and not suited for systematic, targeted testing based on a known framework like MITRE ATT&CK.  
upvoted 2 times

🗳️ 👤 **vicbersong** 1 month ago

**Selected Answer: B**

To test and verify capabilities to detect and/or prevent specific TTPs (Tactics, Techniques, and Procedures) from the MITRE ATT&CK framework — especially those used by Advanced Persistent Threats (APTs) — an organization needs a realistic, controlled simulation of attacks.

A penetration test (or more specifically, a red team engagement) can be tailored to emulate adversary behavior mapped directly to the MITRE ATT&CK framework. This allows the organization to:

Actively test defenses against known APT TTPs.

Identify detection gaps and improve response.

Measure how well existing security controls and processes perform.

upvoted 2 times

IoCs were missed during a recent security incident due to the reliance on a signature-based detection platform. A security engineer must recommend a solution that can be implemented to address this shortcoming. Which of the following would be the most appropriate recommendation?

- A. FIM
- B. SASEC. UEBA
- D. CSPM
- E. EAP

**Correct Answer:** D

Community vote distribution

D (100%)

🗳️ **vicbersong** 1 month ago

**Selected Answer: D**

✗ Why the Others Are Less Suitable:

A. FIM (File Integrity Monitoring)

Monitors changes to files – good for detecting unauthorized modifications, but not sufficient for behavioral analysis or detecting unknown threats.

B. SASE (Secure Access Service Edge)

Network architecture concept combining networking and security – doesn't directly address IoC detection.

D. CSPM (Cloud Security Posture Management)

Ensures cloud configurations comply with best practices – useful for preventative controls, not detection of novel attacks.

E. EAP (Extensible Authentication Protocol)

Authentication framework – not related to threat detection.

upvoted 2 times

🗳️ **vicbersong** 1 month ago

**Selected Answer: D**

✓ C. UEBA (User and Entity Behavior Analytics)

Explanation:

The issue described – missed IoCs due to reliance on signature-based detection – highlights a gap in detecting unknown or novel threats. Signature-based systems only catch known threats, so behavioral-based detection is needed to address this shortcoming.

UEBA (User and Entity Behavior Analytics):

Uses machine learning and analytics to establish baselines of normal behavior.

Detects anomalies and suspicious patterns (e.g., unusual logins, data exfiltration) that may indicate compromise – even if there's no known signature.

Excellent for catching insider threats, account compromise, and sophisticated attacks that evade traditional tools.

upvoted 2 times

🗳️ **\_Jannat** 3 months ago

**Selected Answer: D**

The best recommendation to address the shortcoming of missed IoCs is C. UEBA (User and Entity Behavior Analytics), as it provides advanced, behavioral-based detection that can identify suspicious activities, even those not matching known attack signatures.

upvoted 2 times

🗳️ **62314b7** 4 months ago

**Selected Answer: D**

Correct answer shows as "C", but there is no "C" option displayed. Just "A,B,D,E".

upvoted 2 times

A company that provides services to clients who work with highly sensitive data would like to provide assurance that the data's confidentiality is maintained in a dynamic, low-risk environment. Which of the following would best achieve this goal? (Choose two.)

- A. Install a SOAR on all endpoints.
- B. Hash all files.
- C. Install SIEM within a SOC.
- D. Encrypt all data and files at rest, in transit, and in use.
- E. Configure SOAR to monitor and intercept files and data leaving the network.
- F. Implement file integrity monitoring.

**Correct Answer:** DF

Community vote distribution

DF (75%)

DE (25%)

🗳️ 👤 **jagoichi** 4 days, 10 hours ago

**Selected Answer: DE**

Question only mentions maintain confidentiality :

E. Configure SOAR to monitor and intercept files and data leaving the network

A SOAR (Security Orchestration, Automation, and Response) system can automate data loss prevention (DLP) actions.

Monitoring and intercepting data exfiltration adds an additional layer of confidentiality assurance, particularly in a dynamic environment  
upvoted 1 times

🗳️ 👤 **vicbersong** 1 month ago

**Selected Answer: DF**

The best choices for ensuring data confidentiality in a dynamic, low-risk environment are:

**\*\*D. Encrypt all data and files at rest, in transit, and in use.\*\***

Encryption is fundamental to protecting sensitive data from unauthorized access. By encrypting data at all stages—whether stored, transmitted, or actively used—organizations can significantly reduce the risk of exposure.

**\*\*F. Implement file integrity monitoring.\*\***

File integrity monitoring helps detect unauthorized changes to sensitive files, ensuring that data remains unaltered and secure. This is particularly useful for identifying potential breaches or insider threats.

While **\*\*C. Installing SIEM within a SOC\*\*** is valuable for security monitoring, it primarily focuses on threat detection rather than directly ensuring confidentiality. **\*\*E. Configuring SOAR to monitor and intercept files\*\*** can help prevent data leaks, but encryption and integrity monitoring provide more direct assurance of confidentiality.

Would you like recommendations on specific tools or implementation strategies?  
upvoted 3 times

An organization wants to implement an access control system based on its data classification policy that includes the following data types:

Confidential -

Restricted -

Internal -

Public Flag for Review -

The access control system should support SSO federation to map users into groups. Each group should only access systems that process and store data at the classification assigned to the group. Which of the following should the organization implement to enforce its requirements with a minimal impact to systems and resources?

- A. A tagging strategy in which all resources are assigned a tag based on the data classification type, and a system that enforces attribute-based access control
- B. Role-based access control that maps data types to internal roles, which are defined in the human resources department's source of truth system
- C. Network microsegmentation based on data types, and a network access control system enforcing mandatory access control based on the user principal
- D. A rule-based access control strategy enforced by the SSO system with rules managed by the internal LDAP and applied on a per-system basis

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **vicbersong** 1 month ago

**Selected Answer: A**

To enforce the organization's requirements with minimal impact to systems and resources, Option A seems to be the most suitable choice:

A. A tagging strategy in which all resources are assigned a tag based on the data classification type, and a system that enforces attribute-based access control

Here's why:

Tagging Strategy: Assigning tags based on data classification types allows for flexible and scalable management of resources.

Attribute-Based Access Control (ABAC): This approach can dynamically enforce access policies based on attributes, such as user roles, data classification, and other contextual information. It supports fine-grained access control and can be integrated with SSO federation to map users into groups.

This method ensures that each group can only access systems that process and store data at the classification assigned to the group, aligning with the organization's data classification policy.

upvoted 1 times

A security analyst was monitoring the networks of a group of companies. The analyst identified several periods of concentrated, coordinated activity by unknown actors. The activity repeated at regular intervals and affected all the companies. Minor hardware outages that correlated with the same times as the discovered activity escalated in severity. Which of the following threat actors was most likely involved?

- A. An organized crime collective running a ransomware campaign
- B. A group of politically motivated hackers
- C. Disgruntled employees who were recently terminated
- D. An advanced persistent threat financed by a nation-state

**Correct Answer:** D

*Community vote distribution*

D (100%)

  **vicbersong** 1 month ago

**Selected Answer:** D

Given the description of the threat, the most likely actor involved is:

- D. An advanced persistent threat (APT) financed by a nation-state

Here's why:

**Coordinated Activity:** APTs are known for their sophisticated, coordinated attacks that can span long periods.

**Regular Intervals:** APTs often conduct their operations in a methodical manner, which can include regular intervals of activity.

**Escalating Severity:** The gradual increase in severity of the hardware outages suggests a strategic approach to weaken defenses over time, a hallmark of APTs.

**Multiple Companies:** APTs typically target multiple organizations, especially those of strategic interest to the sponsoring nation-state

upvoted 1 times



The company's client service team is receiving a large number of inquiries from clients regarding a new vulnerability. Which of the following would provide the customer service team with a consistent message to deliver directly to clients?

- A. Communication plan
- B. Response playbook
- C. Disaster recovery procedure
- D. Automated runbook

**Correct Answer:** B

*Community vote distribution*

B (100%)

 **vicbersong** 1 month ago

**Selected Answer: B**

The best option for providing the customer service team with a consistent message to deliver directly to clients would be:

B. Response playbook

A response playbook is a predefined guide designed to ensure consistent communication and response during specific incidents, such as addressing a new vulnerability. It typically contains templates, instructions, and key messages for customer-facing teams, ensuring they can communicate accurate and consistent information to clients.

upvoted 1 times

A company wants to use a process to embed a sign of ownership covertly inside a proprietary document without adding any identifying attributes. Which of the following would be best to use as part of the process to support copyright protections of the document?

- A. Steganography
- B. E-signature
- C. Watermarking
- D. Cryptography

**Correct Answer:** A

Community vote distribution

A (100%)

🗲️ 👤 **vichersong** 1 month ago

**Selected Answer: A**

Why the other options are less suitable:

B. E-signature: An electronic signature is a visible and verifiable signature used for authentication and validation of a document. It doesn't hide ownership but instead provides clear identification and verification.

C. Watermarking: Watermarking typically involves adding visible or semi-visible marks on a document that signify ownership. While it provides copyright protection, it's not covert since it can often be seen.

D. Cryptography: Cryptography involves securing data, but it's generally used to protect the integrity and confidentiality of a document, not to covertly indicate ownership.

upvoted 1 times

🗲️ 👤 **vichersong** 1 month ago

**Selected Answer: A**

The best option for embedding a sign of ownership covertly inside a proprietary document without adding any identifying attributes would be:

A. Steganography

Steganography is the practice of hiding data (such as a sign of ownership or a copyright mark) inside a file or document in a way that is not easily detectable. This method allows the owner to embed a covert mark of ownership that is hidden within the document, thus providing protection without revealing any visible identifying attributes.

upvoted 1 times

Which of the following utilizes policies that route packets to ensure only specific types of traffic are being sent to the correct destination based on application usage?

- A. SDN
- B. pcap
- C. vmstat
- D. DNSSEC
- E. VPC

**Correct Answer:** A

*Community vote distribution*



 **vicbersong** 1 month ago

**Selected Answer: A**

A. SDN (Software-Defined Networking)

SDN (Software-Defined Networking) is a networking architecture that allows for more flexible control over how network traffic is routed. It utilizes centralized control and policies to direct packets to specific destinations based on factors like application usage. This means traffic can be routed based on application needs, network conditions, and security policies, ensuring that only specific types of traffic reach their intended destinations.

upvoted 1 times

An incident response team completed recovery from offline backup for several workstations. The workstations were subjected to a ransomware attack after users fell victim to a spear-phishing campaign, despite a robust training program. Which of the following questions should be considered during the lessons-learned phase to most likely reduce the risk of reoccurrence? (Choose two.)

- A. Are there opportunities for legal recourse against the originators of the spear-phishing campaign?
- B. What internal and external stakeholders need to be notified of the breach?
- C. Which methods can be implemented to increase speed of offline backup recovery?
- D. What measurable user behaviors were exhibited that contributed to the compromise?
- E. Which technical controls, if implemented, would provide defense when user training fails?
- F. Which user roles are most often targeted by spear phishing attacks?

**Correct Answer:** DE

*Community vote distribution*

DE (100%)

  **vicbersong** 1 month ago

**Selected Answer: DE**

D. What measurable user behaviors were exhibited that contributed to the compromise?

Understanding the specific behaviors that led to the compromise is crucial in refining both training and security awareness programs. By analyzing what users did (e.g., opening attachments, clicking links) and correlating that with patterns of failure, the organization can tailor future training and prevention efforts to target those specific behaviors.

E. Which technical controls, if implemented, would provide defense when user training fails?

Even with robust training programs, users can still fall victim to phishing attacks. Implementing technical controls (like advanced email filtering, multi-factor authentication, or endpoint detection and response systems) can help mitigate the impact when training fails. These defences can provide an additional layer of security to prevent or lessen the severity of successful attacks.

upvoted 1 times

Two companies that recently merged would like to unify application access between the companies, without initially merging internal authentication stores. Which of the following technical strategies would best meet this objective?

- A. Federation
- B. RADIUS
- C. TACACS+
- D. MFA
- E. ABAC

**Correct Answer:** A

*Community vote distribution*



 **vicbersong** 1 month ago

**Selected Answer: A**

The best technical strategy to unify application access between two companies without merging their internal authentication stores is A. Federation.

Federation allows different organizations to establish trust relationships, enabling users to access applications across organizational boundaries without needing to merge authentication stores

upvoted 2 times

An analyst needs to evaluate all images and documents that are publicly shared on a website. Which of the following would be the best tool to evaluate the metadata of these files?

- A. OllyDbg
- B. ExifTool
- C. Volatility
- D. Ghidra

**Correct Answer:** B

*Community vote distribution*

B (100%)

🗨️ 👤 **vicbersong** 1 month ago

**Selected Answer: B**

B. ExifTool

ExifTool is a powerful and widely used command-line tool for reading, writing, and editing metadata in a wide variety of file types, including images and documents. It can extract metadata such as timestamps, camera info, GPS coordinates, authorship, and software used — making it ideal for evaluating files shared publicly on a website.

upvoted 1 times

An organization has deployed a cloud-based application that provides virtual event services globally to clients. During a typical event, thousands of users access various entry pages within a short period of time. The entry pages include sponsor-related content that is relatively static and is pulled from a database. When the first major event occurs, users report poor response time on the entry pages. Which of the following features is the most appropriate for the company to implement?

- A. Horizontal scalability
- B. Vertical scalability
- C. Containerization
- D. Static code analysis
- E. Caching

**Correct Answer:** E

*Community vote distribution*

E (100%)

  **vichersong** 1 month ago

**Selected Answer: E**

Why the other options are less optimal on their own:

A. Horizontal scalability: Helps handle more traffic, but without caching, the load on the database remains high, especially for static content.

B. Vertical scalability: Limited benefits, and scaling up a server won't fix inefficient use of resources (e.g., querying static data repeatedly).

C. Containerization: Useful for deployment and isolation, but doesn't solve performance issues related to database access.

D. Static code analysis: Relevant to security and code quality, not performance during runtime.

upvoted 1 times

  **vichersong** 1 month ago

**Selected Answer: E**

The performance issue is occurring on entry pages that contain static sponsor-related content which is pulled from a database. This is a classic use case for caching, which can significantly reduce database load and response times by storing frequently accessed data closer to the user or application.

✓ Caching would:

Store the static sponsor content either in memory (e.g., Redis, Memcached) or at the edge (e.g., CDN).

Reduce the number of repeated database queries for the same static data.

Improve response times and scalability under heavy user loads.

upvoted 1 times

An organization's board of directors has asked the Chief Information Security Officer to build a third-party management program. Which of the following best explains a reason for this request?

- A. Risk transference
- B. Supply chain visibility
- C. Support availability
- D. Vulnerability management

**Correct Answer:** B

*Community vote distribution*

B (100%)

 **vichersong** 1 month ago

**Selected Answer: B**

The board asking the Chief Information Security Officer (CISO) to build a third-party management program is most likely motivated by the need for supply chain visibility – understanding and managing the security risks posed by vendors, partners, and service providers that interact with the organization's systems or data.

A third-party management program helps the organization:

Identify and assess third-party vendors.

Understand what data and systems those vendors access.

Monitor and reduce risks in the supply chain.

Ensure compliance with regulatory and security standards.

upvoted 1 times



A company is rewriting a vulnerable application and adding the `mprotect()` system call in multiple parts of the application's code that was being leveraged by a recent exploitation tool. Which of the following should be enabled to ensure the application can leverage the new system call against similar attacks in the future?

- A. TPM
- B. Secure boot
- C. NX bit
- D. HSM

**Correct Answer:** C

Community vote distribution

C (100%)

🗉 👤 **vicbersong** 1 month ago

**Selected Answer: C**

Why the other options are incorrect:

A. TPM (Trusted Platform Module): Used for secure hardware-based storage and cryptographic functions, but not directly related to memory execution protection.

B. Secure boot: Ensures that the OS boots using trusted software only, but doesn't control memory execution behavior at runtime.

D. HSM (Hardware Security Module): Used for secure cryptographic key storage and operations, unrelated to memory protection or application-level exploit mitigations.

upvoted 1 times

🗉 👤 **vicbersong** 1 month ago

**Selected Answer: C**

Explanation:

The `mprotect()` system call allows a program to change the memory protection of a region of memory – for example, marking certain areas as non-executable to prevent code execution from those regions. This is a mitigation technique commonly used against buffer overflow and code injection attacks.

To make this protection effective, the system must support and enforce non-executable memory regions, which is exactly what the NX bit (No eXecute bit) does.

✔ NX bit:

Hardware-level feature that marks memory pages as non-executable.

Helps prevent execution of code from data regions like the stack or heap.

Complements the `mprotect()` system call to enforce memory safety.

upvoted 1 times

Which of the following items should be included when crafting a disaster recovery plan?

- A. Redundancy
- B. Testing exercises
- C. Autoscaling
- D. Competitor locations

**Correct Answer:** B

*Community vote distribution*

B (100%)

 **vichersong** 1 month ago

**Selected Answer: B**

A Disaster Recovery Plan (DRP) outlines how an organization will recover from disruptive events (e.g., cyberattacks, natural disasters, hardware failures). One of the most critical components of a DRP is testing exercises – these ensure the plan actually works when needed and help identify gaps or areas for improvement.

✓ Testing exercises should be included because:

They validate the effectiveness of the recovery procedures.

They prepare staff for real-world incidents.

They help refine the plan over time based on actual outcomes.

upvoted 1 times

A web application server is running a legacy operating system with an unpatched RCE vulnerability. The server cannot be upgraded until the corresponding application code is changed. Which of the following compensating controls would best prevent successful exploitation?

- A. Segmentation
- B. CASB
- C. HIPS
- D. UEBA

**Correct Answer:** A

*Community vote distribution*

A (100%)

  **vichbersong** 1 month ago

**Selected Answer: A**

The best compensating control in this scenario would be A. Segmentation.

Since the server is running a legacy OS with an unpatched remote code execution (RCE) vulnerability, segmentation can help isolate it from the rest of the network, reducing the risk of exploitation. By placing the vulnerable server in a separate network zone with strict access controls, attackers would have a harder time reaching it.

upvoted 1 times

Which of the following is the reason why security engineers often cannot upgrade the security of embedded facility automation systems?

- A. They are constrained by available compute.
- B. They lack x86-64 processors.
- C. They lack EEPROM.
- D. They are not logic-bearing devices.

**Correct Answer:** A

*Community vote distribution*

A (100%)

  **vicbersong** 1 month ago

**Selected Answer: A**

✗ Why the other options are incorrect:

B. They lack x86-64 processors

Many embedded systems use ARM or other architectures, but security upgrades don't necessarily require x86-64. So, this isn't the main reason.

C. They lack EEPROM

EEPROM (used for storing firmware) is not a primary limiting factor in most security upgrades. Many embedded systems have some form of non-volatile storage.

D. They are not logic-bearing devices

This would mean they don't process instructions, which isn't true — automation systems are logic-bearing by nature (they run firmware and software).  
upvoted 1 times

  **vicbersong** 1 month ago

**Selected Answer: A**

✓ A. They are constrained by available compute.

□ Explanation:

Embedded facility automation systems — like those used in HVAC, lighting, access control, or SCADA — are typically designed with limited processing power, memory, and storage to reduce cost and power consumption. This lack of resources often makes it difficult or even impossible to install traditional security software or implement complex cryptographic protections.

upvoted 1 times

A security analyst identified a vulnerable and deprecated runtime engine that is supporting a public-facing banking application. The developers anticipate the transition to modern development environments will take at least a month. Which of the following controls would best mitigate the risk without interrupting the service during the transition?

- A. Shutting down the systems until the code is ready
- B. Uninstalling the impacted runtime engine
- C. Selectively blocking traffic on the affected port
- D. Configuring IPS and WAF with signatures

**Correct Answer:** D

Community vote distribution

D (100%)

  **vichersong** 1 month ago

**Selected Answer: D**

✗ Why the other options are not ideal:

A. Shutting down the systems until the code is ready

Not viable since the application is public-facing and in active use.

B. Uninstalling the impacted runtime engine

Would break the application and cause downtime, defeating the goal of maintaining service continuity.

C. Selectively blocking traffic on the affected port

May inadvertently block legitimate users or critical functionality, and doesn't provide nuanced protection.

upvoted 1 times

  **vichersong** 1 month ago

**Selected Answer: D**

✓ D. Configuring IPS and WAF with signatures

□ Why this is the best option:

The application must remain online during the transition to modern environments.

The deprecated runtime engine presents a security risk, likely with known vulnerabilities.

Deploying Intrusion Prevention Systems (IPS) and a Web Application Firewall (WAF) with custom or vendor-provided signatures can detect and block known attack patterns, SQL injection, RCE attempts, or other web-based exploits targeting the vulnerable engine — without taking the service offline.

upvoted 1 times

A security architect wants to ensure a remote host's identity and decides that pinning the X.509 certificate to the device is the most effective solution. Which of the following must happen first?

- A. Use Distinguished Encoding Rules (DER) for the certificate.
- B. Extract the private key from the certificate.
- C. Use an out-of-band method to obtain the certificate.
- D. Compare the retrieved certificate with the embedded certificate.

**Correct Answer:** C

Community vote distribution

C (100%)

🗳️ 👤 **vicbersong** 1 month ago

**Selected Answer: C**

✖ Why the others are incorrect:

A. Use Distinguished Encoding Rules (DER)

DER is a binary format for encoding certificates, but it's not a required first step and doesn't ensure trust by itself.

B. Extract the private key from the certificate

This is not only unnecessary but also a serious security violation. The private key should never be extracted or shared.

D. Compare the retrieved certificate with the embedded certificate

This is the verification step, which happens after pinning – not before.

upvoted 1 times

🗳️ 👤 **vicbersong** 1 month ago

**Selected Answer: C**

✔ C. Use an out-of-band method to obtain the certificate.

📖 Explanation:

Certificate pinning is a security technique used to associate a host (e.g., a server) with its expected X.509 certificate or public key. This helps prevent man-in-the-middle (MitM) attacks where an attacker could present a fraudulent certificate.

Before you can "pin" a certificate (i.e., embed or store a known-good certificate or public key in the app or system):

You first need to obtain the correct certificate securely, usually via an out-of-band method (i.e., not over the same channel that could be compromised).

Once you have the authentic certificate, you can pin it, and then compare it at runtime against what is presented by the host.

upvoted 1 times

A company hired a third-party consultant to run a cybersecurity incident simulation in order to identify security gaps and prepare stakeholders for a potential incident. Which of the following best describes this activity?

- A. Tabletop exercise
- B. Walk-through review
- C. Lessons learned
- D. Business impact analysis

**Correct Answer:** A

Community vote distribution

A (100%)

🗨️ 👤 **vicbersong** 1 month ago

**Selected Answer: A**

✖ Why the other options are incorrect:

B. Walk-through review

More of a step-by-step review of procedures or documentation, not a live scenario simulation.

C. Lessons learned

Happens after a real or simulated incident, to analyze what went well or badly.

D. Business impact analysis (BIA)

Focuses on understanding how disruptions affect business operations, not simulating incident response.

upvoted 1 times

🗨️ 👤 **vicbersong** 1 month ago

**Selected Answer: A**

✔ A. Tabletop exercise

📖 Explanation:

A tabletop exercise is a simulated, discussion-based incident response activity where stakeholders – including technical teams, management, and other key roles – walk through a hypothetical cybersecurity scenario. The goal is to:

Evaluate incident response plans

Identify communication gaps

Test decision-making processes

Improve coordination and readiness

This is exactly what a third-party cybersecurity simulation is meant to achieve.

upvoted 1 times

A security officer is requiring all personnel working on a special project to obtain a security clearance requisite with the level of all information being accessed. Data on this network must be protected at the same level of each clearance holder. The need to know must be verified by the data owner. Which of the following should the security officer do to meet these requirements?

- A. Create a rule to authorize personnel only from certain IPs to access the files.
- B. Assign labels to the files and require formal access authorization.
- C. Assign attributes to each file and allow authorized users to share the files.
- D. Assign roles to users and authorize access to files based on the roles.

**Correct Answer:** B

Community vote distribution

B (100%)

🗳️ 👤 **vichersong** 1 month ago

**Selected Answer: B**

✖ Why the other options are less effective:

A. Create a firewall rule to prevent those users from accessing sensitive data

Overly broad – may block legitimate access and doesn't stop exfiltration if access is already granted.

C. Enable packet captures

Good for investigation, but not mitigation – this is reactive, not preventive.

D. Disable login activity for those users after business hours

Might help reduce attack surface, but attackers can still operate within business hours or use compromised credentials at those times.  
upvoted 1 times

🗳️ 👤 **vichersong** 1 month ago

**Selected Answer: B**

✖ Why the others are incorrect:

A. IP-based rules

Only restrict where users connect from, not who they are or what data they're authorized to access.

C. Attributes and sharing

This sounds more like attribute-based access control (ABAC), and sharing by users doesn't align with the strict controls described.

D. Role-based access control (RBAC)

Assigns access based on job functions, but does not account for classification levels and need-to-know, which are crucial in this scenario.  
upvoted 1 times

🗳️ 👤 **vichersong** 1 month ago

**Selected Answer: B**

✔ B. Assign labels to the files and require formal access authorization.

📖 Explanation:

The scenario clearly describes a mandatory access control (MAC) environment where:

Personnel must have security clearances matching the sensitivity of the data.

Need-to-know access must be verified by a data owner.



Access is based on formal authorization, not just technical capabilities.

In a MAC system, files are labeled with classifications (e.g., Confidential, Secret), and users must have:

A matching security clearance, and

An explicit need-to-know, usually granted by a data custodian or owner.

upvoted 1 times

A security team receives alerts regarding impossible travel and possible brute-force attacks after normal business hours. After reviewing more logs, the team determines that specific users were targeted and attempts were made to transfer data to an unknown site. Which of the following should the team do to help mitigate these issues?

- A. Create a firewall rule to prevent those users from accessing sensitive data.
- B. Restrict uploading activity to only authorized sites.
- C. Enable packet captures to continue to run for the source and destination related to the file transfer.
- D. Disable login activity for those users after business hours.

**Correct Answer:** B

*Community vote distribution*

B (100%)

 **vicbersong** 1 month ago

**Selected Answer:** B

✓ B. Restrict uploading activity to only authorized sites.

□ Explanation:

The scenario describes signs of a targeted attack (e.g., brute force + impossible travel) that may have resulted in data exfiltration attempts to an unauthorized external site. To prevent data from being leaked, the most effective control is to:

Limit file uploads to trusted, authorized destinations only – for example, blocking uploads to unknown IPs or domains using a DLP solution, CASB, or proxy.

This approach directly mitigates the core issue: preventing unauthorized data transfers even if an account is compromised.

upvoted 1 times

A company recently acquired a SaaS company and performed a gap analysis. The results of the gap analysis indicate security controls are absent throughout the SDLC and have led to several vulnerable production releases. Which of the following security tools best reduces the risk of vulnerable code being pushed to production in the future?

- A. Static application security testing
- B. Regression testing
- C. Code signing
- D. Sandboxing

**Correct Answer: A**

*Community vote distribution*

A (100%)

🗳️ 👤 **vicbersong** 1 month ago

**Selected Answer: A**

✖ Why the others are not the best fit:

B. Regression testing

Checks if recent changes broke existing functionality – it's not focused on security flaws.

C. Code signing

Verifies the integrity and authenticity of code, but doesn't detect vulnerabilities in the code itself.

D. Sandboxing

Isolates potentially unsafe programs, useful at runtime, but doesn't prevent vulnerable code from being deployed.

upvoted 1 times

🗳️ 👤 **vicbersong** 1 month ago

**Selected Answer: A**

✔ A. Static Application Security Testing (SAST)

📖 Explanation:

The scenario highlights a lack of security controls in the software development life cycle (SDLC), leading to vulnerabilities in production. The best way to prevent vulnerable code from reaching production is to:

Identify and fix issues early in the development process.

SAST is a tool used during the coding phase to analyze source code, bytecode, or binaries without executing the program. It helps developers detect security flaws early, when they're cheaper and easier to fix – reducing the risk of deploying vulnerable applications.

upvoted 1 times

Which of the following is the best reason for obtaining file hashes from a confiscated laptop?

- A. To prevent metadata tampering on each file
- B. To later validate the integrity of each file
- C. To generate unique identifiers for each file
- D. To preserve the chain of custody of files

**Correct Answer:** B

Community vote distribution

B (100%)

  **vicbersong** 1 month ago

**Selected Answer: B**

✗ Why the other options are incorrect:

A. To prevent metadata tampering on each file

Hashes don't prevent tampering — they detect it.

C. To generate unique identifiers for each file

Hashes can serve as identifiers, but the main purpose in forensics is to verify integrity.

D. To preserve the chain of custody of files

Chain of custody refers to tracking who has handled the evidence, not to hashing the files  
upvoted 1 times

  **vicbersong** 1 month ago

**Selected Answer: B**

✓ B. To later validate the integrity of each file

□ Explanation:

Obtaining file hashes (like MD5, SHA-1, or SHA-256) from a confiscated laptop is a forensic best practice used to:

Ensure files have not been altered since the time of seizure.

Validate the integrity of the data at later stages of an investigation or in court.

By comparing the original hash values to those calculated later, investigators can prove the files remain unchanged, maintaining their evidentiary value.

upvoted 1 times

A security analyst is using data provided from a recent penetration test to calculate CVSS scores to prioritize remediation. Which of the following metric groups would the analyst need to determine to get the overall scores? (Choose three.)

- A. Temporal
- B. Availability
- C. Integrity
- D. Confidentiality
- E. Base
- F. Environmental
- G. Impact
- H. Attack vector

**Correct Answer:** AEF

Community vote distribution

AEF (100%)

  **vicbersong** 1 month ago

**Selected Answer:** AEF

✗ Incorrect Options:

B. Availability, C. Integrity, D. Confidentiality, G. Impact, H. Attack Vector

These are sub-metrics within the Base group, not top-level metric groups on their own.

upvoted 1 times

  **vicbersong** 1 month ago

**Selected Answer:** AEF

- ✓ A. Temporal
- ✓ E. Base
- ✓ F. Environmental

□ Explanation:

The Common Vulnerability Scoring System (CVSS) calculates a score for vulnerabilities based on three main metric groups:

upvoted 1 times

Which of the following describes how a risk assessment is performed when an organization has a critical vendor that provides multiple products?

- A. At the individual product level
- B. Through the selection of a random product
- C. Using a third-party audit report
- D. By choosing a major product

**Correct Answer: A**

*Community vote distribution*

A (100%)

  **vichersong** 1 month ago

**Selected Answer: A**

✓ A. At the individual product level

□ Explanation:

When a critical vendor supplies multiple products, a proper risk assessment should be conducted for each product individually. This is because:

Each product may have different security risks, data sensitivities, compliance requirements, or integration points with your systems.

Assessing risk at the vendor level alone may miss product-specific vulnerabilities or operational dependencies.

✗ Why the other options are incorrect:

B. Through the selection of a random product

This introduces bias and does not ensure full visibility into the vendor's risk posture.

C. Using a third-party audit report

Helpful as supplemental evidence, but not a replacement for a tailored risk assessment.

D. By choosing a major product

May miss risks in less critical but still impactful products.

upvoted 1 times

A security engineer is performing a vulnerability management scan on multihomed Linux systems. The engineer notices that the vulnerability count is high due to the fact that each vulnerability is multiplied by the number of NICs on each system. Which of the following should the engineer do to deduplicate the vulnerabilities and to associate the vulnerabilities with a particular host?

- A. Use a SCAP scanner.
- B. Deploy an agent.
- C. Initiate a discovery scan.
- D. Perform an Nmap scan.

**Correct Answer: B**

*Community vote distribution*

B (100%)

  **vicbersong** 1 month ago

**Selected Answer: B**

✓ B. Deploy an agent.

□ Explanation:

When scanning multihomed systems (systems with multiple network interfaces), vulnerability scanners often detect the same vulnerabilities on each interface, causing duplicate entries. To accurately correlate vulnerabilities to a specific host and eliminate redundancy, the best approach is to:

Deploy an agent on the host – this allows the scanner to:

Identify the host uniquely regardless of its IP addresses.

Access detailed system-level data (e.g., installed packages, patches).

Avoid duplicate reporting across interfaces.

✗ Why the other options are incorrect:

A. Use a SCAP scanner

SCAP (Security Content Automation Protocol) is a standard, not a deduplication solution on its own.

C. Initiate a discovery scan

A discovery scan helps identify assets, but won't resolve deduplication of vulnerabilities.

D. Perform an Nmap scan

Nmap can detect open ports and some vulnerabilities, but it doesn't correlate host-level vulnerabilities like an agent would.

upvoted 1 times

Which of the following best describes a risk associated with using facial recognition to locally authenticate to a mobile device?

- A. Data remanence
- B. Deepfake
- C. Metadata scraping
- D. Biometric impersonation

**Correct Answer:** D

Community vote distribution

D (100%)

 **vichbersong** 1 month ago

**Selected Answer:** D

✓ D. Biometric impersonation

□ Explanation:

Facial recognition is a form of biometric authentication. One of the key risks associated with it is:

Biometric impersonation – the unauthorized replication or spoofing of someone's biometric data (in this case, their face) to gain access to a system or device.

Attackers might use photos, 3D models, or videos to trick facial recognition systems.

Once biometric data is compromised, it cannot be changed, unlike passwords.

✗ Why the other options are incorrect:

A. Data remanence

Refers to residual data left on storage devices after deletion – not specific to facial recognition.

B. Deepfake

A deepfake is a synthetically altered video or image, which could be used as a method of biometric impersonation, but it's not the risk itself – it's a tool for impersonation.

C. Metadata scraping

Involves extracting metadata from files or communications – unrelated to facial recognition authentication.

upvoted 1 times



The principal security analyst for a global manufacturer is investigating a security incident related to abnormal behavior in the ICS network. A controller was restarted as part of the troubleshooting process, and the following issue was identified when the controller was restarted:  
SECURE BOOT FAILED:

FIRMWARE MISMATCH EXPECTED UXFDC479 ACTUAL 0x79F31B

During the investigation, this modified firmware version was identified on several other controllers at the site. The official vendor firmware versions do not have this checksum. Which of the following stages of the MITRE ATT&CK framework for ICS includes this technique?

- A. Evasion
- B. Persistence
- C. Collection
- D. Lateral movement

**Correct Answer: B**

*Community vote distribution*

B (50%)

D (50%)

  **tytexas1111** 1 week, 4 days ago

**Selected Answer: D**

I think its lateral movement. I feel they would've left the part about them spreading to the other controllers out of the question if it wasn't.

upvoted 1 times

  **vicbersong** 1 month ago

**Selected Answer: B**

✓ B. Persistence

□ Explanation:

The MITRE ATT&CK for ICS (Industrial Control Systems) framework includes tactics and techniques tailored to ICS environments. In this scenario:

The firmware of controllers was modified with a non-official version (evidenced by the checksum mismatch).

This suggests an attacker modified the firmware to maintain long-term access or influence over the system.

This behavior aligns with the Persistence tactic — which involves techniques that allow the adversary to maintain their foothold in the ICS environment even after reboots or disconnections.

✗ Why the other options are incorrect:

A. Evasion:

Involves avoiding detection. While custom firmware might help evade detection, the main purpose here is continued access, not stealth.

C. Collection:

Involves gathering information, such as process data or credentials — not modifying firmware.

D. Lateral Movement:

Involves moving between systems to expand access — this scenario is more about establishing a foothold, not expanding access.

upvoted 1 times

A web service provider has just taken on a very large contract that comes with requirements that are currently not being implemented. In order to meet contractual requirements, the company must achieve the following thresholds:

99.99% uptime

Load time in 3 seconds -

Response time = <1.0 seconds -

Starting with the computing environment, which of the following should a security engineer recommend to best meet the requirements? (Choose three.)

- A. Installing a firewall at corporate headquarters
- B. Deploying a content delivery network
- C. Implementing server clusters
- D. Employing bare-metal loading of applications
- E. Lowering storage input/output
- F. Implementing RAID on the backup servers
- G. Utilizing redundant power for all developer workstations

**Correct Answer:** BCE

Community vote distribution

BCE (100%)

 **vichersong** 1 month ago

**Selected Answer: BCE**

Likely Correct Answers:

✓ 1. Horizontal scaling (e.g., auto-scaling groups)

Dynamically adds/removes servers based on demand

Helps maintain uptime and fast response times under heavy load

✓ 2. Content Delivery Network (CDN)

Distributes static content (images, scripts, etc.) closer to users globally

Greatly improves load time and response time

✓ 3. Load balancing

Distributes traffic evenly across multiple servers

Reduces risk of single points of failure and improves availability and speed

upvoted 1 times

An analyst is working to address a potential compromise of a corporate endpoint and discovers the attacker accessed a user's credentials. However, it is unclear if the system baseline was modified to achieve persistence. Which of the following would most likely support forensic activities in this scenario?

- A. Side-channel analysis
- B. Bit-level disk duplication
- C. Software composition analysis
- D. SCAP scanner

**Correct Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!

A company is decommissioning old servers and hard drives that contain sensitive data. Which of the following best protects against data leakage?

- A. Purging
- B. Clearing
- C. Shredding
- D. Degaussing

**Correct Answer:** C

Community vote distribution

C (100%)

  **tytexas1111** 1 week, 4 days ago

**Selected Answer:** C

Shredding is the best option here. It turns the hard drive into tiny fragments that are impossible to recover.

upvoted 1 times

  **vichersong** 1 month ago

**Selected Answer:** C

✓ C. Shredding

□ Explanation:

When decommissioning hard drives with sensitive data, the most secure method to prevent data leakage is physically destroying the drives—which is what shredding does.

□ Breakdown of options:

A. Purging:

A general term for making data inaccessible, often includes degaussing or overwriting multiple times, but doesn't guarantee physical destruction.

B. Clearing:

Refers to logically removing data, usually via standard delete or overwrite methods, which may still be recoverable with advanced tools.

✓ C. Shredding:

Involves physically destroying the drive by grinding or cutting it into tiny pieces. It is highly effective and irreversible, making it ideal for preventing data leakage.

D. Degaussing:

Involves demagnetizing the drive to erase data. Effective on magnetic media (like HDDs), but not useful for SSDs, and doesn't destroy the physical device.

upvoted 3 times

An engineer has had scaling issues with a web application hosted on premises and would like to move to a serverless architecture. Which of the following cloud benefits would be best to utilize for this project?

- A. Cost savings for hosting
- B. Automation of resource provisioning
- C. Providing geo-redundant hosting
- D. Eliminating need to patch

**Correct Answer:** B

Community vote distribution

B (100%)

  **vicbersong** 1 month ago

**Selected Answer: B**

✓ B. Automation of resource provisioning

□ Explanation:

When moving from an on-premises web application to a serverless architecture, one of the key cloud benefits is the automatic provisioning and scaling of resources based on demand.

Why this fits best:

Serverless computing (like AWS Lambda, Azure Functions) automatically provisions, scales, and de-provisions resources based on workload.

It eliminates the need for manual intervention or pre-planned capacity – solving scaling issues directly.

Resources scale dynamically and instantly, which is ideal for applications with unpredictable or variable traffic.

upvoted 1 times

An organization needs to classify its systems and data in accordance with external requirements. Which of the following roles is best qualified to perform this task?

- A. Systems administrator
- B. Data owner
- C. Data processor
- D. Data custodian
- E. Data steward

**Correct Answer:** B

Community vote distribution

B (100%)

 **vickersong** 1 month ago

**Selected Answer: B**

Explanation:

Data Owner: This role is ultimately responsible for the data and its classification based on business value and regulatory or compliance requirements. The data owner decides how sensitive the data is and determines who should have access to it.

Other options:

Systems Administrator: Manages the infrastructure but doesn't determine data classification.

Data Processor: Processes data on behalf of the data controller (a GDPR-related term); not responsible for classification.

Data Custodian: Maintains and protects the data according to the owner's guidelines.

Data Steward: Ensures data quality and governance but doesn't usually determine classification levels.

✓ So, when it comes to aligning systems and data with external compliance or regulatory needs, the data owner is the best qualified.  
upvoted 1 times

A company is developing an application that will be used to perform e-commerce transactions for a subscription-based service. The application must be able to use previously saved payment methods to perform recurring transactions. Which of the following is the most appropriate?

- A. Tokenization through an HSM
- B. Self-encrypting disks with field-level encryption
- C. NX/XN Implementation to minimize data retention
- D. Token-based access for application users
- E. Address space layout randomization

**Correct Answer:** A

*Community vote distribution*

A (100%)

  **vicbersong** 1 month ago

**Selected Answer: A**

Tokenization through a Hardware Security Module (HSM) is the most appropriate solution for securely storing and using previously saved payment methods. It allows sensitive payment data (like credit card numbers) to be replaced with non-sensitive tokens that can be used in place of the actual data to perform recurring transactions.

An HSM provides secure, tamper-resistant cryptographic operations, ensuring that the real cardholder data never needs to be stored in the application, reducing PCI DSS compliance scope.

Why not the others?

B. Self-encrypting disks with field-level encryption: Good for protecting data at rest but doesn't solve the problem of using payment data securely for recurring transactions.

C. NX/XN Implementation: Related to preventing execution of code in non-executable memory regions – irrelevant to payment data storage/usage.

D. Token-based access for application users: Refers to user authentication/authorization, not payment method storage.

E. Address Space Layout Randomization (ASLR): A memory protection mechanism – not applicable to secure payment data handling.  
upvoted 2 times

A security technician is trying to connect a remote site to the central office over a site-to-site VPN. The technician has verified the source and destination IP addresses are correct, but the technician is unable to get the remote site to connect. The following error message keeps repeating: An error has occurred during Phase 1 handshake. Deleting keys and retrying...

Which of the following is most likely the reason the connection is failing?

- A. The IKE hashing algorithm uses different key lengths on each VPN device.
- B. The IPSec settings allow more than one cipher suite on both devices.
- C. The Diffie-Hellman group on both sides matches but is a legacy group.
- D. The remote VPN is attempting to connect with a protocol other than SSL/TLS.

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **vichersong** 1 month ago

**Selected Answer: A**

Why A is the best answer:

IKE hashing algorithm mismatch: If the hashing algorithm (e.g., SHA-1 vs. SHA-256) or key lengths differ on each VPN endpoint, Phase 1 negotiation will fail, which aligns exactly with the error message being shown.

Why not the others?

B. The IPSec settings allow more than one cipher suite on both devices: Multiple suites can actually help compatibility, not hinder it — and IPSec cipher suites are negotiated in Phase 2, not Phase 1.

C. The Diffie-Hellman group on both sides matches but is a legacy group: If they match, even if legacy, Phase 1 would usually succeed. Most systems still support legacy groups for compatibility unless explicitly disabled.

D. The remote VPN is attempting to connect with a protocol other than SSL/TLS: Irrelevant in this context. Site-to-site VPNs typically use IPSec, not SSL/TLS.

upvoted 1 times



A security analyst received the following finding from a cloud security assessment tool:

Virtual Machine Data Disk is encrypted with the default encryption key.

Because the organization hosts highly sensitive data files, regulations dictate it must be encrypted so it is unreadable to the CSP. Which of the following should be implemented to remediate the finding and meet the regulatory requirement? (Choose two.)

- A. Disk encryption with customer-provided keys
- B. Disk encryption with keys from a third party
- C. Row-level encryption with a key escrow
- D. File-level encryption with cloud vendor-provided keys
- E. File-level encryption with customer-provided keys
- F. Disk-level encryption with a cross-signed certificate

**Correct Answer: AE**

Community vote distribution

AE (100%)

 **vichersong** 1 month ago

**Selected Answer: AE**

✓ Explanation:

The key issue in the finding is that encryption is being done using the default keys provided by the cloud service provider (CSP). Regulatory compliance often requires that the CSP must not have access to the keys, meaning the organization must control and manage the encryption keys.

▮ Best Solutions:

A. Disk encryption with customer-provided keys

This ensures that the organization, not the CSP, owns and controls the encryption keys used to protect data-at-rest.

Commonly referred to as Bring Your Own Key (BYOK).

This directly addresses the regulatory requirement for the data to be unreadable to the CSP.

E. File-level encryption with customer-provided keys

Adds another layer of security where sensitive files are encrypted before being stored, using keys managed by the organization.

This ensures data confidentiality even if disk encryption is bypassed.

upvoted 1 times

A security analyst discovers a new device on the company's dedicated IoT subnet during the most recent vulnerability scan. The scan results show numerous open ports and insecure protocols in addition to default usernames and passwords. A camera needs to transmit video to the security server in the IoT subnet. Which of the following should the security analyst recommend to securely operate the camera?

- A. Harden the camera configuration.
- B. Send camera logs to the SIEM.
- C. Encrypt the camera's video stream.
- D. Place the camera on an isolated segment.

**Correct Answer: A**

*Community vote distribution*

A (100%)

🗳️ 👤 **vicbersong** 1 month ago

**Selected Answer: A**

✖ Why not the others?

B. Send camera logs to the SIEM

Useful for monitoring, but does not fix the vulnerabilities on the device itself.

C. Encrypt the camera's video stream

Important for data confidentiality, but doesn't address device compromise risks (e.g., via default credentials or insecure services).

D. Place the camera on an isolated segment

It's already on a dedicated IoT subnet (as mentioned), and isolation alone doesn't fix the existing security misconfigurations.

upvoted 1 times

🗳️ 👤 **vicbersong** 1 month ago

**Selected Answer: A**

✔ Explanation:

The vulnerability scan revealed that the camera has open ports, insecure protocols, and default credentials, which are all classic signs of a poorly configured and vulnerable device.

Hardening the configuration typically includes:

Changing default usernames and passwords.

Disabling unused services and insecure protocols (e.g., Telnet, HTTP).

Enabling secure communication protocols (e.g., HTTPS, RTSP over TLS).

Limiting access via IP whitelisting or firewall rules.

Ensuring firmware is updated to patch known vulnerabilities.

All of these directly address the security issues identified in the scan and are essential first steps before considering more advanced options.

upvoted 1 times

The Chief Information Security Officer of a large multinational organization has asked the security risk manager to use risk scenarios during a risk analysis. Which of the following is the most likely reason for this approach?

- A. To connect risks to business objectives
- B. To ensure a consistent approach to risk
- C. To present a comprehensive view of risk
- D. To provide context to the relevancy of risk

**Correct Answer:** D

Community vote distribution

D (100%)

  **vicbersong** 1 month ago

**Selected Answer: D**

✗ Why not the others?

A. To connect risks to business objectives

This is a broader risk management goal, but risk scenarios specifically help make risks relatable, not necessarily tie them directly to business objectives.

B. To ensure a consistent approach to risk

Consistency is achieved through frameworks and methodologies, not necessarily through scenarios.

C. To present a comprehensive view of risk

A comprehensive view involves looking at all risk categories and sources. Scenarios typically focus on specific examples, not the entire risk landscape.

upvoted 1 times

  **vicbersong** 1 month ago

**Selected Answer: D**

D. To provide context to the relevancy of risk

✓ Explanation:

Risk scenarios are hypothetical situations that help an organization understand how risks could materialize in real-world terms, and what their impact would be. They provide a tangible context that makes abstract risks more understandable and relevant to business decision-makers.

By using risk scenarios, the security risk manager is:

Illustrating how a specific threat could affect the organization.

Helping prioritize risks based on their business impact and likelihood.

Providing clarity and context to stakeholders who may not be familiar with technical risk language.

upvoted 1 times

A security engineer would like to control configurations on mobile devices while fulfilling the following requirements:

Support and control Apple and Android devices.

The device must be corporate-owned.

Which of the following would enable the engineer to meet these requirements? (Choose two.)

- A. Create a group policy to lock down mobile devices.
- B. Update verbiage in the acceptable use policy for the internet.
- C. Implement an MDM solution.
- D. Implement a captive portal solution.
- E. Update policy to prohibit the use of BYOD devices.
- F. Implement a RADIUS solution.

**Correct Answer:** CE

Community vote distribution

CE (100%)

 **vichersong** 1 month ago

**Selected Answer:** CE

To control configurations on corporate-owned Apple and Android mobile devices, the most effective approach includes:

C. Implement an MDM solution

A Mobile Device Management (MDM) solution allows security engineers to:

Centrally manage device settings and configurations

Enforce security policies across both Apple and Android devices

Push applications, wipe devices, and monitor compliance

This is the primary technical control for managing mobile device configurations.

E. Update policy to prohibit the use of BYOD devices

Since the requirement is for corporate-owned devices, it's important to:

Clearly define that BYOD (Bring Your Own Device) is not allowed

Ensure employees understand only corporate-owned devices are permitted, allowing full control via MDM.

This supports the enforcement of your MDM policies and avoids non-compliant or unmanaged devices.

upvoted 1 times

A pharmaceutical company uses a cloud provider to host thousands of independent resources in object storage. The company needs a practical and effective means of discovering data, monitoring changes, and identifying suspicious activity. Which of the following would best meet these requirements?

- A. A machine-learning-based data security service
- B. A file integrity monitoring service
- C. A cloud configuration assessment and compliance service
- D. An automated data classification system

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **vicbersong** 1 month ago

**Selected Answer: A**

✓ A. A machine-learning-based data security service

✓ Explanation:

In a cloud environment with thousands of independent resources in object storage, you need a solution that can:

Automatically discover sensitive or regulated data

Continuously monitor for changes to files or objects

Identify suspicious activity or behavior patterns

A machine-learning-based data security service is designed exactly for this scenario – especially in large-scale, dynamic environments like object storage.

These services use AI/ML to:

Detect anomalies and unusual access patterns

Correlate behaviors across users and services

Identify risky configurations or exposed data

Scale automatically with cloud-native architectures

upvoted 1 times

A security analyst is assessing a new application written in Java. The security analyst must determine which vulnerabilities exist during runtime. Which of the following would provide the most exhaustive list of vulnerabilities while meeting the objective?

- A. Input validation
- B. Dynamic analysis
- C. Side-channel analysis
- D. Fuzz testing
- E. Static analysis

**Correct Answer:** B

*Community vote distribution*



None

Recently, two large engineering companies in the same line of business decided to approach cyberthreats in a united way. Which of the following best describes this unified approach?

- A. NDA
- B. SOW
- C. SLA
- D. MOU

**Correct Answer:** D

Community vote distribution

D (100%)

 **vicbersong** 1 month ago

**Selected Answer:** D

D. MOU (Memorandum of Understanding)

Explanation:

A Memorandum of Understanding (MOU) is a formal agreement between two or more parties that outlines a mutual intention to work together towards a common goal – in this case, addressing cyberthreats jointly.

It's non-binding, but shows a serious commitment to collaboration.

Commonly used between organizations that want to cooperate without yet entering into a legally enforceable contract.

Suitable for joint efforts, like information sharing, incident response collaboration, or threat intelligence exchange.

The other options:

A. NDA (Non-Disclosure Agreement) – Ensures confidentiality of shared information.

B. SOW (Statement of Work) – Describes the specific deliverables and timelines for a project.

C. SLA (Service Level Agreement) – Defines performance and service expectations between a service provider and a customer.

So, in this context, MOU best fits the scenario of a unified approach to cybersecurity between two companies.

upvoted 1 times

A regulated company is in the process of refreshing its entire infrastructure. The company has a business-critical process running on an old 2008 Windows server. If this server fails, the company would lose millions of dollars in revenue. Which of the following actions should the company should take?

- A. Accept the risk as the cost of doing business.
- B. Create an organizational risk register for project prioritization.
- C. Implement network compensating controls.
- D. Purchase insurance to offset the cost if a failure occurred.

**Correct Answer:** B

*Community vote distribution*

B (100%)

  **vicbersong** 1 month ago

**Selected Answer:** B

The best option in this scenario is:

B. Create an organizational risk register for project prioritization.

Here's why:

The server hosts a business-critical process on unsupported legacy infrastructure, meaning the risk of failure is high, and the impact is severe.

By documenting it in the risk register, leadership can prioritize remediation, such as migration, virtualization, or building in high availability or backups – actions aligned with a regulated environment.

This approach also satisfies governance and compliance requirements by demonstrating risk awareness and action.

Why not the others?

A. Accept the risk: Not acceptable in a regulated environment with high financial impact.

C. Network compensating controls: Good for security, but won't protect against hardware or OS failure.

D. Insurance: Might cover some financial loss, but won't prevent service interruption or regulatory consequences.

upvoted 1 times



A security engineer needs to ensure production containers are automatically scanned for vulnerabilities before they are accepted into the production environment. Which of the following should the engineer use to automatically incorporate vulnerability scanning on every commit?

- A. Code repository
- B. CI/CD pipeline
- C. Integrated development environment
- D. Container orchestrator

**Correct Answer:** B

Community vote distribution

C (100%)

  **vicbersong** 3 weeks, 4 days ago

**Selected Answer: C**

Why B. CI/CD pipeline is correct:

The CI/CD (Continuous Integration/Continuous Deployment) pipeline automates various stages of the development and deployment process.

It allows you to hook in vulnerability scanning tools (e.g., Trivy, Clair, Anchore, Snyk) that scan container images after they're built.

Scanning can be triggered automatically on every commit, merge, or build – ensuring insecure containers never make it to production.

Why the others are incorrect:

A. Code repository: While it stores the code and can trigger actions (like webhooks), it doesn't itself perform scanning. That happens in the pipeline.

C. Integrated development environment (IDE): An IDE helps developers write and test code locally. It's not designed for automated scanning on commits.

D. Container orchestrator: Tools like Kubernetes manage containers in production but are not responsible for scanning them pre-deployment.  
upvoted 1 times

A security architect recommends replacing the company's monolithic software application with a containerized solution. Historically, secrets have been stored in the application's configuration files. Which of the following changes should the security architect make in the new system?

- A. Use a secrets management tool.
- B. Save secrets in key escrow.
- C. Store the secrets inside the Dockerfiles.
- D. Run all Dockerfiles in a randomized namespace.

**Correct Answer:** A

*Community vote distribution*

A (100%)

🗉 👤 **vichersong** 3 weeks, 4 days ago

**Selected Answer: A**

A security architect recommends replacing the company's monolithic software application with a containerized solution. Historically, secrets have been stored in the application's configuration files. Which of the following changes should the security architect make in the new system?

- A. Use a secrets management tool.
- B. Save secrets in key escrow.
- C. Store the secrets inside the Dockerfiles.
- D. Run all Dockerfiles in a randomized namespace

upvoted 1 times

A security engineer is assessing a new tool to segment data and communications between domains. The assessment must determine how data transmission controls can be bypassed without detection. Which of the following techniques should the security engineer use?

- A. Machine-learning statistical analysis
- B. Fuzz testing
- C. Covert channel analysis
- D. Protocol analysis

**Correct Answer:** C

Community vote distribution

C (100%)

  **vichbersong** 3 weeks, 4 days ago

**Selected Answer:** C

✓ C. Covert channel analysis

Covert channels are methods used to transfer information in a way that violates a system's security policy.

These channels can be used to sneak data across domain boundaries without triggering standard detection mechanisms.

Covert channel analysis involves identifying and evaluating these hidden paths of communication, which is exactly what the question is asking about.

Why the other options are incorrect:

A. Machine-learning statistical analysis

Useful for anomaly detection and predictive analysis, but not specific to detecting covert or hidden transmission channels.

B. Fuzz testing

Primarily used to find software vulnerabilities and bugs by sending random data to inputs. It's not aimed at identifying how data controls can be bypassed stealthily.

D. Protocol analysis

Involves examining network protocols for proper behavior or misconfigurations, but it does not specifically target hidden or covert data transmissions.

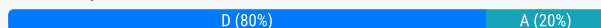
upvoted 1 times

During an adversarial simulation exercise, an external team was able to gain access to sensitive information and systems without the organization detecting this activity. Which of the following mitigation strategies should the organization use to best resolve the findings?

- A. Configuring a honeypot for adversary characterization
- B. Leveraging simulators for attackers
- C. Setting up a honey network for attackers
- D. Utilizing decoy accounts and documents

**Correct Answer:** D

Community vote distribution



🗨️ 👤 **vicbersong** 3 weeks, 4 days ago

**Selected Answer: D**

✖ Why the other options are less effective:

A. Configuring a honeypot for adversary characterization

A honeypot is useful, but it's often a single system and may not attract or detect attackers once they're inside the network unless specifically accessed.

B. Leveraging simulators for attackers

Simulators are great for training or pre-deployment testing, but they don't directly address real-time detection or help catch adversaries already in your network.

C. Setting up a honey network for attackers

Similar to a honeypot but on a larger scale; effective, but complex and overkill for a first step. It also requires significant resources to manage and doesn't guarantee interaction from attackers.

upvoted 2 times

🗨️ 👤 **vicbersong** 3 weeks, 4 days ago

**Selected Answer: D**

✔ Explanation:

The scenario describes a failure to detect unauthorized access during an adversarial simulation — likely a red team exercise. This points to gaps in detection and deception capabilities.

D. Utilizing decoy accounts and documents

These are deception techniques designed to lure attackers and trigger alerts when accessed.

They help identify lateral movement, privilege escalation, and unauthorized access in real-time.

When attackers interact with fake credentials or sensitive-looking files (e.g., fake HR records or fake SSH keys), alerts can be generated without compromising real assets.

This is a proactive detection strategy ideal for catching stealthy adversaries.

upvoted 2 times

🗨️ 👤 **Pmonty4** 1 month, 3 weeks ago

**Selected Answer: A**

Fixing man

upvoted 1 times

A help desk technician is troubleshooting an issue with an employee's laptop that will not boot into its operating system. The employee reported the laptop had been stolen but then found it one day later. The employee has asked the technician for help recovering important data. The technician has identified the following:

The laptop operating system was not configured with BitLocker.

The hard drive has no hardware failures.

Data is present and readable on the hard drive, although it appears to be illegible.

Which of the following is the most likely reason the technician is unable to retrieve legible data from the hard drive?

A. The employee's password was changed, and the new password needs to be used.

B. The PKI certificate was revoked, and a new one must be installed.

C. The hard drive experienced crypto-shredding.

D. The technician is using the incorrect cipher to read the data.

**Correct Answer:** C

Community vote distribution

C (100%)

  **vickersong** 3 weeks, 4 days ago

**Selected Answer: C**

✗ Why the other options are incorrect:

A. The employee's password was changed, and the new password needs to be used

This would not make the data unreadable unless full-disk encryption was involved – and we're told BitLocker was not configured.

B. The PKI certificate was revoked, and a new one must be installed

PKI issues would impact encrypted emails, VPNs, or certain authentication, not raw file readability on a hard drive.

D. The technician is using the incorrect cipher to read the data

There's no indication that the technician is using any specific decryption tools. If standard tools show the data but it's unreadable, it's likely due to data being wiped/encrypted without key recovery – consistent with crypto-shredding.

upvoted 1 times

  **vickersong** 3 weeks, 4 days ago

**Selected Answer: C**

✓ Explanation:

Given the scenario:

The laptop was reported stolen, then recovered.

BitLocker was not configured, so OS-level encryption is not protecting the data.

The hard drive has no hardware failure, and data is present but illegible.

This implies the data was deliberately rendered unreadable, not corrupted or encrypted in transit.

C. Crypto-shredding:

Crypto-shredding is a secure data destruction technique where encryption keys are destroyed, making the encrypted data permanently inaccessible, even though it still exists on the drive.

It's commonly used by remote wipe or anti-theft tools, which some laptops perform automatically when flagged as lost or stolen.

Since the laptop was reported stolen, it's highly likely some anti-theft or endpoint protection triggered crypto-shredding to protect the data.

upvoted 2 times

## SIMULATION

-

You are about to enter the virtual environment.

DO NOT perform the following actions within the virtual environment. Making any of these changes will cause the virtual environment to fail and prevent proper scoring.

1. Disable ssh
2. Disable systemd
3. Alter the network adapter 172.162.0.0
4. Change the password on the lab admin account
5. Reboot the machine

Once you have completed the item in the virtual environment, you will NOT be allowed to return to this item.

## TEST QUESTION

-

This system was recently patched following the exploitation of a vulnerability by an attacker to enable data exfiltration.

Despite the vulnerability being patched, it is likely that a malicious TCP service is still running and the adversary has achieved persistence by creating a systemd service.

Examples of commands to use:

kill, killall

lsuf

man, --help (use for assistance)

netstat (useful flags: a, n, g, u)

ps (useful flag: a)

systemctl (to control systemd)

Please note: the list of commands shown above is not exhaustive. All native commands are available.

## INSTRUCTIONS

-

Using the following credentials:

- Username: labadmin
- Password: Passw0rd!

Investigate to identify indicators of compromise and then remediate them. You will need to make at least two changes:

1. End the compromised process that is using a malicious TCP service.
2. Remove the malicious persistence agent by disabling the service's ability to start on boot.

### STEP 1: Identify and Kill the Malicious TCP Process

#### 1. List listening TCP services with associated processes:

```
sudo netstat -tulnp
```

Look for suspicious services (e.g., uncommon ports like 4444, 1337, etc.)

#### 2. Verify the process details:

```
ps aux | grep <PID>
```

#### 3. Terminate the suspicious process:

```
sudo kill <PID>
```

Or use `sudo killall <process-name>` if needed.

### STEP 2: Disable the Malicious systemd Service (Persistence)

#### 1. List all systemd services:

```
systemctl list-units --type=service
```

2. Look for any unusual or suspicious service (often not part of a typical system, e.g., `revshell.service`, `malicious.service`, `backdoor.service`, etc.)

#### 3. Check the service path and content (optional but helpful):

```
systemctl status <suspicious-service>
```

```
cat /etc/systemd/system/<suspicious-service>.service
```

#### 4. Disable the malicious service:

```
sudo systemctl disable <suspicious-service>
```

#### 5. Stop the service (if still running):

```
sudo systemctl stop <suspicious-service>
```

Once these steps are done, you will have:

- Ended the malicious process.
- Disabled its persistence via systemd.

**Avoid:** Disabling SSH or systemd, changing passwords, rebooting, or touching the `172.162.0.0` network adapter.

Correct Answer:

Currently there are no comments in this discussion, be the first to comment!



## HOTSPOT

-

You are tasked with integrating a new B2B client application with an existing OAuth workflow that must meet the following requirements:

- The application does not need to know the users' credentials.
- An approval interaction between the users and the HTTP service must be orchestrated.
- The application must have limited access to users' data.

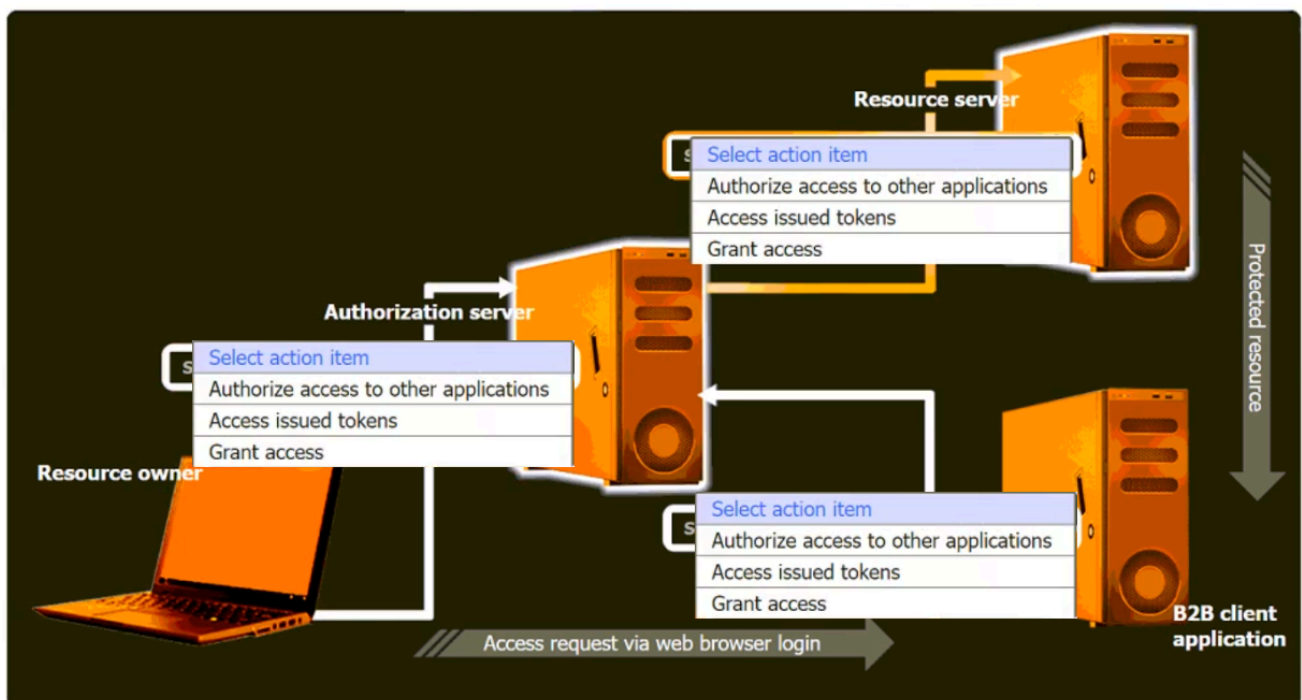
## INSTRUCTIONS

-

Use the drop-down menus to select the action items for the appropriate locations. All placeholders must be filled.

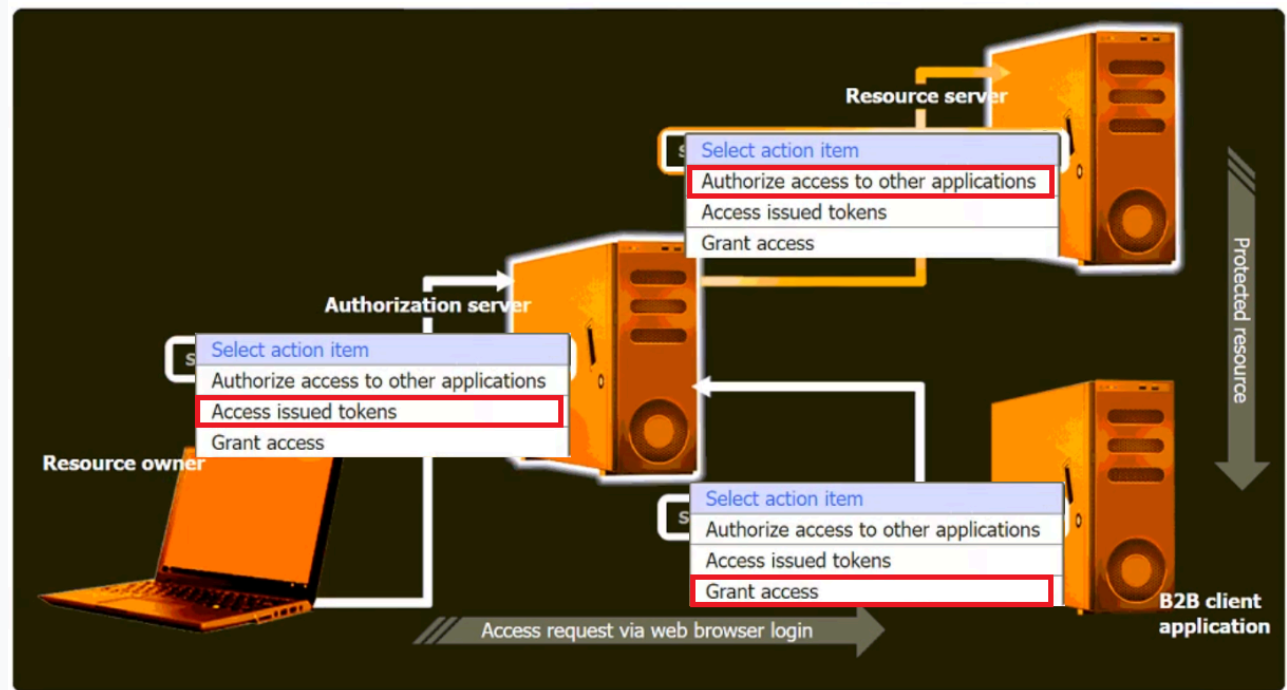
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

## Answer Area



Correct Answer:

**Answer Area**



Currently there are no comments in this discussion, be the first to comment!

## SIMULATION

-

An IPSec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram.

Complete the configuration files to meet the following requirements:

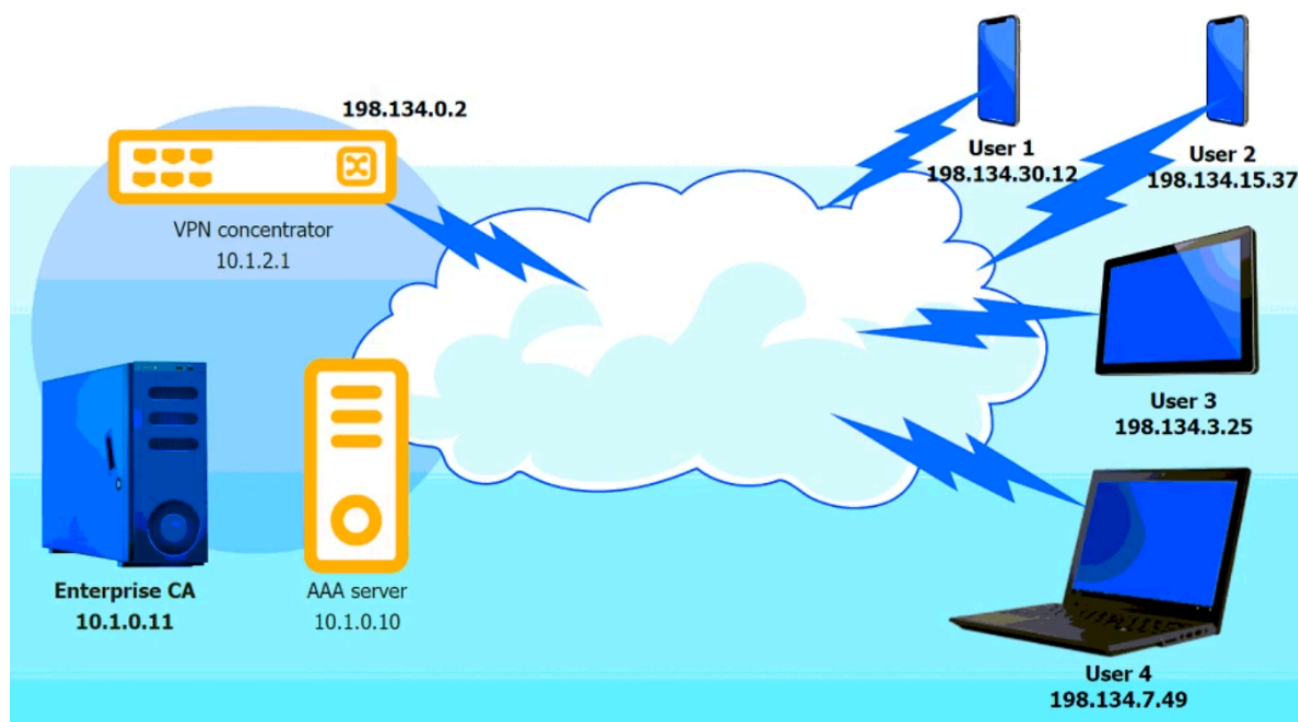
- The EAP method must use mutual certificate-based authentication (with issued client certificates).
- The IKEv2 cipher suite must be configured to the most secure authenticated mode of operation.
- The secret must contain at least one uppercase character, one lowercase character, one numeric character, and one special character, and it must meet a minimum length requirement of eight characters.

## INSTRUCTIONS

-

Click on the AAA server and VPN concentrator to complete the configuration. Fill in the appropriate fields and make selections from the drop-down menus.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



## VPN concentrator



```
...
re-eap {
...
  proposals = 
  ...
}
...
plugins {
  eap-radius {
    secret = 
    server = 
  }
}
...
```

Select proposal

- Select proposal
- tls
- camellia256ctr
- peap
- ttls
- blowfish256
- cast128
- aes256gcm128

Select IP address

- Select IP address
- 198.134.15.37
- 198.134.3.25
- 10.1.2.1
- 10.1.0.10
- 198.134.30.12
- 10.1.0.11
- 198.134.0.2
- 198.134.7.49

Reset to Default

Close

## AAA server



```
...
eap {
  default_eap_type = 
  ...
}
...
ip addr = 

secret = 
require_message_authenticator = yes
}
...
```

Select eap

- Select eap
- tls
- aes256gcm128
- cast128
- camellia256ctr
- blowfish256
- ttls
- peap

Select IP address

- Select IP address
- 198.134.15.37
- 198.134.3.25
- 10.1.2.1
- 10.1.0.10
- 198.134.30.12
- 10.1.0.11
- 198.134.0.2
- 198.134.7.49

Reset to Default

Save

Close

Correct Answer:

**VPN Concentrator**

- **Proposal:** aes256gcm128
- **Server IP:** 10.1.0.10 (this is the AAA server)
- **Secret:** Str0ng@Key (example that meets all character requirements)

**AAA Server**

- **Default EAP type:** tls
- **IP Address:** 10.1.2.1 (this is the VPN concentrator)
- **Secret:** Str0ng@Key (must match the VPN concentrator)

Currently there are no comments in this discussion, be the first to comment!

## SIMULATION

-

An incident occurred at Site A when an attacker successfully caused water pressure to increase in the pump room.

The organization is concerned about reoccurrence of this attack and that similar attacks might be successful on other cyber-physical systems within the network.

All devices and components reside on a flat network within the 10.1.0.0/16 space.

## INSTRUCTIONS

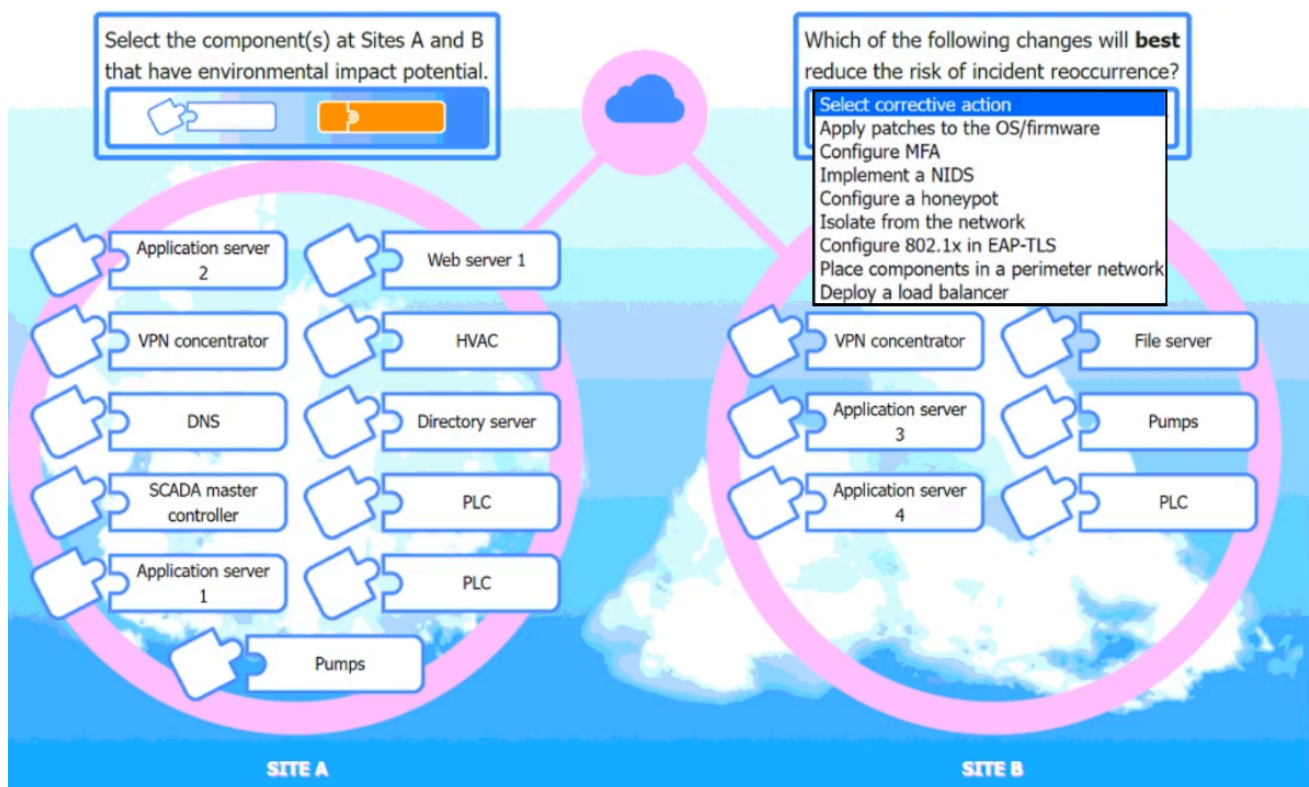
-

Take the appropriate actions to reduce the risk of reoccurrence of this and other environmental security vulnerabilities.

Select the component(s) at Sites A and B that have environmental impact potential. Then, select the corrective action that will best reduce the risk of incident reoccurrence.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

## Answer Area



Correct Answer:

**At Site A:**

- **SCADA master controller** – Controls and monitors physical processes.
- **PLC (both)** – Programmable Logic Controllers directly interface with pumps/valves.
- **Pumps** – Direct environmental impact (increased water pressure in incident).

**At Site B:**

- **PLC** – As above, interfaces with physical systems.
- **Pumps** – As above, environmental impact through pressure, flow, etc.

**Corrective Action – Isolate from the network**

The devices reside on a flat network, increasing risk. **Isolation** (e.g., segmentation or VLANs) limits lateral movement and access to critical cyber-physical systems (CPS) like PLCs and pumps.

None

## SIMULATION

-

During the course of normal SOC operations, three anomalous events occurred and were flagged as potential IoCs. Evidence for each of these potential IoCs is provided.

## INSTRUCTIONS

-

Review each of the events and select the appropriate analysis and action options for each IoC.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

IoC 1		IoC 2		IoC 3	
Source	Svc	Type	Dest	Data	
Apache_httpd		DNSQ	@10.1.1.1:53	update.s.domain	
Apache_httpd		DNSQR	@10.1.2.5	CNAME 3a129sk219r0slsmfkzz000.s.domain	
Apache_httpd		DNSQ	@10.1.1.1:53	3a129sk219r0slsmfkzz000.s.domain	
Apache_httpd		DNSQR	@10.1.2.5	IN A 108.158.253.253	

**Select analysis**

Someone is footprinting a network subnet.  
 Service identification and fingerprinting are occurring.  
 Canonical name records in a public DNS cache are being updated.  
 An employee is attempting to access a blocked website.  
 An employee is using P2P services to download files.  
 The service is attempting to resolve a malicious domain.  
 A host is participating in an IRC-based botnet.  
 An application is performing an automatic update.

Analysis Select analysis

**Action**

Select action

Select action

Configure the DNS server to perform recursion.  
 Block ping requests across the WAN interface.  
 Deploy a network-based DLP solution.  
 Enforce endpoint controls on third-party software installations.  
 Implement a blocklist for known malicious ports.  
 Close ticket as resolved.  
 Investigate for software supply-chain attacks.



IoC 1	IoC 2	IoC 3
Src	Dst	Proto Data Action
10.0.5.5	10.1.2.1	IP_ICMP ECHO Drop
10.0.5.5	10.1.2.2	IP_ICMP ECHO Drop
10.0.5.5	10.1.2.3	IP_ICMP ECHO Drop
10.0.5.5	10.1.2.4	IP_ICMP ECHO Drop
10.0.5.5	10.1.2.5	IP_ICMP ECHO Drop

Select analysis

Someone is footprinting a network subnet.  
Service identification and fingerprinting are occurring.  
Canonical name records in a public DNS cache are being updated.  
An employee is attempting to access a blocked website.  
An employee is using P2P services to download files.  
The service is attempting to resolve a malicious domain.  
A host is participating in an IRC-based botnet.  
An application is performing an automatic update.

Analysis

Select analysis

Action

Select action

Select action

Configure the DNS server to perform recursion.  
Block ping requests across the WAN interface.  
Deploy a network-based DLP solution.  
Enforce endpoint controls on third-party software installations.  
Implement a blocklist for known malicious ports.  
Close ticket as resolved.  
Investigate for software supply-chain attacks.

IoC 1	IoC 2	IoC 3
Proxylog> > GET /announce?info_hash=%01d%FE%7E%F1%10%5CwAp%ED%F6%03%C49%D6B%14%F1& > peer_id=%B8js%7F%E8%0C%AFh%02Y%967%24e%27V%EEM%16%5B&port=41730& > uploaded=0&downloaded=0&left=3767869&compact=1&ip=10.5.1.26&event=started > HTTP/1.1 > Accept: application/x-bittorrent > Accept-Encoding: gzip > User-Agent: RAZA 2.1.0.0 > Host: localhost > Connection: Keep-Alive < < HTTP 200 OK		

Select analysis

Someone is footprinting a network subnet.  
Service identification and fingerprinting are occurring.  
Canonical name records in a public DNS cache are being updated.  
An employee is attempting to access a blocked website.  
An employee is using P2P services to download files.  
The service is attempting to resolve a malicious domain.  
A host is participating in an IRC-based botnet.  
An application is performing an automatic update.

Analysis

Select analysis

Action

Select action

Select action

Configure the DNS server to perform recursion.  
Block ping requests across the WAN interface.  
Deploy a network-based DLP solution.  
Enforce endpoint controls on third-party software installations.  
Implement a blocklist for known malicious ports.  
Close ticket as resolved.  
Investigate for software supply-chain attacks.

Correct Answer:

### IoC 1

#### Indicators:

- DNS queries for a suspicious subdomain (update.s.domain, \*.s.domain)
- Responses include odd CNAME and A records
- Activity resembles contacting a **malicious domain**

#### Correct Selections:

- **Analysis:** The service is attempting to resolve a malicious domain
- **Action:** Implement a blocklist for known malicious ports

### IoC 2

#### Indicators:

- ICMP Echo (ping) requests from 10.0.5.5 to multiple hosts
- All packets are dropped
- Suggests a device is **probing** the network

#### Correct Selections:

- **Analysis:** Someone is footprinting a network subnet
- **Action:** Block ping requests across the WAN interface

### IoC 3

#### Indicators:

- BitTorrent traffic (/announce?info\_hash, peer\_id, application/x-bittorrent)
- Indicates P2P protocol activity

#### Correct Selections:

- **Analysis:** An employee is using P2P services to download files
- **Action:** Enforce endpoint controls on third-party software installations

Currently there are no comments in this discussion, be the first to comment!

A security administrator needs to automate alerting. The server generates structured log files that need to be parsed to determine whether an alarm has been triggered. Given the following code function:

```
def parse_logs(logfile):  
    with open(logfile) as log_file:  
        parsed_log = json.load(log_file)  
        if parsed_log["error_log"]["system_1"]["InAlarmState"]:  
            print("System 1 is in an alarm state!")
```

Which of the following is most likely the log input that the code will parse?

- A. 

```
["error_log"  
  ["system_1"  
    ["InAlarmState": True]
```
- B. `<"error_log"><"system_1">`
- C. 

```
error_log:  
  - system_1:  
    InAlarmState: True
```
- D. `<"error_log": {"system_1": {"InAlarmState": True }}>`

**Correct Answer:** A

Currently there are no comments in this discussion, be the first to comment!

A financial technology firm works collaboratively with business partners in the industry to share threat intelligence within a central platform. This collaboration gives partner organizations the ability to obtain and share data associated with emerging threats from a variety of adversaries. Which of the following should the organization most likely leverage to facilitate this activity? (Choose two.)

- A. CWPP
- B. YARA
- C. ATT&CK
- D. STIX
- E. TAXII
- F. JTAG

**Correct Answer:** DE

Community vote distribution

DE (100%)

🗨️ 👤 **vichersong** 3 weeks, 2 days ago

**Selected Answer: DE**

Why not the others?

A. CWPP (Cloud Workload Protection Platform):

Focuses on protecting cloud workloads, not for sharing intel across orgs.

B. YARA:

Used for defining malware patterns and rules for scanning files – not for sharing intelligence.

C. ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge):

A knowledge base of attacker behavior – useful for analysis, but not a format or method for sharing intel.

F. JTAG (Joint Test Action Group):

A hardware debugging standard, not relevant to threat intelligence sharing.

upvoted 1 times

🗨️ 👤 **vichersong** 3 weeks, 2 days ago

**Selected Answer: DE**

The correct answers are:

D. STIX and E. TAXII

Explanation:

This scenario involves sharing threat intelligence in a structured and automated way between organizations. The technologies best suited for that purpose are:

✓ D. STIX (Structured Threat Information eXpression)

A standardized language for describing cyber threat intelligence (CTI).

Enables organizations to share and consume information in a consistent format.

Ideal for structuring data on threats, indicators, TTPs, and more.

✓ E. TAXII (Trusted Automated eXchange of Indicator Information)

A protocol specifically designed to transport cyber threat information (often formatted in STIX).

Enables real-time automated exchange of threat intel between systems and partners.

upvoted 1 times



A company wants to invest in research capabilities with the goal to operationalize the research output. Which of the following is the best option for a security architect to recommend?

- A. Dark web monitoring
- B. Threat intelligence platform
- C. Honeypots
- D. Continuous adversary emulation

**Correct Answer:** B

*Community vote distribution*

B (100%)

 **vicbersong** 3 weeks, 2 days ago

**Selected Answer: B**

B. Threat Intelligence Platform

Why?

The company wants to invest in research capabilities and operationalize the output — meaning it wants to turn research insights into actionable security measures.

A Threat Intelligence Platform (TIP) is specifically designed to:

Collect, aggregate, and analyze threat data from various sources.

Provide a centralized location for threat research.

Correlate indicators and context for decision-making.

Distribute intelligence to relevant security tools (e.g., SIEM, SOAR, firewalls).

This makes it the most fitting choice for a structured, scalable, and operational use of threat research.

upvoted 2 times

A company is concerned about the security of customer data. The IT department has configured all web applications with appropriate access controls to restrict to only authorized users. Which of the following solutions addresses this concern?

- A. SIEM
- B. Vulnerability scanner
- C. DLP
- D. Threat intelligence platform

**Correct Answer:** C

Community vote distribution

C (100%)

🗉 👤 **vichersong** 3 weeks, 2 days ago

**Selected Answer: C**

Why not the others?

A. SIEM (Security Information and Event Management):

Useful for detecting suspicious activity via log aggregation and analysis, but not focused on data protection.

B. Vulnerability Scanner:

Helps identify security weaknesses in systems or applications, but does not control or monitor data usage.

D. Threat Intelligence Platform:

Gathers and analyzes external threat data, but doesn't provide direct protection or monitoring of internal data.

upvoted 1 times

🗉 👤 **vichersong** 3 weeks, 2 days ago

**Selected Answer: C**

✓ C. DLP (Data Loss Prevention)

Why?

The company is concerned about the security of customer data, and while access controls are in place, data could still be leaked or mishandled by authorized users (accidentally or maliciously).

A Data Loss Prevention (DLP) solution helps address this concern by:

Monitoring data in use, in motion, and at rest.

Preventing unauthorized sharing of sensitive data like customer information.

Enforcing policies around how data can be accessed, copied, emailed, uploaded, or printed.

Alerting or blocking data exfiltration attempts.

upvoted 1 times

A security analyst reviews the following report:

	Location	Chassis manufacturer	OS	Application developer	Vendor
Product A	United States	Local company A	Debian 11	Unknown	Charlie Security Consulting
Product B	United States	Global company B	Red Hat Enterprise Linux	Developer B	BigBox Vulnerabilities

Which of the following assessments is the analyst performing?

- A. System
- B. Supply chain
- C. Quantitative
- D. Organizational

**Correct Answer:** B

Currently there are no comments in this discussion, be the first to comment!



A security researcher tells a company that one of its solutions is vulnerable to buffer overflow, leading to a malicious coding execution. Which of the following is the best way to avoid this vulnerability in future versions?

- A. Testing for CSRF vulnerabilities before the application goes to production
- B. Using SAST tools to find vulnerabilities as part of the pipeline
- C. Implementing canary protection in an earlier life-cycle stage
- D. Implementing pair programming to improve development capabilities

**Correct Answer:** B

Community vote distribution

B (100%)

  **vichersong** 3 weeks, 2 days ago

**Selected Answer:** B

✓ B. Using SAST tools to find vulnerabilities as part of the pipeline

Why?

A buffer overflow vulnerability typically occurs due to unsafe coding practices, such as improper memory handling. The best way to catch and prevent such issues early in the development lifecycle is by:

Static Application Security Testing (SAST):

Analyzes source code early in the SDLC (Software Development Life Cycle).

Identifies code-level vulnerabilities like buffer overflows before code is compiled or deployed.

Integrates well into CI/CD pipelines to provide automated, continuous feedback to developers.

This proactive approach helps ensure secure coding practices are enforced from the beginning.

upvoted 1 times

Users are experiencing a variety of issues when trying to access corporate resources. Examples include:

- Connectivity issues between local computers and file servers between branch offices
- Inability to download corporate applications on mobile endpoints while working remotely
- Certificate errors when accessing internal web applications

Which of the following actions are the most relevant when troubleshooting the reported issues? (Choose two.)

- A. Review VPN throughput.
- B. Check IDS rules.
- C. Restore static content on the CDN.
- D. Enable secure authentication using NAC.
- E. Implement advanced WAF rules.
- F. Validate MDM asset compliance.

**Correct Answer:** AF

*Community vote distribution*

AF (100%)

 **vichersong** 3 weeks, 2 days ago

**Selected Answer: AF**

1. Connectivity issues between local computers and file servers between branch offices

This points to potential network-related issues.

Reviewing VPN throughput (Answer A) helps determine if the VPN is overloaded, congested, or misconfigured, affecting communication between sites.

2. Inability to download corporate applications on mobile endpoints while working remotely

This is typically tied to Mobile Device Management (MDM) policies and device compliance.

Validating MDM asset compliance (Answer F) ensures that mobile devices meet security and policy requirements, and are allowed to access corporate resources and apps.

upvoted 2 times

A network engineer recorded the following test results:

Source	Destination	Latency	Action
192.168.1.55	192.168.1.205	10ms	Allow
192.168.1.55	192.168.1.68	8ms	Allow
192.168.1.55	192.168.1.101	11ms	Allow
192.168.1.55	192.168.1.30	9ms	Allow

After a new network security appliance was deployed, the results of the network test are as follows:

Source	Destination	Latency	Action
192.168.1.55	192.168.1.205	710ms	Allow
192.168.1.55	192.168.1.68	-	Drop
192.168.1.55	192.168.1.101	211ms	Allow
192.168.1.55	192.168.1.30	109ms	Allow

Which of the following network infrastructure components most likely produced these results?

- A. IPS
- B. CDN
- C. VPN
- D. IDS

**Correct Answer: A**

*Community vote distribution*

A (100%)

 **vichersong** 3 weeks, 2 days ago

**Selected Answer: A**

Before deploying the new appliance:

All connections were allowed with low latency (8–11ms).

After deploying the new appliance:

Significantly increased latency on allowed connections (e.g., 710ms, 211ms).

One connection was dropped entirely.

Indicates deep packet inspection or inline filtering happening.

Why it points to an IPS:

IPS (Intrusion Prevention System) works inline, actively analyzing and potentially blocking traffic in real time.

It introduces latency due to deep inspection.

Can drop suspicious traffic, as seen with 192.168.1.68.

upvoted 1 times

A developer needs to improve the cryptographic strength of a password-storage component in a web application without completely replacing the crypto-module. Which of the following is the most appropriate technique?

- A. Key splitting
- B. Key escrow
- C. Key rotation
- D. Key encryption
- E. Key stretching

**Correct Answer:** E

Community vote distribution

E (100%)

🗨️ 👤 **vichersong** 3 weeks, 2 days ago

**Selected Answer: E**

✖ Why not the others?

A. Key splitting: Used to divide a key into parts, mainly for shared access or trust models, not password strength.

B. Key escrow: Involves storing keys with a third party for recovery—not related to password hashing.

C. Key rotation: Refers to changing encryption keys periodically, mostly for data encryption, not password hashing.

D. Key encryption: Encrypting keys with other keys—not related to strengthening password hashing.

upvoted 1 times

🗨️ 👤 **vichersong** 3 weeks, 2 days ago

**Selected Answer: E**

✔ E. Key stretching

📖 Explanation:

When storing passwords securely, it's essential to increase the time it takes to brute-force each password hash, especially when you can't change the entire crypto module. That's where key stretching comes in.

What is Key Stretching?

It's a technique used to enhance the security of weak or short cryptographic keys, like passwords.

It uses methods like PBKDF2, bcrypt, or scrypt to repeatedly hash a password, making brute-force attacks computationally expensive.

Ideal for upgrading existing password-storage mechanisms without rewriting the crypto module entirely.

upvoted 2 times

A company wants to implement hardware security key authentication for accessing sensitive information systems. The goal is to prevent unauthorized users from gaining access with a stolen password. Which of the following models should the company implement to best solve this issue?

- A. Rule-based
- B. Time-based
- C. Role-based
- D. Context-based

**Correct Answer:** D

*Community vote distribution*

D (100%)

🗨️ 👤 **vicbersong** 3 weeks, 2 days ago

**Selected Answer: D**

Context-based authentication takes into account additional factors beyond just the password, such as the location, device, and user behavior, to determine whether access should be granted. In this case, it would be used alongside the hardware security key to enhance security by verifying the user's identity based on contextual factors, thereby preventing unauthorized access even if a password is stolen.

The other models are less suitable for this specific issue:

- A. Rule-based focuses on predefined rules for access control but doesn't address the dynamic context of authentication.
- B. Time-based typically uses factors like time of day or session duration, but it's not directly linked to preventing unauthorized access due to stolen credentials.
- C. Role-based is concerned with access control based on the user's role within the organization, but it doesn't specifically address the risk of stolen passwords.

upvoted 1 times

Which of the following is the main reason quantum computing advancements are leading companies and countries to deploy new encryption algorithms?

- A. Encryption systems based on large prime numbers will be vulnerable to exploitation.
- B. Zero Trust security architectures will require homomorphic encryption.
- C. Perfect forward secrecy will prevent deployment of advanced firewall monitoring techniques.
- D. Quantum computers will enable malicious actors to capture IP traffic in real time.

**Correct Answer:** A

*Community vote distribution*

A (100%)

None

A company is adopting microservice architecture in order to quickly remediate vulnerabilities and deploy to production. All of the microservices run on the same Linux platform. Significant time was spent updating the base OS before deploying code. Which of the following should the company do to make the process efficient?

- A. Use Terraform scripts while creating golden images.
- B. Create a cron job to run apt-update every 30 days.
- C. Use snapshots to deploy code to existing compute instances.
- D. Deploy a centralized update server.

**Correct Answer:** A

*Community vote distribution*

A (100%)

None

During a gap assessment, an organization notes that BYOD usage is a significant risk. The organization implemented administrative policies prohibiting BYOD usage. However, the organization has not implemented technical controls to prevent the unauthorized use of BYOD assets when accessing the organization's resources. Which of the following solutions should the organization implement to best reduce the risk of BYOD devices? (Choose two.)

- A. Cloud IAM, to enforce the use of token-based MFA
- B. Conditional access, to enforce user-to-device binding
- C. NAC, to enforce device configuration requirements
- D. PAM, to enforce local password policies
- E. SD-WAN, to enforce web content filtering through external proxies
- F. DLP, to enforce data protection capabilities

**Correct Answer:** BC

None



An organization has several systems deployed in a public cloud and wants to confirm that when data retention periods are reached, the data is properly disposed of. Which of the following best meets the organization's needs?

- A. Double encrypting the data using both asymmetric and symmetric keys managed by the cloud service provider
- B. Utilizing a data-wiping software to overwrite the existing data
- C. Encrypting the data with customer-managed keys and then deleting both the encryption key and the volume
- D. Asking the cloud provider for copies of certificates of destruction

**Correct Answer:** C

None

A security engineer reviews an after-action report from a previous security breach and notes a long lag time between detection and containment of a compromised account. The engineer suggests using SOAR to address this concern. Which of the following best explains the engineer's goal?

- A. To prevent accounts from being compromised
- B. To enable log correlation using machine learning
- C. To orchestrate additional reporting for the security operations center
- D. To prepare runbooks to automate future incident response

**Correct Answer:** *D*

None

During an audit at an organization, auditors find that developers are able to promote code to production. The auditors request a full review of all production changes. Which of the following should the organization implement to prevent a full review in the future?

- A. Branch protection
- B. Centralized code repositories
- C. Interactive application security testing
- D. Change control board

**Correct Answer:** *D*

None

A systems engineer is configuring SSO for a business that will be using SaaS applications for its remote-only workforce. Privileged actions in SaaS applications must be allowed only from corporate mobile devices that meet minimum security requirements, but BYOD must also be permitted for other activity. Which of the following would best meet this objective?

- A. Block any connections from outside the business's network security boundary.
- B. Install machine certificates on corporate devices and perform checks against the clients.
- C. Configure device attestations and continuous authorization controls.
- D. Deploy application protection policies using a corporate, cloud-based MDM solution.

**Correct Answer:** C

None

A systems administrator wants to reduce the number of failed patch deployments in an organization. The administrator discovers that system owners modify systems or applications in an ad hoc manner. Which of the following is the best way to reduce the number of failed patch deployments?

- A. Compliance tracking
- B. Situational awareness
- C. Change management
- D. Quality assurance

**Correct Answer:** C

None

A network engineer must ensure that always-on VPN access is enabled but restricted to company assets. Which of the following best describes what the engineer needs to do?

- A. Generate device certificates using the specific template settings needed.
- B. Modify signing certificates in order to support IKE version 2.
- C. Create a wildcard certificate for connections from public networks.
- D. Add the VPN hostname as a SAN entry on the root certificate.

**Correct Answer:** A

None

A security administrator is reviewing the following code snippet from a website component:

```
<link rel="stylesheet" type="text/css" font-weight: normal;
font-style: normal;
if ((is_admin() " (function_exists ('get_hex_cache')) != true {add_action('wp-head' . 'get_hex_cache',12) function get_hex_cache () {
return print (hex2bin('3c7', (file_get_contents ('dir_' /inc.tmp )....
```

A review of the inc.tmp file shows the following:

21487592579325342038509345083453432452523435235345523453242353424523453452345389627656385793257839537854362038263053  
2804508325

Which of the following is most likely the reason for inaccuracies?

- A. A content management solution plug-in has been exploited.
- B. A search engine's bots are being blocked at the firewall.
- C. The relevant stylesheet has become corrupted.
- D. The WAF is configured to be in transparent mode.

**Correct Answer: A**

None

An organization wants to implement a platform to better identify which specific assets are affected by a given vulnerability. Which of the following components provides the best foundation to achieve this goal?

- A. SASE
- B. CMDB
- C. SBoM
- D. SIEM

**Correct Answer:** *B*

None



Which of the following best explains why AI output could be inaccurate?

- A. Model poisoning
- B. Social engineering
- C. Output handling
- D. Prompt injections

**Correct Answer: A**

None

A company runs a DAST scan on a web application. The tool outputs the following recommendations:

- Use Cookie prefixes.
- Content Security Policy - SameSite=strict is not set.

Which of the following vulnerabilities has the tool identified?

- A. RCE
- B. XSS
- C. CSRF
- D. TOCTOU

**Correct Answer:** C

None

Which of the following best describes the reason a network architect would enable forward secrecy on all VPN tunnels?

- A. This process is a requirement to enable hardware-accelerated cryptography.
- B. This process reduces the success of attackers performing cryptanalysis.
- C. The business requirements state that confidentiality is a critical success factor.
- D. Modern cryptographic protocols list this process as a prerequisite for use.

**Correct Answer:** *B*

None

Which of the following best explains the importance of determining organizational risk appetite when operating with a constrained budget?

- A. Risk appetite directly impacts acceptance of high-impact, low-likelihood events.
- B. Organizational risk appetite varies from organization to organization.
- C. Budgetary pressure drives risk mitigation planning in all companies.
- D. Risk appetite directly influences which breaches are disclosed publicly.

**Correct Answer: A**

None

A company hired an email service provider called my-email.com to deliver company emails. The company started having several issues during the migration. A security engineer is troubleshooting and observes the following configuration snippet:

@	MX	10	email.company.com	45000
www	IN	CNAME	web01.company.com.	
email	IN	CNAME	srv01.company.com	
srv01	IN	A	192.168.1.10	
web01	IN	A	192.168.1.11	
@	IN	TXT	"v=dmARC include:company.com ~all"	

Which of the following should the security engineer modify to fix the issue? (Choose two.)

- A. The email CNAME record must be changed to a type A record pointing to 192.168.1.11
- B. The TXT record must be changed to "v=dmARC ip4:192.168.1.10 include:my-email.com ~all"
- C. The srv01 A record must be changed to a type CNAME record pointing to the email server
- D. The email CNAME record must be changed to a type A record pointing to 192.168.1.10
- E. The TXT record must be changed to "v=dkim ip4:192.168.1.11 include:my-email.com ~all"
- F. The TXT record must be changed to "v=spf ip4:192.168.1.10 include:my-email.com ~all"
- G. The srv01 A record must be changed to a type CNAME record pointing to the web01 server

**Correct Answer:** DF

None

After a company discovered a zero-day vulnerability in its VPN solution, the company plans to deploy cloud-hosted resources to replace its current on-premises systems. An engineer must find an appropriate solution to facilitate trusted connectivity. Which of the following capabilities is the most relevant?

- A. Container orchestration
- B. Microsegmentation
- C. Conditional access
- D. Secure access service edge

**Correct Answer:** *D*

None

Recent reports indicate that a software tool is being exploited. Attackers were able to bypass user access controls and load a database. A security analyst needs to find the vulnerability and recommend a mitigation. The analyst generates the following output:

```
C:\>whoami
local-user
C:\>netuser local-user Welcome!
The command completed successfully!
C:\>dbloader.exe local-user Welcome!
Insufficient Permissions. Now Closing...
C:\>strings dbloader.exe
!This program cannot be run in DOS Mode
dB10ad3r!
Load Database jmp
182(*nx
(i3jN*jk
fahn82mk0a
C:\>dbloader.exe admin dB10ad3r!
Loading Database. Please Wait...
```

Which of the following would the analyst most likely recommend?

- A. Installing appropriate EDR tools to block pass-the-hash attempts
- B. Adding additional time to software development to perform fuzz testing
- C. Removing hard-coded credentials from the source code
- D. Not allowing users to change their local passwords

**Correct Answer:** C

None

The identity and access management team is sending logs to the SIEM for continuous monitoring. The deployed log collector is forwarding logs to the SIEM. However, only false positive alerts are being generated. Which of the following is the most likely reason for the inaccurate alerts?

- A. The compute resources are insufficient to support the SIEM.
- B. The SIEM indexes are too large.
- C. The data is not being properly parsed.
- D. The retention policy is not properly configured.

**Correct Answer:** C

None



The security team is receiving escalated support tickets stating that one of the company's publicly available websites is not loading as expected. Given the following observations:

Server	URL	Installed certificate	Age of installed certificate
SALES10	www.sales.com	*.sales.com	282 days
SALES10	fulfillment.sales.com	*.sales.com	282 days
WEB27	www.website.com	website.com	418 days
SALES20	tracking.sales.com	tracking.sales.com	240 days
EVENT2	event.sales.com	event.sales.com	57 days

Which of the following is most likely the root cause?

- A. A certificate signed by a global root certification authority has expired.
- B. A protocol mismatch error is expected to occur when using outdated browsers.
- C. One certificate is being bound to multiple websites on the same server.
- D. Subject alternative names were not used appropriately for subdomains.

**Correct Answer:** A

None

A company acquires a location with a large infrastructure of legacy devices. Because of the hardware's age and the legacy software's limitations, the OS cannot be upgraded, and the machines cannot be virtualized. These machines are not publicly facing, but they do have internet access. The following controls are currently in place:

- EDR
- Anti-malware
- Logging and monitoring
- Host-based firewall
- Proxied internet access

A security architect needs to supplement the existing control strategy with one that restricts unauthorized software. Which of the following controls should the architect recommend to best supplement the existing environment?

- A. SIEM
- B. Isolation
- C. Conditional access
- D. Application control

**Correct Answer:** D

None

An organization wants to create a threat model to identify vulnerabilities in its infrastructure. Which of the following should be prioritized first?

- A. External-facing infrastructure with known exploited vulnerabilities
- B. Internal infrastructure with high-severity and known exploited vulnerabilities
- C. External-facing infrastructure with a low risk score and no known exploited vulnerabilities
- D. External-facing infrastructure with a high risk score that can only be exploited with local access to the resource

**Correct Answer: A**

None

A Chief Information Security Officer requests an action plan to remediate vulnerabilities. A security analyst reviews the output from a recent vulnerability scan and notices hundreds of unique vulnerabilities. The output includes the CVSS score, IP address, hostname, and the list of vulnerabilities. The analyst determines more information is needed in order to decide which vulnerabilities should be fixed immediately. Which of the following is the best source for this information?

- A. Third-party risk review
- B. Business impact analysis
- C. Incident response playbook
- D. Crisis management plan

**Correct Answer:** *B*

None

A security operations analyst is reviewing network traffic baselines for nightly database backups. Given the following information:

Date	Time	Bandwidth consumed	SRC server	DST server
12/1	12:01 a.m.	11.24GB	PRDDB01	BACKUP01
12/2	12:01 a.m.	11.57GB	PRDDB01	BACKUP01
12/3	12:01 a.m.	11.70GB	PRDDB01	BACKUP01
12/3	12:46 a.m.	97.00GB	PRDDB01	85.34.17.98
12/4	12:01 a.m.	10.95GB	PRDDB01	BACKUP01

Which of the following should the security analyst do next?

- A. Consult with a network engineer to determine the impact of bandwidth usage.
- B. Quarantine PRDDB01 and then alert the database engineers.
- C. Refer to the incident response playbook for the proper response.
- D. Review all the network logs for further data exfiltration.

**Correct Answer:** C

None

A company has a requirement in customer contracts that states applications must undergo external audits to identify vulnerabilities. Which of the following is the best action for the company to complete before hiring an external auditor?

- A. Gather evidence for the audit.
- B. Conduct an internal audit assessment.
- C. Identify lessons learned from the audit.
- D. Select samples for audit testing.

**Correct Answer:** *B*

None

During DAST scanning, applications are consistently reporting code defects in open-source libraries that were used to build web applications. Most of the code defects are from using libraries with known vulnerabilities. The code defects are causing product deployment delays. Which of the following is the best way to uncover these issues earlier in the life cycle?

- A. Directing application logs to the SIEM for continuous monitoring
- B. Modifying the WAF policies to block against known vulnerabilities
- C. Completing an IAST scan against the web application
- D. Using a software dependency management solution

**Correct Answer:** *D*

None