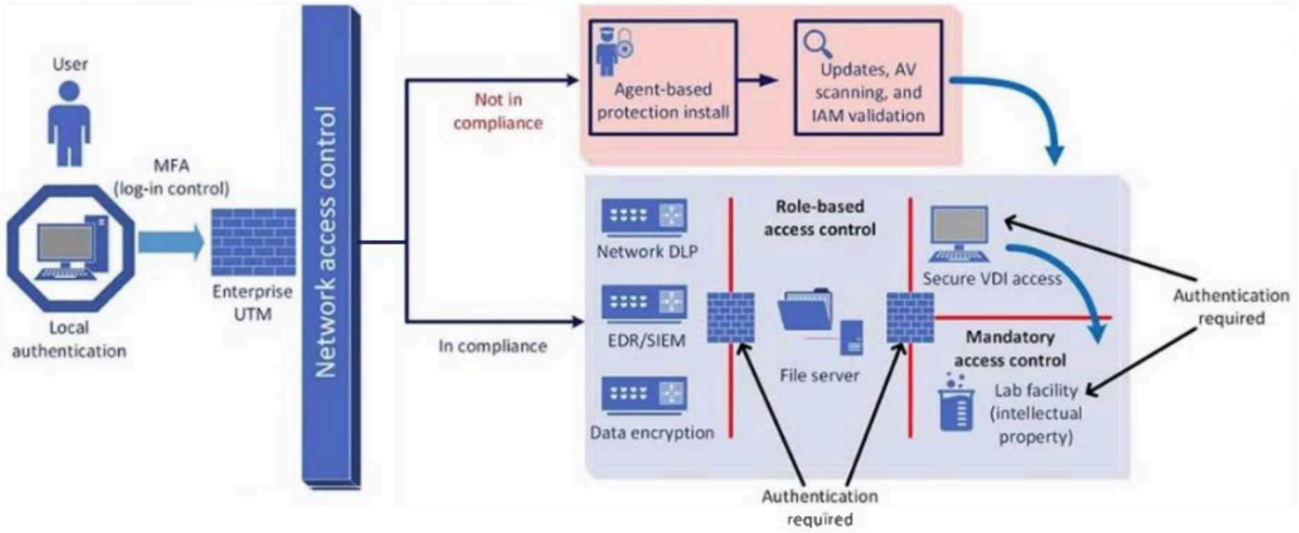
Question #1 Topic 1

A company plans to implement a research facility with intellectual property data that should be protected. The following is the security diagram proposed by the security architect:



Which of the following security architect models is illustrated by the diagram?

A. Identity and access management model

B. Agent-based security model

C. Perimeter protection security model

D. Zero Trust security model

Correct Answer: *D*

Community vote distribution

D (100%)

rvv1978 Highly Voted 4 months, 3 weeks ago

Selected Answer: D

every user and device must authenticate and be verified at multiple points (MFA, NAC posture checks, role-based and mandatory access controls, etc.)—this architecture is indicative of Zero Trust principles. Zero Trust requires continuous verification of users and devices, minimal implicit trust inside the network, and strict segmentation of resources.

upvoted 5 times

Question #2 *Topic 1*

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%)

rvv1978 4 months, 3 weeks ago

Selected Answer: DE

The two most appropriate choices for facilitating a shared threat-intelligence platform are:

D. STIX (Structured Threat Information eXpression) – A standardized language/format for structuring and communicating cyber-threat information.
E. TAXII (Trusted Automated eXchange of Indicator Information) – A transport mechanism/protocol that automates and standardizes the exchange of STIX-formatted threat data.

upvoted 3 times

Question #3 *Topic 1*

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*

Community vote distribution

BC (100%)

rvv1978 4 months, 3 weeks ago

Selected Answer: BC

Conditional Access (B) ensures only approved and compliant devices can access sensitive resources by checking the device's identity and security context. This prevents personal BYOD devices from logging in unless they meet organizational requirements.

Network Access Control (NAC) (C) enforces security policies at the network layer by assessing device health (e.g., antivirus status, patch levels) before allowing access. Devices failing to meet these requirements are blocked or quarantined, further mitigating BYOD risks.

upvoted 2 times

Question #4 *Topic 1*

A security administrator is performing a gap assessment against a specific OS benchmark. The benchmark requires the following configurations be applied to endpoints:

- Full disk encryption
- Host-based firewall
- Time synchronization
- Password policies
- Application allow listing
- Zero Trust application access

Which of the following solutions best addresses the requirements? (Choose two.)

A. MDM

B. CASB

C. SBoM

D. SCAP

E. SASE

F. HIDS

Correct Answer: *AD*

Community vote distribution

AD (80%) AE (20%)

rvv1978 4 months, 3 weeks ago

Selected Answer: AD

MDM (A) can enforce endpoint security settings (e.g., full-disk encryption, host-based firewall, password policies) and manage application allow lists, addressing the bulk of the OS benchmark requirements at the device level.

SCAP (D) automates compliance checks against the benchmark, verifying configurations like encryption, firewalls, and password policies to ensure continuous adherence.

upvoted 2 times

Jimwade1985 5 months ago

Selected Answer: AD

It's definitely MDM and SCAP

upvoted 1 times

landyxtran 5 months, 2 weeks ago

Selected Answer: AD

As the prior user states, MDM provides FDE, a host-based firewall, password policies, and application allowing.

SCAP fulfills the OS benchmark requirements they are intending to do.

upvoted 1 times

martin451 5 months, 3 weeks ago

Selected Answer: AE

MDM (Mobile Device Management) can enforce full disk encryption, host-based firewalls, password policies, and application allow listing across devices.

SASE (Secure Access Service Edge) integrates Zero Trust network access and other security functions, making it ideal for secure application access.

While F. HIDS (Host-based Intrusion Detection System) is critical for monitoring and detecting suspicious activities, it doesn't directly address all the configurations specified in the benchmark, such as Zero Trust application access or application allow listing.

upvoted 1 times

landyxtran 5 months, 2 weeks ago

I understand HIDS is not part of the equation, but the question is about performing a gap assessment and checking for a benchmark. I would lean toward SCAP, wouldn't you? I feel SASE is suitable for cloud and network services; in this case, the question explicitly states OS Benchmark.

upvoted 1 times

Question #5 *Topic 1*

A global organization is reviewing potential vendors to outsource a critical payroll function. Each vendor's plan includes using local resources in multiple regions to ensure compliance with all regulations. The organization's Chief Information Security Officer is conducting a risk assessment on the potential outsourcing vendors' subprocessors. Which of the following best explains the need for this risk assessment?

A. Risk mitigations must be more comprehensive than the existing payroll provider.

B. Due care must be exercised during all procurement activities.

C. The responsibility of protecting PII remains with the organization.

D. Specific regulatory requirements must be met in each jurisdiction.

Correct Answer: *C*

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

Question #6 *Topic 1*

A manufacturing plant is updating its IT services. During discussions, the senior management team created the following list of considerations:

- Staff turnover is high and seasonal.
- Extreme conditions often damage endpoints.
- Losses from downtime must be minimized.
- Regulatory data retention requirements exist.

Which of the following best addresses the considerations?

A. Establishing further environmental controls to limit equipment damage

B. Using a non-persistent virtual desktop interface with thin clients

C. Deploying redundant file servers and configuring database journaling

D. Maintaining an inventory of spare endpoints for rapid deployment

Correct Answer: *B*

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

Question #7

Topic 1

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

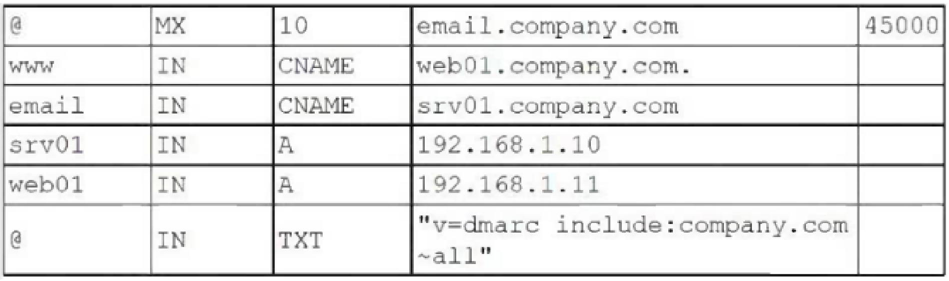
D. TOCTOU

Correct Answer: *C*

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

Question #8 *Topic 1*

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"

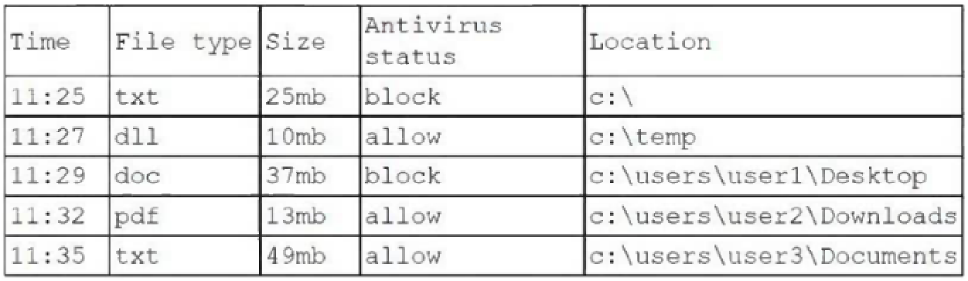
G. The srv01 A record must be changed to a type CNAME record pointing to the web01 server

Correct Answer: *DF*

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

Question #9 Topic 1

A security analyst is reviewing the following log:



Time	File type	Size	Antivirus status	Location
11:25	txt	25mb	block	c:\
11:27	dll	10mb	allow	c:\temp
11:29	doc	37mb	block	c:\users\user1\Desktop
11:32	pdf	13mb	allow	c:\users\user2\Downloads
11:35	txt	49mb	allow	c:\users\user3\Documents

Which of the following possible events should the security analyst investigate further?

A. A macro that was prevented from running

B. A text file containing passwords that were leaked

C. A malicious file that was run in this environment

D. A PDF that exposed sensitive information improperly

Correct Answer: *C*

Community vote distribution

B (100%)

tytexas1111 2 months, 2 weeks ago

Selected Answer: B

The last entry in the table shows a big .txt file that was allowed

upvoted 1 times

Question #10 *Topic 1*

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*

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

Question #11 Topic 1

SIMULATION -

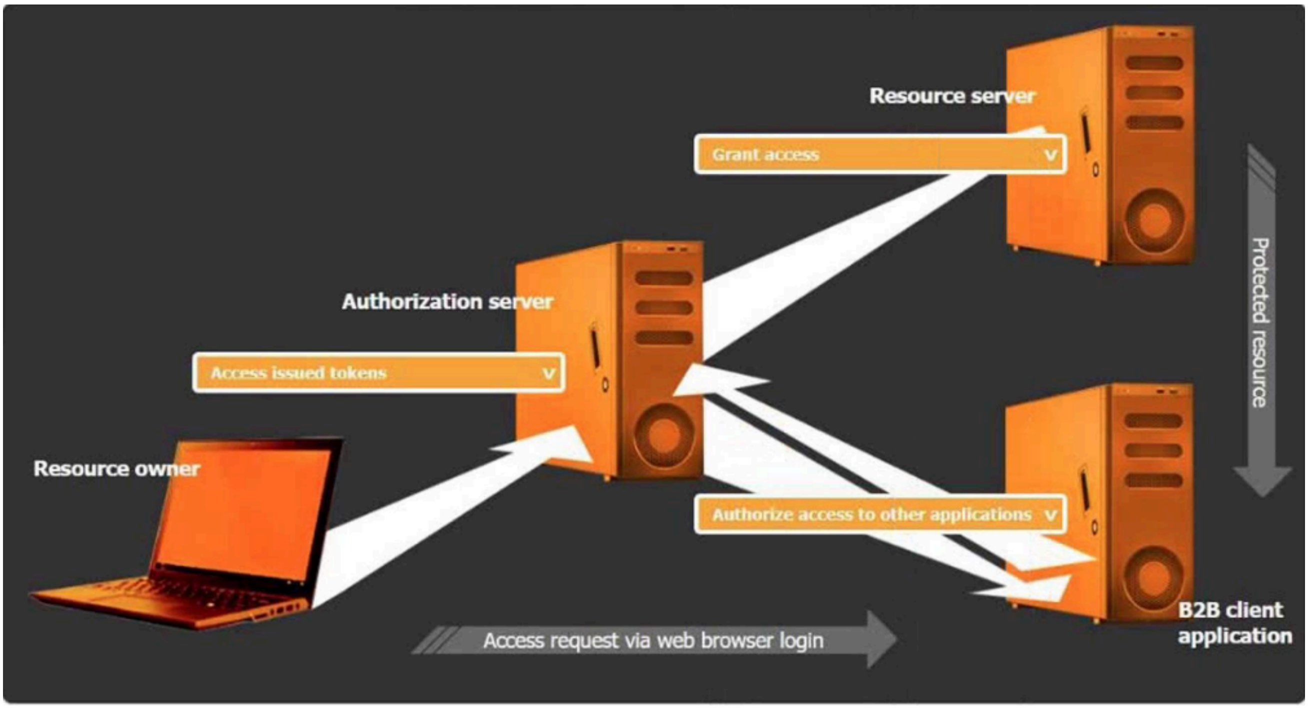
You are tasked with integrating a new B2B client application with an existing OAuth workflow that must meet the following requirements:

- 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.

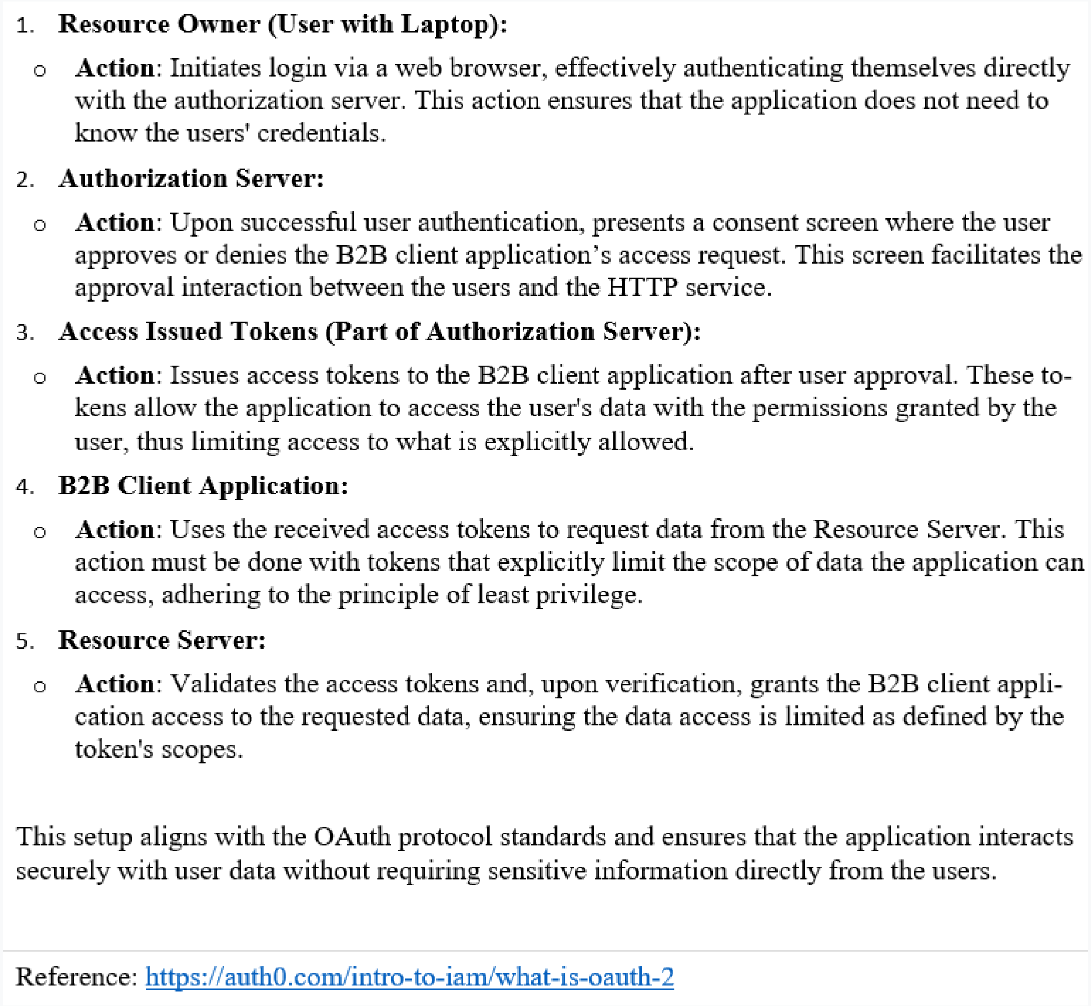
INSTRUCTIONS -

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.



Correct Answer:



1. **Resource Owner (User with Laptop):**
   - **Action**: Initiates login via a web browser, effectively authenticating themselves directly with the authorization server. This action ensures that the application does not need to know the users' credentials.
2. **Authorization Server:**
   - **Action**: Upon successful user authentication, presents a consent screen where the user approves or denies the B2B client application's access request. This screen facilitates the approval interaction between the users and the HTTP service.
3. **Access Issued Tokens (Part of Authorization Server):**
   - **Action**: Issues access tokens to the B2B client application after user approval. These tokens allow the application to access the user's data with the permissions granted by the user, thus limiting access to what is explicitly allowed.
4. **B2B Client Application:**
   - **Action**: Uses the received access tokens to request data from the Resource Server. This action must be done with tokens that explicitly limit the scope of data the application can access, adhering to the principle of least privilege.
5. **Resource Server:**
   - **Action**: Validates the access tokens and, upon verification, grants the B2B client application access to the requested data, ensuring the data access is limited as defined by the token's scopes.

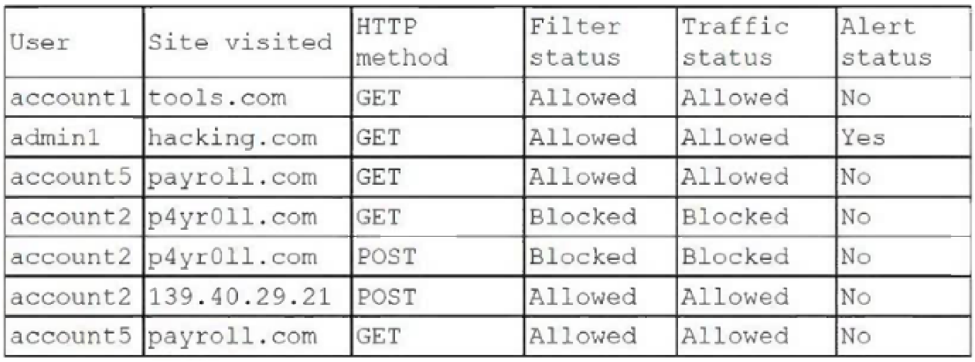
This setup aligns with the OAuth protocol standards and ensures that the application interacts securely with user data without requiring sensitive information directly from the users.

Reference: https://auth0.com/intro-to-iam/what-is-oauth-2

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

Question #12 *Topic 1*

A security analyst wants to use lessons learned from a prior incident response to reduce dwell time in the future. The analyst is using the following data points:



User	Site visited	HTTP method	Filter status	Traffic status	Alert status
account1	tools.com	GET	Allowed	Allowed	No
admin1	hacking.com	GET	Allowed	Allowed	Yes
account5	payroll.com	GET	Allowed	Allowed	No
account2	p4yr0ll.com	GET	Blocked	Blocked	No
account2	p4yr0ll.com	POST	Blocked	Blocked	No
account2	139.40.29.21	POST	Allowed	Allowed	No
account5	payroll.com	GET	Allowed	Allowed	No

Which of the following would the analyst most likely recommend?

A. Adjusting the SIEM to alert on attempts to visit phishing sites

B. Allowing TRACE method traffic to enable better log correlation

C. Enabling alerting on all suspicious administrator behavior

D. Utilizing allow lists on the WAF for all users using GET methods

Correct Answer: *A*

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

Question #13 *Topic 1*

An organization recently implemented a policy that requires all passwords to be rotated every 90 days. An administrator sees a large volume of failed sign-on logs from multiple servers that are often accessed by users. The administrator determines users are disconnecting from the RDP session but not logging off. Which of the following should the administrator do to prevent account lockouts?

A. Increase the account lockout threshold.

B. Enforce password complexity.

C. Force daily reboots.

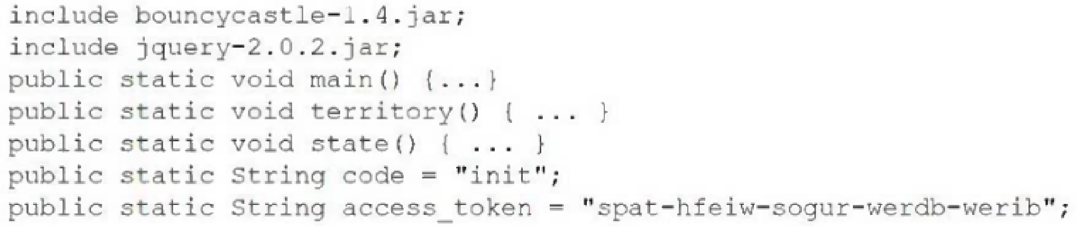
D. Extend the allowed session length.

Correct Answer: *C*

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

Question #14 *Topic 1*

A security analyst is reviewing the following code in the public repository for potential risk concerns:



```
include bouncycastle-1.4.jar;
include jquery-2.0.2.jar;
public static void main() {...}
public static void territory() { ... }
public static void state() { ... }
public static String code = "init";
public static String access_token = "spat-hfeiw-sogur-werdb-werib";
```

Which of the following should the security analyst recommend first to remediate the vulnerability?

A. Developing role-based security awareness training

B. Revoking the secret used in the solution

C. Purging code from public view

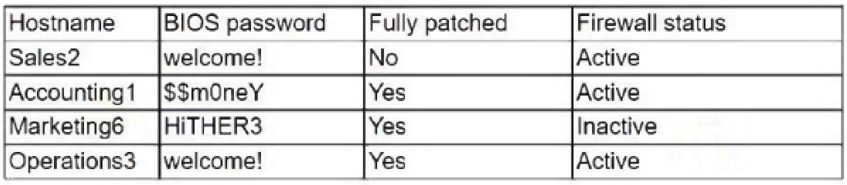
D. Scanning the application with SAST

Correct Answer: *B*

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

Question #15 *Topic 1*

During a recent assessment, a security analyst observed the following:



Hostname	BIOS password	Fully patched	Firewall status
Sales2	welcome!	No	Active
Accounting1	$$m0neY	Yes	Active
Marketing6	HiTHER3	Yes	Inactive
Operations3	welcome!	Yes	Active

Which of the following should the analyst use to address the vulnerabilities in the future?

A. System image hardening

B. Least privilege

C. Defense in depth

D. OS update

Correct Answer: *C*

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

Question #16 Topic 1

The material findings from a recent compliance audit indicate a company has an issue with excessive permissions. The findings show that employees changing roles or departments results in privilege creep. Which of the following solutions are the best ways to mitigate this issue? (Choose two.)

A. Setting different access controls defined by business area

B. Implementing a role-based access policy

C. Designing a least-needed privilege policy

D. Establishing a mandatory vacation policy

E. Performing periodic access reviews

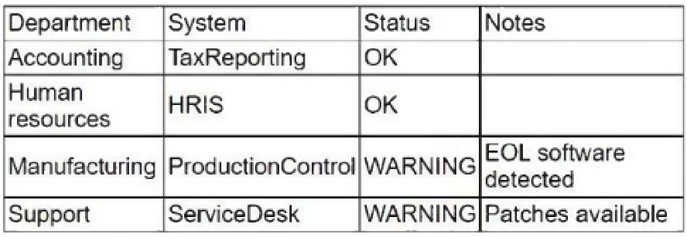
F. Requiring periodic job rotation

Correct Answer: *BE*

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

Question #17 Topic 1

During a recent audit, a company's systems were assessed. Given the following information:



Department	System	Status	Notes
Accounting	TaxReporting	OK	
Human resources	HRIS	OK	
Manufacturing	ProductionControl	WARNING	EOL software detected
Support	ServiceDesk	WARNING	Patches available

Which of the following is the best way to reduce the attack surface?

A. Deploying an EDR solution to all impacted machines in manufacturing

B. Segmenting the manufacturing network with a firewall and placing the rules in monitor mode

C. Setting up an IDS inline to monitor and detect any threats to the software

D. Implementing an application-aware firewall and writing strict rules for the application access

Correct Answer: *A*

Community vote distribution

B (100%)

96abed2 1 month, 1 week ago

Selected Answer: B

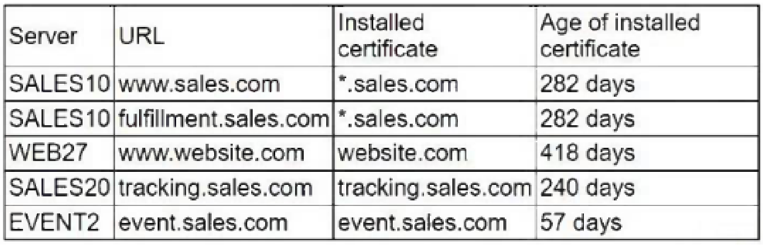
Manufacturing can be ICS/SCADA. You would not put EDR on that. Rather you would segment the network.

upvoted 2 times

Question #18

Topic 1

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: *D*

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

Question #19 *Topic 1*

A company implemented a new NAC solution based on 802.1X. However, the IT support team notices that some devices are not being enrolled in the new policies, causing access disruptions for key users. Which of the following solutions will most likely solve this issue and prevent reoccurrence?

A. Include the monitoring agent and digital certificate as part of the patching/updating program, keeping all the corporate devices updated and enrolled.

B. Check whether the certificate is signed by a certification authority and manually deployed to each device.

C. Check all the devices without proper access, enrolling them via the solution agent and authenticating to the network.

D. Implement default credentials to automate RADIUS authentication and grant access to the network if the device owner is an employee.

Correct Answer: *C*

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

Question #20

Topic 1

An analyst wants to conduct a risk assessment on a new application that is being deployed. Given the following information:

- Total budget allocation for the new application is unavailable.
- Recovery time objectives have not been set.
- Downtime loss calculations cannot be provided.

Which of the following statements describes the reason a qualitative assessment is the best option?

A. The analyst has previous work experience in application development.

B. Sufficient metrics are not available to conduct other risk assessment types.

C. An organizational risk register tracks all risks and mitigations across business units.

D. The organization wants to find the monetary value of any outages.

Correct Answer: *B*

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

Question #21 *Topic 1*

An organization's load balancers have reached EOL and are scheduled to be replaced. The organization identified a new, critical vulnerability that affects an unused function of the load balancers. Which of the following are the best ways to address the risk to the organization? (Choose two.)

A. Request a risk acceptance for the vulnerability indefinitely.

B. Request a risk acceptance for the vulnerability for 90 days.

C. Exclude the devices from vulnerability scans.

D. Do not allow any network traffic to or from the hardware.

E. Disable the vulnerable service.

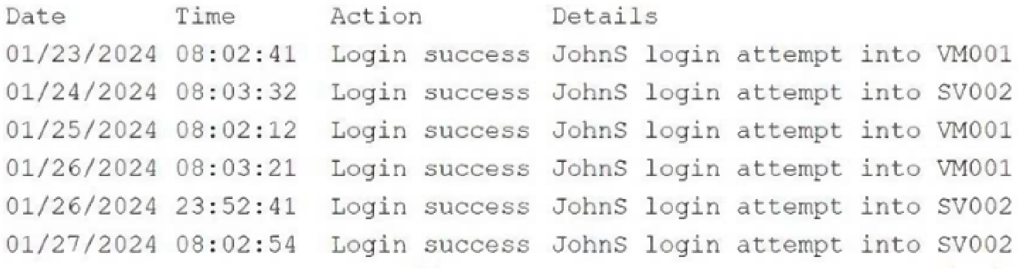
F. Immediately decommission the hardware.

Correct Answer: *BE*

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

Question #22 *Topic 1*

A security engineer receives an alert from the SIEM platform indicating a possible malicious action on the internal network. The engineer generates a report that outputs the logs associated with the incident:



```
Date       Time     Action        Details
01/23/2024 08:02:41  Login success JohnS login attempt into VM001
01/24/2024 08:03:32  Login success JohnS login attempt into SV002
01/25/2024 08:02:12  Login success JohnS login attempt into VM001
01/26/2024 08:03:21  Login success JohnS login attempt into VM001
01/26/2024 23:52:41  Login success JohnS login attempt into SV002
01/27/2024 08:02:54  Login success JohnS login attempt into SV002
```

Which of the following actions best enables the engineer to investigate further?

A. Consulting logs from the enterprise password manager

B. Searching dark web monitoring resources for exposure

C. Reviewing audit logs from privileged actions

D. Querying user behavior analytics data

Correct Answer: *D*

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

Question #23 *Topic 1*

After an increase in adversarial activity, a company wants to implement security measures to mitigate the risk of a threat actor using compromised accounts to mask unauthorized activity. Which of the following is the best way to mitigate the issue?

A. Web application firewall

B. Threat intelligence platforms

C. User and entity behavior analytics

D. Reverse engineering

Correct Answer: *C*

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

Question #24 *Topic 1*

Which of the following best describes the advantage of homomorphic encryption when compared to other encryption methodologies?

A. The need for a pre-shared key is removed.

B. Resource utilization is lower.

C. Support for field-specific tokenization is added.

D. Data integrity is protected by advanced hashing routines.

Correct Answer: *A*

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

Question #25 *Topic 1*

A compliance officer is reviewing the data sovereignty laws in several countries where the organization has no presence. Which of the following is the most likely reason for reviewing these laws?

A. The organization is performing due diligence of potential tax issues.

B. The organization has been subject to legal proceedings in countries where it has a presence.

C. The organization is concerned with new regulatory enforcement in other countries.

D. The organization has suffered brand reputation damage from incorrect media coverage.

Correct Answer: *C*

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

Question #26 Topic 1

A systems administrator needs to address risks associated with corporate brand impersonation via email. The systems administrator wants a method that permits recipient servers to validate the source authenticity of emails received. Which of the following is the most appropriate?

A. SPF

B. DKIM

C. S/MIME

D. DMARC

Correct Answer: *D*

Community vote distribution

B (100%)

mansamusa 4 months, 3 weeks ago

Selected Answer: B

DKIM ensures the email's content has not been altered in transit by adding a digital signature to the email header.

How it works: The domain owner generates a pair of cryptographic keys. The public key is published in the DNS, and the private key is used by the sending server to sign emails.
Validation: Recipient servers retrieve the public key to verify the signature's authenticity.

upvoted 3 times

Question #27 *Topic 1*

An organization receives OSINT reports about an increase in ransomware targeting fileshares at peer companies. The organization wants to deploy hardening policies to its servers and workstations in order to contain potential ransomware. Which of the following should an engineer do to best achieve this goal?

A. Allow only interactive log-in for users on workstations and restrict port 445 traffic to fileshares.

B. Enable biometric authentication mechanisms on user workstations and block port 53 traffic.

C. Instruct users to use a password manager when generating new credentials and secure port 443 traffic.

D. Give users permission to rotate administrator passwords and deny port 80 traffic.

Correct Answer: *A*

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

Question #28 *Topic 1*

A security engineer is reviewing the following piece of code for an internally developed web application that allows employees to manipulate documents from a number of internal servers. Users can specify the document to be parsed by passing the document URL to the application as a parameter. The application then executes the following Python call: response = requests.get(url)
The engineer wants to improve the security of the application before deployment. Which of the following is the best to implement?

A. Indexing

B. Output encoding

C. A code scanner

D. A WAF

Correct Answer: *D*

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

Question #29 *Topic 1*

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 polices to block against known vulnerabilities

C. Completing an IAST scan against the web application

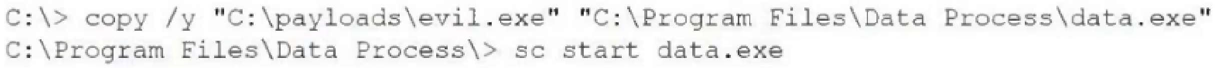
D. Using a software dependency management solution

Correct Answer: *D*

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

Question #30 *Topic 1*

During a security assessment, a penetration tester executed the following attack:



```
C:\> copy /y "C:\payloads\evil.exe" "C:\Program Files\Data Process\data.exe"
C:\Program Files\Data Process\> sc start data.exe
```

The tester then shared the results with the security analyst. Which of the following should the analyst do to remediate the attack?

A. Enable user control access on the endpoint.

B. Enable a PowerShell execution policy on the endpoint.

C. Disable services with unquoted paths on the endpoint.

D. Implement a security endpoint solution.

Correct Answer: *C*

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

Question #31 *Topic 1*

Company A acquired Company B and needs to determine how the acquisition will impact the attack surface of the organization as a whole. Which of the following is the best way to achieve this goal? (Choose two.)

A. Implementing DLP controls preventing sensitive data from leaving Company B's network

B. Documenting third-party connections used by Company B

C. Reviewing the privacy policies currently adopted by Company B

D. Requiring data sensitivity labeling for all files shared with Company B

E. Forcing a password reset requiring more stringent passwords for users on Company B's network

F. Performing an architectural review of Company B's network

Correct Answer: *BF*

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

Question #32 *Topic 1*

A security engineer wants to reduce the attack surface of a public-facing containerized application. Which of the following will best reduce the application's privilege escalation attack surface?

A. Implementing the following commands in the Dockerfile:

```
RUN echo user:x:1000:1000:user:/home/user:/dev/null > /etc/passwd
```

B. Installing an EDR on the container's host, with reporting configured to log to a centralized SIEM, and implementing the following alerting rule:

```
IF PROCESS_USER==root ALERT_TYPE==critical
```

C. Designing a multicontainer solution, with one set of containers that runs the main application, and another set of containers that performs automatic remediation by replacing compromised containers or disabling compromised accounts

D. Running the container in an isolated network and placing a load balancer in a public-facing network. Adding the following ACL to the load balancer:

```
PERMIT HTTPS from 0.0.0.0.0/0 port 443
```

Correct Answer: *A*

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

Question #33 *Topic 1*

A company that uses containers to run its applications is required to identify vulnerabilities on every container image in a private repository. The security team needs to be able to quickly evaluate whether to respond to a given vulnerability. Which of the following will allow the security team to achieve the objective with the least effort?

A. SAST scan reports

B. Centralized SBoM

C. CIS benchmark compliance reports

D. Credentialed vulnerability scan

Correct Answer: *B*

Community vote distribution

D (100%)

CYBERSafe23 1 month ago

Selected Answer: D

A credentialed vulnerability scan uses specialized tools to access the container image and directly analyze its contents for known vulnerabilities.

upvoted 1 times

Question #34 *Topic 1*

A company currently uses manual processes to regularly address incidents occurring outside of working hours. Hiring or implementing a SOC is not an option because of budget limitations. Which of the following solutions would most likely decrease the current risk?

A. Improve logging capabilities, integrating those logs with the existing SIEM and creating better security dashboards.

B. Implement a NIPS integrated with the firewall, raising new rules to block any malicious access attempts coming from the external perimeter.

C. Evaluate and implement new endpoint security tools, helping to prevent attack attempts.

D. Design proper runbooks and implement security orchestration and automation with integrated security tools.

Correct Answer: *D*

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

Question #35 *Topic 1*

A security architect is implementing more restrictive policies to improve secure coding practices. Which of the following solutions are the best ways to improve the security coding practices? (Choose two.)

A. Hire a third-party company to perform regular software tests, including quality and unity tests.

B. Deliver regular training for the software developers based on best practices.

C. Perform regular vulnerability assessments on production software, defining tight SLAs for treatment.

D. Define security gates and tests along the CI/CD flow with strict exception rules.

E. Perform regular code reviews and implement pair programming methodology.

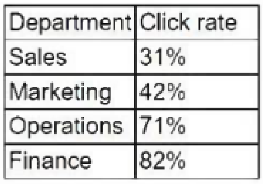
F. Implement a SAST tool along the pipeline for every new commit.

Correct Answer: *BF*

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

Question #36 *Topic 1*

A Chief Information Security Officer assigns a team to create malicious communications for a social engineering campaign. The purpose of this campaign is to determine the number of employees who might be susceptible to social engineering attacks. The following is a summary report from a previous campaign:



Department	Click rate
Sales	31%
Marketing	42%
Operations	71%
Finance	82%

Which of the following training modules would reduce click rates in the future?

A. Phishing

B. Whaling

C. Smishing

D. Tailgating

Correct Answer: *A*

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

Question #37 *Topic 1*

A security architect is onboarding a new EDR agent on servers that traditionally do not have internet access. In order for the agent to receive updates and report back to the management console, some changes must be made. Which of the following should the architect do to best accomplish this requirement? (Choose two.)

A. Create a firewall rule to only allow traffic from the subnet to the internet via a proxy.

B. Configure a proxy policy that blocks all traffic on port 443.

C. Configure a proxy policy that allows only fully qualified domain names needed to communicate to a portal.

D. Create a firewall rule to only allow traffic from the subnet to the internet via port 443.

E. Create a firewall rule to only allow traffic from the subnet to the internet to fully qualified names that are not identified as malicious by the firewall vendor.

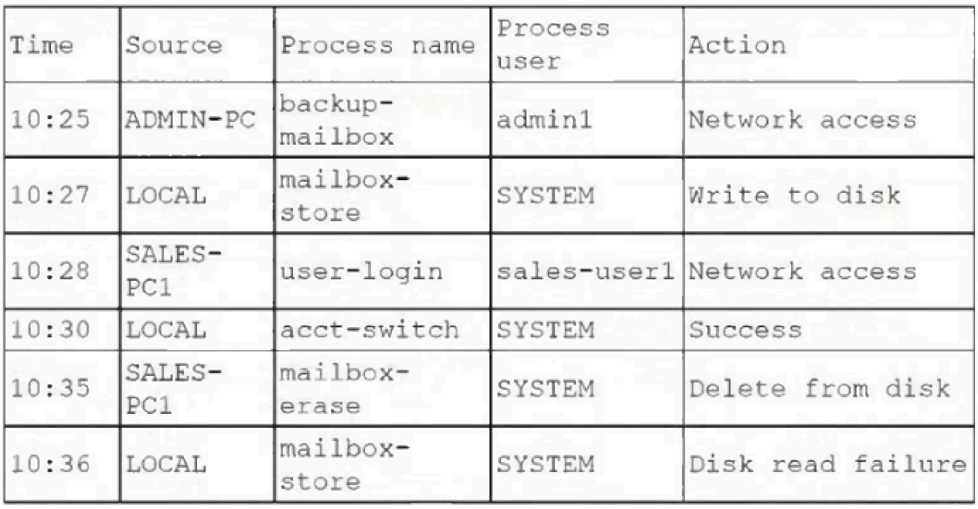
F. Configure a proxy policy that blocks only lists of known-bad, fully qualified domain names.

Correct Answer: *AC*

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

Question #38 *Topic 1*

While investigating an email server that crashed, an analyst reviews the following log files:



Time	Source	Process name	Process user	Action
10:25	ADMIN-PC	backup-mailbox	admin1	Network access
10:27	LOCAL	mailbox-store	SYSTEM	Write to disk
10:28	SALES-PC1	user-login	sales-user1	Network access
10:30	LOCAL	acct-switch	SYSTEM	Success
10:35	SALES-PC1	mailbox-erase	SYSTEM	Delete from disk
10:36	LOCAL	mailbox-store	SYSTEM	Disk read failure

Which of the following is most likely the root cause?

A. The administrator's account credentials were intercepted and reused.

B. The backup process did not complete and caused cascading failure.

C. A hardware failure in the storage array caused the mailboxes to be inaccessible.

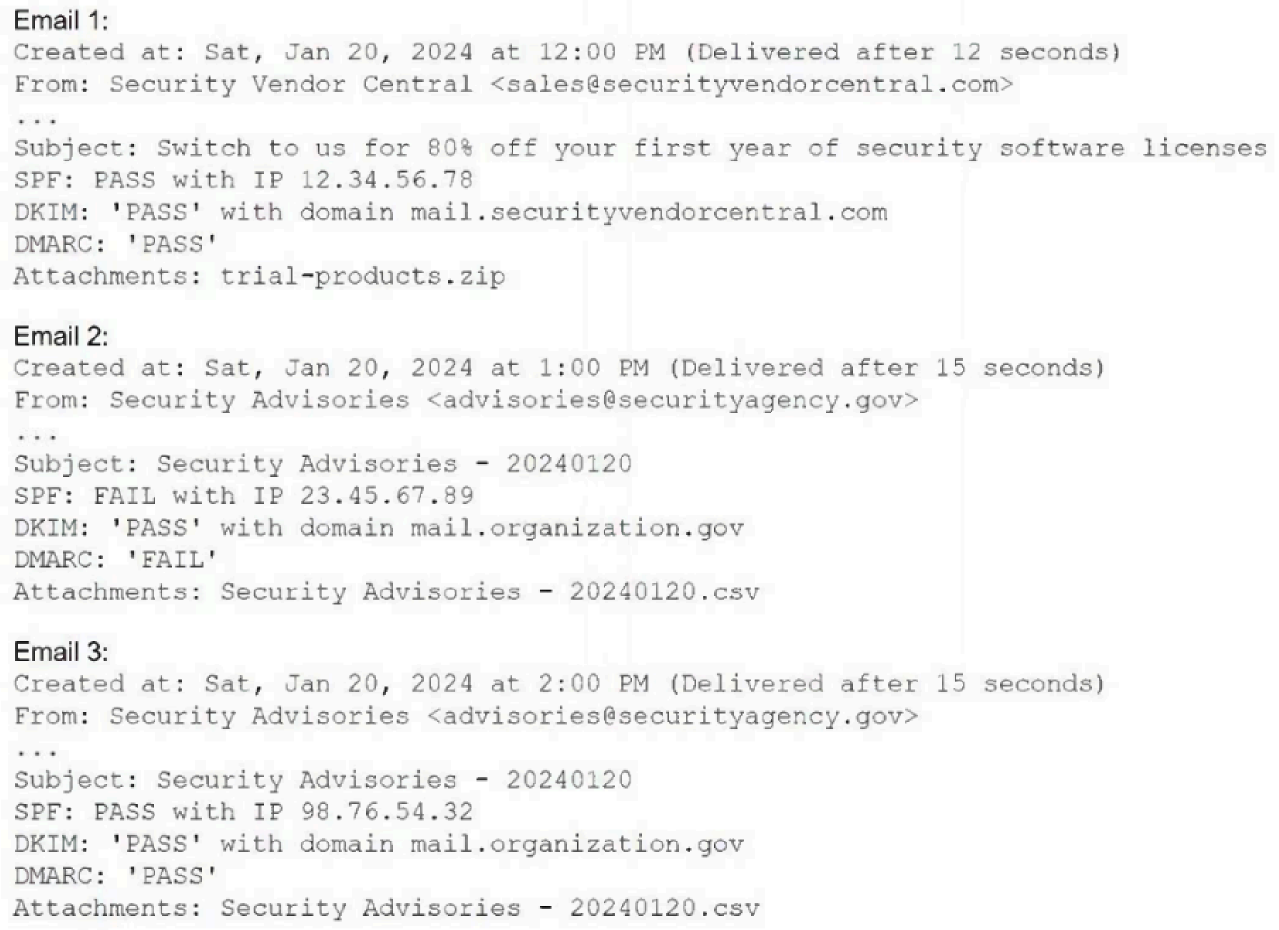
D. A user with low privileges was able to escalate and erase all mailboxes.

Correct Answer: *C*

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

Question #39 *Topic 1*

Incident responders determine that a company email server was the first compromised machine in an attack. The server was infected by malware. The following are abbreviated headers from three emails that the incident responders could not confidently determine to be safe:



Email 1:

```
Created at: Sat, Jan 20, 2024 at 12:00 PM (Delivered after 12 seconds)
From: Security Vendor Central <sales@securityvendorcentral.com>
...
Subject: Switch to us for 80% off your first year of security software licenses
SPF: PASS with IP 12.34.56.78
DKIM: 'PASS' with domain mail.securityvendorcentral.com
DMARC: 'PASS'
Attachments: trial-products.zip
```

Email 2:

```
Created at: Sat, Jan 20, 2024 at 1:00 PM (Delivered after 15 seconds)
From: Security Advisories <advisories@securityagency.gov>
...
Subject: Security Advisories - 20240120
SPF: FAIL with IP 23.45.67.89
DKIM: 'PASS' with domain mail.organization.gov
DMARC: 'FAIL'
Attachments: Security Advisories - 20240120.csv
```

Email 3:

```
Created at: Sat, Jan 20, 2024 at 2:00 PM (Delivered after 15 seconds)
From: Security Advisories <advisories@securityagency.gov>
...
Subject: Security Advisories - 20240120
SPF: PASS with IP 98.76.54.32
DKIM: 'PASS' with domain mail.organization.gov
DMARC: 'PASS'
Attachments: Security Advisories - 20240120.csv
```

Which of the following is the most likely reason the malware was delivered?

A. An attachment scan could not be completed.

B. The DMARC security check failed.

C. Repeated emails were sent from the same address.

D. The SPF check failed.

Correct Answer: *B*

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

Question #40 *Topic 1*

An engineer wants to automate several tasks by running commands daily on a UNIX server. The engineer only has built-in default tools available. Which of the following should the engineer use to best assist with this endeavor? (Choose two.)

A. Python

B. Cron

C. Ansible

D. PowerShell

E. Bash

F. Task Scheduler

Correct Answer: *BE*

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

Question #41

Topic 1

After an organization met with its ISAC, the organization decided to test the resiliency of its security controls against a small number of advanced threat actors. Which of the following will enable the security administrator to accomplish this task?

A. Adversary emulation

B. Reliability factors

C. Deployment of a honeypot

D. Internal reconnaissance

Correct Answer: *A*

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

Question #42 *Topic 1*

A small number but steady series of attempts to breach the network has been occurring over a long period of time. During an investigation, a SOC analyst finds that traffic is exiting the network to known malicious hosts and is originating from a rogue network device. Which of the following attack vectors is most likely being used to breach the network?

A. Supply chain

B. Buffer overflow

C. Social engineering

D. Ransomware

Correct Answer: *A*

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

Question #43 *Topic 1*

A security analyst detects a possible RAT infection on a computer in the internal network. After reviewing the details of the alert, the analyst identifies the initial vector of the attack was an email that was forwarded to multiple recipients in the same organizational unit. Which of the following should the analyst do first to minimize this type of threat in the future?

A. Move from an anti-malware software to an EDR solution.

B. Perform a penetration test to detect technology gaps on the anti-spam solution.

C. Configure an IPS solution in the internal network to mitigate infections.

D. Implement a security awareness program in the organization.

Correct Answer: *D*

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

Question #44 *Topic 1*

An organization that performs real-time financial processing is implementing a new backup solution. Given the following business requirements:

- The backup solution must reduce the risk for potential backup compromise.
- The backup solution must be resilient to a ransomware attack.
- The time to restore from backups is less important than the backup data integrity.
- Multiple copies of production data must be maintained.

Which of the following backup strategies best meets these requirements?

A. Creating a secondary, immutable storage array and updating it with live data on a continuous basis

B. Utilizing two connected storage arrays and ensuring the arrays constantly sync

C. Enabling remote journaling on the databases to ensure real-time transactions are mirrored

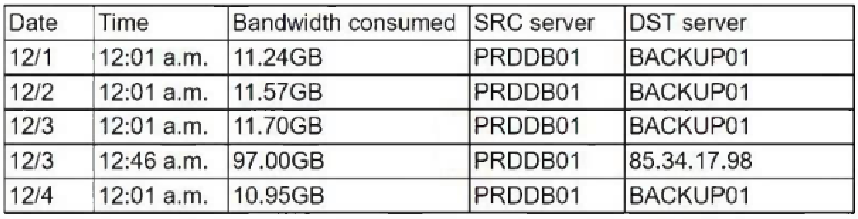
D. Setting up antitampering on the databases to ensure data cannot be changed unintentionally

Correct Answer: *A*

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

Question #45 *Topic 1*

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: *D*

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

Question #46 *Topic 1*

While performing threat-hunting functions, an analyst is using the Diamond Model of Intrusion Analysis. The analyst identifies the likely adversary, the infrastructure involved, and the target. Which of the following must the threat hunter document to use the model effectively?

A. Knowledge

B. Capabilities

C. Phase

D. Methodologies

Correct Answer: *D*

Community vote distribution

B (100%)

7ac1fdf 5 days ago

Selected Answer: B

The Diamond Model of Intrusion Analysis is a model to describe cyber attacks. It contains 4 parts - adversary, infrastructure, capability, and target.

upvoted 1 times

Question #47 *Topic 1*

An organization plans to deploy new software. The project manager compiles a list of roles that will be involved in different phases of the deployment life cycle. Which of the following should the project manager use to track these roles?

A. CMDB

B. Recall tree

C. ITIL

D. RACI matrix

Correct Answer: *D*

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

Question #48 *Topic 1*

A security engineer added a new server to the company email cluster. The server has a new external IP address associated with it. After a few days, the service desk started receiving complaints from users about their outgoing messages to customers being flagged as spam. Which of the following records should the security engineer update to fix the issue? (Choose two.)

A. DMARC

B. CNAME

C. MX

D. SPF

E. MIME

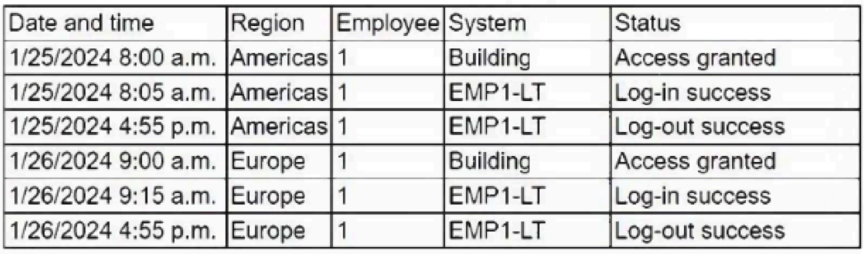
F. PTR

Correct Answer: *DF*

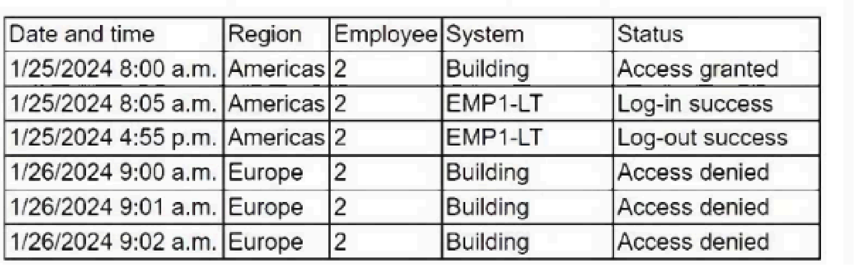
Currently there are no comments in this discussion, be the first to comment!

Question #49 *Topic 1*

Due to an infrastructure optimization plan, a company has moved from a unified architecture to a federated architecture divided by region. Long-term employees now have a better experience, but new employees are experiencing major performance issues when traveling between regions. The company is reviewing the following information:



Date and time	Region	Employee	System	Status
1/25/2024 8:00 a.m.	Americas	1	Building	Access granted
1/25/2024 8:05 a.m.	Americas	1	EMP1-LT	Log-in success
1/25/2024 4:55 p.m.	Americas	1	EMP1-LT	Log-out success
1/26/2024 9:00 a.m.	Europe	1	Building	Access granted
1/26/2024 9:15 a.m.	Europe	1	EMP1-LT	Log-in success
1/26/2024 4:55 p.m.	Europe	1	EMP1-LT	Log-out success



Date and time	Region	Employee	System	Status
1/25/2024 8:00 a.m.	Americas	2	Building	Access granted
1/25/2024 8:05 a.m.	Americas	2	EMP1-LT	Log-in success
1/25/2024 4:55 p.m.	Americas	2	EMP1-LT	Log-out success
1/26/2024 9:00 a.m.	Europe	2	Building	Access denied
1/26/2024 9:01 a.m.	Europe	2	Building	Access denied
1/26/2024 9:02 a.m.	Europe	2	Building	Access denied

Which of the following is the most effective action to remediate the issue?

A. Creating a new user entry in the affected region for the affected employee

B. Synchronizing all regions' user identities and ensuring ongoing synchronization

C. Restarting European region physical access control systems

D. Resyncing single sign-on application with connected security appliances

Correct Answer: *B*

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

Question #50 *Topic 1*

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*

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

Question #51 *Topic 1*

A large organization deployed a generative AI platform for its global user population to use. Based on feedback received during beta testing, engineers have identified issues with user interface latency and page-loading performance for international users. The infrastructure is currently maintained within two separate data centers, which are connected using high-availability networking and load balancers. Which of the following is the best way to address the performance issues?

A. Configuring the application to use a CDN

B. Implementing RASP to enable large language models queuing

C. Remote journaling within a third data center

D. Traffic shaping through the use of a SASE

Correct Answer: *A*

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

Question #52 *Topic 1*

A company discovers intellectual property data on commonly known collaboration web applications that allow the use of slide templates. The systems administrator is reviewing the configurations of each tool to determine how to prevent this issue. The following security solutions are deployed:

- CASB
- SASE
- WAF
- EDR
- Firewall
- IDS
- SIEM
- DLP endpoints

Which of the following should the administrator do to address the issue?

A. Enable blocking for all WAF policies.

B. Enforce a policy to block unauthorized web applications within CASB.

C. Create an alert within the SIEM for outgoing network traffic to the suspected website.

D. Configure DLP endpoints to block sensitive data to the mass media.

Correct Answer: *B*

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

Question #53 *Topic 1*

A security audit of a company's application finds that customer account passwords are manually set and never expire. The company wants to fix the password issue on a minimal budget within 30 days while minimizing the impact to customers. Which of the following should the company do?

A. Contact each user to reset their password.

B. Migrate authentication methods to allow for OAuth 2.

C. Implement a self-service credential reset portal.

D. Configure a privilege access management solution.

Correct Answer: *C*

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

Question #54 *Topic 1*

A security team receives an escalated support ticket for a user who is unable to access specific corporate resources. The following configurations exist in the corporation:

- A device certificate is deployed on all corporate assets.
- Templates for unique user certificates are configured.
- Security updates are installed every 30 days.
- Administrator access is tied to specific hosts.

The ticket contains the following observations:

- The user has been on leave for more than 90 days.
- Internal vulnerability scans indicate no device issues.
- Single sign-on works as expected.
- Privileged systems are not accessible.

Which of the following best describes the root cause?

A. The user's administrator credentials likely expired after 90 days.

B. The device being utilized does not have user binding established.

C. Several patch cycles have been missed while the user was on leave.

D. Incorrect certificate extensions have been added to the templates.

Correct Answer: *A*

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

Question #55 *Topic 1*

A web application server that provides services to hybrid modern and legacy financial applications recently underwent a scheduled upgrade to update common libraries, including OpenSSL. Multiple users are now reporting failed connection attempts to the server. The technician performing initial triage identified the following:

- Client applications more than five years old appear to be the most affected.
- Web server logs show initial connection attempts by affected hosts.
- For the failed connections, logs indicate "cipher unavailable."

Which of the following is most likely to safely remediate this situation?

A. The server needs to be configured for backward compatibility to SSL 3.0 applications.

B. The client applications need to be modified to support AES in Galois/Counter Mode or equivalent.

C. The client TLS configuration must be set to enforce electronic codebook modes of operation.

D. The server-side digital signature algorithm needs to be modified to support elliptic curve cryptography.

Correct Answer: *B*

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

Question #56 *Topic 1*

A cloud engineer configured mail security protocols to support email authenticity and wants to enable the flow of email security information to a third-party platform for further analysis. Which of the following must be configured correctly?

A. DMARC

B. DKIM

C. TLS

D. SPF

Correct Answer: *A*

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