

## Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam

<https://www.2passeasy.com/dumps/CS0-003/>



### NEW QUESTION 1

During a security test, a security analyst found a critical application with a buffer overflow vulnerability. Which of the following would be best to mitigate the vulnerability at the application level?

- A. Perform OS hardening.
- B. Implement input validation.
- C. Update third-party dependencies.
- D. Configure address space layout randomization.

**Answer: B**

#### Explanation:

Implementing input validation is the best way to mitigate the buffer overflow vulnerability at the application level. Input validation is a technique that checks the data entered by users or attackers against a set of rules or constraints, such as data type, length, format, or range. Input validation can prevent common web application attacks such as SQL injection, cross-site scripting (XSS), or command injection, which exploit the lack of input validation to execute malicious code or commands on the server or the client side. By validating the input before allowing submission, the web application can reject or sanitize any malicious or unexpected input, and protect the application from being compromised<sup>12</sup>. References: How to detect, prevent, and mitigate buffer overflow attacks - Synopsys, How to mitigate buffer overflow vulnerabilities | Infosec

### NEW QUESTION 2

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

**Answer: D**

#### Explanation:

This VM has a public IP and an open port 80, which violates the company's security requirements of no public IPs and no insecure ports/protocols. It also exposes the VM to potential attacks from the internet. This VM should be updated first to use a private IP and close the port 80, or use a secure protocol such as HTTPS.

References[CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition], Chapter 2: Cloud and Hybrid Environments, page 67.[What is a Public IP Address?][What is Port 80?]

### NEW QUESTION 3

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. QVVASP

**Answer: C**

#### Explanation:

SOAR stands for security orchestration, automation, and response, which is a term that describes a set of tools, technologies, or platforms that can help streamline, standardize, and automate security operations and incident response processes and tasks. SOAR can help minimize human engagement and aid in process improvement in security operations by reducing manual work, human errors, response time, or complexity. SOAR can also help enhance collaboration, coordination, efficiency, or effectiveness of security operations and incident response teams.

### NEW QUESTION 4

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/1: 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

**Answer:** A

**Explanation:**

This answer matches the description of the zero-day threat. The attack vector is network (AV:N), the attack complexity is low (AC:L), no privileges are required (PR:N), no user interaction is required (UI:N), the scope is unchanged (S:U), the confidentiality and integrity impacts are high (C:H/I:H), and the availability impact is low (A:L). Official References: <https://nvd.nist.gov/vuln-metrics/cvss>

**NEW QUESTION 5**

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

**Answer:** C

**Explanation:**

The MTTD (Mean Time To Detect) is calculated by averaging the time elapsed in detecting incidents. From the given data:  $(180+150+170+140)/4 = 160$  minutes. This is the correct answer according to the CompTIA CySA+ CS0-003 Certification Study Guide1, Chapter 4, page 161. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4, page 153; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 4, page 161.

**NEW QUESTION 6**

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

**Answer:** D

**Explanation:**

Beaconsing is the best term to describe the activity that is taking place, as it refers to the periodic communication between an infected host and a blocklisted external server. Beaconsing is a common technique used by malware to establish a connection with a command-and-control (C2) server, which can provide instructions, updates, or exfiltration capabilities to the malware. Beaconsing can vary in frequency, duration, and payload, depending on the type and sophistication of the malware. The other terms are not as accurate as beaconsing, as they describe different aspects of malicious activity. Data exfiltration is the unauthorized transfer of data from a compromised system to an external destination, such as a C2 server or a cloud storage service. Data exfiltration can be a goal or a consequence of malware infection, but it does not necessarily involve blocklisted servers or consistent requests. Rogue device is a device that is connected to a network without authorization or proper security controls. Rogue devices can pose a security risk, as they can introduce malware, bypass firewalls, or access sensitive data. However, rogue devices are not necessarily infected with malware or communicating with blocklisted servers. Scanning is the process of probing a network or a system for vulnerabilities, open ports, services, or other information. Scanning can be performed by legitimate administrators or malicious actors, depending on the intent and authorization. Scanning does not imply consistent requests or blocklisted servers, as it can target any network or system.

**NEW QUESTION 7**

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

**Answer:** A

**Explanation:**

Eradication is a step in the incident response process that involves removing any traces or remnants of the incident from the affected systems or networks, such as malware, backdoors, compromised accounts, or malicious files. Eradication also involves restoring the systems or networks to their normal or secure state, as well as verifying that the incident is completely eliminated and cannot recur. In this case, the analyst is remediating items associated with a recent incident by isolating the vulnerability and actively removing it from the system. This describes the eradication step of the incident response process.

### NEW QUESTION 8

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/AVP/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

**Answer: C**

#### Explanation:

CVSS 3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H is the attack vector that the analyst should remediate first, as it has the highest CVSSv3 score of 8.1. CVSSv3 (Common Vulnerability Scoring System version 3) is a standard framework for rating the severity of vulnerabilities, based on various metrics that reflect the characteristics and impact of the vulnerability. The CVSSv3 score is calculated from three groups of metrics: Base, Temporal, and Environmental. The Base metrics are mandatory and reflect the intrinsic qualities of the vulnerability, such as how it can be exploited, what privileges are required, and what impact it has on confidentiality, integrity, and availability. The Temporal metrics are optional and reflect the current state of the vulnerability, such as whether there is a known exploit, a patch, or a workaround. The Environmental metrics are also optional and reflect the context of the vulnerability in a specific environment, such as how it affects the asset value, security requirements, or mitigating controls. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.

The attack vector in question has the following Base metrics:

? Attack Vector (AV): Network (N). This means that the vulnerability can be exploited remotely over a network connection.

? Attack Complexity (AC): Low (L). This means that the attack does not require any special conditions or changes to the configuration of the target system.

? Privileges Required (PR): Low (L). This means that the attacker needs some privileges on the target system to exploit the vulnerability, such as user-level access.

? User Interaction (UI): None (N). This means that the attack does not require any user action or involvement to succeed.

? Scope (S): Unchanged (U). This means that the impact of the vulnerability is confined to the same security authority as the vulnerable component, such as an application or an operating system.

? Confidentiality Impact ©: High (H). This means that the vulnerability results in a total loss of confidentiality, such as unauthorized disclosure of all data on the system.

? Integrity Impact (I): High (H). This means that the vulnerability results in a total loss of integrity, such as unauthorized modification or deletion of all data on the system.

? Availability Impact (A): High (H). This means that the vulnerability results in a total loss of availability, such as denial of service or system crash.

Using these metrics, we can calculate the Base score using this formula: Base Score = Roundup(Minimum[(Impact + Exploitability), 10])

Where:  
 Impact =  $6.42 \times [1 - ((1 - \text{Confidentiality}) \times (1 - \text{Integrity}) \times (1 - \text{Availability}))]$  Exploitability =  $8.22 \times \text{Attack Vector} \times \text{Attack Complexity} \times \text{Privileges Required} \times \text{User Interaction}$

Using this formula, we get:

Impact =  $6.42 \times [1 - ((1 - 0.56) \times (1 - 0.56) \times (1 - 0.56))] = 5.9$

Exploitability =  $8.22 \times 0.85 \times 0.77 \times 0.62 \times 0.85 = 2.8$

Base Score = Roundup(Minimum[(5.9 + 2.8), 10]) = Roundup(8.7) = 8.8

Therefore, this attack vector has a Base score of 8.8, which is higher than any other option. The other attack vectors have lower Base scores, as they have different values for some of the Base metrics:

? CVSS:3.0/AV:P/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has a Base score of 6.2, as it

has a lower value for Attack Vector (Physical), which means that the vulnerability can only be exploited by having physical access to the target system.

? CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has a Base score of 7.4, as it

has a lower value for Attack Vector (Adjacent Network), which means that the vulnerability can only be exploited by being on the same physical or logical network as the target system.

? CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has a Base score of 6.8, as it has

a lower value for Attack Vector (Local), which means that the vulnerability can only be exploited by having local access to the target system, such as through a terminal or a command shell.

### NEW QUESTION 9

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

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

**Answer: A**

#### Explanation:

A credentialed scan is a type of vulnerability scan that uses valid credentials to log in to the scanned systems and perform a more thorough and accurate assessment of their vulnerabilities. A credentialed scan can access more information than a non-credentialed scan, such as registry keys, patch levels, configuration settings, and installed applications. A credentialed scan can also reduce the number of false positives and false negatives, as it can verify the actual state of the system rather than relying on inference or assumptions. The other types of scans are not related to the issue of incomplete findings, as they refer to different aspects of vulnerability scanning, such as the scope, location, or frequency of the scan. An external scan is a scan that is performed from outside the network perimeter, usually from the internet. An external scan can reveal how an attacker would see the network and what vulnerabilities are exposed to the public. An external scan cannot access internal systems or resources that are behind firewalls or other security controls. A differential scan is a scan that compares the results of two scans and highlights the differences between them. A differential scan can help identify changes in the network environment, such as new vulnerabilities, patched vulnerabilities, or new devices. A differential scan does not provide a complete list of findings by itself, but rather a summary of changes. A network scan is a scan that focuses on the network layer of the OSI model and detects vulnerabilities related to network devices, protocols, services, and configurations. A network scan can discover open ports, misconfigured firewalls, unencrypted traffic, and other network-related issues. A network scan does not provide information about the application layer or the host layer of the OSI model, such as web applications or operating systems.

### NEW QUESTION 10

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

**Answer:** A

**Explanation:**

Non-repudiation ensures that a message sender cannot deny the authenticity of their sent message. This is crucial in banking communications for legal and security reasons.

The goal of allowing a message recipient to prove the message's origin is non-repudiation. This ensures that the sender cannot deny the authenticity of their message. Non- repudiation is a fundamental aspect of secure messaging systems, especially in banking and financial communications.

**NEW QUESTION 10**

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.

**Answer:** D

**Explanation:**

Determining the asset value of each system is the best action to perform first, as it helps to categorize and prioritize the systems based on the sensitivity of the data they host. The asset value is a measure of how important a system is to the organization, in terms of its financial, operational, or reputational impact. The asset value can help the security analyst to assign a risk level and a protection level to each system, and to allocate resources accordingly. The other actions are not as effective as determining the asset value, as they do not directly address the goal of promoting confidentiality, availability, and integrity of the data.

Interviewing the users who access these systems may provide some insight into how the systems are used and what data they contain, but it may not reflect the actual value or sensitivity of the data from an organizational perspective. Scanning the systems to see which vulnerabilities currently exist may help to identify and remediate some security issues, but it does not help to categorize or prioritize the systems based on their data sensitivity. Configuring alerts for vendor-specific zero-day exploits may help to detect and respond to some emerging threats, but it does not help to protect the systems based on their data sensitivity.

**NEW QUESTION 15**

**HOTSPOT**

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.



Firewall log:

**Firewall log** ✕

Traffic denied:

Dec 1 14:10:46 fire00 fire00: NetScreen device\_id=fire00 [Root]system-notification-00257(traffic): policy\_id=119 service=udp/port:7001 proto=17 src zone=Trust dst zone=Untrust action=Deny sent=0 rcvd=0 src=192.168.2.1 dst=1.2.3.4 src\_port=3036 dst\_port=7001

Dec 1 14:12:31 fire00 aka1: NetScreen device\_id=aka1 [Root]system-notification-00257(traffic): policy\_id=120 service=udp/port:20721 proto=17 src zone=Trust dst zone=DMZ action=Deny sent=0 rcvd=0 src=192.168.2.2 dst=1.2.3.4 src\_port=53 dst\_port=20721

Dec 1 14:14:31 fire00 aka1: NetScreen device\_id=aka1 [Root]system-notification-00257(traffic): policy\_id=120 service=udp/port:17210 proto=17 src zone=Trust dst zone=DMZ action=Deny sent=0 rcvd=0 src=192.168.2.2 dst=1.2.3.4 src\_port=53 dst\_port=17210

Alert messages:

Dec 1 14:03:19 [xx] ns5gt: NetScreen device\_id=ns5gt [Root]system-alert-00016: invoice.exe From 81.161.63.253, proto TCP (zone Untrust, int untrust). Occurred 1 times.

Critical messages:

Dec 1 11:24:16 fire00 sav00: NetScreen device\_id=sav00 [Root]system-critical-00436: Large ICMP packet! From 1.2.3.4 to 2.3.4.5, proto 1 (zone Untrust, int ethernet1/2). Occurred 1 times.

[00001] 2005-05-16 12:55:10 [Root]system-critical-00042: Replay packet detected on IPSec tunnel on ethernet3 with tunnel ID 0x1c! From z.y.x.w to a.b.c.d/336, ESP, SPI 0xf63af637, SEQ 0xe337.

[00001] 2006-05-25 13:34:33 [Root]system-alert-00008: IP spoofing! From 10.1.1.238:80 to a.b.c.d:49807, proto TCP (zone Untrust, int ethernet3). Occurred 1 times.

File integrity Monitoring Report:

**File integrity monitoring report** ✕

Shows files, folders, shares, and permissions that were created, deleted, or modified.

| Action                                       | Object type           | What                                       | Who               | When                 |
|--|-----------------------|--|-------------------|----------------------|
| <b>Added</b>                                 | File                  | \\host1\users\user1\Downloads\payroll.xlsx | Domainusers\user1 | 11/30/19<br>12:05:34 |
| Where:<br>Workstation:                       | Host1<br>172.30.0.152 |  |                   |                      |
| <b>Removed</b>                               | File                  | \\host1\users\user1\Downloads\payroll.xlsx | Domainusers\user1 | 11/30/19<br>12:25:13 |
| Where:<br>Workstation:<br>Date created:      | Host1<br>172.30.0.152 | "11/30/19 12:05:34"                        |                   |                      |
| <b>Added</b>                                 | File                  | \\host1\users\user1\Downloads\resume1.docx | Domainusers\user1 | 12/1/19<br>13:59:25  |
| Where:<br>Workstation:                       | Host1<br>172.30.0.152 |  |                   |                      |
| <b>Added</b>                                 | File                  | \\host1\users\user1\Downloads\invoice.exe  | Domainusers\user1 | 12/1/19<br>14:03:55  |
| Where:<br>Workstation:                       | Host1<br>172.30.0.152 |  |                   |                      |
| <b>Renamed</b>                               | File                  |  | Domainusers\user1 | 12/1/19<br>14:25:30  |
| Where:<br>Workstation:<br>Name changed from: | Host1<br>172.30.0.152 | resume1.docx to resume2.docx               |                   |                      |

Malware domain list:

## Malware domain list

```
# MalwareDomainList.com Host List #
# http://www.maowaredomainlist.com/hostlist/hosts.txt #
# Last updated: 3 Dec 2019, 21:00:00 #
# IP #

171.25.193.20
171.25.193.25
185.220.101.194
81.161.63.103
81.161.63.253
77.247.181.162
141.98.81.194
46.101.220.225
139.59.95.60
51.254.37.192
81.161.63.104
139.59.116.115
```

Vulnerability Scan Report:

## Vulnerability scan report

**HIGH SEVERITY**

**Title:** Cleartext transmission of sensitive information  
**Description:** The software transmits sensitive or security-critical data in Cleartext in a communication channel that can be sniffed by authorized users.  
**Affected asset:** 172.30.0.150  
**Risk:** Anyone can read the information by gaining access to the channel being used for communication.  
**Reference:** CVE-2002-1949

**HIGH SEVERITY**

**Title:** Elevated privileges not required for software installations  
**Description:** All account types can install software, requirements for privileged accounts for installation capabilities is not configured.  
**Affected asset:** 172.30.0.152  
**Risk:** Enhanced risk for unauthorized or malicious software installation  
**Reference:** n/a

**MEDIUM SEVERITY**

**Title:** Sensitive cookie in HTTPS session without "secure" attribute  
**Description:** The secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over HTTP session.  
**Affected asset:** 172.30.0.157  
**Risk:** Session sidejacking  
**Reference:** CVE-2004-0462

**LOW SEVERITY**

**Title:** Untrusted SSL/TLS Server X.509 certificate  
**Description:** The server's TLS/SSL certificate is signed by a certificate authority that is untrusted or unknown.  
**Affected asset:** 172.30.0.153  
**Risk:** May allow on-path attackers to insert a spoofed certificate for any distinguished name (DN).  
**Reference:** CVE-2005-1234

Phishing Email:

Phishing email

From: IT HelpDesk <it-helpdesk@company.com>  
 Sent: Sun 12/01/2019 2:00:00  
 To: Global Users <globalusers@company.com>  
 Subject: Moving our mail servers

Hi,

In the upcoming days, we will be moving our mail servers. Check out the new Company Webmail to know if it has started working for you.

Visit the new Company Webmail to see all the new features.  
 Use your current username and password at [Company Webmail](#).

Download the latest mail client located [here](#).

Thank you.

IT HelpDesk

The screenshot displays a security tool interface with two main panels. The left panel, titled 'Kill chain item', shows a vertical flow of attack stages: Phishing email, Active links, Malicious website access, and Malware download. The right panel, titled 'Identify the following:', shows a list of controls for various attack stages: Malicious executable, Malicious IP address, Date/time malware entered organization, Malware install, Malware execution, and File encryption. Each stage has a dropdown menu labeled 'Select control' with a list of security controls.

**Kill chain item controls:**

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

**Identify the following: controls:**

- Malicious executable: Select option, invoice.exe, resume1.docx, resume2.docx, payroll.xlsx
- Malicious IP address: Select option, 81.161.63.103, 81.161.63.253, 171.25.193.20, 185.220.101.194, 192.168.2.1, 171.25.193.25, 10.1.1.238
- Date/time malware entered organization: Select option, 1 Dec 2019 11:24:16, 1 Dec 2019 14:03:19, 1 Dec 2019 14:03:55, 30 Nov 2019 12:05:34, 1 Dec 2019 14:25:30, 1 Dec 2019 13:59:25, 30 Nov 2019 12:25:13
- Malware install: Select control, Firewall file type filter, Honeypot, MFA, MAC filtering, Restricted local user permissions, Email filtering, Disk-level encryption, Updated antivirus, Network segmentation, Plain text email format, VPN, IP blocklist, Backups
- Malware execution: Select control, Firewall file type filter, Honeypot, MFA, MAC filtering, Restricted local user permissions, Email filtering, Disk-level encryption, Updated antivirus, Network segmentation, Plain text email format, VPN, IP blocklist, Backups
- File encryption: Select control, Firewall file type filter, Honeypot, MFA, MAC filtering, Restricted local user permissions, Email filtering, Disk-level encryption, Updated antivirus, Network segmentation, Plain text email format, VPN, IP blocklist, Backups

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**



**NEW QUESTION 18**

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

**Answer: C**

**Explanation:**

Automation is the best concept to describe the example, as it reflects the use of technology to perform tasks or processes without human intervention. Automation can help to improve efficiency, accuracy, consistency, and scalability of various operations, such as identity and access management (IAM). IAM is a security framework that enables organizations to manage the identities and access rights of users and devices across different systems and applications. IAM can help to ensure that only authorized users and devices can access the appropriate resources at the appropriate time and for the appropriate purpose. IAM can involve various tasks or processes, such as authentication, authorization, provisioning, deprovisioning, auditing, or reporting. Automation can help to simplify and streamline these tasks or processes by using software tools or scripts that can execute predefined actions or workflows based on certain triggers or conditions. For example, automation can help to create, update, or delete user accounts in bulk based on a file or a database, rather than manually entering or modifying each account individually. The example in the question shows that an API is used to insert bulk access requests from a file into an identity management system. An API (Application Programming Interface) is a set of rules or specifications that defines how different software components or systems can communicate and exchange data with each other. An API can help to enable automation by providing a standardized and consistent way to access and manipulate data or functionality of a software component or system. The example in the question shows that an API is used to automate the process of inserting bulk access requests from a file into an identity management system, rather than manually entering each request one by one. The other options are not correct, as they describe different concepts or techniques. Command and control is a term that refers to the ability of an attacker to remotely control a compromised system or device, such as using malware or backdoors. Command and control is not related to what is described in the example. Data enrichment is a term that refers to the process of enhancing or augmenting existing data with additional information from external sources, such as adding demographic or behavioral attributes to customer profiles. Data enrichment is not related to what is described in the example. Single sign-on is a term that refers to an authentication method that allows users to access multiple systems or applications with one set of credentials, such as using a single username and password for different websites or services. Single sign-on is not related to what is described in the example.

**NEW QUESTION 19**

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

**Answer: D**

**Explanation:**

A lessons-learned review is a process of evaluating the effectiveness and efficiency of the incident response plan after an incident or an exercise. The purpose of the review is to identify the strengths and weaknesses of the incident response plan, and to update it accordingly to improve the future performance and resilience of the organization. Therefore, the incident response plan should be updated after a lessons-learned review. References: The answer was based on the NCSC CAF guidance from the National Cyber Security Centre, which states: "You should use post-incident and post-exercise reviews to actively reduce the risks associated with the same, or similar, incidents happening in future. Lessons learned can inform any aspect of your cyber security, including: System configuration Security monitoring and reporting Investigation procedures Containment/recovery strategies"

**NEW QUESTION 20**

An analyst discovers unusual outbound connections to an IP that was previously blocked at the web proxy and firewall. Upon further investigation, it appears that the proxy and firewall rules that were in place were removed by a service account that is not recognized. Which of the following parts of the Cyber Kill Chain does this describe?

- A. Delivery
- B. Command and control
- C. Reconnaissance
- D. Weaponization

**Answer: B**

**Explanation:**

The Command and Control stage of the Cyber Kill Chain describes the communication between the attacker and the compromised system. The attacker may use this channel to send commands, receive data, or update malware. If the analyst discovers unusual outbound connections to an IP that was previously blocked, it may indicate that the attacker has established a command and control channel and bypassed the security controls. References: Cyber Kill Chain® | Lockheed Martin

**NEW QUESTION 22**

An attacker recently gained unauthorized access to a financial institution's database, which contains confidential information. The attacker exfiltrated a large amount of data before being detected and blocked. A security analyst needs to complete a root cause analysis to determine how the attacker was able to gain access. Which of the following should the analyst perform first?

- A. Document the incident and any findings related to the attack for future reference.
- B. Interview employees responsible for managing the affected systems.
- C. Review the log files that record all events related to client applications and user access.
- D. Identify the immediate actions that need to be taken to contain the incident and minimize damage.

**Answer: C**

**Explanation:**

In a root cause analysis following unauthorized access, the initial step is usually to review relevant log files. These logs can provide critical information about how and when the attacker gained access.

The first step in a root cause analysis after a data breach is typically to review the logs. This helps the analyst understand how the attacker gained access by providing a detailed record of all events, including unauthorized or abnormal activities. Documenting the incident, interviewing employees, and identifying immediate containment actions are important steps, but they usually follow the initial log review.

**NEW QUESTION 27**

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

**Answer: C**

**NEW QUESTION 32**

**HOTSPOT**

The developers recently deployed new code to three web servers. A daffy automated external device scan report shows server vulnerabilities that are failure items according to PCI DSS.

If the vulnerability is not valid, the analyst must take the proper steps to get the scan clean. If the vulnerability is valid, the analyst must remediate the finding.

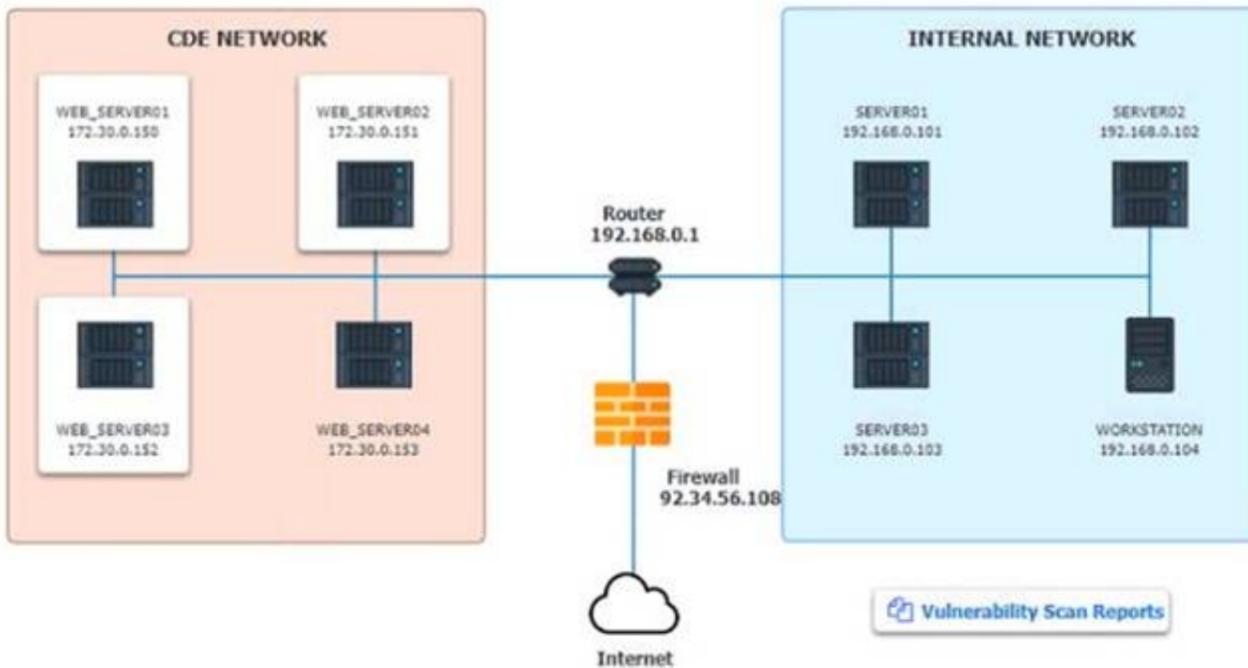
After reviewing the information provided in the network diagram, select the STEP 2 tab to

complete the simulation by selecting the correct Validation Result and Remediation Action for each server listed using the drop-down options.

**INSTRUCTIONS:**

The simulation includes 2 steps.

Step1:Review the information provided in the network diagram and then move to the STEP 2 tab.



### Vulnerability Scan Report

**HIGH SEVERITY**

**Title:** Cleartext Transmission of Sensitive Information

**Description:** The software transmits sensitive or securitycritical data in Cleartext in a communication channel that can be sniffed by authorized users.

**Affected Asset:** 172.30.0.15

**Risk:** Anyone can read the information by gaining access to the channel being used for communication.

**Reference:** CVE-2002-1949

**MEDIUM SEVERITY**

**Title:** Sensitive Cookie in HTTPS session without 'Secure' Attribute

**Description:** The Secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the use agent to send those cookies in plaintext over HTTP session.

**Affected Asset:** 172.30.0.152

**Risk:** Session Sidejacking

**Reference:** CVE-2004-0462

**LOW SEVERITY**

**Title:** Untrusted SSL/TLS Server X.509 Certificate

**Description:** The server's TLS/SSL certificate is signed by a Certification Authority that is untrusted or unknown.

**Affected Asset:** 172.30.0.153

**Risk:** May allow man-in-the-middle attackers to insert a spoofed certificate for any Distinguished Name (DN).

**Reference:** CVE-2005-1234

STEP 2: Given the Scenario, determine which remediation action is required to address the vulnerability.

**Network Diagram**

**INSTRUCTIONS**

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

| System       | Validate Result  | Remediation Action   |
|--------------|--|--|
| WEB_SERVER01 | <input type="text"/><br>False Positive<br>False Negative<br>True Positive<br>True Negative | <input type="text"/><br>Encrypt Entire Session<br>Encrypt All Session Cookies<br>Implement Input Validation<br>Submit as Non-Issue<br>Employ Unique Token in Hidden Field<br>Avoid Using Redirects and Forwards<br>Disable HTTP<br>Request Certificate from a Public CA<br>Renew the Current Certificate |
| WEB_SERVER02 | <input type="text"/><br>False Positive<br>False Negative<br>True Positive<br>True Negative | <input type="text"/><br>Encrypt Entire Session<br>Encrypt All Session Cookies<br>Implement Input Validation<br>Submit as Non-Issue<br>Employ Unique Token in Hidden Field<br>Avoid Using Redirects and Forwards<br>Disable HTTP<br>Request Certificate from a Public CA<br>Renew the Current Certificate |
| WEB_SERVER03 | <input type="text"/><br>False Positive<br>False Negative<br>True Positive<br>True Negative | <input type="text"/><br>Encrypt Entire Session<br>Encrypt All Session Cookies<br>Implement Input Validation<br>Submit as Non-Issue<br>Employ Unique Token in Hidden Field<br>Avoid Using Redirects and Forwards<br>Disable HTTP<br>Request Certificate from a Public CA<br>Renew the Current Certificate |

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**INSTRUCTIONS**

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

| System       | Validate Result | Remediation Action                   |
|--------------|-----------------|--------------------------------------|
| WEB_SERVER01 | True Positive   | Encrypt Entire Session               |
| WEB_SERVER02 | True Positive   | Encrypt All Session Cookies          |
| WEB_SERVER03 | True Positive   | Request Certificate from a Public CA |

**NEW QUESTION 37**

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 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.

**Answer:** C

**Explanation:**

The firewall certificate expired. If the firewall uses a certificate to authenticate and encrypt the feed, and the certificate expires, the feed will stop working until the certificate is renewed or replaced. This can affect the data enrichment process and the security analysis. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 161.

**NEW QUESTION 40**

A security manager is looking at a third-party vulnerability metric (SMITTEN) to improve upon the company's current method that relies on CVSSv3. Given the following:

**Vulnerability 1**

|   |
|---|
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N - Base Score: 7.5<br>High          |
| SMITTEN: Malware exploitable: No; Exploit Activity: Low; Exposed Externally: No |

**Vulnerability 2**

|  |
|--|
| CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N - Base Score: 5.4<br>Medium           |
| SMITTEN: Malware exploitable: Yes; Exploit Activity: HIGH; Exposed Externally: Yes |

**Vulnerability 3**

|   |
|---|
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H - Base Score: 9.8<br>Critical        |
| SMITTEN: Malware exploitable: No; Exploit Activity: None; Exposed Externally: Yes |

**Vulnerability 4**

|   |
|---|
| CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H - Base Score: 9.9<br>Critical          |
| SMITTEN: Malware exploitable: Yes; Exploit Activity: Medium; Exposed Externally: No |

Which of the following vulnerabilities should be prioritized?

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

**Answer:** B

**Explanation:**

Vulnerability 2 should be prioritized as it is exploitable, has high exploit activity, and is exposed externally according to the SMITTEN metric. References: Vulnerability Management Metrics: 5 Metrics to Start Measuring in Your Program, Section: Vulnerability Severity.

**NEW QUESTION 44**

Given the following CVSS string- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/3:U/C:K/I:K/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.

**Answer:** B

**Explanation:**

The vulnerability is network based is the correct attribute that describes this vulnerability, as it can be inferred from the CVSS string. CVSS stands for Common Vulnerability Scoring System, which is a framework that assigns numerical scores and ratings to vulnerabilities based on their characteristics and severity. The CVSS string consists of several metrics that define different aspects of the vulnerability, such as the attack vector, the attack complexity, the privileges required, the user interaction, the scope, and the impact on confidentiality, integrity and availability. The first metric in the CVSS string is the attack vector (AV), which indicates how the vulnerability can be exploited. The value of AV in this case is N, which stands for network. This means that the vulnerability can be exploited remotely over a network connection, without physical or logical access to the target system. Therefore, the vulnerability is network based. Official References:  
? <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>  
? <https://www.comptia.org/certifications/cybersecurity-analyst>  
? <https://packitforwarding.com/index.php/2019/01/10/comptia-cysa-common-vulnerability-scoring-system-cvss/>

**NEW QUESTION 46**

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.

**Answer:** A

**Explanation:**

Updating the system firmware and reimaging the hardware is the best action to perform to remediate the infected device, as it helps to ensure that the device is restored to a clean and secure state and that any traces of malware are removed. Firmware is a type of software that controls the low-level functions of a hardware device, such as a motherboard, hard drive, or network card. Firmware can be updated or flashed to fix bugs, improve performance, or enhance security. Reimaging is a process of erasing and restoring the data on a storage device, such as a hard drive or a solid state drive, using an image file that contains a copy of the operating system, applications, settings, and files. Reimaging can help to recover from system failures, data corruption, or malware infections. Updating the system firmware and reimaging the hardware can help to remediate the infected device by removing any malicious code or configuration changes that may have been made by the malware, as well as restoring any missing or damaged files or settings that may have been affected by the malware. This can help to prevent further damage, data loss, or compromise of the device or the network. The other actions are not as effective or appropriate as updating the system firmware and reimaging the hardware, as they do not address the root cause of the infection or ensure that the device is fully cleaned and secured. Installing an additional malware scanner that will send email alerts to the analyst may help to detect and remove some types of malware, but it may not be able to catch all malware variants or remove them completely. It may also create conflicts or performance issues with other security tools or systems on the device. Configuring the system to use a proxy server for Internet access may help to filter or monitor some types of malicious traffic or requests, but it may not prevent or remove malware that has already infected the device or that uses other methods of communication or propagation. Deleting the user profile and restoring data from backup may help to recover some data or settings that may have been affected by the malware, but it may not remove malware that has infected other parts of the system or that has persisted on the device.

**NEW QUESTION 51**

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.

**Answer:** D

**Explanation:**

The MITRE ATT&CK framework is a knowledge base of cybercriminals' adversarial behaviors based on cybercriminals' known tactics, techniques and procedures (TTPs). It helps security teams model, detect, prevent and fight cybersecurity threats by simulating cyberattacks, creating security policies, controls and incident response plans, and sharing information with other security professionals. It is an open-source project that evolves with input from a global community of cybersecurity professionals<sup>1</sup>. References: What is the MITRE ATT&CK Framework? | IBM

**NEW QUESTION 55**

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

**Answer: C**

**Explanation:**

SOAR stands for Security Orchestration, Automation and Response, which is a set of features that can help security teams manage, prioritize and respond to security incidents more efficiently and effectively. SOAR can help decrease the workload without increasing staff by automating repetitive tasks, streamlining workflows, integrating different tools and platforms, and providing actionable insights and recommendations. SOAR is also one of the current trends that CompTIA CySA+ covers in its exam objectives. Official References:

? <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>

? <https://www.comptia.org/certifications/cybersecurity-analyst>

? <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>

**NEW QUESTION 58**

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

**Answer: D**

**Explanation:**

Under the terms of PCI DSS, an organization that has experienced a breach of customer transactions should report the breach to the card issuer. The card issuer is the financial institution that issues the payment cards to the customers and that is responsible for authorizing and processing the transactions. The card issuer may have specific reporting requirements and procedures for the organization to follow in the event of a breach. The organization should also notify other parties that may be affected by the breach, such as customers, law enforcement, or regulators, depending on the nature and scope of the breach. Official References: <https://www.pcisecuritystandards.org/>

**NEW QUESTION 62**

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

**Answer: A**

**Explanation:**

Geoblocking is the best mitigation technique for unusual network scanning activity coming from a country that the company does not do business with, as it can prevent any potential attacks or data breaches from that country. Geoblocking is the practice of restricting access to websites or services based on geographic location, usually by blocking IP addresses associated with a certain country or region. Geoblocking can help reduce the overall attack surface and protect against malicious actors who may be trying to exploit vulnerabilities or steal information. The other options are not as effective as geoblocking, as they may not block all the possible sources of the scanning activity, or they may not address the root cause of the problem. Official References:

? <https://www.blumira.com/geoblocking/>

? <https://www.avg.com/en/signal/geo-blocking>

**NEW QUESTION 65**

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

**Answer: D**

**Explanation:**

Deduplication is a process that involves removing any duplicate or redundant data or information from a data set or source. Deduplication can help consolidate several threat intelligence feeds by eliminating any overlapping or repeated indicators of compromise (IoCs), alerts, reports, or recommendations. Deduplication can also help reduce the volume and complexity of threat intelligence data, as well as improve its quality, accuracy, or relevance.

**NEW QUESTION 69**

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

**Answer:** A

**Explanation:**

SLA (Service Level Agreement) is the best term to describe the document that defines the expectation to network customers that patching will only occur between 2:00 a.m. and 4:00 a.m., as it reflects the agreement between a service provider and a customer that specifies the services, quality, availability, and responsibilities that are agreed upon. An SLA is a common type of document that is used in various industries and contexts, such as IT, telecom, cloud computing, or outsourcing. An SLA typically includes metrics and indicators to measure the performance and quality of the service, such as uptime, response time, or resolution time. An SLA also defines the consequences or remedies for any breaches or failures of the service, such as penalties, refunds, or credits. An SLA can help to manage customer expectations, formalize communication, improve productivity, and strengthen relationships. The other terms are not as accurate as SLA, as they describe different types of documents or concepts. LOI (Letter of Intent) is a document that outlines the main terms and conditions of a proposed agreement between two or more parties, before a formal contract is signed. An LOI is usually non-binding and expresses the intention or interest of the parties to enter into a future agreement. An LOI can help to clarify the key points of a deal, facilitate negotiations, or demonstrate commitment. MOU (Memorandum of Understanding) is a document that describes a mutual agreement or cooperation between two or more parties, without creating any legal obligations or commitments. An MOU is usually more formal than an LOI, but less formal than a contract. An MOU can help to establish a common ground, define roles and responsibilities, or outline expectations and goals. KPI (Key Performance Indicator) is a concept that refers to a measurable value that demonstrates how effectively an organization or individual is achieving its key objectives or goals. A KPI is usually quantifiable and specific, such as revenue growth, customer satisfaction, or employee retention. A KPI can help to track progress, evaluate performance, or identify areas for improvement.

**NEW QUESTION 73**

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.

**Answer:** C

**Explanation:**

Rolling out a CDN is the best control to mitigate the Layer 4 DDoS attacks against the company website. A CDN is a Content Delivery Network, which is a system of distributed servers that deliver web content to users based on their geographic location, the origin of the web page, and the content delivery server. A CDN can help protect against Layer 4 DDoS attacks, which are volumetric attacks that aim to exhaust the network bandwidth or resources of the target website by sending a large amount of traffic, such as SYN floods, UDP floods, or ICMP floods. A CDN can mitigate these attacks by distributing the traffic across multiple servers, caching the web content closer to the users, filtering out malicious or unwanted traffic, and providing scalability and redundancy for the website<sup>12</sup>. References: How to Stop a DDoS Attack: Mitigation Steps for Each OSI Layer, Application layer DDoS attack | Cloudflare

**NEW QUESTION 78**

A SOC analyst is analyzing traffic on a network and notices an unauthorized scan. Which of the following types of activities is being observed?

- A. Potential precursor to an attack
- B. Unauthorized peer-to-peer communication
- C. Rogue device on the network
- D. System updates

**Answer:** A

**NEW QUESTION 81**

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

**Answer:** A

**Explanation:**

An SLA (Service Level Agreement) is a contract or agreement between a service provider and a customer that defines the expected level of service, performance, quality, and availability of the service. An SLA also specifies the responsibilities, obligations, and penalties for both parties in case of non-compliance or breach of the agreement. An SLA can help organizations to ensure that their security services are delivered in a timely and effective manner, and that any security incidents or vulnerabilities are addressed and resolved within a specified time frame. An SLA can also help to establish clear communication, expectations, and accountability between the service provider and the customer<sup>12</sup>

An MOU (Memorandum of Understanding) is a document that expresses a mutual agreement or understanding between two or more parties on a common goal or objective. An MOU is not legally binding, but it can serve as a basis for future cooperation or collaboration. An MOU may not be suitable for requiring remediation of a known threat within a given time frame, as it does not have the same level of enforceability, specificity, or measurability as an SLA.

Best-effort patching is an informal and ad hoc approach to applying security patches or updates to systems or software. Best-effort patching does not follow any defined process, policy, or schedule, and relies on the availability and discretion of the system administrators or users. Best-effort patching may not be effective or efficient for requiring remediation of a known threat within a given time frame, as it does not guarantee that the patches are applied correctly, consistently, or promptly. Best-effort patching may also introduce new risks or vulnerabilities due to human error, compatibility issues, or lack of testing. Organizational governance is the framework of rules, policies, procedures, and processes that guide and direct the activities and decisions of an organization. Organizational governance can help to establish the roles, responsibilities, and accountabilities of different stakeholders within the organization, as well as the goals, values, and principles that shape the organizational culture and behavior. Organizational governance can also help to ensure compliance with internal and external standards, regulations, and laws. Organizational governance may not be sufficient for requiring remediation of a known threat within a given time frame, as it does not specify the details or metrics of the service delivery or performance. Organizational governance may also vary depending on the size, structure, and nature of the organization.

#### NEW QUESTION 82

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

**Answer:** B

#### Explanation:

Single Sign-On (SSO) allows users to log in with a single ID and password to access multiple applications. It eliminates the need for different passwords for various internal applications, streamlining the authentication process.

#### NEW QUESTION 85

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/

**Answer:** A

#### Explanation:

/etc/shadow is the pattern that the security analyst can use to search the web server logs for evidence of exploitation of the LFI vulnerability that can be exploited to extract credentials from the underlying host. LFI stands for Local File Inclusion, which is a vulnerability that allows an attacker to include local files on the web server into the output of a web application. LFI can be exploited to extract sensitive information from the web server, such as configuration files, passwords, or source code. The /etc/shadow file is a file that stores the encrypted passwords of all users on a Linux system. If an attacker can exploit the LFI vulnerability to include this file into the web application output, they can obtain the credentials of the users on the web server. Therefore, the security analyst can look for /etc/shadow in the request line of the web server logs to see if any attacker has attempted or succeeded in exploiting the LFI vulnerability. Official References:  
? <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>  
? <https://www.comptia.org/certifications/cybersecurity-analyst>  
? <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>

#### NEW QUESTION 89

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? (Select two).

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

**Answer:** AB

#### Explanation:

A signal-shielded bag and a tamper-evident seal are tools that can be used to maintain the integrity of the mobile phone while it is transported. A signal-shielded bag prevents the phone from receiving or sending any signals that could compromise the data or evidence on the device. A tamper-evident seal ensures that the phone has not been opened or altered during the transportation. References: Mobile device forensics, Section: Acquisition

#### NEW QUESTION 92

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

**Answer:** B

#### Explanation:

A risk score is a numerical value that represents the potential impact and likelihood of a vulnerability being exploited. It can help to identify the potential loss incurred by an issue and prioritize remediation efforts accordingly. <https://www.comptia.org/training/books/cysa-cs0-003-study-guide>

#### NEW QUESTION 93

An analyst is evaluating the following vulnerability report:

**Vulnerability:**

Vulnerability Name: Remote Code Execution  
Group: Information Disclosure  
OWASP: A9 Using Components with Known Vulnerabilities

**Metrics:**

CVE Dictionary Entry: CVE-2022-9999  
Base Score: 9.3  
CVSS:3.1 /AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

**Profile:**

Authentication: Not used  
Times detected: View history  
Aggressiveness: High

**Payloads:**

[Click here for Request Payload](#)  
[Click here for Response Payload](#)

Which of the following vulnerability report sections provides information about the level of impact on data confidentiality if a successful exploitation occurs?

- A. Payloads
- B. Metrics
- C. Vulnerability
- D. Profile

**Answer:** B

**Explanation:**

The correct answer is B. Metrics.

The Metrics section of the vulnerability report provides information about the level of impact on data confidentiality if a successful exploitation occurs. The Metrics section contains the CVE dictionary entry and the CVSS base score of the vulnerability. CVE stands for Common Vulnerabilities and Exposures and it is a standardized system for identifying and naming vulnerabilities. CVSS stands for Common Vulnerability Scoring System and it is a standardized system for measuring and rating the severity of vulnerabilities.

The CVSS base score is a numerical value between 0 and 10 that reflects the intrinsic characteristics of a vulnerability, such as its exploitability, impact, and scope. The CVSS base score is composed of three metric groups: Base, Temporal, and Environmental. The Base metric group captures the characteristics of a vulnerability that are constant over time and across user environments. The Base metric group consists of six metrics: Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, and Impact. The Impact metric measures the effect of a vulnerability on the confidentiality, integrity, and availability of the affected resources.

In this case, the CVSS base score of the vulnerability is 9.8, which indicates a critical severity level. The Impact metric of the CVSS base score is 6.0, which indicates a high impact on confidentiality, integrity, and availability. Therefore, the Metrics section provides information about the level of impact on data confidentiality if a successful exploitation occurs.

The other sections of the vulnerability report do not provide information about the level of impact on data confidentiality if a successful exploitation occurs. The Payloads section contains links to request and response payloads that demonstrate how the vulnerability can be exploited. The Payloads section can help an analyst to understand how the attack works, but it does not provide a quantitative measure of the impact. The Vulnerability section contains information about the type, group, and description of the vulnerability. The Vulnerability section can help an analyst to identify and classify the vulnerability, but it does not provide a numerical value of the impact. The Profile section contains information about the authentication, times viewed, and aggressiveness of the vulnerability. The Profile section can help an analyst to assess the risk and priority of the vulnerability, but it does not provide a specific measure of the impact on data confidentiality.

References:

- ? [1] CVE - Common Vulnerabilities and Exposures (CVE)
- ? [2] Common Vulnerability Scoring System SIG
- ? [3] CVSS v3.1 Specification Document
- ? [4] CVSS v3.1 User Guide
- ? [5] How to Read a Vulnerability Report - Security Boulevard

**NEW QUESTION 95**

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

**Answer:** C

**Explanation:**

After detecting a compromised email server and unusual network traffic, the next step in incident response is containment, to prevent further damage or spread of the compromise. References: ompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5: Incident Response, page 197.

**NEW QUESTION 98**

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

**Answer: C**

**Explanation:**

The OWASP Web Security Testing Guide (WSTG) includes a section on threat modeling, which is a structured approach to identify, quantify, and address the security risks associated with an application. The first step in the threat modeling process is decomposing the application, which involves creating use cases, identifying entry points, assets, trust levels, and data flow diagrams for the application. This helps to understand the application and how it interacts with external entities, as well as to identify potential threats and vulnerabilities<sup>1</sup>. The other options are not part of the OWASP WSTG threat modeling process.

**NEW QUESTION 101**

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.

**Answer: B**

**Explanation:**

The correct answer is B. Replace the current MD5 with SHA-256.

The vulnerability that the security analyst is able to exploit is a hash collision, which is a situation where two different files produce the same hash value. Hash collisions can allow an attacker to bypass the integrity or authentication checks that rely on hash values, and submit malicious files to the system. The web application uses MD5, which is a hashing algorithm that is known to be vulnerable to hash collisions. Therefore, the analyst should suggest replacing the current MD5 with SHA-256, which is a more secure and collision-resistant hashing algorithm.

The other options are not the best suggestions to mitigate the vulnerability with the fewest changes to the current script and infrastructure. Deploying a WAF (web application firewall) to the front of the application (A) may help protect the web application from some common attacks, but it may not prevent hash collisions or detect malicious files. Deploying an antivirus application on the hosting system (C) may help scan and remove malicious files from the system, but it may not prevent hash collisions or block malicious files from being submitted. Replacing the MD5 with digital signatures (D) may help verify the authenticity and integrity of the files, but it may require significant changes to the current script and infrastructure, as digital signatures involve public-key cryptography and certificate authorities.

**NEW QUESTION 102**

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

**Answer: A**

**Explanation:**

An information sharing organization is a group or network of organizations that share threat intelligence, best practices, or lessons learned related to cybersecurity issues or incidents. An information sharing organization can help security analysts learn about new ransomware campaigns or other emerging threats, as well as get recommendations or guidance on how to prevent, detect, or respond to them. An information sharing organization can also help security analysts collaborate or coordinate with other organizations in the same industry or region that may face similar threats or challenges.

**NEW QUESTION 105**

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

**Answer: B**

**Explanation:**

A vulnerability that is related to a specific adversary campaign, with IoCs found in the SIEM, should have the highest priority for the mitigation process. This is because it indicates that the vulnerability is actively being exploited by a known threat actor, and that the organization's security monitoring system has detected signs of compromise. This poses a high risk of data breach, service disruption, or other adverse impacts. References: How to Prioritize Vulnerabilities Effectively: Vulnerability Prioritization Explained, Section: How to prioritize vulnerabilities step by step to avoid drowning in sea of problems; CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156.

**NEW QUESTION 106**

A security analyst is reviewing events that occurred during a possible compromise. The analyst obtains the following log:

| Time stamp | Message  |
|------------|--|
| 20:06:05   | LDAP: A read operation was performed on an object: Domain Admins       |
| 20:06:05   | LDAP: A read operation was performed on an object: Domain Servers      |
| 20:06:09   | EDR: A local group was enumerated: Administrators                      |
| 20:06:23   | EDR: SMB connection attempts to multiple hosts from single host: PC021 |

Which of the following is most likely occurring, based on the events in the log?

- A. An adversary is attempting to find the shortest path of compromise.
- B. An adversary is performing a vulnerability scan.
- C. An adversary is escalating privileges.
- D. An adversary is performing a password stuffing attack..

**Answer: B**

**Explanation:**

Based on the events in the log, the most likely occurrence is that an adversary is performing a vulnerability scan. The log shows LDAP read operations and EDR enumerating local groups, which are indicative of an adversary scanning the system to find vulnerabilities or sensitive information. The final entry shows SMB connection attempts to multiple hosts from a single host, which could be a sign of network discovery or lateral movement. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 161; Monitor logs from vulnerability scanners, Section: Reports on Nessus vulnerability data.

**NEW QUESTION 107**

While a security analyst for an organization was reviewing logs from web servers. the analyst found several successful attempts to downgrade HTTPS sessions to use cipher modes of operation susceptible to padding oracle attacks. Which of the following combinations of configuration changes should the organization make to remediate this issue? (Select two).

- A. Configure the server to prefer TLS 1.3.
- B. Remove cipher suites that use CBC.
- C. Configure the server to prefer ephemeral modes for key exchange.
- D. Require client browsers to present a user certificate for mutual authentication.
- E. Configure the server to require HSTS.
- F. Remove cipher suites that use GCM.

**Answer: AB**

**Explanation:**

The correct answer is A. Configure the server to prefer TLS 1.3 and B. Remove cipher suites that use CBC.

A padding oracle attack is a type of attack that exploits the padding validation of a cryptographic message to decrypt the ciphertext without knowing the key. A padding oracle is a system that responds to queries about whether a message has a valid padding or not, such as a web server that returns different error messages for invalid padding or invalid MAC. A padding oracle attack can be applied to the CBC mode of operation, where the attacker can manipulate the ciphertext blocks and use the oracle's responses to recover the plaintext<sup>12</sup>.

To remediate this issue, the organization should make the following configuration changes:

? Configure the server to prefer TLS 1.3. TLS 1.3 is the latest version of the Transport Layer Security protocol, which provides secure communication between clients and servers. TLS 1.3 has several security improvements over previous versions, such as:

? Remove cipher suites that use CBC. Cipher suites are combinations of cryptographic algorithms that specify how TLS connections are secured. Cipher suites that use CBC mode are vulnerable to padding oracle attacks, as well as other attacks such as BEAST and Lucky 13. Therefore, they should be removed from the server's configuration and replaced with cipher suites that use more secure modes of operation, such as GCM or CCM78.

The other options are not effective or necessary to remediate this issue.

Option C is not effective because configuring the server to prefer ephemeral modes for key exchange does not prevent padding oracle attacks. Ephemeral modes for key exchange are methods that generate temporary and random keys for each session, such as Diffie- Hellman or Elliptic Curve Diffie-Hellman. Ephemeral modes provide forward secrecy, which means that compromising the long-term keys does not affect the security of past sessions. However, ephemeral modes do not protect against padding oracle attacks, which exploit the padding validation of the ciphertext rather than the key exchange<sup>9</sup>.

Option D is not necessary because requiring client browsers to present a user certificate for mutual authentication does not prevent padding oracle attacks. Mutual authentication is a process that verifies the identity of both parties in a communication, such as using certificates or passwords. Mutual authentication enhances security by preventing impersonation or spoofing attacks. However, mutual authentication does not protect against padding oracle attacks, which exploit the padding validation of the ciphertext rather than the authentication.

Option E is not necessary because configuring the server to require HSTS does not prevent padding oracle attacks. HSTS stands for HTTP Strict Transport Security and it is a mechanism that forces browsers to use HTTPS connections instead of HTTP connections when communicating with a web server. HSTS enhances security by preventing downgrade or man-in-the-middle attacks that try to intercept or modify HTTP traffic. However, HSTS does not protect against padding oracle attacks, which exploit the padding validation of HTTPS traffic rather than the protocol.

Option F is not effective because removing cipher suites that use GCM does not prevent padding oracle attacks. GCM stands for Galois/Counter Mode and it is a mode of operation that provides both encryption and authentication for block ciphers, such as AES. GCM is more secure and efficient than CBC mode, as it prevents various types of attacks, such as padding oracle, BEAST, Lucky 13, and IV reuse attacks. Therefore, removing cipher suites that use GCM would reduce security rather than enhance it .

References:

- ? 1 Padding oracle attack - Wikipedia
- ? 2 flast101/padding-oracle-attack-explained - GitHub
- ? 3 A Cryptographic Analysis of the TLS 1.3 Handshake Protocol | Journal of Cryptology
- ? 4 Which block cipher mode of operation does TLS 1.3 use? - Cryptography Stack Exchange
- ? 5 The Essentials of Using an Ephemeral Key Under TLS 1.3
- ? 6 Guidelines for the Selection, Configuration, and Use of ... - NIST
- ? 7 CBC decryption vulnerability - .NET | Microsoft Learn
- ? 8 The Padding Oracle Attack | Robert Heaton

- ? 9 What is Ephemeral Diffie-Hellman? | Cloudflare
- ? [10] What is Mutual TLS? How mTLS Authentication Works | Cloudflare
- ? [11] What is HSTS? HTTP Strict Transport Security Explained | Cloudflare
- ? [12] Galois/Counter Mode - Wikipedia
- ? [13] AES-GCM and its IV/nonce value - Cryptography Stack Exchange

**NEW QUESTION 110**

A cloud team received an alert that unauthorized resources were being auto-provisioned. After investigating, the team suspects that crypto mining 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

**Answer:** A

**Explanation:**

High GPU utilization is the most likely indicator that cryptomining is occurring, as it reflects the intensive computational work that is required to solve the complex mathematical problems involved in mining cryptocurrencies. Cryptomining is the process of generating new units of a cryptocurrency by using computing power to verify transactions and create new blocks on the blockchain. Cryptomining can be done legitimately by individuals or groups who participate in a mining pool and share the rewards, or illegitimately by threat actors who use malware or scripts to hijack the computing resources of unsuspecting victims and use them for their own benefit. This practice is called cryptojacking, and it can cause performance degradation, increased power consumption, and security risks for the affected systems. Cryptomining typically relies on the GPU (graphics processing unit) rather than the CPU (central processing unit), as the GPU is better suited for parallel processing and can handle more calculations per second. Therefore, a high GPU utilization rate can be a sign that cryptomining is taking place on a system, especially if there is no other explanation for the increased workload. The other options are not as indicative of cryptomining as high GPU utilization, as they can have other causes or explanations. Bandwidth consumption can be affected by many factors, such as network traffic, streaming services, downloads, or updates. It is not directly related to cryptomining, which does not require a lot of bandwidth to communicate with the mining pool or the blockchain network. Unauthorized changes can be a result of many types of malware or cyberattacks, such as ransomware, spyware, or trojans. They are not specific to cryptomining, which does not necessarily alter any files or settings on the system, but rather uses its processing power. Unusual traffic spikes can also be caused by various factors, such as legitimate surges in demand, distributed denial-of-service attacks, or botnets. They are not indicative of cryptomining, which does not generate a lot of traffic or requests to or from the system.

**NEW QUESTION 112**

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.

**Answer:** B

**Explanation:**

An incident response plan is a set of predefined procedures and guidelines that an organization follows when faced with a security breach or attack. An incident response plan helps to ensure that the organization can quickly and effectively contain, analyze, eradicate, and recover from the incident, as well as prevent or minimize the damage and impact to the business operations, reputation, and customers. An incident response plan also defines the roles and responsibilities of the incident response team, the communication channels and protocols, the escalation and reporting procedures, and the tools and resources available for the incident response.

By following the company's incident response plan, the administrator can ensure that they are following the best practices and standards for handling a security incident, and that they are coordinating and collaborating with the relevant stakeholders and authorities. Following the company's incident response plan can also help to avoid or reduce any legal, regulatory, or contractual liabilities or penalties that may arise from the incident.

The other options are not as effective or appropriate as following the company's incident response plan. Informing the internal incident response team (A) is a good step, but it should be done according to the company's incident response plan, which may specify who, when, how, and what to report. Reviewing the lessons learned for the best approach (C) is a good step, but it should be done after the incident has been resolved and closed, not during the active response phase. Determining when the access started (D) is a good step, but it should be done as part of the analysis phase of the incident response plan, not before following the plan.

**NEW QUESTION 113**

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

**Answer:** C

**Explanation:**

Performing input validation before allowing submission is the best recommendation for remediation of this application vulnerability. Input validation is a technique that checks the data entered by users or attackers against a set of rules or constraints, such as data type, length, format, or range. Input validation can prevent common web application attacks such as SQL injection, cross-site scripting (XSS), or command injection, which exploit the lack of input validation to execute malicious code or commands on the server or the client side. By validating the input before allowing submission, the web application can reject or sanitize any malicious or unexpected input, and protect the user credentials and other sensitive data from being compromised. References: Input Validation - OWASP, 4 Most Common Application Vulnerabilities and Possible Remediation

**NEW QUESTION 116**

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

**Answer: B**

**Explanation:**

Cloud-specific misconfigurations are security issues that arise from improper or inadequate configuration of cloud resources, such as storage buckets, databases, virtual machines, or containers. Cloud-specific misconfigurations may not be detected by the current scanners that are designed for on-premises environments, as they may not have the visibility or access to the cloud resources or the cloud provider's APIs. Therefore, one of the implications that should be considered on the new hybrid environment is that cloud- specific misconfigurations may not be detected by the current scanners.

**NEW QUESTION 117**

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

**Answer: B**

**Explanation:**

Vulnerability B is the vulnerability that the analyst should be most concerned about, knowing that end users frequently click on malicious links sent via email. Vulnerability B is a remote code execution vulnerability in Microsoft Outlook that allows an attacker to run arbitrary code on the target system by sending a specially crafted email message. This vulnerability is very dangerous, as it does not require any user interaction or attachment opening to trigger the exploit. The attacker only needs to send an email to the victim's Outlook account, and the code will execute automatically when Outlook connects to the Exchange server. This vulnerability has a high severity rating of 9.8 out of 10, and it affects all supported versions of Outlook. Therefore, the analyst should prioritize patching this vulnerability as soon as possible to prevent potential compromise of the workstations.

**NEW QUESTION 118**

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

**Answer: D**

**Explanation:**

The observed activity from a privileged account indicates an insider attack, which is when a trusted user or employee misuses their access rights to compromise the security of the organization. Accessing emails and sensitive information, modifying audit logs, and logging in at abnormal times are all signs of malicious behavior by a privileged user who may be trying to steal, tamper, or destroy data, or cover their tracks. An insider attack can cause significant damage to the organization's reputation, operations, and compliance. References: The Privileged Identity Playbook Guides Management of Privileged User Accounts, How to Track Privileged Users' Activities in Active Directory

**NEW QUESTION 121**

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

**Answer: B**

**Explanation:**

The first thing that must be done when starting an investigation is to secure the scene. Securing the scene involves isolating and protecting the area where the incident occurred, as well as any potential evidence or witnesses. Securing the scene can help prevent any tampering, contamination, or destruction of evidence, as well as any interference or obstruction of the investigation.

#### NEW QUESTION 123

An organization discovered a data breach that resulted in PII being released to the public. During the lessons learned review, the panel identified discrepancies regarding who was responsible for external reporting, as well as the timing requirements. Which of the following actions would best address the reporting issue?

- A. Creating a playbook denoting specific SLAs and containment actions per incident type
- B. Researching federal laws, regulatory compliance requirements, and organizational policies to document specific reporting SLAs
- C. Defining which security incidents require external notifications and incident reporting in addition to internal stakeholders
- D. Designating specific roles and responsibilities within the security team and stakeholders to streamline tasks

**Answer: B**

#### Explanation:

Researching federal laws, regulatory compliance requirements, and organizational policies to document specific reporting SLAs is the best action to address the reporting issue. Reporting SLAs are service level agreements that specify the time frame and the format for notifying the relevant authorities and the affected individuals of a data breach. Reporting SLAs may vary depending on the type and severity of the breach, the type and location of the data, the industry and jurisdiction of the organization, and the internal policies of the organization. By researching and documenting the reporting SLAs for different scenarios, the organization can ensure that it complies with the legal and ethical obligations of data breach notification, and avoid any penalties, fines, or lawsuits that may result from failing to report a breach in a timely and appropriate manner<sup>12</sup>. References: When and how to report a breach: Data breach reporting best practices, Incident and Breach Management

#### NEW QUESTION 128

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

**Answer: D**

#### Explanation:

EDR stands for Endpoint Detection and Response, which is a layer of defense that monitors endpoints for malicious activity and provides automated or manual response capabilities. EDR can protect against external threats regardless of the device's operating system, as it can detect and respond to attacks based on behavioral analysis and threat intelligence. EDR is also one of the tools that CompTIA CySA+ covers in its exam objectives. Official References:  
? <https://www.comptia.org/certifications/cybersecurity-analyst>  
? <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>  
? <https://resources.infosecinstitute.com/certification/cysa-plus-ia-levels/>

#### NEW QUESTION 132

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

**Answer: A**

#### Explanation:

The most likely explanation for this traffic pattern is C2 beaconing activity. C2 stands for command and control, which is a phase of the Cyber Kill Chain that involves the adversary attempting to establish communication with a successfully exploited target. C2 beaconing activity is a type of network traffic that indicates a compromised system is sending periodic messages or signals to an attacker's system using various protocols, such as HTTP(S), DNS, ICMP, or UDP. C2 beaconing activity can enable the attacker to remotely control or manipulate the target system or network using various methods, such as malware callbacks, backdoors, botnets, or covert channels.

#### NEW QUESTION 137

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

**Answer: B**

#### Explanation:

Compensating controls are alternative controls that provide a similar level of protection as the original controls, but are used when the original controls are not feasible or cost-effective. In this case, the CISO implemented compensating controls by reviewing logs and audit trails to mitigate the risk of error and fraud in payroll management, since segregating duties was not possible due to the small staff size

#### NEW QUESTION 142

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.

**Answer:** D

#### **Explanation:**

Searching for other mail users who have received the same file is the best activity to perform next, as it helps to identify and contain the scope of the ransomware attack and prevent further damage. Ransomware is a type of malware that encrypts files on a system and demands payment for their decryption. Ransomware can spread through phishing emails that contain malicious attachments or links that download the ransomware. By searching for other mail users who have received the same file, the analyst can alert them not to open it, delete it from their inboxes, and scan their systems for any signs of infection. The other activities are not as urgent or effective as searching for other mail users who have received the same file, as they do not address the immediate threat of ransomware spreading or affecting more systems. Wiping the computer and reinstalling software may restore the functionality of the affected workstation, but it will also erase any evidence of the ransomware attack and make recovery of encrypted files impossible. Shutting down the email server and quarantining it from the network may stop the delivery of more phishing emails, but it will also disrupt normal communication and operations for the organization. Acquiring a bit-level image of the affected workstation may preserve the evidence of the ransomware attack, but it will not help to stop or remove the ransomware or decrypt the files.

#### NEW QUESTION 145

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CS0-003 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CS0-003 Product From:

<https://www.2passeasy.com/dumps/CS0-003/>

## Money Back Guarantee

### CS0-003 Practice Exam Features:

- \* CS0-003 Questions and Answers Updated Frequently
- \* CS0-003 Practice Questions Verified by Expert Senior Certified Staff
- \* CS0-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* CS0-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year