

## Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam

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



#### NEW QUESTION 1

Several critical bugs were identified during a vulnerability scan. The SLA risk requirement is that all critical vulnerabilities should be patched within 24 hours. After sending a notification to the asset owners, the patch cannot be deployed due to planned, routine system upgrades. Which of the following is the best method to remediate the bugs?

- A. Reschedule the upgrade and deploy the patch
- B. Request an exception to exclude the patch from installation
- C. Update the risk register and request a change to the SLA
- D. Notify the incident response team and rerun the vulnerability scan

**Answer: C**

#### Explanation:

When a patch cannot be deployed due to conflicting routine system upgrades, updating the risk register and requesting a change to the Service Level Agreement (SLA) is a practical approach. It allows for re-evaluation of the risk and adjustment of the SLA to reflect the current situation.

#### NEW QUESTION 2

A company is in the process of implementing a vulnerability management program. Which of the following scanning methods should be implemented to minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process?

- A. Non-credentialed scanning
- B. Passive scanning
- C. Agent-based scanning
- D. Credentialed scanning

**Answer: B**

#### Explanation:

Passive scanning is a method of vulnerability identification that does not send any packets or probes to the target devices, but rather observes and analyzes the network traffic passively. Passive scanning can minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process, as it does not interfere with the normal operation of the devices or cause any network disruption. Passive scanning can also detect vulnerabilities that active scanning may miss, such as misconfigured devices, rogue devices or unauthorized traffic. Official References:

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

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

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

#### NEW QUESTION 3

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 4

Which of the following best describes the importance of implementing TAXII as part of a threat intelligence program?

- A. It provides a structured way to gain information about insider threats.
- B. It proactively facilitates real-time information sharing between the public and private sectors.
- C. It exchanges messages in the most cost-effective way and requires little maintenance once implemented.

D. It is a semi-automated solution to gather threat intelligence about competitors in the same sector.

**Answer:** B

**Explanation:**

The correct answer is B. It proactively facilitates real-time information sharing between the public and private sectors. TAXII, or Trusted Automated eXchange of Intelligence Information, is a standard protocol for sharing cyber threat intelligence in a standardized, automated, and secure manner. TAXII defines how cyber threat information can be shared via services and message exchanges, such as discovery, collection management, inbox, and poll. TAXII is designed to support STIX, or Structured Threat Information eXpression, which is a standardized language for describing cyber threat information in a readable and consistent format. Together, STIX and TAXII form a framework for sharing and using threat intelligence, creating an open-source platform that allows users to search through records containing attack vectors details such as malicious IP addresses, malware signatures, and threat actors<sup>123</sup>. The importance of implementing TAXII as part of a threat intelligence program is that it proactively facilitates real-time information sharing between the public and private sectors. By using TAXII, organizations can exchange cyber threat information with various entities, such as security vendors, government agencies, industry associations, or trusted groups. TAXII enables different sharing models, such as hub and spoke, source/subscriber, or peer-to-peer, depending on the needs and preferences of the information producers and consumers. TAXII also supports different levels of access control, encryption, and authentication to ensure the security and privacy of the shared information<sup>123</sup>. By implementing TAXII as part of a threat intelligence program, organizations can benefit from the following advantages:

- ? They can receive timely and relevant information about the latest threats and vulnerabilities that may affect their systems or networks.
- ? They can leverage the collective knowledge and experience of other organizations that have faced similar or related threats.
- ? They can improve their situational awareness and threat detection capabilities by correlating and analyzing the shared information.
- ? They can enhance their incident response and mitigation strategies by applying the best practices and recommendations from the shared information.
- ? They can contribute to the overall improvement of cyber security by sharing their own insights and feedback with other organizations<sup>123</sup>.

The other options are incorrect because they do not accurately describe the importance of implementing TAXII as part of a threat intelligence program. Option A is incorrect because TAXII does not provide a structured way to gain information about insider threats. Insider threats are malicious activities conducted by authorized users within an organization, such as employees, contractors, or partners. Insider threats can be detected by using various methods, such as user behavior analysis, data loss prevention, or anomaly detection. However, TAXII is not designed to collect or share information about insider threats specifically. TAXII is more focused on external threats that originate from outside sources, such as hackers, cybercriminals, or nation-states<sup>4</sup>. Option C is incorrect because TAXII does not exchange messages in the most cost- effective way and requires little maintenance once implemented. TAXII is a protocol that defines how messages are exchanged, but it does not specify the cost or maintenance of the exchange. The cost and maintenance of implementing TAXII depend on various factors, such as the type and number of services used, the volume and frequency of data exchanged, the security and reliability requirements of the exchange, and the availability and compatibility of existing tools and platforms. Implementing TAXII may require significant resources and efforts from both the information producers and consumers to ensure its functionality and performance<sup>5</sup>. Option D is incorrect because TAXII is not a semi-automated solution to gather threat intelligence about competitors in the same sector. TAXII is a fully automated solution that enables the exchange of threat intelligence among various entities across different sectors. TAXII does not target or collect information about specific competitors in the same sector. Rather, it aims to foster collaboration and cooperation among organizations that share common interests or goals in cyber security. Moreover, gathering threat intelligence about competitors in the same sector may raise ethical and legal issues that are beyond the scope of TAXII.

References:

- ? 1 What is STIX/TAXII? | Cloudflare
- ? 2 What Are STIX/TAXII Standards? - Anomali Resources
- ? 3 What is STIX and TAXII? - EclecticlQ
- ? 4 What Is an Insider Threat? Definition & Examples | Varonis
- ? 5 Implementing STIX/TAXII - GitHub Pages
- ? [6] Cyber Threat Intelligence: Ethical Hacking vs Unethical Hacking | Infosec

**NEW QUESTION 5**

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

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

**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 6**

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 Guide<sup>1</sup>, 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 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**

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

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

**Answer:** A

**Explanation:**

A mean time to remediate (MTTR) is a metric that measures how long it takes to fix a vulnerability after it is discovered. A MTTR of 30 days would best protect the organization from the new attacks that are exploited 45 days after a patch is released, as it would ensure that the vulnerabilities are fixed before they are exploited

**NEW QUESTION 9**

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

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

**Answer:** D

**Explanation:**

Data exfiltration is the theft or unauthorized transfer or movement of data from a device or network. It can occur as part of an automated attack or manually, on-site or through an internet connection, and involve various methods. It can affect personal or corporate data, such as sensitive or confidential information. Data exfiltration can be prevented or detected by using compression, encryption, authentication, authorization, and other controls<sup>1</sup>

The network activity shows that a device on the network is sending an outbound email via a mail client to a non-company email address daily at 10:00 p.m. This could indicate that the device is compromised by malware or an insider threat, and that the email is used to exfiltrate data from the network to an external party. The email could contain attachments, links, or hidden data that contain the stolen information. The timing of the email could be designed to avoid detection by normal network monitoring or security systems.

**NEW QUESTION 10**

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**

A security team identified several rogue Wi-Fi access points during the most recent network scan. The network scans occur once per quarter. Which of the following controls would best allow the organization to identify rogue devices more quickly?

- A. Implement a continuous monitoring policy.
- B. Implement a BYOD policy.
- C. Implement a portable wireless scanning policy.
- D. Change the frequency of network scans to once per month.

**Answer:** A

**Explanation:**

The best control to allow the organization to identify rogue devices more quickly is A. Implement a continuous monitoring policy. A continuous monitoring policy is a set of procedures and tools that enable an organization to detect and respond to unauthorized or anomalous activities on its network in real time or near real time. A continuous monitoring policy can help identify rogue access points as soon as they appear on the network, rather than waiting for quarterly or monthly scans. A continuous monitoring policy can also help improve the overall security posture and compliance of the organization by providing timely and accurate information about its network assets, vulnerabilities, threats, and incidents<sup>1</sup>.

**NEW QUESTION 15**

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

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

**Answer:** C

**Explanation:**

The correct answer is C. Impact.

The impact metric is the best way to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The impact metric quantifies the consequences of the outage in terms of lost revenue, productivity, reputation, customer satisfaction, or other relevant factors. The impact metric can help prioritize the recovery efforts and justify the resources needed to restore the service<sup>1</sup>.

The other options are not the best ways to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The timeline metric (A) measures the duration and frequency of the outage, but not its effects. The evidence metric (B) measures the sources and types of data that can be used to investigate and analyze the outage, but not its effects. The scope metric (D) measures the extent and severity of the outage, but not its effects.

**NEW QUESTION 19**

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 24**

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

(Select two).

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

**Answer:** BC

**Explanation:**

Registry artifacts and EDR data are two data sources that can provide valuable information about the root cause of a malware outbreak. Registry artifacts can reveal changes made by the malware to the system configuration, such as disabling security services, modifying startup items, or creating persistence mechanisms<sup>1</sup>. EDR data can capture the behavior and network activity of the malware, such as the initial infection vector, the command and control communication, or the lateral movement<sup>2</sup>. These data sources can help the analyst identify the malware family, the attack technique, and the threat actor behind the outbreak.

References: Malware Analysis | CISA, Malware Analysis: Steps & Examples - CrowdStrike

**NEW QUESTION 25**

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 30**

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

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

**Answer:** B

**Explanation:**

Business process interruption is the inhibitor to remediation that this scenario illustrates. Business process interruption is when the remediation of a vulnerability or an incident requires the disruption or suspension of a critical or essential business process, such as the point-of-sale application. This can cause operational, financial, or reputational losses for the organization, and may outweigh the benefits of the remediation. Therefore, the organization may decide to postpone or avoid the remediation until a more convenient time, such as a change freeze window, which is a period of time when no changes are allowed to the IT environment<sup>12</sup>. Service-level agreement, degrading functionality, and proprietary system are other possible inhibitors to remediation, but they are not relevant to this scenario. Service-level agreement is when the remediation of a vulnerability or an incident violates or affects the contractual obligations or expectations of the service provider or the customer. Degrading functionality is when the remediation of a vulnerability or an incident reduces or impairs the performance or usability of a system or an application. Proprietary system is when the remediation of a vulnerability or an incident involves a system or an application that is owned or controlled by a third party, and the organization has limited or no access or authority to modify it<sup>3</sup>. References: Inhibitors to Remediation — SOC Ops Simplified, Remediation Inhibitors - CompTIA CySA+, Information security Vulnerability Management Report (Remediation...

**NEW QUESTION 33**

**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 12:05:34
Where: Workstation:	Host1 172.30.0.152			
<b>Removed</b>	File	\\host1\users\user1\Downloads\payroll.xlsx	Domainusers\user1	11/30/19 12:25:13
Where: Workstation: Date created:	Host1 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 13:59:25
Where: Workstation:	Host1 172.30.0.152			
<b>Added</b>	File	\\host1\users\user1\Downloads\invoice.exe	Domainusers\user1	12/1/19 14:03:55
Where: Workstation:	Host1 172.30.0.152			
<b>Renamed</b>	File		Domainusers\user1	12/1/19 14:25:30
Where: Workstation: Name changed from:	Host1 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

### Kill chain item

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

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

### Identify the following:

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

- A. Mastered
- B. Not Mastered

Answer: A

#### Explanation:

Kill chain item			
Phishing email	Email filtering	Malware install	Restricted local user permissions
Active links	VPN	Malware execution	Updated antivirus
Malicious website access	IP blocklist	File encryption	Backups
Malware download	Firewall file type filter		

Identify the following:	
Malicious executable	payroll.xlsx
Malicious IP address	81.161.63.103
Date/time malware entered organization	1 Dec 2019 14:03:19

#### NEW QUESTION 37

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

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

**Answer: C**

#### Explanation:

In environments with fragile and legacy equipment, passive scanning is preferred to prevent any potential disruptions that active scanning might cause. When assessing the security of an Operational Technology (OT) network, especially one with fragile and legacy equipment, it's crucial to use passive instead of active vulnerability scans. Active scanning can sometimes disrupt the operation of sensitive or older equipment. Passive scanning listens to network traffic without sending probing requests, thus minimizing the risk of disruption.

#### NEW QUESTION 38

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

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

**Answer: A**

#### Explanation:

Header analysis is the technique of examining the metadata of an email, such as the sender, recipient, date, subject, and routing information. It can help to identify the source of a malicious email by revealing the IP address and domain name of the originator, as well as any spoofing or redirection attempts. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 6, page 240; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 6, page 249.

#### NEW QUESTION 42

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 45

A security analyst is trying to identify possible network addresses from different source networks belonging to the same company and region. Which of the

following shell script functions could help achieve the goal?

- A. function w() { a=\$(ping -c 1 \$1 | awk -F "/" 'END{print \$1}') && echo "\$1 | \$a" }
- B. function x() { b=traceroute -m 40 \$1 | awk 'END{print \$1}' && echo "\$1 | \$b" }
- C. function y() { dig \$(dig -x \$1 | grep PTR | tail -n 1 | awk -F "." 'in-addr' '{print \$1}').origin.asn.cymru.com TXT +short }
- D. function z() { c=\$(geoiplookup \$1) && echo "\$1 | \$c" }

**Answer:** C

**Explanation:**

The shell script function that could help identify possible network addresses from different source networks belonging to the same company and region is:

```
function y() { dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F "." 'in-addr' '{print $1}').origin.asn.cymru.com TXT +short }
```

This function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number (ASN) and other information related to the IP address, such as the country code, registry, or allocation date. The function then prints the IP address and the ASN information, which can help identify any network addresses that belong to the same ASN or region

**NEW QUESTION 49**

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 52**

A security analyst is reviewing the logs of a web server and notices that an attacker has attempted to exploit a SQL injection vulnerability. Which of the following tools can the analyst use to analyze the attack and prevent future attacks?

- A. A web application firewall
- B. A network intrusion detection system
- C. A vulnerability scanner
- D. A web proxy

**Answer:** A

**Explanation:**

A web application firewall (WAF) is a tool that can protect web servers from attacks such as SQL injection, cross-site scripting, and other web-based threats. A WAF can filter, monitor, and block malicious HTTP traffic before it reaches the web server. A WAF can also be configured with rules and policies to detect and prevent specific types of attacks.

References: CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition, Chapter 3, "Security Architecture and Tool Sets", page 91; CompTIA CySA+ Certification Exam Objectives Version 4.0, Domain 1.0 "Threat and Vulnerability Management", Objective 1.2 "Given a scenario, analyze the results of a network reconnaissance", Sub-objective "Web application attacks", page 9

CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition : CompTIA CySA+ Certification Exam Objectives Version 4.0.pdf)

**NEW QUESTION 54**

**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

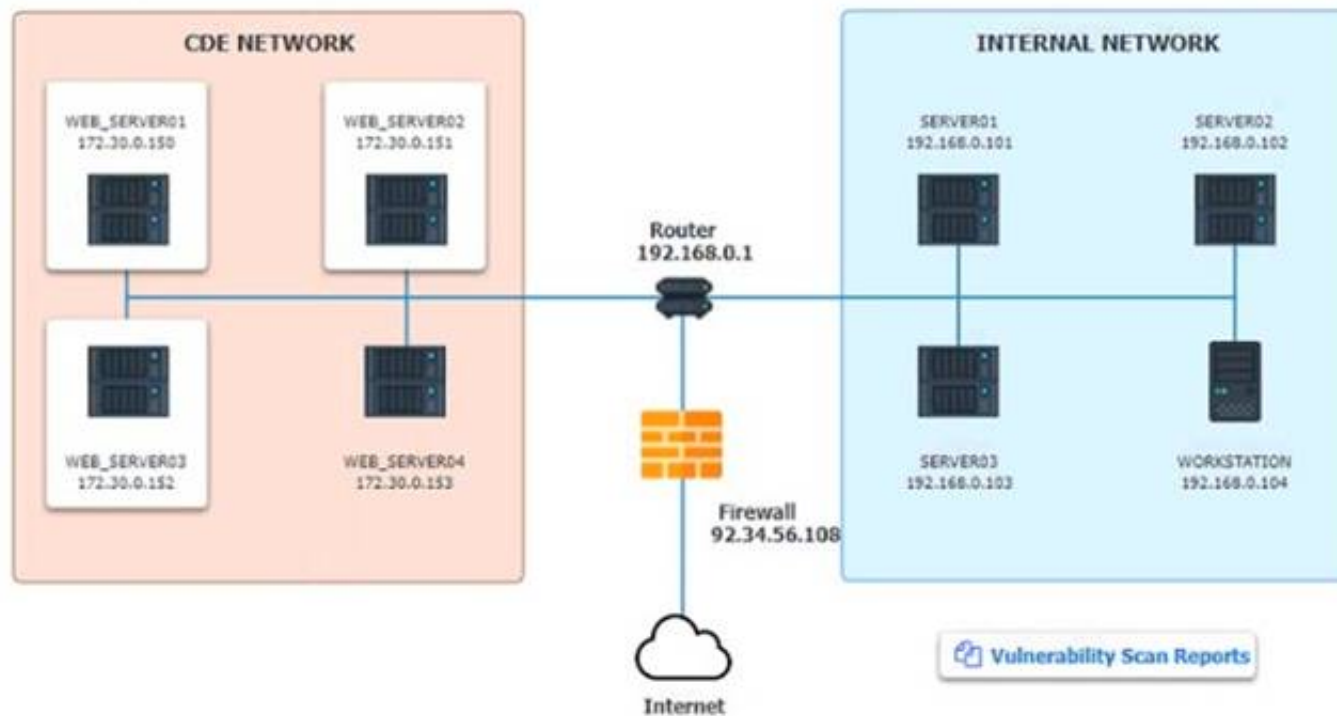
complete the simulation by selecting the correct Validation Result and Remediation Action for each server listed using the drop-down options.

**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	<div>False Positive</div> <div>False Negative</div> <div>True Positive</div> <div>True Negative</div>	<div>Encrypt Entire Session</div> <div>Encrypt All Session Cookies</div> <div>Implement Input Validation</div> <div>Submit as Non-Issue</div> <div>Employ Unique Token in Hidden Field</div> <div>Avoid Using Redirects and Forwards</div> <div>Disable HTTP</div> <div>Request Certificate from a Public CA</div> <div>Renew the Current Certificate</div>
WEB_SERVER02	<div>False Positive</div> <div>False Negative</div> <div>True Positive</div> <div>True Negative</div>	<div>Encrypt Entire Session</div> <div>Encrypt All Session Cookies</div> <div>Implement Input Validation</div> <div>Submit as Non-Issue</div> <div>Employ Unique Token in Hidden Field</div> <div>Avoid Using Redirects and Forwards</div> <div>Disable HTTP</div> <div>Request Certificate from a Public CA</div> <div>Renew the Current Certificate</div>
WEB_SERVER03	<div>False Positive</div> <div>False Negative</div> <div>True Positive</div> <div>True Negative</div>	<div>Encrypt Entire Session</div> <div>Encrypt All Session Cookies</div> <div>Implement Input Validation</div> <div>Submit as Non-Issue</div> <div>Employ Unique Token in Hidden Field</div> <div>Avoid Using Redirects and Forwards</div> <div>Disable HTTP</div> <div>Request Certificate from a Public CA</div> <div>Renew the Current Certificate</div>

- 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 57

A security audit for unsecured network services was conducted, and the following output was generated:

```
#nmap --top-ports 7 192.29.0.5
```

PORT	STATE	SERVICE
21	closed	ftp
22	open	ssh
23	filtered	telnet
636	open	ldaps
1723	open	pptp
443	closed	https
3389	closed	ms-term-server

Which of the following services should the security team investigate further? (Select two).

- A. 21
- B. 22
- C. 23
- D. 636

E. 1723  
F. 3389

**Answer:** CD

**Explanation:**

The output shows the results of a port scan, which is a technique used to identify open ports and services running on a network host. Port scanning can be used by attackers to discover potential vulnerabilities and exploit them, or by defenders to assess the security posture and configuration of their network devices<sup>1</sup>. The output lists six ports that are open on the target host, along with the service name and version associated with each port. The service name indicates the type of application or protocol that is using the port, while the version indicates the specific release or update of the service. The service name and version can provide useful information for both attackers and defenders, as they can reveal the capabilities, features, and weaknesses of the service. Among the six ports listed, two are particularly risky and should be investigated further by the security team: port 23 and port 636. Port 23 is used by Telnet, which is an old and insecure protocol for remote login and command execution. Telnet does not encrypt any data transmitted over the network, including usernames and passwords, which makes it vulnerable to eavesdropping, interception, and modification by attackers. Telnet also has many known vulnerabilities that can allow attackers to gain unauthorized access, execute arbitrary commands, or cause denial-of-service attacks on the target host<sup>23</sup>. Port 636 is used by LDAP over SSL/TLS (LDAPS), which is a protocol for accessing and modifying directory services over a secure connection. LDAPS encrypts the data exchanged between the client and the server using SSL/TLS certificates, which provide authentication, confidentiality, and integrity. However, LDAPS can also be vulnerable to attacks if the certificates are not properly configured, verified, or updated. For example, attackers can use self-signed or expired certificates to perform man-in-the-middle attacks, spoofing attacks, or certificate revocation attacks on LDAPS connections. Therefore, the security team should investigate further why port 23 and port 636 are open on the target host, and what services are running on them. The security team should also consider disabling or replacing these services with more secure alternatives, such as SSH for port 23 and StartTLS for port 636<sup>2</sup>.

**NEW QUESTION 61**

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

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

**Answer:** B

**Explanation:**

A successful information security program consists of several key elements that align with the organization's goals and objectives, and address the risks and threats to its information assets.  
? Security policy implementation: This is the process of developing, documenting, and enforcing the rules and standards that govern the security of the organization's information assets. Security policies define the scope, objectives, roles, and responsibilities of the security program, as well as the acceptable use, access control, incident response, and compliance requirements for the information assets.  
? Assignment of roles and responsibilities: This is the process of identifying and assigning the specific tasks and duties related to the security program to the appropriate individuals or groups within the organization. Roles and responsibilities define who is accountable, responsible, consulted, and informed for each security activity, such as risk assessment, vulnerability management, threat detection, incident response, auditing, and reporting.  
? Information asset classification: This is the process of categorizing the information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps to determine the appropriate level of protection and controls for each asset, as well as the impact and likelihood of a security breach or loss. Information asset classification also facilitates the prioritization of security resources and efforts based on the risk level of each asset.

**NEW QUESTION 65**

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

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

**Answer:** A

**Explanation:**

The first step that should be performed when establishing a disaster recovery plan is to agree on the goals and objectives of the plan. The goals and objectives of the plan should define what the plan aims to achieve, such as minimizing downtime, restoring critical functions, ensuring data integrity, or meeting compliance requirements. The goals and objectives of the plan should also be aligned with the business needs and priorities of the organization and be measurable and achievable.

**NEW QUESTION 69**

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

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

**Answer:** A

**Explanation:**

The analyst should focus on the impact of the events in order to move the incident forward. Impact is the measure of the potential or actual damage caused by an incident, such as data loss, financial loss, reputational damage, or regulatory penalties. Impact can help the analyst prioritize the events that need to be investigated based on their severity and urgency, and allocate the appropriate resources and actions to contain and remediate them. Impact can also help the analyst communicate the status and progress of the incident to the stakeholders and customers, and justify the decisions and recommendations made during the incident response<sup>12</sup>. Vulnerability score, mean time to detect, and isolation are all important metrics or actions for incident response, but they are not the main focus for moving the incident forward. Vulnerability score is the rating of the likelihood and severity of a vulnerability being exploited by a threat actor. Mean time to detect is the average time it takes to discover an incident. Isolation is the process of disconnecting an affected system from the network to prevent further damage or spread of the incident<sup>34</sup>. References: Incident Response: Processes, Best Practices & Tools - Atlassian, Incident Response Metrics: What You Should Be



Measuring, Vulnerability Scanning Best Practices, How to Track Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to Cybersecurity Incidents, [Isolation and Quarantine for Incident Response]

#### NEW QUESTION 71

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  
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  
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  
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  
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 76

A systems analyst is limiting user access to system configuration keys and values in a Windows environment. Which of the following describes where the analyst can find these configuration items?

- A. confi
- B. ini
- C. ntds.dit
- D. Master boot record
- E. Registry

**Answer:** D

#### Explanation:

The correct answer is D. Registry.

The registry is a database that stores system configuration keys and values in a Windows environment. The registry contains information about the hardware, software, users, and preferences of the system. The registry can be accessed and modified using the Registry Editor tool (regedit.exe) or the command-line tool (reg.exe). The registry is organized into five main sections, called hives, which are further divided into subkeys and values.

The other options are not the best descriptions of where the analyst can find system configuration keys and values in a Windows environment. config.ini (A) is a file that stores configuration settings for some applications, but it is not a database that stores system configuration keys and values. ntds.dit (B) is a file that stores the Active Directory data for a domain controller, but it is not a database that stores system configuration keys and values. Master boot record © is a section of the hard disk that contains information about the partitions and the boot loader, but it is not a database that stores system configuration keys and values.

#### NEW QUESTION 80

A security analyst noticed the following entry on a web server log:  
Warning: fopen (http://127.0.0.1:16) :  
failed to open stream:  
Connection refused in /hj/var/www/showimage.php on line 7  
Which of the following malicious activities was most likely attempted?

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

**Answer: C**

**Explanation:**

The malicious activity that was most likely attempted is SSRF (Server-Side Request Forgery). This is a type of attack that exploits a vulnerable web application to make requests to other resources on behalf of the web server. In this case, the attacker tried to use the fopen function to access the local loopback address (127.0.0.1) on port 16, which could be a service that is not intended to be exposed to the public. The connection was refused, indicating that the port was closed or filtered. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 2: Software and Application Security, page 66.

**NEW QUESTION 85**

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

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

**Answer: C**

**Explanation:**

Implementing a central place to manage IT assets is the best solution to decrease the inconsistencies regarding versions and patches in the existing infrastructure. A central place to manage IT assets, such as a configuration management database (CMDB), can help the vulnerability assessment team to have an accurate and up-to-date inventory of all the hardware and software components in the network, as well as their relationships and dependencies. A CMDB can also track the changes and updates made to the IT assets, and provide a single source of truth for the vulnerability assessment team and other teams to compare and verify the versions and patches of the infrastructure<sup>12</sup>. Implementing credentialed scanning, changing from a passive to an active scanning approach, and performing agentless scanning are all methods to improve the vulnerability scanning process, but they do not address the root cause of the inconsistencies, which is the lack of a central place to manage IT assets<sup>3</sup>. References: What is a Configuration Management Database (CMDB)?, How to Use a CMDB to Improve Vulnerability Management, Vulnerability Scanning Best Practices

**NEW QUESTION 86**

An employee downloads a freeware program to change the desktop to the classic look of legacy Windows. Shortly after the employee installs the program, a high volume of random DNS queries begin to originate from the system. An investigation on the system reveals the following: Add-MpPreference -ExclusionPath '%Program Filest\kysysconfig'  
Which of the following is possibly occurring?

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

**Answer: D**

**Explanation:**

Defense evasion is the technique of avoiding detection or prevention by security tools or mechanisms. In this case, the freeware program is likely a malware that generates random DNS queries to communicate with a command and control server or exfiltrate data. The command Add-MpPreference -ExclusionPath '%Program Filest\kysysconfig' is used to add an exclusion path to Windows Defender, which is a built-in antivirus software, to prevent it from scanning the malware folder. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page 204; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 212. pr

**NEW QUESTION 88**

A vulnerability management team is unable to patch all vulnerabilities found during their weekly scans. Using the third-party scoring system described below, the team patches the most urgent vulnerabilities:

Metric	Description
Cobain	Exploitable by malware
Grohl	Externally facing
Novo	Exploit PoC available
Smear	Older than 2 years
Channing	Vulnerability research activity

Additionally, the vulnerability management team feels that the metrics Smear and Channing are less important than the others, so these will be lower in priority. Which of the following vulnerabilities should be patched first, given the above third-party scoring system?

A. InLoud: Cobain: Yes Grohl: No Novo: Yes Smear: Yes Channing: No B.TSpirit: Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No C.ENameless: Cobain: Yes Grohl: No Novo: Yes Smear: No Channing: No D.PBleach: Cobain: Yes Grohl: No Novo: No Smear: No Channing: Yes

**Answer:** B

**Explanation:**

The vulnerability that should be patched first, given the above third-party scoring system, is:

TSpirit: Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No

This vulnerability has three out of five metrics marked as Yes, which indicates a high severity level. The metrics Cobain, Grohl, and Novo are more important than Smear and Channing, according to the vulnerability management team. Therefore, this vulnerability poses a greater risk than the other vulnerabilities and should be patched first.

**NEW QUESTION 90**

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 93**

During an internal code review, software called "ACE" was discovered to have a vulnerability that allows the execution of arbitrary code. The vulnerability is in a legacy, third-party vendor resource that is used by the ACE software. ACE is used worldwide and is essential for many businesses in this industry. Developers informed the Chief Information Security Officer that removal of the vulnerability will take time. Which of the following is the first action to take?

- A. Look for potential IoCs in the company.
- B. Inform customers of the vulnerability.
- C. Remove the affected vendor resource from the ACE software.
- D. Develop a compensating control until the issue can be fixed permanently.

**Answer:** D

**Explanation:**

A compensating control is an alternative measure that provides a similar level of protection as the original control, but is used when the original control is not feasible or cost-effective. In this case, the CISO should develop a compensating control to mitigate the risk of the vulnerability in the ACE software, such as implementing additional monitoring, firewall rules, or encryption, until the issue can be fixed permanently by the developers. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page 197; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 205.

**NEW QUESTION 98**

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

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

**Answer:** D

**Explanation:**

A threshold value is a parameter that defines the minimum or maximum level of a metric or event that triggers an alert. For example, a threshold value can be set to alert when the number of failed login attempts exceeds 10 in an hour, or when the CPU usage drops below 20% for more than 15 minutes. By setting a threshold value, the process can filter out irrelevant or insignificant alerts and focus on the ones that indicate a potential problem or anomaly. A threshold value can help to reduce the noise and false positives in the alert system, and improve the efficiency and accuracy of the analysis<sup>12</sup>

**NEW QUESTION 99**

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

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

**Answer:** B



**Explanation:**

The NTP configuration on each system should be checked first, as it is essential for ensuring accurate and consistent time stamps across different systems. NTP is the Network Time Protocol, which is used to synchronize the clocks of computers over a network. NTP uses a hierarchical system of time sources, where each level is assigned a stratum number. The most accurate time sources, such as atomic clocks or GPS receivers, are at stratum 0, and the devices that synchronize with them are at stratum 1, and so on. NTP clients can query multiple NTP servers and use algorithms to select the best time source and adjust their clocks accordingly<sup>1</sup>. If the NTP configuration is not consistent or correct on each system, the time stamps of the logs and events may differ, making it difficult to correlate incidents across different systems. This can affect the security analysis and correlation of events, as well as the compliance and auditing of the network<sup>23</sup>.

References: How the Windows Time Service Works, Time Synchronization - All You Need To Know, What is SIEM? | Microsoft Security

**NEW QUESTION 103**

An analyst views the following log entries:

```
202.180.158.22 - - [12/Aug/2018:11:42:20 -0200] "GET /src/sourceCode.bat\HTTP/1.0" 404 291
134.17.188.5 - - [12/Aug/2018:13:04:16 -0200] "GET /img/orgChart.jpg\HTTP/1.0" 200 291
121.19.30.221 - - [12/Aug/2018:13:04:17 -0200] "GET /cgi-bin/stats.pl?month=12\HTTP/1.0" 200 291
134.17.188.5 - - [12/Aug/2018:13:04:17 -0200] "GET /img/orgChartDirectors.jpg\HTTP/1.0" 200 291
134.17.188.5 - - [12/Aug/2018:13:04:17 -0200] "GET /img/orgChartStaff.jpg\HTTP/1.0" 200 291
134.17.188.5 - - [12/Aug/2018:13:04:18 -0200] "GET /img/orgChartUnderlings.jpg\HTTP/1.0" 404 291
216.122.5.5 - - [12/Aug/2018:13:04:18 -0200] "GET /cgi-bin/quarterly.pl?qtr=3\HTTP/1.0" 404 291
134.17.188.5 - - [12/Aug/2018:13:04:18 -0200] "GET /img/orgChartUnderUnderlings.jpg.jpg\HTTP/1.0" 404 291
```

The organization has a partner vendor with hosts in the 216.122.5.x range. This partner vendor is required to have access to monthly reports and is the only external vendor with authorized access. The organization prioritizes incident investigation according to the following hierarchy: unauthorized data disclosure is more critical than denial of service attempts.

which are more important than ensuring vendor data access.

Based on the log files and the organization's priorities, which of the following hosts warrants additional investigation?

- A. 121.19.30.221
- B. 134.17.188.5
- C. 202.180.1582
- D. 216.122.5.5

**Answer:** A

**Explanation:**

The correct answer is A. 121.19.30.221.

Based on the log files and the organization's priorities, the host that warrants additional investigation is 121.19.30.221, because it is the only host that accessed a file containing sensitive data and is not from the partner vendor's range.

The log files show the following information:

? The IP addresses of the hosts that accessed the web server

? The date and time of the access

? The file path of the requested resource

? The number of bytes transferred

The organization's priorities are:

? Unauthorized data disclosure is more critical than denial of service attempts

? Denial of service attempts are more important than ensuring vendor data access According to these priorities, the most serious threat to the organization is unauthorized data disclosure, which occurs when sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, altered, or used by an individual unauthorized to do so<sup>123</sup>. Therefore, the host that accessed a file containing sensitive data and is not from the partner vendor's range poses the highest risk to the organization.

The file that contains sensitive data is /reports/2023/financials.pdf, as indicated by its name and path. This file was accessed by two hosts: 121.19.30.221 and 216.122.5.5. However, only 121.19.30.221 is not from the partner vendor's range, which is 216.122.5.x. Therefore, 121.19.30.221 is a potential unauthorized data disclosure threat and warrants additional investigation.

The other hosts do not warrant additional investigation based on the log files and the organization's priorities.

Host 134.17.188.5 accessed /index.html multiple times in a short period of time, which could indicate a denial of service attempt by flooding the web server with requests<sup>45</sup>. However, denial of service attempts are less critical than unauthorized data disclosure according to the organization's priorities, and there is no evidence that this host succeeded in disrupting the web server's normal operations.

Host 202.180.1582 accessed /images/logo.png once, which does not indicate any malicious activity or threat to the organization.

Host 216.122.5.5 accessed /reports/2023/financials.pdf once, which could indicate unauthorized data disclosure if it was not authorized to do so. However, this host is from the partner vendor's range, which is required to have access to monthly reports and is the only external vendor with authorized access according to the organization's requirements. Therefore, based on the log files and the organization's priorities, host 121.19.30.221 warrants additional investigation as it poses the highest risk of unauthorized data disclosure to the organization.

**NEW QUESTION 106**

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

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

Which of the following has most likely occurred?

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

**Answer:** A

**Explanation:**

An Office document with a malicious macro was opened is the most likely explanation for the suspicious activity on the company laptop, as it reflects the common technique of using macros to execute PowerShell commands that download and run malware. A macro is a piece of code that can automate tasks or perform actions in an Office document, such as a Word file or an Excel spreadsheet. Macros can be useful and legitimate, but they can also be abused by threat actors to deliver malware or perform malicious actions on the system. A malicious macro can be embedded in an Office document that is sent as an attachment in a phishing email or hosted on a compromised website. When the user opens the document, they may be prompted to enable macros or content, which will trigger the execution of the malicious code. The malicious macro can then use PowerShell, which is a scripting language and command-line shell that is built into Windows, to perform various tasks, such as downloading and running malware from a remote URL, bypassing security controls, or establishing persistence on the system. The log excerpt shows that PowerShell was used to download a string from a URL using the WebClient.DownloadString method, which is a common way to fetch and execute malicious code from the internet. The log also shows that PowerShell was used to invoke an expression (iex) that contains obfuscated code, which is another common way to evade detection and analysis. The other options are not as likely as an Office document with a malicious macro was opened, as they do not match the evidence in the log excerpt. A credential-stealing website was visited is possible, but it does not explain why PowerShell was used to download and execute code from a URL. A phishing link in an email was clicked is also possible, but it does not explain what happened after the link was clicked or how PowerShell was involved. A web browser vulnerability was exploited is unlikely, as it does not explain why PowerShell was used to download and execute code from a URL.

**NEW QUESTION 107**

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

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

**Answer:** A

**Explanation:**

OpenVAS is an open-source tool that performs comprehensive vulnerability scanning and assessment on the network. It can generate reports and evidence of the scan results, which can be used for auditing purposes. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page 199; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 207.

**NEW QUESTION 111**

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

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

**Answer:** C

**Explanation:**

Mitigate is the best term to describe the risk management principle that the company is exercising, as it means to reduce the likelihood or impact of a risk. By implementing a patch management program to remediate vulnerabilities, the company is mitigating the threat of cyberattacks that could exploit those vulnerabilities and compromise the security or functionality of the systems. The other terms are not as accurate as mitigate, as they describe different risk management principles. Transfer means to shift the responsibility or burden of a risk to another party, such as an insurer or a contractor. Accept means to acknowledge the existence of a risk and decide not to take any action to reduce it, usually because the risk is low or the cost of mitigation is too high. Avoid means to eliminate the

possibility of a risk by changing the plans or activities that could cause it, such as cancelling a project or discontinuing a service.

#### NEW QUESTION 113

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 116

An employee is suspected of misusing a company-issued laptop. The employee has been suspended pending an investigation by human resources. Which of the following is the best step to preserve evidence?

- A. Disable the user's network account and access to web resources
- B. Make a copy of the files as a backup on the server.
- C. Place a legal hold on the device and the user's network share.
- D. Make a forensic image of the device and create a SRA-I hash.

**Answer: D**

#### Explanation:

Making a forensic image of the device and creating a SRA-I hash is the best step to preserve evidence, as it creates an exact copy of the device's data and verifies its integrity. A forensic image is a bit-by-bit copy of the device's storage media, which preserves all the information on the device, including deleted or hidden files. A SRA-I hash is a cryptographic value that is calculated from the forensic image, which can be used to prove that the image has not been altered or tampered with. The other options are not as effective as making a forensic image and creating a SRA-I hash, as they may not capture all the relevant data, or they may not provide sufficient verification of the evidence's authenticity. Official References:

? <https://www.sans.org/blog/forensics-101-acquiring-an-image-with-ftk-imager/>

? <https://swailescomputerforensics.com/digital-forensics-imaging-hash-value/>

#### NEW QUESTION 119

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 121

There are several reports of sensitive information being disclosed via file sharing services. The company would like to improve its security posture against this threat. Which of the following security controls would best support the company in this scenario?

- A. Implement step-up authentication for administrators
- B. Improve employee training and awareness
- C. Increase password complexity standards
- D. Deploy mobile device management

**Answer: B**

#### Explanation:

The best security control to implement against sensitive information being disclosed via file sharing services is to improve employee training and awareness. Employee training and awareness can help educate employees on the risks and consequences of using file sharing services for sensitive information, as well as the policies and procedures for handling such information securely and appropriately. Employee training and awareness can also help foster a security culture and encourage employees to report any incidents or violations of information security.

#### NEW QUESTION 125

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

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

**Answer: C**



**Explanation:**

An unintentional insider threat is a type of network security threat that occurs when a legitimate user of the network unknowingly exposes the network to malicious activity, such as opening a phishing email or a malware-infected attachment from an unknown source. This can compromise the network security and allow attackers to access sensitive data or systems. The other options are not related to the threat concept of ensuring that all network users only open attachments from known sources.

ReferencesCompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 1: Threat and Vulnerability Management, page 13.What is Network Security | Threats, Best Practices

| Imperva, Network Security Threats and Attacks, Phishing section.Five Ways to Defend Against Network Security Threats, 2. Use Firewalls section.

**NEW QUESTION 129**

A security analyst must preserve a system hard drive that was involved in a litigation request Which of the following is the best method to ensure the data on the device is not modified?

- A. Generate a hash value and make a backup image.
- B. Encrypt the device to ensure confidentiality of the data.
- C. Protect the device with a complex password.
- D. Perform a memory scan dump to collect residual data.

**Answer:** A

**Explanation:**

Generating a hash value and making a backup image is the best method to ensure the data on the device is not modified, as it creates a verifiable copy of the original data that can be used for forensic analysis. Encrypting the device, protecting it with a password, or performing a memory scan dump do not prevent the data from being altered or deleted. Verified References: CompTIA CySA+ CS0-002 Certification Study Guide, page 3291

**NEW QUESTION 134**

An analyst needs to provide recommendations based on a recent vulnerability scan:

Plug-in name	Family
SMB use domain SID to enumerate users	Windows : User management
SYN scanner	Port scanners
SSL certificate cannot be trusted	General
Scan not performed with admin privileges	Settings

Which of the following should the analyst recommend addressing to ensure potential vulnerabilities are identified?

- A. SMB use domain SID to enumerate users
- B. SYN scanner
- C. SSL certificate cannot be trusted
- D. Scan not performed with admin privileges

**Answer:** D

**Explanation:**

This is because scanning without admin privileges can limit the scope and accuracy of the vulnerability scan, and potentially miss some critical vulnerabilities that require higher privileges to detect. According to the OWASP Vulnerability Management Guide<sup>1</sup>, “scanning without administrative privileges will result in a large number of false negatives and an incomplete scan”. Therefore, the analyst should recommend addressing this issue to ensure potential vulnerabilities are identified.

**NEW QUESTION 138**

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

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

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

Which of the following vulnerabilities should be patched first?

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

**Answer:** A

**NEW QUESTION 142**

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

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

**Answer:** D

**Explanation:**

Transfer is the risk management principle that is accomplished by purchasing cyber insurance. Transfer is a strategy that involves shifting the risk or its consequences to another party, such as an insurance company, a vendor, or a partner. Transfer does not eliminate the risk, but it reduces the potential impact or liability of the risk for the original party. Cyber insurance is a type of insurance that covers the losses and damages resulting from cyberattacks, such as data breaches, ransomware, denial-of-service attacks, or network disruptions. Cyber insurance can help transfer the risk of cyber incidents by providing financial compensation, legal assistance, or recovery services to the insured party. 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 147

An analyst has received an IPS event notification from the SIEM stating an IP address, which is known to be malicious, has attempted to exploit a zero-day vulnerability on several web servers. The exploit contained the following snippet:

/wp-json/trx\_addons/V2/get/sc\_layout?sc=wp\_insert\_user&role=administrator

Which of the following controls would work best to mitigate the attack represented by this snippet?

- A. Limit user creation to administrators only.
- B. Limit layout creation to administrators only.
- C. Set the directory trx\_addons to read only for all users.
- D. Set the directory v2 to read only for all users.

**Answer:** A

#### Explanation:

Limiting user creation to administrators only would work best to mitigate the attack represented by this snippet. The snippet shows an attempt to exploit a zero-day vulnerability in the ThemeREX Addons WordPress plugin, which allows remote code execution by invoking arbitrary PHP functions via the REST-API endpoint /wp-json/trx\_addons/V2/get/sc\_layout. In this case, the attacker tries to use the wp\_insert\_user function to create a new administrator account on the WordPress site<sup>12</sup>. Limiting user creation to administrators only would prevent the attacker from succeeding, as they would need to provide valid administrator credentials to create a new user. This can be done by using a plugin or a code snippet that restricts user registration to administrators<sup>34</sup>. Limiting layout creation to administrators only, setting the directory trx\_addons to read only for all users, and setting the directory v2 to read only for all users are not effective controls to mitigate the attack, as they do not address the core of the vulnerability, which is the lack of input validation and sanitization on the REST-API endpoint. Moreover, setting directories to read only may affect the functionality of the plugin or the WordPress site<sup>56</sup>. References: Zero-Day Vulnerability in ThemeREX Addons Now Patched - Wordfence, Mitigating Zero Day Attacks With a Detection, Prevention ... - Spiceworks, How to Restrict WordPress User Registration to Specific Email ..., How to Limit WordPress User Registration to Specific Domains, WordPress File Permissions: A Guide to Securing Your Website, WordPress File Permissions: What is the Ideal Setting?

#### NEW QUESTION 149

A technician is analyzing output from a popular network mapping tool for a PCI audit:

```
PORT STATE SERVICE VERSION
22/tcp open  ssh Cisco SSH 1.25 (protocol 2.0)
443/tcp open  ssl/http OpenResty web app server
|_http-server-header: openresty
|_ssl-enum-ciphers:
|_ TLSv1.1:
|_ ciphers:
|_ TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
|_ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
|_ compressors:
|_ NULL
|_ cipher preference: server
|_ warnings:
|_ Insecure certificate signature (SHA1), score capped at F
|_ TLSv1.2:
|_ ciphers:
|_ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - F
|_ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - F
|_ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - F
|_ TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - F
|_ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - F
|_ TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - F
|_ TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - F
|_ TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - F
|_ TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
|_ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
|_ compressors:
|_ NULL
|_ cipher preference: server
|_ warnings:
|_ Insecure certificate signature (SHA1), score capped at F
|_ least strength: F
```

Which of the following best describes the output?

- A. The host is not up or responding.
- B. The host is running excessive cipher suites.
- C. The host is allowing insecure cipher suites.
- D. The Secure Shell port on this host is closed

**Answer:** C

**Explanation:**

The output shows the result of running the ssl-enum-ciphers script with Nmap, which is a tool that can scan web servers for supported SSL/TLS cipher suites. Cipher suites are combinations of cryptographic algorithms that are used to establish secure communication between a client and a server. The output shows the cipher suites that are supported by the server, along with a letter grade (A through F) indicating the strength of the connection. The output also shows the least strength, which is the strength of the weakest cipher offered by the server. In this case, the least strength is F, which means that the server is allowing insecure cipher suites that are vulnerable to attacks or have been deprecated. For example, the output shows that the server supports SSLv3, which is an outdated and insecure protocol that is susceptible to the POODLE attack. The output also shows that the server supports RC4, which is a weak and broken stream cipher that should not be used. Therefore, the best description of the output is that the host is allowing insecure cipher suites. The other descriptions are not accurate, as they do not reflect what the output shows. The host is not up or responding is incorrect, as the output clearly shows that the host is up and responding to the scan. The host is running excessive cipher suites is incorrect, as the output does not indicate how many cipher suites the host is running, only which ones it supports. The Secure Shell port on this host is closed is incorrect, as the output does not show anything about port 22, which is the default port for Secure Shell (SSH). The output only shows information about port 443, which is the default port for HTTPS.

**NEW QUESTION 154**

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 155**

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

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

**Answer:** C

**Explanation:**

Time synchronization is the process of ensuring that all systems in a network have the same accurate time, which is essential for correlating data points from different sources. If the system has an issue with time synchronization, the analyst may have difficulty matching events that occurred at the same time or in a specific order. Access rights, network segmentation, and invalid playbook are not directly related to the issue of correlating data points. Verified References: [CompTIA CySA+ CS0-002 Certification Study Guide], page 23

**NEW QUESTION 159**

AXSS vulnerability was reported on one of the non-sensitive/non-mission-critical public websites of a company. The security department confirmed the finding and needs to provide a recommendation to the application owner. Which of the following recommendations will best prevent this vulnerability from being exploited? (Select two).

- A. Implement an IPS in front of the web server.
- B. Enable MFA on the website.
- C. Take the website offline until it is patched.
- D. Implement a compensating control in the source code.
- E. Configure TLS v1.3 on the website.
- F. Fix the vulnerability using a virtual patch at the WAF.

**Answer:** DF

**Explanation:**

The best recommendations to prevent an XSS vulnerability from being exploited are to implement a compensating control in the source code and to fix the vulnerability using a virtual patch at the WAF. A compensating control is a technique that mitigates the risk of a vulnerability by adding additional security measures, such as input validation, output encoding, or HTML sanitization. A virtual patch is a rule that blocks or modifies malicious requests or responses at the WAF level, without modifying the application code. These recommendations are effective, efficient, and less disruptive than the other options. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156; Cross Site Scripting Prevention Cheat Sheet, Section: XSS Defense Philosophy.

**NEW QUESTION 164**

During a recent site survey, an analyst discovered a rogue wireless access point on the network. Which of the following actions should be taken first to protect the network while preserving evidence?

- A. Run a packet sniffer to monitor traffic to and from the access point.
- B. Connect to the access point and examine its log files.
- C. Identify who is connected to the access point and attempt to find the attacker.
- D. Disconnect the access point from the network

**Answer:** D



#### Explanation:

The correct answer is D. Disconnect the access point from the network.

A rogue access point is a wireless access point that has been installed on a network without the authorization or knowledge of the network administrator. A rogue access point can pose a serious security risk, as it can allow unauthorized users to access the network, intercept network traffic, or launch attacks against the network or its devices<sup>1234</sup>.

The first action that should be taken to protect the network while preserving evidence is to disconnect the rogue access point from the network. This will prevent any further damage or compromise of the network by blocking the access point from communicating with other devices or users. Disconnecting the rogue access point will also preserve its state and configuration, which can be useful for forensic analysis and investigation. Disconnecting the rogue access point can be done physically by unplugging it from the network port or wirelessly by disabling its radio frequency<sup>5</sup>.

The other options are not the best actions to take first, as they may not protect the network or preserve evidence effectively.

Option A is not the best action to take first, as running a packet sniffer to monitor traffic to and from the access point may not stop the rogue access point from causing harm to the network. A packet sniffer is a tool that captures and analyzes network packets, which are units of data that travel across a network. A packet sniffer can be useful for identifying and troubleshooting network problems, but it may not be able to prevent or block malicious traffic from a rogue access point. Moreover, running a packet sniffer may require additional time and resources, which could delay the response and mitigation of the incident<sup>5</sup>.

Option B is not the best action to take first, as connecting to the access point and examining its log files may not protect the network or preserve evidence.

Connecting to the access point may expose the analyst's device or credentials to potential attacks or compromise by the rogue access point. Examining its log files may provide some information about the origin and activity of the rogue access point, but it may also alter or delete some evidence that could be useful for forensic analysis and investigation. Furthermore, connecting to the access point and examining its log files may not prevent or stop the rogue access point from continuing to harm the network<sup>5</sup>.

Option C is not the best action to take first, as identifying who is connected to the access point and attempting to find the attacker may not protect the network or preserve evidence. Identifying who is connected to the access point may require additional tools or techniques, such as scanning for wireless devices or analyzing network traffic, which could take time and resources away from responding and mitigating the incident. Attempting to find the attacker may also be difficult or impossible, as the attacker may use various methods to hide their identity or location, such as encryption, spoofing, or proxy servers. Moreover, identifying who is connected to the access point and attempting to find the attacker may not prevent or stop the rogue access point from causing further damage or compromise to the network<sup>5</sup>.

References:

? 1 CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives

? 2 Cybersecurity Analyst+ - CompTIA

? 3 CompTIA CySA+ CS0-002 Certification Study Guide

? 4 CertMaster Learn for CySA+ Training - CompTIA

? 5 How to Protect Against Rogue Access Points on Wi-Fi - Byos

? 6 Wireless Access Point Protection: 5 Steps to Find Rogue Wi-Fi Networks ...

? 7 Rogue Access Point - Techopedia

? 8 Rogue access point - Wikipedia

? 9 What is a Rogue Access Point (Rogue AP)? - Contextual Security

#### NEW QUESTION 169

A company brings in a consultant to make improvements to its website. After the consultant leaves, a web developer notices unusual activity on the website and submits a suspicious file containing the following code to the security team:

```
<html>
<body>

<?php
echo '<H1>This website is under maintenance</H1>';
alert('Exit');
exec($_GET['cmd']);
echo $_SERVER['REMOTE_ADDR']
?>
</body>
</html>
```

Which of the following did the consultant do?

- A. Implanted a backdoor
- B. Implemented privilege escalation
- C. Implemented clickjacking
- D. Patched the web server

**Answer:** A

#### Explanation:

The correct answer is A. Implanted a backdoor.

A backdoor is a method that allows an unauthorized user to access a system or network without the permission or knowledge of the owner. A backdoor can be installed by exploiting a software vulnerability, by using malware, or by physically modifying the hardware or firmware of the device. A backdoor can be used for various malicious purposes, such as stealing data, installing malware, executing commands, or taking control of the system.

In this case, the consultant implanted a backdoor in the website by using an HTML and PHP code snippet that displays an image of a shutdown button and an alert message that says "Exit". However, the code also echoes the remote address of the server, which means that it sends the IP address of the visitor to the attacker.

This way, the attacker can identify and target the visitors of the website and use their IP addresses to launch further attacks or gain access to their devices.

The code snippet is an example of a clickjacking attack, which is a type of interface-based attack that tricks a user into clicking on a hidden or disguised element on a webpage. However, clickjacking is not the main goal of the consultant, but rather a means to implant the backdoor. Therefore, option C is incorrect.

Option B is also incorrect because privilege escalation is an attack technique that allows an attacker to gain higher or more permissions than they are supposed to have on a system or network. Privilege escalation can be achieved by exploiting a software vulnerability, by using malware, or by abusing misconfigurations or weak access controls. However, there is no evidence that the consultant implemented privilege escalation on the website or gained any elevated privileges.

Option D is also incorrect because patching is a process of applying updates to software to fix errors, improve performance, or enhance security. Patching can prevent or mitigate various types of attacks, such as exploits, malware infections, or denial-of-service attacks. However, there is no indication that the consultant patched the web server or improved its security in any way.

References:

? 1 What Is a Backdoor & How to Prevent Backdoor Attacks (2023)

? 2 What is Clickjacking? Tutorial & Examples | Web Security Academy

? 3 What Is Privilege Escalation and How It Relates to Web Security | Acunetix  
? 4 What Is Patching? | Best Practices For Patch Management - cWatch Blog

NEW QUESTION 173

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 176

A cryptocurrency service company is primarily concerned with ensuring the accuracy of the data on one of its systems. A security analyst has been tasked with prioritizing vulnerabilities for remediation for the system. The analyst will use the following CVSSv3.1 impact metrics for prioritization:

Vulnerability	CVSSv3.1 impact metrics
1	C:L/I:L/A:L
2	C:N/I:L/A:H
3	C:H/I:N/A:N
4	C:L/I:H/A:L

Which of the following vulnerabilities should be prioritized for remediation?

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

**Answer:** B

**Explanation:**

Vulnerability 2 has the highest impact metrics, specifically the highest attack vector (AV) and attack complexity (AC) values. This means that the vulnerability is more likely to be exploited and more difficult to remediate.

References:

? CVSS v3.1 Specification Document, section 2.1.1 and 2.1.2

? The CVSS v3 Vulnerability Scoring System, section 3.1 and 3.2

**NEW QUESTION 179**

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. ReferencesC: ompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5: Incident Response, page 197.

**NEW QUESTION 182**

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 184**

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

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

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

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

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

**Answer:** D

**Explanation:**

A cross-site scripting (XSS) attack is a type of web application attack that injects malicious code into a web page that is then executed by the browser of a victim user. A reflected XSS attack is a type of XSS attack where the malicious code is embedded in a URL or a form parameter that is sent to the web server and then reflected back to the user's browser. In this case, the Nmap scan shows that the web server is vulnerable to a reflected XSS attack, as it returns the characters > and " without any filtering or encoding. The vulnerable parameter is id in the URL `http://172.31.15.2/1.php?id=2`.

**NEW QUESTION 189**

During an incident, some IoCs of possible ransomware contamination were found in a group of servers in a segment of the network. Which of the following steps



should be taken next?

- A. Isolation
- B. Remediation
- C. Reimaging
- D. Preservation

**Answer:** A

**Explanation:**

Isolation is the first step to take after detecting some indicators of compromise (IoCs) of possible ransomware contamination. Isolation prevents the ransomware from spreading to other servers or segments of the network, and allows the security team to investigate and contain the incident. Isolation can be done by disconnecting the infected servers from the network, blocking the malicious traffic, or applying firewall rules<sup>12</sup>.

References: 10 Things You Should Do After a Ransomware Attack, How to Recover from a Ransomware Attack: A Step-by-Step Guide

**NEW QUESTION 191**

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

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

**Answer:** CE

**Explanation:**

An incident manager should work with the legal and public relations entities to ensure correct processes are adhered to when communicating incident reporting to the general public, as a best practice. The legal entity can provide guidance on the legal implications and obligations of disclosing the incident, such as compliance with data protection laws, contractual obligations, and liability issues. The public relations entity can help craft the appropriate message and tone for the public communication, as well as manage the reputation and image of the organization in the aftermath of the incident. These two entities can help the incident manager balance the need for transparency and accountability with the need for confidentiality and security<sup>12</sup>. References: Incident Communication Templates, Incident Management: Processes, Best Practices & Tools - Atlassian

**NEW QUESTION 194**

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

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

**Answer:** D

**Explanation:**

A single pane of glass is a term that describes a unified view or interface that integrates multiple tools or data sources into one dashboard or console. A single pane of glass can help improve security operations by providing visibility, correlation, analysis, and alerting capabilities across various security controls and systems. A single pane of glass can also help reduce complexity, improve efficiency, and enhance decision making for security analysts. In this case, a security program was able to achieve a 30% improvement in MTTR by integrating security controls into a SIEM, which provides a single pane of glass for security operations. Official References: <https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack>

**NEW QUESTION 197**

Which of the following would an organization use to develop a business continuity plan?

- A. A diagram of all systems and interdependent applications
- B. A repository for all the software used by the organization
- C. A prioritized list of critical systems defined by executive leadership
- D. A configuration management database in print at an off-site location

**Answer:** C

**Explanation:**

A prioritized list of critical systems defined by executive leadership is the best option to use to develop a business continuity plan. A business continuity plan (BCP) is a system of prevention and recovery from potential threats to a company. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster<sup>1</sup>. A BCP should include a business impact analysis, which identifies the critical systems and processes that are essential for the continuity of the business operations, and the potential impacts of their disruption<sup>2</sup>. The executive leadership should be involved in defining the critical systems and their priorities, as they have the strategic vision and authority to make decisions that affect the whole organization<sup>3</sup>. A diagram of all systems and interdependent applications, a repository for all the software used by the organization, and a configuration management database in print at an off-site location are all useful tools for documenting and managing the IT infrastructure, but they are not sufficient to develop a comprehensive BCP that covers all aspects of the business continuity<sup>4</sup>. References: What Is a Business Continuity Plan (BCP), and How Does It Work?, Business continuity plan (BCP) in 8 steps, with templates, Business continuity planning | Business Queensland, Understanding the Essentials of a Business Continuity Plan

**NEW QUESTION 201**

When investigating a potentially compromised host, an analyst observes that the process BGInfo.exe (PID 1024), a Sysinternals tool used to create desktop

backgrounds containing host details, has been running for over two days. Which of the following activities will provide the best insight into this potentially malicious process, based on the anomalous behavior?

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

**Answer:** D

**Explanation:**

The activities taken by the process with PID 1024 will provide the best insight into this potentially malicious process, based on the anomalous behavior. BGInfo.exe is a legitimate tool that displays system information on the desktop background, but it can also be used by attackers to gather information about the compromised host or to disguise malicious processes<sup>12</sup>. By monitoring the activities of PID 1024, such as the files it accesses, the network connections it makes, or the commands it executes, the analyst can determine if the process is benign or malicious.  
References: bginfo.exe Windows process - What is it?, What is bginfo.exe? Is it Safe or a Virus? How to remove or fix it

**NEW QUESTION 205**

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

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

**Answer:** A

**Explanation:**

Mean time to detect (MTTD) is the best metric for an organization to focus on given recent investments in SIEM, SOAR, and a ticketing system. MTTD is a metric that measures how long it takes to detect a security incident or threat from the time it occurs. MTTD can be improved by using tools and processes that can collect, correlate, analyze, and alert on security data from various sources. SIEM, SOAR, and ticketing systems are examples of such tools and processes that can help reduce MTTD and enhance security operations. Official References: <https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack>

**NEW QUESTION 208**

Which of the following makes STIX and OpenIOC information readable by both humans and machines?

- A. XML
- B. URL
- C. OVAL
- D. TAXII

**Answer:** A

**Explanation:**

The correct answer is A. XML.  
STIX and OpenIOC are two standards for representing and exchanging cyber threat intelligence (CTI) information. STIX stands for Structured Threat Information Expression and OpenIOC stands for Open Location and Identity Coordinates. Both standards use XML as the underlying data format to encode the information in a structured and machine-readable way. XML stands for Extensible Markup Language and it is a widely used standard for defining and exchanging data on the web. XML uses tags, attributes, and elements to describe the structure and meaning of the data. XML is also human-readable, as it uses plain text and follows a hierarchical and nested structure.  
XML is not the only format that can be used to make STIX and OpenIOC information readable by both humans and machines, but it is the most common and widely supported one. Other formats that can be used include JSON, CSV, or PDF, depending on the use case and the preferences of the information producers and consumers. However, XML has some advantages over other formats, such as:  
? XML is more expressive and flexible than JSON or CSV, as it can define complex data types, schemas, namespaces, and validation rules.  
? XML is more standardized and interoperable than PDF, as it can be easily parsed, transformed, validated, and queried by various tools and languages.  
? XML is more compatible with existing CTI standards and tools than other formats, as it is the basis for STIX 1.x, TAXII 1.x, MAEC, CybOX, OVAL, and others.  
References:  
? 1 Introduction to STIX - GitHub Pages  
? 2 5 Best Threat Intelligence Feeds in 2023 (Free & Paid Tools) - Comparitech  
? 3 What Are STIX/TAXII Standards? - Anomali Resources  
? 4 What is STIX/TAXII? | Cloudflare  
? 5 Sample Use | TAXII Project Documentation - GitHub Pages  
? 6 Trying to retrieve xml data with taxii - Stack Overflow  
? 7 CISA AIS TAXII Server Connection Guide  
? 8 CISA AIS TAXII Server Connection Guide v2.0 | CISA

**NEW QUESTION 213**

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

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

**Answer:** B

**Explanation:**

The scanner is running in active mode, which is the cause of this issue. Active mode is a type of vulnerability scanning that sends probes or requests to the target

systems to test their responses and identify potential vulnerabilities. Active mode can provide more accurate and comprehensive results, but it can also cause more network traffic, performance degradation, or system instability. In some cases, active mode can trigger denial-of-service (DoS) conditions or crash the target systems, especially if they are not configured to handle the scanning requests or if they have underlying vulnerabilities that can be exploited by the scanner<sup>12</sup>. Therefore, the analyst should use caution when performing active mode scanning, and avoid scanning business-critical or sensitive systems without proper authorization and preparation<sup>3</sup>. References: Vulnerability Scanning for my Server - Spiceworks Community, Negative Impacts of Automated Vulnerability Scanners and How ... - Acunetix, Vulnerability Scanning Best Practices

#### NEW QUESTION 216

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

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

**Answer:** A

#### Explanation:

Integrating an IT service delivery ticketing system to track remediation and closure is the best approach to ensure all vulnerabilities are patched in accordance with the SLA. A ticketing system is a software tool that helps manage, organize, and track the tasks and workflows related to IT service delivery, such as incident management, problem management, change management, and vulnerability management. A ticketing system can help the security team to prioritize, assign, monitor, and document the remediation of the vulnerabilities, and to ensure that they are completed within the specified time frame and quality standards. A ticketing system can also help the security team to communicate and collaborate with other teams, such as the IT operations team, the development team, and the business stakeholders, and to report on the status and progress of the remediation efforts<sup>12</sup>. Creating a compensating control item, accepting the risk, and requesting an exception are not the best approaches to ensure all vulnerabilities are patched in accordance with the SLA, as they do not address the root cause of the problem, which is the large number of critical and high findings that require patching. These approaches may also introduce more risks or challenges for the security team, such as compliance issues, resource constraints, or business impacts<sup>3</sup>. References: What is a Ticketing System? | Freshservice ITSM Glossary, Vulnerability Management Best Practices, Compensating Controls: An Impermanent Solution to an IT ... - Tripwire, [Risk Acceptance in Information Security - Infosec Resources], [Exception Management - ISACA]

#### NEW QUESTION 217

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

```
..\./..\./boot.ini
```

Which of the following is being attempted?

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

**Answer:** A

#### Explanation:

The log entry ".....\boot.ini" is indicative of a directory traversal attack, where an attacker attempts to access files and directories that are stored outside the web root folder.

The log snippet ".....\boot.ini" is indicative of a directory traversal attack. This type of attack aims to access files and directories that are stored outside the web root folder. By manipulating variables that reference files with "..\" (dot-dot-slash), the attacker may be able to access arbitrary files and directories stored on the file system.

#### NEW QUESTION 218

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

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

**Answer:** D

#### Explanation:

Data loss prevention (DLP) is a tool that can prevent the exposure of PII outside of an organization by monitoring, detecting, and blocking sensitive data in motion, in use, or at rest.

#### NEW QUESTION 219

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 © 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 224

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

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

**Answer: A**

#### Explanation:

The correct answer is A. To provide metrics and test continuity controls.

A disaster recovery exercise is a simulation or a test of the disaster recovery plan, which is a set of procedures and resources that are used to restore the normal operations of an organization after a disaster or a major incident. The goal of a disaster recovery exercise is to provide metrics and test continuity controls, which are the measures that ensure the availability and resilience of the critical systems and processes of an organization. A disaster recovery exercise can help evaluate the effectiveness, efficiency, and readiness of the disaster recovery plan, as well as identify and address any gaps or issues .

The other options are not the best descriptions of the goal of a disaster recovery exercise. Verifying the roles of the incident response team (B) is a goal of an incident response exercise, which is a simulation or a test of the incident response plan, which is a set of procedures and roles that are used to detect, contain, analyze, and remediate an incident. Providing recommendations for handling vulnerabilities © is a goal of a vulnerability assessment, which is a process of identifying and prioritizing the weaknesses and risks in an organization's systems or network. Performing tests against implemented security controls (D) is a goal of a penetration test, which is an authorized and simulated attack on an organization's systems or network to evaluate their security posture and identify any vulnerabilities or misconfigurations.

#### NEW QUESTION 226

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 compromised12. References: Input Validation - OWASP, 4 Most Common Application Vulnerabilities and Possible Remediation

#### NEW QUESTION 230

Patches for two highly exploited vulnerabilities were released on the same Friday afternoon. Information about the systems and vulnerabilities is shown in the tables below:

Vulnerability name	Description
inter.drop	Remote Code Execution (RCE)
slow.roll	Denial of Service (DoS)

System name	Vulnerability	Network segment
manning	slow.roll	internal
brees	inter.drop	internal
brady	inter.drop	external
rogers	slow.roll; inter.drop	isolated vlan

Which of the following should the security analyst prioritize for remediation?

- A. rogers

- B. brady
- C. bree
- D. manning

**Answer:** B

**Explanation:**

Brady should be prioritized for remediation, as it has the highest risk score and the highest number of affected users. The risk score is calculated by multiplying the CVSS score by the exposure factor, which is the percentage of systems that are vulnerable to the exploit. Brady has a risk score of  $9 \times 0.8 = 7.2$ , which is higher than any other system. Brady also has 500 affected users, which is more than any other system. Therefore, patching brady would reduce the most risk and impact for the organization. The other systems have lower risk scores and lower numbers of affected users, so they can be remediated later.

**NEW QUESTION 231**

A threat hunter seeks to identify new persistence mechanisms installed in an organization's environment. In collecting scheduled tasks from all enterprise workstations, the following host details are aggregated:

Task name	Target process	Number of hosts	Task user account
RtkAudUService64_BG	C:\Windows\System32\RtkAudUService64.exe	502	NT Authority\SYSTEM
BatteryGaugeMaintenance	%ProgramData%\Lenovo\Plugins\BGHelper.exe	410	NT Authority\SYSTEM
RtHVBg_PushButton	C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe	870	NT Authority\SYSTEM
UpdateService	C:\Users\sam\AppData\Roaming\Temp\taskhw.exe	1	PROD\sam

Which of the following actions should the hunter perform first based on the details above?

- A. Acquire a copy of taskhw.exe from the impacted host
- B. Scan the enterprise to identify other systems with taskhw.exe present
- C. Perform a public search for malware reports on taskhw.exe.
- D. Change the account that runs the -caskh
- E. exe scheduled task

**Answer:** C

**Explanation:**

The first step should be to perform a public search for malware reports on taskhw.exe, as this file is suspicious for several reasons: it is located in a non-standard path, it has a high CPU usage, it is signed by an unknown entity, and it is only present on one host. A public search can help to determine if this file is a known malware or a legitimate program. If it is malware, the hunter can then take appropriate actions to remove it and prevent further damage. The other options are either premature or ineffective, as they do not provide enough information to assess the threat level of taskhw.exe. References: Cybersecurity Analyst+ - CompTIA, taskhw.exe Windows process - What is it? - file.net, Taskhostw.exe - What Is Taskhostw.exe & Is It Malware? - MalwareTips Forums

**NEW QUESTION 233**

A cybersecurity team lead is developing metrics to present in the weekly executive briefs. Executives are interested in knowing how long it takes to stop the spread of malware that enters the network.

Which of the following metrics should the team lead include in the briefs?

- A. Mean time between failures
- B. Mean time to detect
- C. Mean time to remediate
- D. Mean time to contain

**Answer:** D

**Explanation:**

Mean time to contain is the metric that the cybersecurity team lead should include in the weekly executive briefs, as it measures how long it takes to stop the spread of malware that enters the network. Mean time to contain is the average time it takes to isolate and neutralize an incident or a threat, such as malware, from the time it is detected. Mean time to contain is an important metric for evaluating the effectiveness and efficiency of the incident response process, as well as the potential impact and damage of the incident or threat. A lower mean time to contain indicates a faster and more successful response, which can reduce the risk and cost of the incident or threat. Mean time to contain can also be compared with other metrics, such as mean time to detect or mean time to remediate, to identify gaps or areas for improvement in the incident response process.

**NEW QUESTION 238**

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 243

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 245

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

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

**Answer: A**

#### Explanation:

Performing a tabletop drill based on previously identified incident scenarios is the best way to test the changes to the BC and DR plans without any impact to the business, as it is a low-cost and low-risk method of exercising the plans and identifying any gaps or issues. A tabletop drill is a type of BC/DR exercise that involves gathering key personnel from different departments and roles and discussing how they would respond to a hypothetical incident scenario. A tabletop drill does not involve any actual simulation or disruption of the systems or processes, but rather relies on verbal communication and documentation review. A tabletop drill can help to ensure that everyone is familiar with the BC/DR plans, that the plans reflect the current state of the organization, and that the plans are consistent and coordinated across different functions. The other options are not as suitable as performing a tabletop drill, as they involve more cost, risk, or impact to the business. Simulating an incident by shutting down power to the primary data center is a type of BC/DR exercise that involves creating an actual disruption or outage of a critical system or process, and observing how the organization responds and recovers. This type of exercise can provide a realistic assessment of the BC/DR capabilities, but it can also cause significant impact to the business operations, customers, and reputation. Migrating active workloads from the primary data center to the secondary location is a type of BC/DR exercise that involves switching over from one system or site to another, and verifying that the backup system or site can support the normal operations. This type of exercise can help to validate the functionality and performance of the backup system or site, but it can also incur high costs, complexity, and potential errors or failures. Comparing the current plan to lessons learned from previous incidents is a type of BC/DR activity that involves reviewing past experiences and outcomes, and identifying best practices or improvement opportunities. This activity can help to update and refine the BC/DR plans, but it does not test or validate them in a simulated or actual scenario

#### NEW QUESTION 249

.....



## 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