Free Questions for CS0-003 by dumpshq

Shared by Barber on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

A- SOAR

B- SIEM

C- MSP

D- NGFW

E- XDR

F- DLP

Answer:

A, B

Explanation:

SOAR (Security Orchestration, Automation and Response) and SIEM (Security Information and Event Management) are solutions that can help centralize the workload for the internal security team by collecting, correlating, and analyzing alerts from different sources, such as EDR. SOAR can also automate and streamline incident response workflows, while SIEM can provide dashboards and reports for security monitoring and compliance. Reference: What is EDR? Endpoint Detection & Response, How Does the Cyber Kill Chain Protect Against Attacks?; What is EDR Solution?, EDR solutions secure diverse endpoints through central monitoring

Question 2

Question Type: MultipleChoice

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

Options:

A- Utilize an RDP session on an unused workstation to evaluate the malware.

B- Disconnect and utilize an existing infected asset off the network.

C- Create a virtual host for testing on the security analyst workstation.

D- Subscribe to an online service to create a sandbox environment.

Answer:

D

Explanation:

A sandbox environment is a safe and isolated way to analyze malware without affecting the organization's network. An online service can provide a sandbox environment without requiring the security analyst to set up a virtual host or use an RDP session. Disconnecting and using an existing infected asset is risky and may not provide accurate results. Reference: Malware Analysis: Steps & Examples, Dynamic Analysis

Question 3

Question Type: MultipleChoice

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

Options:

A- Delivery

B- Reconnaissance

C- Exploitation

D- Weaponizatign

Answer:

D

Explanation:

Weaponization is the stage of the Cyber Kill Chain where the threat actor creates or modifies a malicious tool to use against a target. In this case, the threat actor compiles and tests a malicious downloader, which is a type of weaponized malware. Reference: Cybersecurity 101, The Cyber Kill Chain: The Seven Steps of a Cyberattack

Question 4

Question Type: **MultipleChoice**

A security team conducts a lessons-learned meeting after struggling to determine who should conduct the next steps following a security event. Which of the following should the team create to address this issue?

Options:

A- Service-level agreement

B- Change management plan

C- Incident response plan

D- Memorandum of understanding

Answer:

C

Explanation:

An incident response plan (IRP) is a document that defines the roles and responsibilities, procedures, and guidelines for responding to a security incident. It helps the security team to act quickly and effectively, minimizing the impact and cost of the incident. An IRP should specify who should conduct the next steps following a security event, such as containment, eradication, recovery, and analysis12.

Reference: CompTIA CySA+ CS0-003 Certification Study Guide, page 362; 6 Incident Response Steps to Take After a Security Event, section 2.

Question 5

Question Type: MultipleChoice

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

Options:

A- DLP

B- NAC

C- EDR

D- NIDS

Answer:

C

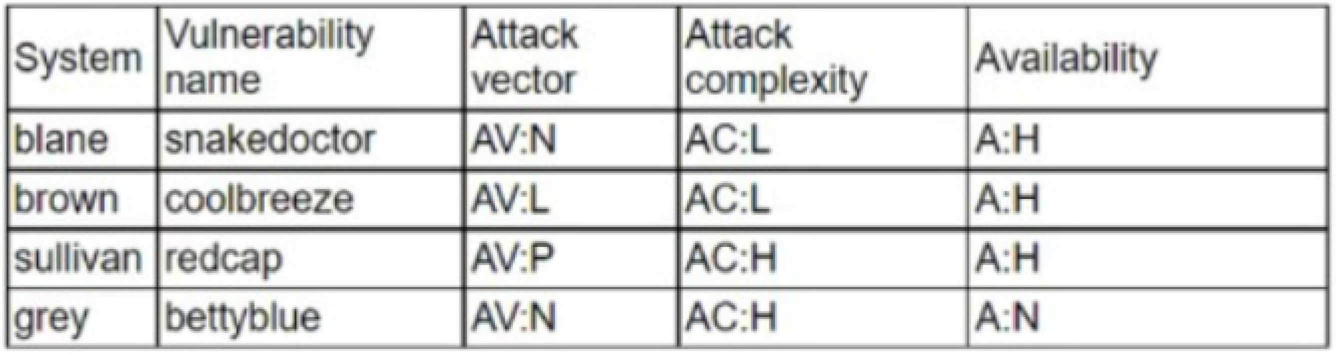
Explanation:

EDR stands for Endpoint Detection and Response, which is a tool that collects and aggregates data from various endpoints, such as laptops, servers, or mobile devices. EDR helps analysts monitor, detect, and respond to threats and incidents on the endpoints. EDR is more suitable than DLP (Data Loss Prevention), NAC (Network Access Control), or NIDS (Network Intrusion Detection System) for data collection and aggregation from endpoints.

Question 6

Question Type: **MultipleChoice**

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



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

Which of the following systems should be prioritized for patching?

Options:

A- brown

B- grey

C- blane

D- sullivan

Answer:

C

Explanation:

The system "blane" with the vulnerability name "snakedoctor" should be prioritized for patching as it has a network attack vector (AV:N), low attack complexity (AC:L), and high availability (A:H). These metrics indicate that it would be relatively easy to exploit this vulnerability over the internet, and the system is highly available. Reference: According to the CVSS v3.1 Specification Document, the exploitability metrics for CVSS are Attack Vector, Attack Complexity, Privileges Required, User Interaction, and Scope. These metrics measure how the vulnerability is accessed, the complexity of the attack, and the level of interaction and privileges required to exploit the vulnerability. The image shows a table with the values of these metrics for each system and vulnerability. Based on these values, the system "blane" has the highest exploitability score, as it has the most favorable conditions for an attacker. The other systems have either a lower attack vector, higher attack complexity, or lower availability, which make them less exploitable. Therefore, the system "blane" should be patched first.

Question 7

Question Type: MultipleChoice

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

Options:

A- Identify and discuss the lessons learned with the prior analyst.

B- Accept all findings and continue to investigate the next item target.

C- Review the steps that the previous analyst followed.

D- Validate the root cause from the prior analyst.

Answer:

C

Explanation:

Reviewing the steps that the previous analyst followed is the most important step during the transition, as it ensures continuity and consistency of the investigation. It also helps the new analyst to understand the current status, scope, and findings of the investigation, and to avoid repeating the same actions or missing any important details. The other options are either less important, premature, or potentially biased. Reference: CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 4: Incident Response and Management, page 191. Incident response best practices and tips, Tip 1: Always pack a jump bag.

Question 8

Question Type: MultipleChoice

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

Options:

A- STRIDE

B- Diamond Model of Intrusion Analysis

C- Cyber Kill Chain

D- MITRE ATT&CK

Answer:

B

Explanation:

The Diamond Model of Intrusion Analysis is a framework that describes the relationship between four components of a cyberattack: adversary, capability, infrastructure, and victim. It helps analysts understand the behavior and motivation of threat actors, as well as the tools and methods they use to compromise their targets12. Reference: Main Analytical Frameworks for Cyber Threat Intelligence, section 4; Strategies, tools, and frameworks for building an effective threat intelligence team, section 3.

Question 9

Question Type: MultipleChoice

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

Options:

A- The risk would not change because network firewalls are in use.

B- The risk would decrease because RDP is blocked by the firewall.

C- The risk would decrease because a web application firewall is in place.

D- The risk would increase because the host is external facing.

Answer:

B

Explanation:

Port 3389 is commonly used by Remote Desktop Protocol (RDP), which is a service that allows remote access to a system. A vulnerability on this port could allow an attacker to compromise the web server or use it as a pivot point to access other systems. However, if the firewall blocks this port, the risk of exploitation is reduced.

Question 10

Question Type: **MultipleChoice**

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

Options:

A- XDR logs

B- Firewall logs

C- IDS logs

D- MFA logs

Answer:

A

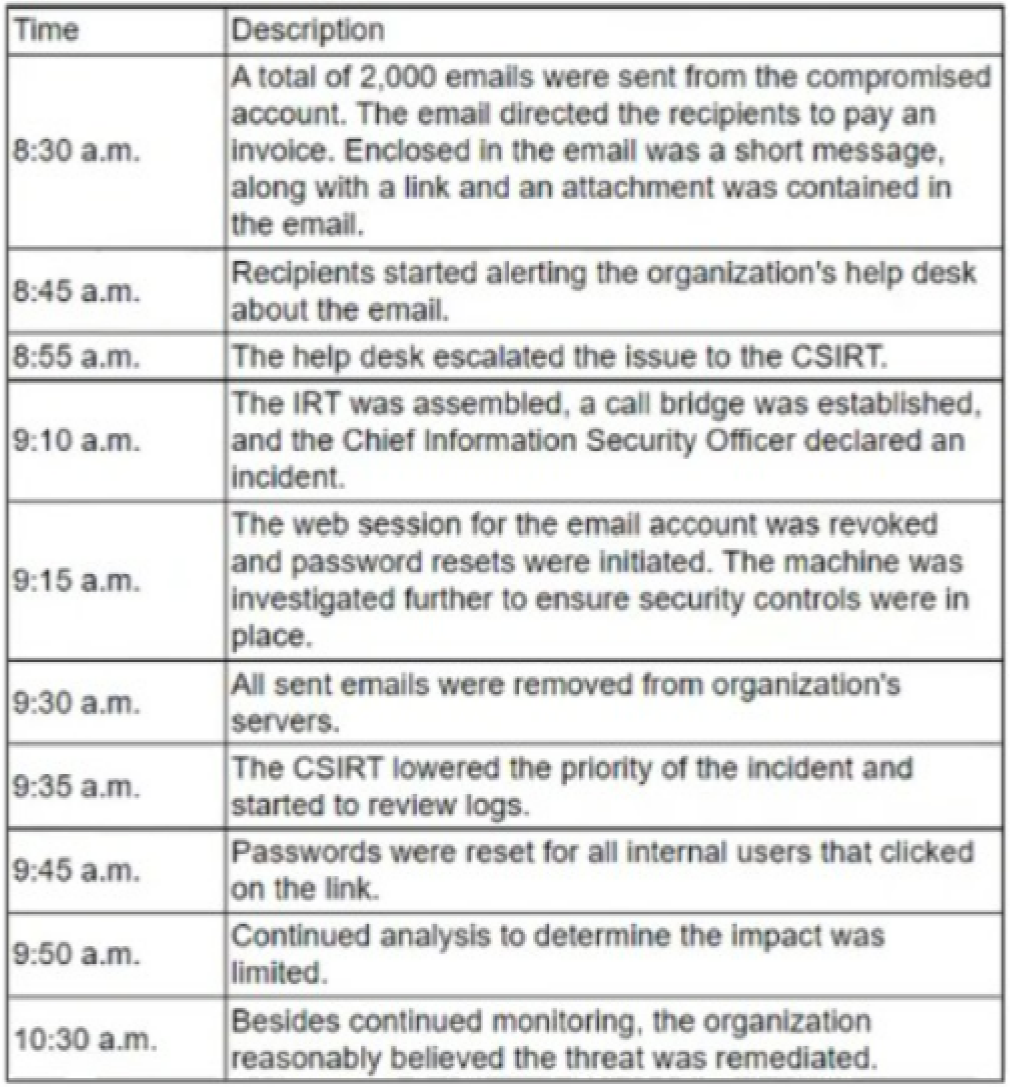
Explanation:

XDR logs will confirm the malware infection because XDR is a system that collects and analyzes data from multiple sources, such as endpoints, networks, cloud applications, and email security, to detect and respond to advanced threats12. XDR can provide a comprehensive view of the attack chain and the context of the malware infection. Firewall logs, IDS logs, and MFA logs are not sufficient to confirm the malware infection, as they only provide partial or indirect information about the network traffic, intrusion attempts, or user authentication. Reference: Cybersecurity Analyst+ - CompTIA, XDR: definition and benefits for MSPs| WatchGuard Blog, Extended detection and response - Wikipedia

Question 11

Question Type: **MultipleChoice**

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



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

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

Options:

A- 25 minutes

B- 40 minutes

C- 45 minutes

D- 2 hours

Answer:

B

Explanation:

The threat was detected from the time the emails were sent at 8:30 a.m. to when the recipients started alerting the organization's help desk about the email at 8:45 a.m., taking a total of 15 minutes. The detection time is the time elapsed between the occurrence of an incident and its discovery by the security team . The other options are either too short or too long based on the given information. Reference: : Detection Time : Incident Response Metrics: Mean Time to Detect and Mean Time to Respond

Question 12

Question Type: **MultipleChoice**

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

Options:

A- Hacktivist

B- Organized crime

C- Nation-state

D- Lone wolf

Answer:

A

Explanation:

Hacktivists are threat actors who use cyberattacks to promote a social or political cause, such as environmentalism, human rights, or democracy. They may target companies that they perceive as violating their values or harming the public interest. Hacktivists often use techniques such as defacing websites, launching denial-of-service attacks, or leaking sensitive data to expose or embarrass their targets12. Reference: An introduction to the cyber threat environment, page 3; What is a Threat Actor? Types & Examples of Cyber Threat Actors, section 2.

To Get Premium Files for CS0-003 Visit

https://www.p2pexams.com/products/cs0-003

For More Free Questions Visit

https://www.p2pexams.com/comptia/pdf/cs0-003

20%
DISCOUNT