CompTIA CySA+ Cybersecurity Analyst Certification all in One Exam Guide

Section: CompTIA Cybersecurity Analyst CySA plus Exams • **Total Questions:** 10 • **Format:** Verified Q&A

1. A security analyst identifies a device on which different malware was detected multiple times, even after the systems were scanned and cleaned several times. Which of the following actions would be most effective to ensure the device does not have residual malware?

(A) Update the device and scan offline in safe mode
(B) Replace the hard drive and reimage the device
(C) Upgrade the device to the latest OS version
(D) Download a secondary scanner and rescan the device

2. A security operations center analyst is using the command line to display specific traffic. The analyst uses the following command: `$ tshark -r file.pcap -Y 'http or udp'`. Which of the following will the command line display?

(A) Encrypted web requests and Domain Name System (DNS) traffic
(B) Unencrypted web requests and DNS traffic
(C) Neither encrypted nor unencrypted web and DNS traffic
(D) Both encrypted and unencrypted web and DNS traffic

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

(A) SMB share
(B) API endpoint
(C) SMTP notification
(D) SNMP trap

4. An analyst reviews a recent government alert on new zero-day threats and finds the following CVE metrics for the most critical of the vulnerabilities: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:W/RC:R. Which of the following represents the exploit code maturity of this critical vulnerability?

(A) E:U
(B) S:C
(C) RC:R
(D) AV:N
(E) AC:L

---

5. A cybersecurity analyst reviews infrastructure as code (IaC) scans of a new application to ensure the infrastructure requires authentication for incoming requests. After running the IaC configuration scanner, the analyst sees the following output:LOW: Ensure that Managed Identity provider is enabled for app services - Checkov (CKV_AZURE_71), MEDIUM: Ensure the web app has 'Client certificates (Incoming Client Certificates)' set - Checkov (CKV_AZURE_17), MEDIUM: Ensure web app redirects all HTTP traffic to HTTPS in Azure App Service - Checkov (CKV_AZURE_14), MEDIUM: Ensure that FTP register with Azure Active Directory is enabled on App Service - Checkov (CKV_AZURE_16), MEDIUM: Ensure that FTP deployments are disabled - Checkov (CKV_AZURE_78), LOW: Ensure that verbose logging is enabled for the web app - Checkov (CKV_AZURE_61), MEDIUM: Ensure that 'HTTP Version' is the latest if used to run the web app - Checkov (CKV_AZURE_18).Which of the following alerts should the analyst address to meet the requirement? (Select two).

(A) CKV_AZURE_14
(B) CKV_AZURE_16
(C) CKV_AZURE_17
(D) CKV_AZURE_18
(E) CKV_AZURE_71
(F) CKV_AZURE_78

---

6. 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

---

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

(A) Disable the user's network account and access to web resources.

(B) Make a copy of the files as a backup on the server.

(C) Place a legal hold on the device and the user's network share.

(D) Make a forensic image of the device and create a SHA-1 hash.

---

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

(A) RADIUS

(B) SDN

(C) ZTNA

(D) SWG

---

9. An analyst uses an AI platform to help correlate events. The AI output contains events that did not happen. This results in inaccurate correlations. Which of the following best describes what has occurred?

(A) Hallucinations

(B) Data exposure

(C) Malicious prompts

(D) Model poisoning

---

10. A security operations (SOC) manager develops response mechanisms as part of playbook development efforts... Which of the following is the most reliable source for this information?

(A) MITRE ATT&CK

(B) Cyber COBRA

(C) Diamond Model of Intrusion Analysis

(D) Cyber Kill Chain
