

DUMPS ARENA

CompTIA Advanced Security Practitioner (CASP+) Exam

CompTIA CAS-004

Version Demo

Total Demo Questions: 15

Total Premium Questions: 254

Buy Premium PDF

<https://dumpsarena.co>

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

city government's IT director was notified by the City council that the following cybersecurity requirements must be met to be awarded a large federal grant:

- + Logs for all critical devices must be retained for 365 days to enable monitoring and threat hunting.
- + All privileged user access must be tightly controlled and tracked to mitigate compromised accounts.
- + Ransomware threats and zero-day vulnerabilities must be quickly identified.

Which of the following technologies would BEST satisfy these requirements? (Select THREE).

A. Endpoint protection

B. Log aggregator

Log aggregator: A log aggregator is a tool that collects, parses, and stores logs from various sources, such as devices, applications, servers, etc. [A log aggregator can help meet the requirement of retaining logs for 365 days by providing a centralized and scalable storage solution1](#) .

C. Zero trust network access

D. PAM

PAM: PAM stands for privileged access management. It is a technology that controls and monitors the access of privileged users (such as administrators) to critical systems and data. PAM can help meet the requirement of controlling and tracking privileged user access by enforcing policies such as least privilege, multifactor authentication, password rotation, session recording, etc. .

E. Cloud sandbox

F. SIEM

SIEM: SIEM stands for security information and event management. It is a technology that analyzes and correlates logs from various sources to detect and respond to security incidents. SIEM can help meet the requirement of identifying ransomware threats and zero-day vulnerabilities by providing real-time alerts, threat intelligence feeds, incident response workflows, etc. .

G. NGFW

ANSWER: B D F**Explanation:**

B. Log aggregator: A log aggregator is a tool that collects, parses, and stores logs from various sources, such as devices, applications, servers, etc. [A log aggregator can help meet the requirement of retaining logs for 365 days by providing a centralized and scalable storage solution1](#) .

D. PAM: PAM stands for privileged access management. It is a technology that controls and monitors the access of privileged users (such as administrators) to critical systems and data. PAM can help meet the requirement of controlling and tracking privileged user access by enforcing policies such as least privilege, multifactor authentication, password rotation, session recording, etc. .

F. SIEM: SIEM stands for security information and event management. It is a technology that analyzes and correlates logs from various sources to detect and respond to security incidents. SIEM can help meet the requirement of identifying

ransomware threats and zero-day vulnerabilities by providing real-time alerts, threat intelligence feeds, incident response workflows, etc. .

QUESTION NO: 2

A small business would like to provide guests who are using mobile devices encrypted WPA3 access without first distributing PSKs or other credentials. Which of the following features will enable the business to meet this objective?

- A. Simultaneous Authentication of Equals
- B. Enhanced open
- C. Perfect forward secrecy
- D. Extensible Authentication Protocol

ANSWER: A**QUESTION NO: 3**

A company that uses AD is migrating services from LDAP to secure LDAP. During the pilot phase, services are not connecting properly to secure LDAP. Block is an excerpt of output from the troubleshooting session:

```
openssl s_client -host ldap1.comptia.com -port 636
CONNECTED(00000003)
***
-----BEGIN CERTIFICATE-----
***
-----END CERTIFICATE-----
Subject=/CN=*.comptia.com
Issuer=/DC=com/DC=danville/CN=chicago
```

Which of the following BEST explains why secure LDAP is not working? (Select TWO.)

- A. The clients may not trust idapt by default.
- B. The secure LDAP service is not started, so no connections can be made.
- C. Danvills.com is under a DDoS-inator attack and cannot respond to OCSP requests.
- D. Secure LDAP should be running on UDP rather than TCP.
- E. The company is using the wrong port. It should be using port 389 for secure LDAP.
- F. Secure LDAP does not support wildcard certificates.
- G. The clients may not trust Chicago by default.

ANSWER: B E

QUESTION NO: 4

A company's employees are not permitted to access company systems while traveling internationally. The company email system is configured to block logins based on geographic location, but some employees report their mobile phones continue to sync email traveling. Which of the following is the MOST likely explanation? (Select TWO.)

- A. Outdated escalation attack
- B. Privilege escalation attack
- C. VPN on the mobile device
- D. Unrestricted email administrator accounts
- E. Chief use of UDP protocols
- F. Disabled GPS on mobile devices

ANSWER: C F**QUESTION NO: 5**

Which of the following controls primarily detects abuse of privilege but does not prevent it?

- A. Off-boarding
- B. Separation of duties
- C. Least privilege
- D. Job rotation

ANSWER: A**QUESTION NO: 6**

A company's finance department acquired a new payment system that exports data to an unencrypted file on the system. The company implemented controls on the file so only appropriate personnel are allowed access. Which of the following risk techniques did the department use in this situation?

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

ANSWER: D

QUESTION NO: 7

A municipal department receives telemetry data from a third-party provider. The server collecting telemetry sits in the municipal department's screened network and accepts connections from the third party over HTTPS. The daemon has a code execution vulnerability from a lack of input sanitization of out-of-bound messages, and therefore, the cybersecurity engineers would like to implement mitigations. Which of the following actions, if combined, would BEST prevent exploitation of this vulnerability? (Select TWO).

- A. Implementing a TLS inspection proxy on-path to enable monitoring and policy enforcement
- B. Creating a Linux namespace on the telemetry server and adding to it the servicing HTTP daemon
- C. Installing and configuring filesystem integrity monitoring service on the telemetry server
- D. Implementing an EDR and alert on identified privilege escalation attempts to the SIEM
- E. Subscribing to a UTM service that enforces privacy controls between the internal network and the screened subnet
- F. Using the published data schema to monitor and block off nominal telemetry messages

ANSWER: A C**Explanation:**

A TLS inspection proxy can be used to monitor and enforce policy on HTTPS connections, ensuring that only valid traffic is allowed through and malicious traffic is blocked. Additionally, a filesystem integrity monitoring service can be installed and configured on the telemetry server to monitor for any changes to the filesystem, allowing any malicious changes to be detected and blocked.

QUESTION NO: 8

A DevOps team has deployed databases, event-driven services, and an API gateway as a PaaS solution that will support a new billing system. Which of the following security responsibilities will the DevOps team need to perform?

- A. Securely configure the authentication mechanisms
- B. Patch the infrastructure at the operating system
- C. Execute port scanning against the services
- D. Upgrade the service as part of life-cycle management

ANSWER: A**QUESTION NO: 9**

A security analyst is investigating a possible buffer overflow attack. The following output was found on a user's workstation:

```
graphic.linux_randomization.prg
```

Which of the following technologies would mitigate the manipulation of memory segments?

- A. NX bit
- B. ASLR
- C. DEP
- D. HSM

ANSWER: B

Explanation:

<https://eklitzke.org/memory-protection-and-aslr>

QUESTION NO: 10

Which of the following are risks associated with vendor lock-in? (Choose two.)

- A. The client can seamlessly move data.
- B. The vendor can change product offerings.
- C. The client receives a sufficient level of service.
- D. The client experiences decreased quality of service.
- E. The client can leverage a multicloud approach.
- F. The client experiences increased interoperability.

ANSWER: B D

Explanation:

Reference: <https://www.cloudflare.com/learning/cloud/what-is-vendor-lock-in/#:~:text=Vendor%20lock%2Din%20can%20become,may%20involve%20reformatting%20the%20data>

QUESTION NO: 11

An IT administrator is reviewing all the servers in an organization and notices that a server is missing crucial practice against a recent exploit that could gain root access.

Which of the following describes the administrator's discovery?

- A. A vulnerability
- B. A threat
- C. A breach
- D. A risk

ANSWER: A**Explanation:**

Reference: <https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained>

QUESTION NO: 12

A company created an external application for its customers. A security researcher now reports that the application has a serious LDAP injection vulnerability that could be leveraged to bypass authentication and authorization.

Which of the following actions would BEST resolve the issue? (Choose two.)

- A. Conduct input sanitization.
- B. Deploy a SIEM.
- C. Use containers.
- D. Patch the OS
- E. Deploy a WAF.
- F. Deploy a reverse proxy
- G. Deploy an IDS.

ANSWER: A E**Explanation:**

A WAF protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, and prevents any unauthorized data from leaving the app. It does this by adhering to a set of policies that help determine what traffic is malicious and what traffic is safe.

QUESTION NO: 13

A technician is reviewing the logs and notices a large number of files were transferred to remote sites over the course of three months. This activity then stopped. The files were transferred via TLS-protected HTTP sessions from systems that do not send traffic to those sites.

The technician will define this threat as:

- A. a decrypting RSA using obsolete and weakened encryption attack.
- B. a zero-day attack.
- C. an advanced persistent threat.
- D. an on-path attack.

ANSWER: C

Explanation:

Reference: <https://www.internetsociety.org/deploy360/tls/basics/>

QUESTION NO: 14

An attacker infiltrated an electricity-generation site and disabled the safety instrumented system. Ransomware was also deployed on the engineering workstation. The environment has back-to-back firewalls separating the corporate and OT systems. Which of the following is the MOST likely security consequence of this attack?

- A. A turbine would overheat and cause physical harm.
- B. The engineers would need to go to the historian.
- C. The SCADA equipment could not be maintained.
- D. Data would be exfiltrated through the data diodes.

ANSWER: A**QUESTION NO: 15**

An auditor needs to scan documents at rest for sensitive text. These documents contain both text and Images. Which of the following software functionalities must be enabled in the DLP solution for the auditor to be able to fully read these documents? (Select TWO).

- A. Document interpolation
- B. Regular expression pattern matching
- C. Optical character recognition functionality
- D. Baseline image matching
- E. Advanced rasterization
- F. Watermarking

ANSWER: A C