

# CompTIA

## Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam



**NEW QUESTION 1**

During a phishing exercise, a few privileged users ranked high on the failure list. The enterprise would like to ensure that privileged users have an extra security-monitoring control in place. Which of the following is the MOST likely solution?

- A. A WAF to protect web traffic
- B. User and entity behavior analytics
- C. Requirements to change the local password
- D. A gap analysis

**Answer: B**

**Explanation:**

User and entity behavior analytics (UEBA) is the best solution to monitor and detect unusual or malicious activity by privileged users who failed the phishing exercise. UEBA uses machine learning and behavioral analytics to establish a baseline of normal activity and identify anomalies that indicate potential threats. UEBA can help detect compromised credentials, insider threats, and advanced persistent threats that may evade traditional security solutions. The other options are either irrelevant or less effective for the given scenario.

**NEW QUESTION 2**

Users are reporting intermittent access issues with a new cloud application that was recently added to the network. Upon investigation, the system 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 3**

A security analyst discovered that a database administrator's workstation was compromised by malware. After examining the logs, 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.
- B) 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 4**

A company recently acquired a SaaS provider and needs to integrate its platform into the company's existing infrastructure without impact to the customer's experience. The SaaS provider does not have a mature security program. A recent vulnerability scan of the SaaS provider's systems shows multiple critical vulnerabilities attributed to very old and outdated OSs. Which of the following solutions would prevent these vulnerabilities from being introduced into the company's existing infrastructure?

- A. Segment the systems to reduce the attack surface if an attack occurs
- B. Migrate the services to new systems with a supported and patched OS.
- C. Patch the systems to the latest versions of the existing OSs
- D. Install anti-malware
- E. HIPS, and host-based firewalls on each of the systems

**Answer: B**

**NEW QUESTION 5**

A company requires a task to be carried by more than one person concurrently. This is an example of:

- A. separation of duties.
- B. dual control

- C. least privilege
- D. job rotation

**Answer: B**

**Explanation:**

Dual control is a security principle that requires two or more authorized individuals to perform a task concurrently. This reduces the risk of fraud, error, or misuse of sensitive assets or information. Verified References: <https://www.comptia.org/training/books/casp-cas-004-study-guide> , <https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/using-dual-control-to-mitigate-risk>

**NEW QUESTION 6**

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 7**

An organization is assessing the security posture of a new SaaS CRM system that handles sensitive PI I and identity information, such as passport numbers. The SaaS CRM system does not meet the organization's current security standards. The assessment identifies the following:

- 1) There will be a 520,000 per day revenue loss for each day the system is delayed going into production.
- 2) The inherent risk is high.
- 3) The residual risk is low.
- 4) There will be a staged deployment to the solution rollout to the contact center. Which of the following risk-handling techniques will BEST meet the organization's requirements?

- A. Apply for a security exemption, as the risk is too high to accept.
- B. Transfer the risk to the SaaS CRM vendor, as the organization is using a cloud service.
- C. Accept the risk, as compensating controls have been implemented to manage the risk.
- D. Avoid the risk by accepting the shared responsibility model with the SaaS CRM provider.

**Answer: D**

**NEW QUESTION 8**

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 9**

A security analyst at a global financial firm was reviewing the design of a cloud-based system to identify opportunities to improve the security of the architecture. The system was recently involved in a data breach after a vulnerability was exploited within a virtual machine's operating system. The analyst observed the VPC in which the system was located was not peered with the security VPC that contained the centralized vulnerability scanner due to the cloud provider's limitations. Which of the following is the BEST course of action to help prevent this situation in the near future?

- A. Establish cross-account trusts to connect all VPCs via API for secure configuration scanning.
- B. Migrate the system to another larger, top-tier cloud provider and leverage the additional VPC peering flexibility.
- C. Implement a centralized network gateway to bridge network traffic between all VPCs.
- D. Enable VPC traffic mirroring for all VPCs and aggregate the data for threat detection.

**Answer: A**

**Explanation:**

The BEST course of action for the security analyst to help prevent a similar situation in the near future is to Establish cross-account trusts to connect all VPCs via API for secure configuration scanning (A). Cross-account trusts allow for VPCs to be securely connected for the purpose of secure configuration scanning, which can help to identify and remediate vulnerabilities within the system.

#### NEW QUESTION 10

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 10

The Chief information Security Officer (CISO) of a small local bank has a compliance requirement that a third-party penetration test of the core banking application must be conducted annually. Which of the following services would fulfill the compliance requirement with the LOWEST resource usage?

- A. Black-box testing
- B. Gray-box testing
- C. Red-team hunting
- D. White-box testing
- E. Blue-team exercises

**Answer:** C

#### NEW QUESTION 11

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 12

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 13

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 18

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 20

A small company recently developed prototype technology for a military program. The company's security engineer is concerned about potential theft of the newly developed, proprietary information.

Which of the following should the security engineer do to BEST manage the threats proactively?

- A. Join an information-sharing community that is relevant to the company.
- B. Leverage the MITRE ATT&CK framework to map the TTR.
- C. Use OSINT techniques to evaluate and analyze the threats.
- D. Update security awareness training to address new threats, such as best practices for data security.

**Answer: A**

#### Explanation:

An information-sharing community is a group or network of organizations that share threat intelligence, best practices, and mitigation strategies related to cybersecurity. An information-sharing community can help the company proactively manage the threats of potential theft of its newly developed, proprietary information by providing timely and actionable insights, alerts, and recommendations. An information-sharing community can also enable collaboration and coordination among its members to enhance their collective defense and resilience. References: <https://us-cert.cisa.gov/ncas/tips/ST04-016>

<https://www.cisecurity.org/blog/what-is-an-information-sharing-community/>

#### NEW QUESTION 23

A company processes data subject to NDAs with partners that define the processing and storage constraints for the covered data. The agreements currently do not permit moving the covered data to the cloud, and the company would like to renegotiate the terms of the agreements.

Which of the following would MOST likely help the company gain consensus to move the data to the cloud?

- A. Designing data protection schemes to mitigate the risk of loss due to multitenancy
- B. Implementing redundant stores and services across diverse CSPs for high availability
- C. Emulating OS and hardware architectures to blur operations from CSP view
- D. Purchasing managed FIM services to alert on detected modifications to covered data

**Answer: A**

#### NEW QUESTION 24

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 25**

A Chief Information Officer (CIO) wants to implement a cloud solution that will satisfy the following requirements:

Support all phases of the SDLC. Use tailored website portal software.

Allow the company to build and use its own gateway software. Utilize its own data management platform.

Continue using agent-based security tools.

Which of the following cloud-computing models should the CIO implement?

- A. SaaS
- B. PaaS
- C. MaaS
- D. IaaS

**Answer:** D

**Explanation:**

Reference: <https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/>

**NEW QUESTION 28**

A penetration tester obtained root access on a Windows server and, according to the rules of engagement, is permitted to perform post-exploitation for persistence.

Which of the following techniques would BEST support this?

- A. Configuring systemd services to run automatically at startup
- B. Creating a backdoor
- C. Exploiting an arbitrary code execution exploit
- D. Moving laterally to a more authoritative server/service

**Answer:** B

**NEW QUESTION 29**

A security engineer at a company is designing a system to mitigate recent setbacks caused competitors that are beating the company to market with the new products. Several of the products incorporate propriety enhancements developed by the engineer's company. The network already includes a SEIM and a NIPS and requires 2FA for all user access. Which of the following system should the engineer consider NEXT to mitigate the associated risks?

- A. DLP
- B. Mail gateway
- C. Data flow enforcement
- D. UTM

**Answer:** A

**Explanation:**

A DLP system is the best option for the company to mitigate the risk of losing its proprietary enhancements to competitors. DLP stands for data loss prevention, which is a set of tools and policies that aim to prevent unauthorized access, disclosure, or exfiltration of sensitive data. DLP can monitor, filter, encrypt, or block data transfers based on predefined rules and criteria, such as content, source, destination, etc. DLP can help protect the company's intellectual property and trade secrets from being compromised by malicious actors or accidental leaks. Verified References: <https://www.comptia.org/training/books/casp-cas-004-study-guide> , <https://www.csoonline.com/article/3245746/what-is-dlp-data-loss-prevention-and-how-does-it-work.html>

**NEW QUESTION 33**

A security architect is reviewing the following proposed corporate firewall architecture and configuration:

```
DMZ architecture
Internet-----70.54.30.1-[Firewall_A]----192.168.1.0/24----[Firewall_B]----10.0.0.0/16----corporate net
```

```
Firewall_A ACL
10 PERMIT FROM 0.0.0.0/0 TO 192.168.1.0/24 TCP 80,443
20 DENY FROM 0.0.0.0/0 TO 0.0.0.0/0 TCP/UDP 0-65535
```

```
Firewall_B ACL
10 PERMIT FROM 10.0.0.0/16 TO 192.168.1.0/24 TCP 80,443
20 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535
30 PERMIT FROM 192.168.1.0/24 TO $DB_SERVERS TCP/UDP 3306
40 DENY FROM 192.168.1.0/24 TO 10.0.0.0/16 TCP/UDP 0-65535
```

Both firewalls are stateful and provide Layer 7 filtering and routing. The company has the following requirements:

Web servers must receive all updates via HTTP/S from the corporate network. Web servers should not initiate communication with the Internet.

Web servers should only connect to preapproved corporate database servers.

Employees' computing devices should only connect to web services over ports 80 and 443. Which of the following should the architect recommend to ensure all requirements are met in the MOST secure manner? (Choose two.)

- A. Add the following to Firewall\_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP 80,443
- B. Add the following to Firewall\_A: 15 PERMIT FROM 192.168.1.0/24 TO 0.0.0.0 TCP80,443
- C. Add the following to Firewall\_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535
- D. Add the following to Firewall\_B: 15 PERMIT FROM 0.0.0.0/0 TO 10.0.0.0/16 TCP/UDP 0-65535
- E. Add the following to Firewall\_B: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0 TCP/UDP 0- 65535
- F. Add the following to Firewall\_B: 15 PERMIT FROM 192.168.1.0/24 TO 10.0.2.10/32 TCP 80,443

**Answer:** AD

#### NEW QUESTION 36

A company publishes several APIs for customers and is required to use keys to segregate customer data sets. Which of the following would be BEST to use to store customer keys?

- A. A trusted platform module
- B. A hardware security module
- C. A localized key store
- D. A public key infrastructure

**Answer:** D

#### Explanation:

A public key infrastructure (PKI) is a system of certificates and keys that can provide encryption and authentication for APIs (application programming interfaces). A PKI can be used to store customer keys for accessing APIs and segregating customer data sets. A trusted platform module (TPM) is a hardware device that provides cryptographic functions and key storage, but it is not suitable for storing customer keys for APIs. A hardware security module (HSM) is similar to a TPM, but it is used for storing keys for applications, not for APIs. A localized key store is a software component that stores keys locally, but it is not as secure or scalable as a PKI. Verified References: <https://www.comptia.org/blog/what-is-pki> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

#### NEW QUESTION 39

A company just released a new video card. Due to limited supply and high demand, attackers are employing automated systems to purchase the device through the company's web store so they can resell it on the secondary market. The company's intended customers are frustrated. A security engineer suggests implementing a CAPTCHA system on the web store to help reduce the number of video cards purchased through automated systems. Which of the following now describes the level of risk?

- A. Inherent Low
- B. Mitigated
- C. Residual
- D. Transferred

**Answer:** A

#### NEW QUESTION 42

A security auditor needs to review the manner in which an entertainment device operates. The auditor is analyzing the output of a port scanning tool to determine the next steps in the security review. Given the following log output. The best option for the auditor to use NEXT is:

```
# nmap -F -T4 192.168.8.11
Starting Nmap 7.60
Nmap scan report for 192.168.8.11
Host is up (0.702s latency).
Not shown: 99 filtered ports
PORT      STATE      SERVICE
80/tcp    open      http
MAC Address: 04:18:18:EB:10:13 (ComptIA)
Nmap done: 1 IP address (1 host up) scanned in 3.18 seconds
```

- A. A SCAP assessment.
- B. Reverse engineering
- C. Fuzzing
- D. Network interception.

**Answer:** A

#### NEW QUESTION 43

An organization is assessing the security posture of a new SaaS CRM system that handles sensitive PII and identity information, such as passport numbers. The SaaS CRM system does not meet the organization's current security standards. The assessment identifies the following:

- 1- There will be a \$20,000 per day revenue loss for each day the system is delayed going into production.
- 2- The inherent risk is high.
- 3- The residual risk is low.
- 4- There will be a staged deployment to the solution rollout to the contact center.

Which of the following risk-handling techniques will BEST meet the organization's requirements?

- A. Apply for a security exemption, as the risk is too high to accept.



- B. Transfer the risk to the SaaS CRM vendor, as the organization is using a cloud service.
- C. Accept the risk, as compensating controls have been implemented to manage the risk.
- D. Avoid the risk by accepting the shared responsibility model with the SaaS CRM provider.

**Answer:** A

#### NEW QUESTION 48

A networking team was asked to provide secure remote access to all company employees. The team decided to use client-to-site VPN as a solution. During a discussion, the Chief Information Security Officer raised a security concern and asked the networking team to route the Internet traffic of remote users through the main office infrastructure. Doing this would prevent remote users from accessing the Internet through their local networks while connected to the VPN. Which of the following solutions does this describe?

- A. Full tunneling
- B. Asymmetric routing
- C. SSH tunneling
- D. Split tunneling

**Answer:** A

#### Explanation:

The concern is users operating in a spit tunnel config which is what is being described. Using a Full Tunnel would route traffic from all applications through a single tunnel. <https://cybernews.com/what-is-vpn/split-tunneling/>

#### NEW QUESTION 49

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 51

A security consultant needs to set up wireless security for a small office that does not have Active Directory. Despite the lack of central account management, the office manager wants to ensure a high level of defense to prevent brute-force attacks against wireless authentication. Which of the following technologies would BEST meet this need?

- A. Faraday cage
- B. WPA2 PSK
- C. WPA3 SAE
- D. WEP 128 bit

**Answer:** C

#### Explanation:

WPA3 SAE prevents brute-force attacks.

“WPA3 Personal (WPA-3 SAE) Mode is a static passphrase-based method. It provides better security than what WPA2 previously provided, even when a non-complex password is used, thanks to Simultaneous Authentication of Equals (SAE), the personal authentication process of WPA3.”

#### NEW QUESTION 52

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

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

**Answer:** A

#### NEW QUESTION 57

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

- A. Simultaneous Authentication of Equals
- B. Enhanced open



- C. Perfect forward secrecy
- D. Extensible Authentication Protocol

**Answer:** A

#### NEW QUESTION 62

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

graphic.linux\_randomization.prg

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

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

**Answer:** B

#### Explanation:

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

ASLR (Address Space Layout Randomization) is a technology that can mitigate the manipulation of memory segments caused by a buffer overflow attack. ASLR randomizes the location of memory segments, such as the stack, heap, or libraries, making it harder for an attacker to predict or control where to inject malicious code or overwrite memory segments. NX bit (No-eXecute bit) is a technology that can mitigate the execution of malicious code injected by a buffer overflow attack. NX bit marks certain memory segments as non-executable, preventing an attacker from running code in those segments. DEP (Data Execution Prevention) is a technology that can mitigate the execution of malicious code injected by a buffer overflow attack. DEP uses hardware and software mechanisms to mark certain memory regions as data-only, preventing an attacker from running code in those regions. HSM (Hardware Security Module) is a device that can provide cryptographic functions and key storage, but it does not mitigate the manipulation of memory segments caused by a buffer overflow attack. Verified References: <https://www.comptia.org/blog/what-is-aslr> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

#### NEW QUESTION 65

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 70

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 or 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 75

An organization's assessment of a third-party, non-critical vendor reveals that the vendor does not have cybersecurity insurance and IT staff turnover is high. The organization uses the vendor to move customer office equipment from one service location to another. The vendor acquires customer data and access to the business via an API. Given this information, which of the following is a noted risk?

- A. Feature delay due to extended software development cycles
- B. Financial liability from a vendor data breach
- C. Technical impact to the API configuration
- D. The possibility of the vendor's business ceasing operations

**Answer:** A

**Explanation:**

Reference: <https://legal.thomsonreuters.com/en/insights/articles/data-breach-liability>

**NEW QUESTION 76**

A Chief information Security Officer (CISO) has launched to create a rebuts BCP/DR plan for the entire company. As part of the initiative , the security team must gather data supporting s operational importance for the applications used by the business and determine the order in which the application must be back online. Which of the following be the FIRST step taken by the team?

- A. Perform a review of all policies an procedures related to BGP a and DR and created an educated educational module that can be assigned to at employees to provide training on BCP/DR events.
- B. Create an SLA for each application that states when the application will come back online and distribute this information to the business units.
- C. Have each business unit conduct a BIA and categories the application according to the cumulative data gathered.
- D. Implement replication of all servers and application data to back up detacenters that are geographically from the central datacenter and release an upload BPA to all clients.

**Answer:** C

**NEW QUESTION 81**

A company recently deployed a SIEM and began importing logs from a firewall, a file server, a domain controller a web server, and a laptop. A security analyst receives a series of SIEM alerts and prepares to respond. The following is the alert information:

Severity	Source device	Event info	Time (UTC)
Medium	abc-usa-fw01	RDP (3389) traffic from abc-admin-lp01 to abc-usa-fs1	1020:08
Low	abc-ger-dcl	Successful logon event for user jdoe on abc-usa-fs1	1020:34
Medium	abc-ger-fw01	RDP (3389) traffic from abc-usa-fs1 to abc-ger-fs1	1021:02
Low	abc-usa-fw01	SMB (445) traffic from abc-usa-fs1 to abc-web01	1020:51
Low	abc-usa-dcl	Successful logon event for user jdoe on abc-ger-fs1	1024:55
High	abc-usa-fw01	FTP (21) traffic from abc-ger-fs1 to abc-web01	1025:16
High	abc-web01	Successful logon event for user Administrator	1126:40

Which of the following should the security analyst do FIRST?

- A. Disable Administrator on abc-uaa-fsl, the local account is compromised
- B. Shut down the abc-usa-fs1 server, a plaintext credential is being used
- C. Disable the jdoe account, it is likely compromised
- D. Shut down abc-usa-fw01; the remote access VPN vulnerability is exploited

**Answer:** C

**Explanation:**

Based on the SIEM alerts, the security analyst should first disable the jdoe account, as it is likely compromised by an attacker. The alerts show that the jdoe account successfully logged on to the abc-usa-fs1 server, which is a file server, and then initiated SMB (445) traffic to the abc-web01 server, which is a web server. This indicates that the attacker may be trying to exfiltrate data from the file server to the web server. Disabling the jdoe account would help stop this unauthorized activity and prevent further damage.

Disabling Administrator on abc-usa-fsl, the local account is compromised, is not the first action to take, as it is not clear from the alerts if the local account is compromised or not. The alert shows that there was a successful logon event for Administrator on abc-usa-fsl, but it does not specify if it was a local or domain account, or if it was authorized or not. Moreover, disabling the local account would not stop the SMB traffic from jdoe to abc- web01.

Shutting down the abc-usa-fs1 server, a plaintext credential is being used, is not the first action to take, as it is not clear from the alerts if a plaintext credential is being used or not. The alert shows that there was RDP (3389) traffic from abc-admin1-logon to abc-usa-fsl, but it does not specify if the credential was encrypted or not. Moreover, shutting down the file server would disrupt its normal operations and affect other users.

Shutting down abc-usa-fw01; the remote access VPN vulnerability is exploited, is not the first action to take, as it is not clear from the alerts if the remote access VPN vulnerability is exploited or not. The alert shows that there was FTP (21) traffic from abc-usa-dcl to abc- web01, but it does not specify if it was related to the VPN or not. Moreover, shutting down the firewall would expose the network to other threats and affect other services. References: What is SIEM? | Microsoft Security, What is a SIEM Alert? | Cofense

**NEW QUESTION 82**

A company security engineer arrives at work to face the following scenario:

- 1) Website defacement
- 2) Calls from the company president indicating the website needs to be fixed Immediately because It Is damaging the brand
- 3) A Job offer from the company's competitor
- 4) A security analyst's investigative report, based on logs from the past six months, describing how lateral movement across the network from various IP addresses

originating from a foreign adversary country resulted in exfiltrated data  
Which of the following threat actors is MOST likely involved?

- A. Organized crime
- B. Script kiddie
- C. APT/nation-state
- D. Competitor

**Answer:** C

**Explanation:**

An Advanced Persistent Threat (APT) is an attack that is targeted, well-planned, and conducted over a long period of time by a nation-state actor. The evidence provided in the scenario indicates that the security analyst has identified a foreign adversary, which is strong evidence that an APT/nation-state actor is responsible for the attack. Resources: CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 5: "Advanced Persistent Threats," Wiley, 2018.  
<https://www.wiley.com/en-us/CompTIA+Advanced+Security+Practitioner+CASP%2B+Study+Guide%2C+2nd+Edition>  
-p-9781119396582

**NEW QUESTION 83**

A security is assisting the marketing department with ensuring the security of the organization's social media platforms. The two main concerns are:  
The Chief marketing officer (CMO) email is being used department wide as the username The password has been shared within the department  
Which of the following controls would be BEST for the analyst to recommend?

- A. Configure MFA for all users to decrease their reliance on other authentication.
- B. Have periodic, scheduled reviews to determine which OAuth configuration are set for each media platform.
- C. Create multiple social media accounts for all marketing user to separate their actions.
- D. Ensure the password being shared is sufficiently and not written down anywhere.

**Answer:** A

**Explanation:**

Configuring MFA for all users to decrease their reliance on other authentication is the best option to improve email security at the company. MFA stands for multi-factor authentication, which is a method of verifying a user's identity by requiring two or more factors, such as something the user knows (e.g., password), something the user has (e.g., token), or something the user is (e.g., biometric). MFA can prevent unauthorized access to email accounts even if the username or password is compromised or shared. Verified References: <https://www.comptia.org/training/books/casp-cas-004-study-guide> , <https://www.csoonline.com/article/3239144/what-is-mfa-how-multi-factor-authentication-works.html>

**NEW QUESTION 85**

A software development company is building a new mobile application for its social media platform. The company wants to gain its users' trust by reducing the risk of on-path attacks between the mobile client and its servers and by implementing stronger digital trust. To support users' trust, the company has released the following internal guidelines:

- \* Mobile clients should verify the identity of all social media servers locally.
- \* Social media servers should improve TLS performance of their certificate status.
- + Social media servers should inform the client to only use HTTPS.

Given the above requirements, which of the following should the company implement? (Select TWO).

- A. Quick UDP internet connection
- B. OCSP stapling
- C. Private CA
- D. DNSSEC
- E. CRL
- F. HSTS
- G. Distributed object model

**Answer:** BF

**Explanation:**

OCSP stapling and HSTS are the best options to meet the requirements of reducing the risk of on-path attacks and implementing stronger digital trust. OCSP stapling allows the social media servers to improve TLS performance by sending a signed certificate status along with the certificate, eliminating the need for the client to contact the CA separately. HSTS allows the social media servers to inform the client to only use HTTPS and prevent downgrade attacks. The other options are either irrelevant or less effective for the given scenario.

**NEW QUESTION 88**

A company just released a new video card. Due to limited supply and high demand, attackers are employing automated systems to purchase the device through the company's web store so they can resell it on the secondary market. The company's intended customers are frustrated. A security engineer suggests implementing a CAPTCHA system on the web store to help reduce the number of video cards purchased through automated systems. Which of the following now describes the level of risk?

- A. Inherent
- B. Low
- C. Mitigated
- D. Residual.
- E. Transferred

**Answer:** D

**NEW QUESTION 91**

Which of the following allows computation and analysis of data within a ciphertext without knowledge of the plaintext?



- A. Lattice-based cryptography
- B. Quantum computing
- C. Asymmetric cryptography
- D. Homomorphic encryption

**Answer:** D

**Explanation:**

Reference: <https://searchsecurity.techtarget.com/definition/cryptanalysis>

Homomorphic encryption is a type of encryption that allows computation and analysis of data within a ciphertext without knowledge of the plaintext. This means that encrypted data can be processed without being decrypted first, which enhances the security and privacy of the data. Homomorphic encryption can enable applications such as secure cloud computing, machine learning, and data analytics. References: <https://www.ibm.com/security/homomorphic-encryption>  
<https://www.synopsys.com/blogs/software-security/homomorphic-encryption/>

**NEW QUESTION 96**

A health company has reached the physical and computing capabilities in its datacenter, but the computing demand continues to increase. The infrastructure is fully virtualized and runs custom and commercial healthcare application that process sensitive health and payment information. Which of the following should the company implement to ensure it can meet the computing demand while complying with healthcare standard for virtualization and cloud computing?

- A. Hybrid IaaS solution in a single-tenancy cloud
- B. PaaS solution in a multi-tenancy cloud
- C. SaaS solution in a community cloud
- D. Private SaaS solution in a single tenancy cloud.

**Answer:** A

**Explanation:**

A hybrid IaaS solution in a single-tenancy cloud is the best option for the company to meet the computing demand while complying with healthcare standards for virtualization and cloud computing. A hybrid IaaS solution allows the company to use both on-premises and cloud-based resources to scale up its capacity and performance. A single-tenancy cloud ensures that the company's data and applications are isolated from other customers and have dedicated resources and security controls. Verified References:

<https://www.comptia.org/training/books/casp-cas-004-study-guide> , <https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html>

**NEW QUESTION 100**

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 104**

A customer reports being unable to connect to a website at [www.test.com](http://www.test.com) to consume services. The customer notices the web application has the following published cipher suite:

```
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
Signature hash algorithm:
sha256
Public key:
RSA (2048 Bits)
.htaccess config:
<VirtualHost> *:80>
ServerName www.test.com
Redirect / https://www.test.com
</VirtualHost>
<VirtualHost _default_:443>
ServerName www.test.com
DocumentRoot /usr/local/apache2/htdocs
SSLEngine On
...
</VirtualHost>
```

Which of the following is the MOST likely cause of the customer's inability to connect?

- A. Weak ciphers are being used.
- B. The public key should be using ECDSA.
- C. The default should be on port 80.
- D. The server name should be test.com.

**Answer:** A

**Explanation:**

Reference: <https://security.stackexchange.com/questions/23383/ssh-key-type-rsa-dsa-ecdsa-are-there-easy-answers-for-which-to-choose-when>



#### NEW QUESTION 107

Which of the following processes involves searching and collecting evidence during an investigation or lawsuit?

- A. E-discovery
- B. Review analysis
- C. Information governance
- D. Chain of custody

**Answer:** A

#### Explanation:

E-discovery is the process of searching and collecting evidence during an investigation or lawsuit. E-discovery involves identifying, preserving, processing, reviewing, analyzing, and producing electronically stored information (ESI) that is relevant for a legal case or investigation. E-discovery can be used to find evidence in email, business communications, social media, online documents, databases, and other digital sources. The other options are either irrelevant or less effective for the given scenario

#### NEW QUESTION 112

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 117

A user from the sales department opened a suspicious file attachment. The sales department then contacted the SOC to investigate a number of unresponsive systems, and the team successfully identified the file and the origin of the attack.

Which of the following is the NEXT step of the incident response plan?

- A. Remediation
- B. Containment
- C. Response
- D. Recovery

**Answer:** B

#### Explanation:

Reference: <https://www.sciencedirect.com/topics/computer-science/containment-strategy>

#### NEW QUESTION 119

A satellite communications ISP frequently experiences outages and degraded modes of operation over one of its legacy satellite links due to the use of deprecated hardware and software. Three days per week, on average, a contracted company must follow a checklist of 16 different high-latency commands that must be run in serial to restore nominal performance. The ISP wants this process to be automated.

Which of the following techniques would be BEST suited for this requirement?

- A. Deploy SOAR utilities and runbooks.
- B. Replace the associated hardware.
- C. Provide the contractors with direct access to satellite telemetry data.
- D. Reduce link latency on the affected ground and satellite segments.

**Answer:** A

#### Explanation:

Deploying SOAR (Security Orchestration Automation and Response) utilities and runbooks is the best technique for automating the process of restoring nominal performance on a legacy satellite link due to degraded modes of operation caused by deprecated hardware and software.

#### NEW QUESTION 121

A security analyst is investigating a series of suspicious emails by employees to the security team. The email appear to come from a current business partner and do not contain images or URLs. No images or URLs were stripped from the message by the security tools the company uses instead, the emails only include the following in plain text.

```
Test email sent from bp_app01 to external_client_app01_mailing_list.
```

Which of the following should the security analyst perform?

- A. Contact the security department at the business partner and alert them to the email event.
- B. Block the IP address for the business partner at the perimeter firewall.

- C. Pull the devices of the affected employees from the network in case they are infected with a zero-day virus.  
D. Configure the email gateway to automatically quarantine all messages originating from the business partner.

**Answer:** A

**Explanation:**

The best option for the security analyst to perform is to contact the security department at the business partner and alert them to the email event. The email appears to be a phishing attempt that tries to trick the employees into revealing their login credentials by impersonating a legitimate sender. The security department at the business partner should be notified so they can investigate the source and scope of the attack and take appropriate actions to protect their systems and users. Verified References: <https://www.comptia.org/training/books/casp-cas-004-study-guide> , <https://us-cert.cisa.gov/ncas/tips/ST04-014>

**NEW QUESTION 124**

A security architect for a large, multinational manufacturer needs to design and implement a security solution to monitor traffic. When designing the solution, which of the following threats should the security architect focus on to prevent attacks against the network?

- A. Packets that are the wrong size or length  
B. Use of any non-DNP3 communication on a DNP3 port  
C. Multiple solicited responses over time  
D. Application of an unsupported encryption algorithm

**Answer:** C

**NEW QUESTION 126**

A software development company is building a new mobile application for its social media platform. The company wants to gain its Users' trust by reducing the risk of on-path attacks between the mobile client and its servers and by implementing stronger digital trust. To support users' trust, the company has released the following internal guidelines:

- \* Mobile clients should verify the identity of all social media servers locally.
- \* Social media servers should improve TLS performance of their certificate status.
- \* Social media servers should inform the client to only use HTTPS.

Given the above requirements, which of the following should the company implement? (Select TWO).

- A. Quick UDP internet connection  
B. OCSP stapling  
C. Private CA  
D. DNSSEC  
E. CRL  
F. HSTS  
G. Distributed object model

**Answer:** BF

**Explanation:**

OCSP stapling and HSTS are the best options to meet the requirements of reducing the risk of on-path attacks and implementing stronger digital trust. OCSP stapling allows the social media servers to improve TLS performance by sending a signed certificate status along with the certificate, eliminating the need for the client to contact the CA separately. HSTS allows the social media servers to inform the client to only use HTTPS and prevent downgrade attacks.

**NEW QUESTION 129**

Given the following log snippet from a web server:

```
84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content/plugins/custom_plugin/check_user.php?userid=1 AND (SELECT 6810 FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(6810=6810,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content/plugins/custom_plugin/check_user.php?userid=(SELECT 7505 FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(7505=7505,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content/plugins/custom_plugin/check_user.php?userid=(SELECT CONCAT(0x7171787671,(SELECT (ELT(1399=1399,1))),0x71707a7871)) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:27 0100] "GET /wordpress/wp-content/plugins/custom_plugin/check_user.php?userid=1 UNION ALL SELECT CONCAT(0x7171787671,0x537653544175467a724f,0x71707a7871),NULL,NULL-- HTTP/1.1" 200 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"
```

Which of the following BEST describes this type of attack?

- A. SQL injection  
B. Cross-site scripting  
C. Brute-force  
D. Cross-site request forgery

**Answer:** A

**NEW QUESTION 134**

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 137**

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 139**

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<sup>12</sup>

. 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<sup>13</sup>.

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 engaged<sup>12</sup>.

? It is transparent to users and causes no performance degradation because it does not interfere with legitimate traffic or resources<sup>13</sup>.

? It allows integration with production and development networks seamlessly because it can create decoys that match the network topology and configuration<sup>13</sup>.

? It enables the security team to hunt and investigate live exploitation techniques because it can record and analyze the attacker's activities on the decoys<sup>13</sup>.

**NEW QUESTION 144**

Which of the following terms refers to the delivery of encryption keys to a CASB or a third-party entity?

- A. Key sharing
- B. Key distribution
- C. Key recovery
- D. Key escrow

**Answer:** D

**Explanation:**

Key escrow is a process that involves storing encryption keys with a trusted third party, such as a CASB (Cloud Access Security Broker) or a government agency. Key escrow can enable authorized access to encrypted data in case of emergencies, legal issues, or data recovery. However, key escrow also introduces some risks and challenges, such as trust, security, and privacy. References: <https://www.techopedia.com/definition/1772/key-escrow>

<https://searchsecurity.techtarget.com/definition/key-escrow>

#### NEW QUESTION 146

An organization's finance system was recently attacked. A forensic analyst is reviewing the contents of the compromised files for credit card data. Which of the following commands should the analyst run to BEST determine whether financial data was lost?

- A. `grep -v '^4[0-9]{12}(:[0-9]{3})?$' file`
- B. `grep '^4[0-9]{12}(:[0-9]{3})?$' file`
- C. `grep '^6(?:011|5[0-9]{2})[0-9]{12}?' file`
- D. `grep -v '^6(?:011|5[0-9]{2})[0-9]{12}?' file`

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

**Answer: C**

#### NEW QUESTION 148

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 149

Which of the following agreements includes no penalties and can be signed by two entities that are working together toward the same goal?

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

**Answer: A**

#### NEW QUESTION 150

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 151**

**SIMULATION**

An IPSec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram.

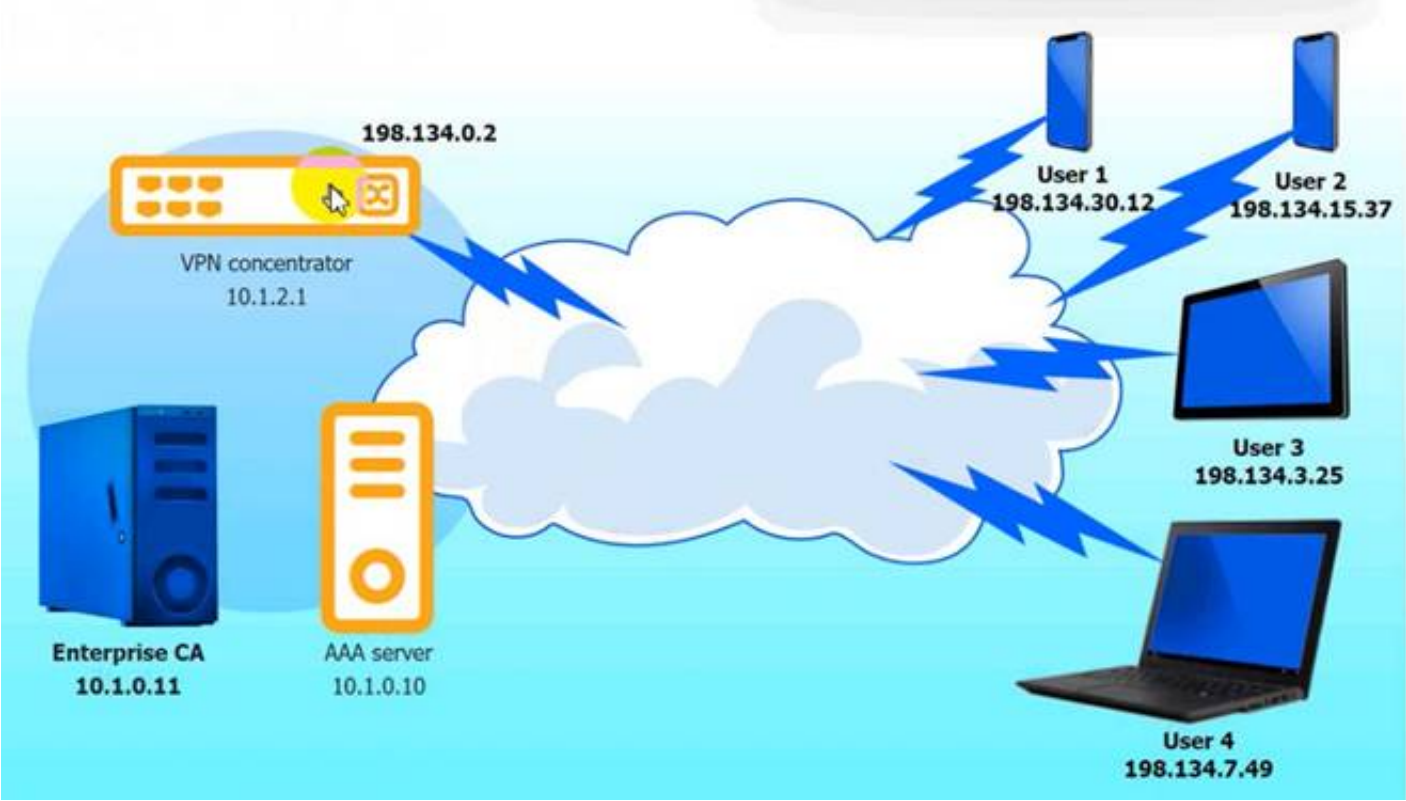
Complete the configuration files to meet the following requirements:

- The EAP method must use mutual certificate-based authentication (With issued client certificates).
- The IKEv2 Cipher suite must be configured to the MOST secure authenticated mode of operation,
- The secret must contain at least one uppercase character, one lowercase character, one numeric character, and one special character, and it must meet a minimum length requirement of eight characters,

**INSTRUCTIONS**

Click on the AAA server and VPN concentrator to complete the configuration.

Fill in the appropriate fields and make selections from the drop-down menus.



VPN Concentrator:

VPN concentrator

Select proposal

peap  
blowfish256  
md5  
aes256ccm128  
aes128ctr  
cast128  
camellia256ctr  
tls  
ttls  
psk  
aes256gcm128

```

...
re-eap {
...
  proposals =
    ...
}
...
plugins {
  eap-radius {
    secret =
    server =
  }
}
...

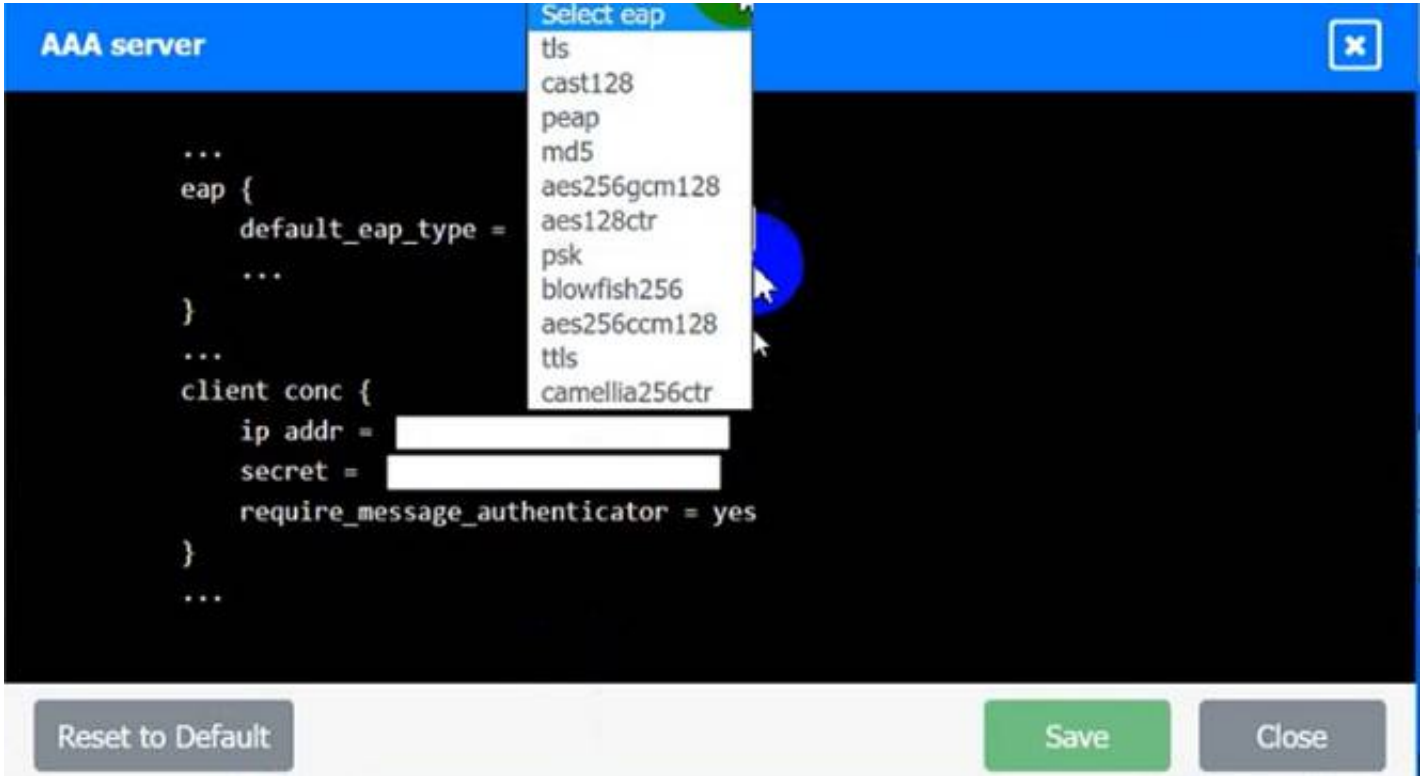
```

Reset to Default

Save

Close

AAA Server:



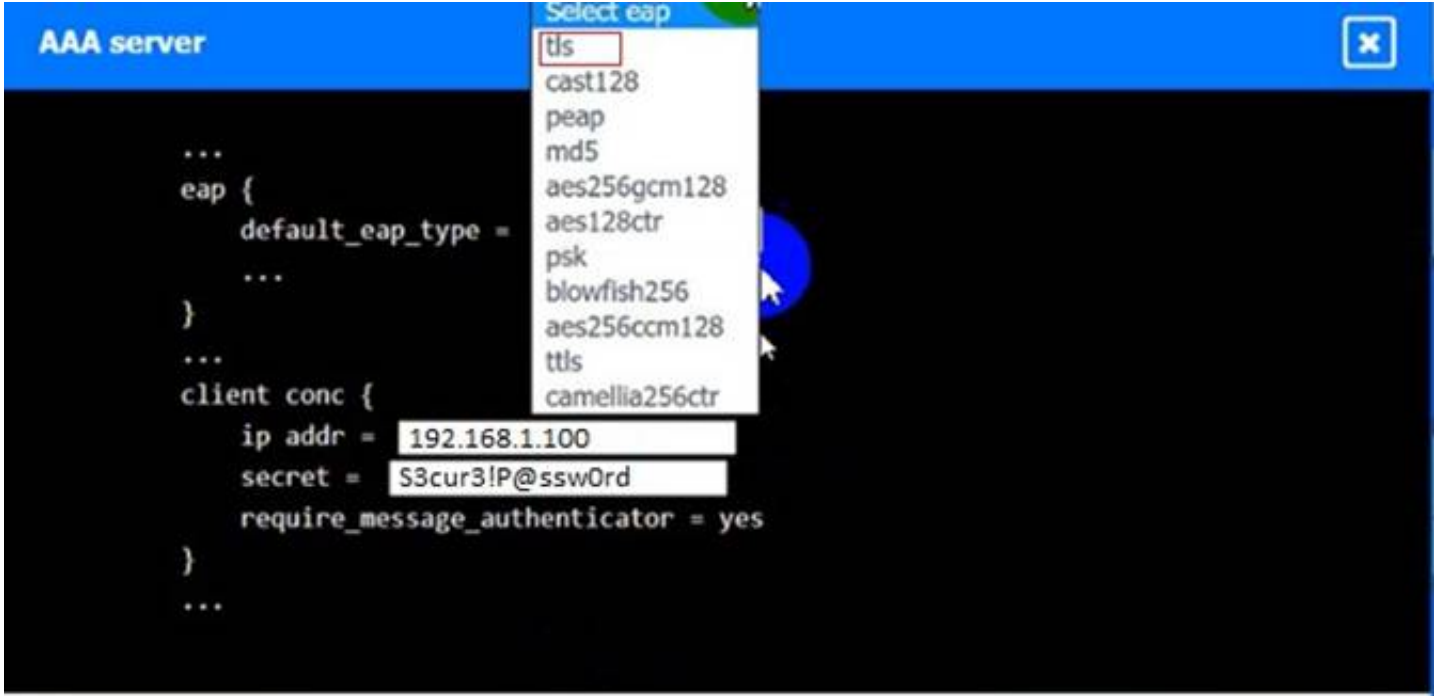
- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
VPN Concentrator:



AAA Server:



NEW QUESTION 154

Which of the following protocols is a low power, low data rate that allows for the creation of PAN networks?

- A. Zigbee
- B. CAN
- C. DNP3

D. Modbus

**Answer:** A

**Explanation:**

Reference: <https://urgentcomm.com/2007/11/01/connecting-on-a-personal-level/>

**NEW QUESTION 155**

A financial institution has several that currently employ the following controls:

- \* The servers follow a monthly patching cycle.
- \* All changes must go through a change management process.
- \* Developers and systems administrators must log into a jumpbox to access the servers hosting the data using two-factor authentication.
- \* The servers are on an isolated VLAN and cannot be directly accessed from the internal production network.

An outage recently occurred and lasted several days due to an upgrade that circumvented the approval process. Once the security team discovered an unauthorized patch was installed, they were able to resume operations within an hour. Which of the following should the security administrator recommend to reduce the time to resolution if a similar incident occurs in the future?

- A. Require more than one approver for all change management requests.
- B. Implement file integrity monitoring with automated alerts on the servers.
- C. Disable automatic patch update capabilities on the servers
- D. Enhanced audit logging on the jump servers and ship the logs to the SIEM.

**Answer:** B

**NEW QUESTION 160**

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>: cmpl $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)
0x014435da <+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 162**

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 165**

Correct Answer: (Answer option in bold)

Short but Comprehensive Explanation of Correct Answer Only: (Short Explanation based on CompTIA CASP+ documents and resources)

Verified References: (Related URLs AND Make sure Links are working and verified references)

=====

A security administrator wants to detect a potential forged sender claim in the envelope of an email. Which of the following should the security administrator implement? (Select TWO).

- A. MX record
- B. DMARC
- C. SPF
- D. DNSSEC
- E. S/MIME
- F. TLS

**Answer:** BC

**Explanation:**

DMARC (Domain-based Message Authentication, Reporting and Conformance) and SPF (Sender Policy Framework) are two mechanisms that can help detect and prevent email spoofing, which is the creation of email messages with a forged sender address. DMARC allows a domain owner to publish a policy that specifies how receivers should handle messages that fail authentication tests, such as SPF or DKIM (DomainKeys Identified Mail). SPF allows a domain owner to specify which mail servers are authorized to send email on behalf of their domain. By checking the DMARC and SPF records of the sender's domain, a receiver can verify if the email is from a legitimate source or not. Verified References:

? [https://en.wikipedia.org/wiki/Email\\_spoofing](https://en.wikipedia.org/wiki/Email_spoofing)

? <https://en.wikipedia.org/wiki/DMARC>

? [https://en.wikipedia.org/wiki/Sender\\_Policy\\_Framework](https://en.wikipedia.org/wiki/Sender_Policy_Framework)

**NEW QUESTION 168**

An organization recently recovered from an attack that featured an adversary injecting Malicious logic into OS bootloaders on endpoint devices Therefore, the organization decided to require the use of TPM for measured boot and attestation, monitoring each component from the IJEFI through the full loading of OS components. of the following TPM structures enables this storage functionality?

- A. Endorsement tickets
- B. Clock/counter structures
- C. Command tag structures with MAC schemes
- D. Platform configuration registers

**Answer:** D

**Explanation:**

TPMs provide the ability to store measurements of code and data that can be used to ensure that code and data remain unchanged over time. This is done through Platform Configuration Registers (PCRs), which are structures used to store measurements of code and data. The measurements are taken during the boot process and can be used to compare the state of the system at different times, which can be used to detect any changes to the system and verify that the system has not been tampered with.

**NEW QUESTION 170**

A home automation company just purchased and installed tools for its SOC to enable incident identification and response on software the company develops. The company would like to prioritize defenses against the following attack scenarios:

Unauthorized insertions into application development environments

Authorized insiders making unauthorized changes to environment configurations

Which of the following actions will enable the data feeds needed to detect these types of attacks on development environments? (Choose two.)

- A. Perform static code analysis of committed code and generate summary reports.
- B. Implement an XML gateway and monitor for policy violations.
- C. Monitor dependency management tools and report on susceptible third-party libraries.
- D. Install an IDS on the development subnet and passively monitor for vulnerable services.
- E. Model user behavior and monitor for deviations from normal.
- F. Continuously monitor code commits to repositories and generate summary logs.

**Answer:** EF

**Explanation:**

Modeling user behavior and monitoring for deviations from normal and continuously monitoring code commits to repositories and generating summary logs are actions that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes to environment configurations. Modeling user behavior and monitoring for deviations from normal is a technique that uses baselines, analytics, machine learning, or other methods to establish normal patterns of user activity and identify anomalies or outliers that could indicate malicious or suspicious behavior. Modeling user behavior and monitoring for deviations from normal can help detect unauthorized insertions into application development environments, as it can alert on unusual or unauthorized access attempts, commands, actions, or transactions by users. Continuously monitoring code commits to



repositories and generating summary logs is a technique that uses tools, scripts, automation, or other methods to track and record changes made to code repositories by developers, testers, reviewers, or other parties involved in the software development process. Continuously monitoring code commits to repositories and generating summary logs can help detect authorized insiders making unauthorized changes to environment configurations, as it can audit and verify the source, time, reason, and impact of code changes made by authorized users. Performing static code analysis of committed code and generate summary reports is not an action that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes to environment configurations, but an action that will enable the data feeds needed to detect vulnerabilities, errors, bugs, or quality issues in committed code. Implementing an XML gateway and monitor for policy violations is not an action that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes to environment configurations, but an action that will enable the data feeds needed to protect XML-based web services from threats or attacks by validating XML messages against predefined policies. Monitoring dependency management tools and report on susceptible third-party libraries is not an action that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes to environment configurations, but an action that will enable the data feeds needed to identify outdated or vulnerable third-party libraries used in software development projects. Installing an IDS (intrusion detection system) on the development subnet and passively monitor for vulnerable services is not an action that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes

**NEW QUESTION 172**

A security analyst discovered that the company's WAF was not properly configured. The main web server was breached, and the following payload was found in one of the malicious requests:

```
(&(objectClass=*)(objectClass=*))(&(objectClass=void)(type=admin))
```

Which of the following would BEST mitigate this vulnerability?

- A. Network intrusion prevention
- B. Data encoding
- C. Input validation
- D. CAPTCHA

**Answer: C**

**NEW QUESTION 177**

The goal of a Chief information Security Officer (CISO) providing up-to-date metrics to a bank's risk committee is to ensure:

- A. Budgeting for cybersecurity increases year over year.
- B. The committee knows how much work is being done.
- C. Business units are responsible for their own mitigation.
- D. The bank is aware of the status of cybersecurity risks

**Answer: A**

**NEW QUESTION 180**

Which of the following is a benefit of using steganalysis techniques in forensic response?

- A. Breaking a symmetric cipher used in secure voice communications
- B. Determining the frequency of unique attacks against DRM-protected media
- C. Maintaining chain of custody for acquired evidence
- D. Identifying least significant bit encoding of data in a .wav file

**Answer: D**

**Explanation:**

Steganalysis is the process of detecting hidden data in files or media, such as images, audio, or video. One technique of steganalysis is to identify least significant bit encoding, which is a method of hiding data by altering the least significant bits of each byte in a file. For example, a .wav file could contain hidden data encoded in the least significant bits of each audio sample. Steganalysis techniques can help forensic responders to discover hidden evidence or malicious payloads.

Breaking a symmetric cipher, determining the frequency of attacks, or maintaining chain of custody are not related to steganalysis. Verified References:

<https://www.comptia.org/blog/what-is-steganography> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

**NEW QUESTION 183**

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 188**

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. AWAF
- D. API mode

**Answer:** A

#### NEW QUESTION 190

A Chief Security Officer (CSO) is concerned about the number of successful ransomware attacks that have hit the company. The data indicates most of the attacks came through a fake email. The company has added training, and the CSO now wants to evaluate whether the training has been successful. Which of the following should the CSO implement?

- A. Simulating a spam campaign
- B. Conducting a sanctioned phishing attack
- C. Performing a risk assessment
- D. Executing a penetration test

**Answer:** A

#### Explanation:

A spam campaign is a mass distribution of unsolicited or fraudulent emails that may contain malicious links, attachments, or requests. Spam campaigns are often used by attackers to deliver ransomware, which is a type of malware that encrypts the victim's data and demands a ransom for its decryption.

Simulating a spam campaign would allow the Chief Security Officer (CSO) to evaluate whether the training has been successful in reducing the number of successful ransomware attacks that have hit the company, because it would:

? Test the employees' ability to recognize and avoid clicking on fake or malicious emails, which is one of the main vectors for ransomware infection.

? Measure the effectiveness of the training by comparing the click-through rate and the infection rate before and after the training.

? Provide feedback and reinforcement to the employees by informing them of their performance and reminding them of the best practices for email security.

#### NEW QUESTION 192

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 195

An organization is implementing a new identity and access management architecture with the following objectives:

Supporting MFA against on-premises infrastructure

Improving the user experience by integrating with SaaS applications

Applying risk-based policies based on location

Performing just-in-time provisioning

Which of the following authentication protocols should the organization implement to support these requirements?

- A. Kerberos and TACACS
- B. SAML and RADIUS
- C. OAuth and OpenID
- D. OTP and 802.1X

**Answer:** C

#### Explanation:

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/migrate-application-authentication-to-azure-active-directory>

OAuth and OpenID are two authentication protocols that can support the objectives of the organization. OAuth is a protocol that allows users to grant access to their resources on one site (or service) to another site (or service) without sharing their credentials. OpenID is a protocol that allows users to use an existing account to sign in to multiple websites without creating new passwords. Both protocols can support MFA, SaaS integration, risk-based policies, and just-in-time provisioning. References: <https://auth0.com/docs/protocols/oauth2> <https://openid.net/connect/>

#### NEW QUESTION 198

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 202

In preparation for the holiday season, a company redesigned the system that manages retail sales and moved it to a cloud service provider. The new infrastructure did not meet the company's availability requirements. During a postmortem analysis, the following issues were highlighted:

- \* 1. International users reported latency when images on the web page were initially loading.
- \* 2. During times of report processing, users reported issues with inventory when attempting to place orders.
- \* 3. Despite the fact that ten new API servers were added, the load across servers was heavy at peak times.

Which of the following infrastructure design changes would be BEST for the organization to implement to avoid these issues in the future?

- A. Serve static content via distributed CDNs, create a read replica of the central database and pull reports from there, and auto-scale API servers based on performance.
- B. Increase the bandwidth for the server that delivers images, use a CDN, change the database to a non-relational database, and split the ten API servers across two load balancers.
- C. Serve images from an object storage bucket with infrequent read times, replicate the database across different regions, and dynamically create API servers based on load.
- D. Serve static-content object storage across different regions, increase the instance size on the managed relational database, and distribute the ten API servers across multiple regions.

**Answer:** A

#### Explanation:

This solution would address the three issues as follows:

? Serving static content via distributed CDNs would reduce the latency for international users by delivering images from the nearest edge location to the user's request.

? Creating a read replica of the central database and pulling reports from there would offload the read-intensive workload from the primary database and avoid affecting the inventory data for order placement.

? Auto-scaling API servers based on performance would dynamically adjust the number of servers to match the demand and balance the load across them at peak times.

#### NEW QUESTION 203

A security engineer needs to implement a solution to increase the security posture of user endpoints by providing more visibility and control over local administrator accounts. The endpoint security team is overwhelmed with alerts and wants a solution that has minimal operational burdens. Additionally, the solution must maintain a positive user experience after implementation.

Which of the following is the BEST solution to meet these objectives?

- A. Implement Privileged Access Management (PAM), keep users in the local administrators group, and enable local administrator account monitoring.
- B. Implement PAM, remove users from the local administrators group, and prompt users for explicit approval when elevated privileges are required.
- C. Implement EDR, remove users from the local administrators group, and enable privilege escalation monitoring.
- D. Implement EDR, keep users in the local administrators group, and enable user behavior analytics.

**Answer:** B

#### Explanation:

PAM (Privileged Access Management) is a solution that can increase the security posture of user endpoints by providing more visibility and control over local administrator accounts. By implementing PAM, removing users from the local administrators group, and prompting users for explicit approval when elevated privileges are required, the security engineer can reduce the attack surface, prevent unauthorized access, and enforce the principle of least privilege. Implementing PAM, keeping users in the local administrators group, and enabling local administrator account monitoring may not provide enough control or visibility over local administrator accounts, as users could still abuse or compromise their privileges. Implementing EDR (Endpoint Detection and Response) may not provide enough control or visibility over local administrator accounts, as EDR is mainly focused on detecting and responding to threats, not managing privileges. Enabling user behavior analytics may not provide enough control or visibility over local administrator accounts, as user behavior analytics is mainly focused on identifying anomalies or risks in user activity, not managing privileges. Verified References: <https://www.comptia.org/blog/what-is-pam>  
<https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

#### NEW QUESTION 208

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 213

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 215

A business wants to migrate its workloads from an exclusively on-premises IT infrastructure to the cloud but cannot implement all the required controls. Which of the following BEST describes the risk associated with this implementation?

- A. Loss of governance
- B. Vendor lockout
- C. Compliance risk
- D. Vendor lock-in

**Answer: C**

#### NEW QUESTION 218

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 219

A company undergoing digital transformation is reviewing the resiliency of a CSP and is concerned about meeting SLA requirements in the event of a CSP incident.

Which of the following would be BEST to proceed with the transformation?

- A. An on-premises solution as a backup
- B. A load balancer with a round-robin configuration
- C. A multicloud provider solution
- D. An active-active solution within the same tenant

**Answer: C**

#### Explanation:

A multicloud provider solution is the best option for proceeding with the digital transformation while ensuring SLA (service level agreement) requirements in the event of a CSP (cloud service provider) incident. A multicloud provider solution is a strategy that involves using multiple CSPs for different cloud services or applications, such as infrastructure, platform, or software as a service. A multicloud provider solution can provide resiliency, redundancy, and availability for cloud services or applications, as it can distribute the workload and risk across different CSPs and avoid single points of failure or vendor lock-in. An on-premises solution as a backup is not a good option for proceeding with the digital transformation, as it could involve high costs, complexity, or maintenance for maintaining both cloud and on-premises resources, as well as affect the scalability or flexibility of cloud services or applications. A load balancer with a round-robin configuration is not a good option for proceeding with the digital transformation, as it could introduce latency or performance issues for cloud services or applications, as well as not provide sufficient resiliency or redundancy in case of a CSP incident. An active-active solution within the same tenant is not a good option for proceeding with the digital transformation, as it could still be affected by a CSP incident that impacts the entire tenant or region, as well as increase the costs or complexity of managing multiple instances of cloud services or applications. Verified References: <https://www.comptia.org/blog/what-is-multicloud>  
<https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

#### NEW QUESTION 222



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 227**

After a security incident, a network security engineer discovers that a portion of the company's sensitive external traffic has been redirected through a secondary ISP that is not normally used.

Which of the following would BEST secure the routes while allowing the network to function in the event of a single provider failure?

- A. Disable BGP and implement a single static route for each internal network.
- B. Implement a BGP route reflector.
- C. Implement an inbound BGP prefix list.
- D. Disable BGP and implement OSPF.

**Answer:** C

**Explanation:**

Defenses against BGP hijacks include IP prefix filtering, meaning IP address announcements are sent and accepted only from a small set of well-defined autonomous systems, and monitoring Internet traffic to identify signs of abnormal traffic flows.

**NEW QUESTION 232**

A network administrator who manages a Linux web server notices the following traffic: <http://corr.ptia.org/../../../../etc/shadow>

Which of the following is the BEST action for the network administrator to take to defend against this type of web attack?

- A. Validate the server certificate and trust chain.
- B. Validate the server input and append the input to the base directory path.
- C. Validate that the server is not deployed with default account credentials.
- D. Validate that multifactor authentication is enabled on the server for all user accounts.

**Answer:** B

**Explanation:**

The network administrator is noticing a web attack that attempts to access the /etc/shadow file on a Linux web server. The /etc/shadow file contains the encrypted passwords of all users on the system and is a common target for attackers. The attack uses a technique called directory traversal, which exploits a vulnerability in the web application that allows an attacker to access files or directories outside of the intended scope by manipulating the file path.

Validating the server input and appending the input to the base directory path would be the best action for the network administrator to take to defend against this type of web attack, because it would:

? Check the user input for any errors, malicious data, or unexpected values before processing it by the web application.

? Prevent directory traversal by ensuring that the user input is always relative to the base directory path of the web application, and not absolute to the root directory of the web server.

? Deny access to any files or directories that are not part of the web application's scope or functionality.

**NEW QUESTION 234**

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 238**

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 242**

Due to adverse events, a medium-sized corporation suffered a major operational disruption that caused its servers to crash and experience a major power outage. Which of the following should be created to prevent this type of issue in the future?

- A. SLA
- B. BIA
- C. BCM
- D. BCP
- E. RTO

**Answer: D**

**Explanation:**

A Business Continuity Plan (BCP) is a set of policies and procedures that outline how an organization should respond to and recover from disruptions [1]. It is designed to ensure that critical operations and services can be quickly restored and maintained, and should include steps to identify risks, develop plans to mitigate those risks, and detail the procedures to be followed in the event of a disruption. Resources:

CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 4: "Business Continuity Planning," Wiley, 2018. <https://www.wiley.com/en-us/CompTIA+Advanced+Security+Practitioner+CASP%2B+Study+Guide%2C+2nd+Edition-p-9781119396582>

**NEW QUESTION 246**

A Chief information Security Officer (CISO) is developing corrective-action plans based on the following from a vulnerability scan of internal hosts:

```
High CVSS: 10.0
CWE: CWE-119 "Buffer Overflow" Vulnerability (Windows) (CWE: 1.3.4.1.4.1.25423.1.0.000001)
Product detection result: nps/arpbrpnp/5.3.6 by SWS Version Detection (Remote) (CWE: 1.3.4.1.4.1.25423.1.0.000001)

Summary
This host is running SWS and is prone to buffer overflow vulnerability.
Vulnerability Detection Result: Installed version: 5.3.6
Fixed version: 5.3.10/5.4.2

Impact
Successful exploitation could allow attackers to execute arbitrary code and failed attempts will likely result in denial-of-service conditions. Impact Level: System/Application
```

Which of the following MOST appropriate corrective action to document for this finding?

- A. The product owner should perform a business impact assessment regarding the ability to implement a WAF.
- B. The application developer should use a static code analysis tool to ensure any application code is not vulnerable to buffer overflows.
- C. The system administrator should evaluate dependencies and perform upgrade as necessary.
- D. The security operations center should develop a custom IDS rule to prevent attacks buffer overflows against this server.

**Answer: A**

**NEW QUESTION 250**

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 252**

Company A acquired Company . During an audit, a security engineer found Company B's environment was inadequately patched. In response, Company A

placed a firewall between the two environments until Company B's infrastructure could be integrated into Company A's security program. Which of the following risk-handling techniques was used?

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

**Answer:** D

**Explanation:**

Reference: <https://www.pivotpointsecurity.com/blog/risk-tolerance-in-business/>

**NEW QUESTION 255**

An organization is designing a network architecture that must meet the following requirements:  
Users will only be able to access predefined services. Each user will have a unique allow list defined for access.  
The system will construct one-to-one subject/object access paths dynamically.  
Which of the following architectural designs should the organization use to meet these requirements?

- A. Peer-to-peer secure communications enabled by mobile applications
- B. Proxied application data connections enabled by API gateways
- C. Microsegmentation enabled by software-defined networking
- D. VLANs enabled by network infrastructure devices

**Answer:** C

**Explanation:**

Microsegmentation enabled by software-defined networking is an architectural design that can meet the requirements of allowing users to access only predefined services, having unique allow lists defined for each user, and constructing one- to-one subject/object access paths dynamically. Microsegmentation is a technique that divides a network into smaller segments or zones based on granular criteria, such as applications, services, users, or devices. Microsegmentation can provide fine-grained access control and isolation for network resources, preventing unauthorized or lateral movements within the network. Software-defined networking is a technology that decouples the control plane from the data plane in network devices, allowing centralized and programmable management of network functions and policies. Software-defined networking can enable microsegmentation by dynamically creating and enforcing network segments or zones based on predefined rules or policies. Peer-to-peer secure communications enabled by mobile applications is not an architectural design that can meet the requirements of allowing users to access only predefined services, having unique allow lists defined for each user, and constructing one-to-one subject/object access paths dynamically, as peer-to-peer secure communications is a technique that allows direct and encrypted communication between two or more parties without relying on a central server or intermediary. Proxied application data connections enabled by API gateways is not an architectural design that can meet the requirements of allowing users to access only predefined services, having unique allow lists defined for each user, and constructing one- to-one subject/object access paths dynamically, as proxied application data connections is a technique that allows indirect and filtered communication between applications or services through an intermediary device or service that can modify or monitor the traffic. VLANs (virtual local area networks) enabled by network infrastructure devices is not an architectural design that can meet the requirements of allowing users to access only predefined services, having unique allow lists defined for each user, and constructing one- to-one subject/object access paths dynamically, as VLANs are logical segments of a physical network that can group devices or users based on common criteria, such as function, department, or location. Verified References: <https://www.comptia.org/blog/what-is-microsegmentation> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

**NEW QUESTION 258**

A network architect is designing a new SD-WAN architecture to connect all local sites to a central hub site. The hub is then responsible for redirecting traffic to public cloud and datacenter applications. The SD-WAN routers are managed through a SaaS, and the same security policy is applied to staff whether working in the office or at a remote location. The main requirements are the following:

- \* 1. The network supports core applications that have 99.99% uptime.
- \* 2. Configuration updates to the SD-WAN routers can only be initiated from the management service.
- \* 3. Documents downloaded from websites must be scanned for malware.

Which of the following solutions should the network architect implement to meet the requirements?

- A. Reverse proxy, stateful firewalls, and VPNs at the local sites
- B. IDSs, WAFs, and forward proxy IDS
- C. DoS protection at the hub site, mutual certificate authentication, and cloud proxy
- D. IPSs at the hub, Layer 4 firewalls, and DLP

**Answer:** C

**NEW QUESTION 259**

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 260**

A university issues badges through a homegrown identity management system to all staff and students. Each week during the summer, temporary summer school students arrive and need to be issued a badge to access minimal campus resources. The security team received a report from an outside auditor indicating the

homegrown system is not consistent with best practices in the security field and leaves the institution vulnerable. Which of the following should the security team recommend FIRST?

- A. Investigating a potential threat identified in logs related to the identity management system
- B. Updating the identity management system to use discretionary access control
- C. Beginning research on two-factor authentication to later introduce into the identity management system
- D. Working with procurement and creating a requirements document to select a new IAM system/vendor

**Answer: D**

**Explanation:**

This is because the homegrown identity management system is not consistent with best practices and leaves the institution vulnerable, which means it needs to be replaced with a more secure and reliable solution. A new IAM system/vendor should be able to provide features such as role-based access control, two-factor authentication, auditing, and compliance that can enhance the security and efficiency of the identity management process. A requirements document can help define the scope, objectives, and criteria for selecting a suitable IAM system/vendor that meets the needs of the institution.

**NEW QUESTION 262**

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-2] \*\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 264**

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 266**

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 267**

A small business requires a low-cost approach to theft detection for the audio recordings it produces and sells.



Which of the following techniques will MOST likely meet the business's needs?

- A. Performing deep-packet inspection of all digital audio files
- B. Adding identifying filesystem metadata to the digital audio files
- C. Implementing steganography
- D. Purchasing and installing a DRM suite

**Answer: C**

**Explanation:**

Steganography is a technique that can hide data within other files or media, such as images, audio, or video. This can provide a low-cost approach to theft detection for the audio recordings produced and sold by the small business, as it can embed identifying information or watermarks in the audio files that can reveal their origin or ownership. Performing deep-packet inspection of all digital audio files may not be feasible or effective for theft detection, as it could consume a lot of bandwidth and resources, and it may not detect hidden data within encrypted packets. Adding identifying filesystem metadata to the digital audio files may not provide enough protection for theft detection, as filesystem metadata can be easily modified or removed by unauthorized parties. Purchasing and installing a DRM (digital rights management) suite may not be a low-cost approach for theft detection, as it could involve licensing fees and hardware requirements. Verified References: <https://www.comptia.org/blog/what-is-steganography> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

**NEW QUESTION 269**

An energy company is required to report the average pressure of natural gas used over the past quarter. A PLC sends data to a historian server that creates the required reports.

Which of the following historian server locations will allow the business to get the required reports in an and IT environment?

- A. In the environment, use a VPN from the IT environment into the environment.
- B. In the environment, allow IT traffic into the environment.
- C. In the IT environment, allow PLCs to send data from the environment to the IT environment.
- D. Use a screened subnet between the and IT environments.

**Answer: D**

**Explanation:**

A screened subnet is a network segment that separates two different environments, such as (operational technology) and IT (information technology), and provides security controls to limit and monitor the traffic between them. This would allow the business to get the required reports from the historian server without exposing the environment to unnecessary risks. Using a VPN, allowing IT traffic, or allowing PLCs to send data are less secure options that could compromise the environment. Verified References: <https://www.comptia.org/blog/what-is-operational-technology> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

**NEW QUESTION 270**

A company's SOC has received threat intelligence about an active campaign utilizing a specific vulnerability. The company would like to determine whether it is vulnerable to this active campaign.

Which of the following should the company use to make this determination?

- A. Threat hunting
- B. A system penetration test
- C. Log analysis within the SIEM tool
- D. The Cyber Kill Chain

**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 271**

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 274

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 laptops in the claims processing department.
- B. Require 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 276

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. No-execute
- C. Total memory encryption
- D. Virtual memory encryption

**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 and executing code. Execute never is a feature that allows each memory region to be tagged as not containing executable code by setting the execute never (XN) bit in the translation table entry. If the XN bit is set to 1, then any attempt to execute an instruction in that region results in a permission fault. If the XN bit is cleared to 0, then code can execute from that memory region. Execute never also prevents speculative instruction fetches from memory regions that are marked as non-executable, which can avoid undesirable side-effects or vulnerabilities. By enabling execute never, the developer can protect the process memory from being hijacked by malware. Verified References:

? <https://developer.arm.com/documentation/ddi0360/f/memory-management-unit/memory-access-control/execute-never-bits>

? <https://developer.arm.com/documentation/den0013/d/The-Memory-Management-Unit/Memory-attributes/Execute-Never>

? <https://developer.arm.com/documentation/ddi0406/c/System-Level-Architecture/Virtual-Memory-System-Architecture-VMSA-/Memory-access-control/Execute-never-restrictions-on-instruction-fetching>

#### NEW QUESTION 278

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions 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](#)**