Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

https://www.2passeasy.com/dumps/CAS-004/

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
Ann, a CIRT member, is conducting incident response activities on a network that consists
of several hundred virtual servers and thousands of endpoints and users. The network generates more than 10,000 log messages per second. The enterprise belong to a large, web-based cryptocurrency startup, Ann has distilled the relevant information into an easily digestible report for executive management . However, she still needs to collect evidence of the intrusion that caused the incident. Which of the following should Ann use to gather the required information?

A. Traffic interceptor log analysis
B. Log reduction and visualization tools
C. Proof of work analysis
D. Ledger analysis software

Answer: B

NEW QUESTION 3
A security engineer performed an assessment on a recently deployed web application. The engineer was able to exfiltration a company report by visiting the following URL:
www.intranet.abc.com/get-files.jsp?file=report.pdf
Which of the following mitigation techniques would be BEST for the security engineer to recommend?

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

Answer: A

Explanation:
Input validation is a technique that checks the user input for any errors, malicious data, or unexpected values before processing it by the application. Input validation can prevent many common web application attacks, such as:
? SQL injection, which exploits a vulnerability in the application's database query to execute malicious SQL commands.
? Cross-site scripting (XSS), which injects malicious JavaScript code into the application's web page to execute on the client-side browser.
? Directory traversal, which accesses files or directories outside of the intended scope by manipulating the file path.
In this case, the security engineer should recommend input validation as the best mitigation technique, because it would:
? Prevent the exfiltration of a company report by validating the file parameter in the
URL and ensuring that it matches a predefined list of allowed files or formats.
? Enhance the security of the web application by filtering out any malicious or invalid input from users or attackers.
? Be more effective and efficient than other techniques, such as firewall, WAF (Web Application Firewall), or DLP (Data Loss Prevention), which may not be able to detect or block all types of web application attacks.

NEW QUESTION 4
Users are reporting intermittent access issues with & new cloud application that was recently added to the network. Upon investigation, he scary administrator notices the human resources department Is able to run required queries with the new application, but the marketing department is unable to pull any needed reports on various resources using the new application. Which of the following MOST likely needs to be done to avoid this in the future?

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

Answer: A

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

NEW QUESTION 5
A security analyst discovered that a database administrator's workstation was compromised by malware. After examining the Jogs. the compromised workstation

was observed connecting to multiple databases through ODBC. The following query behavior was captured:

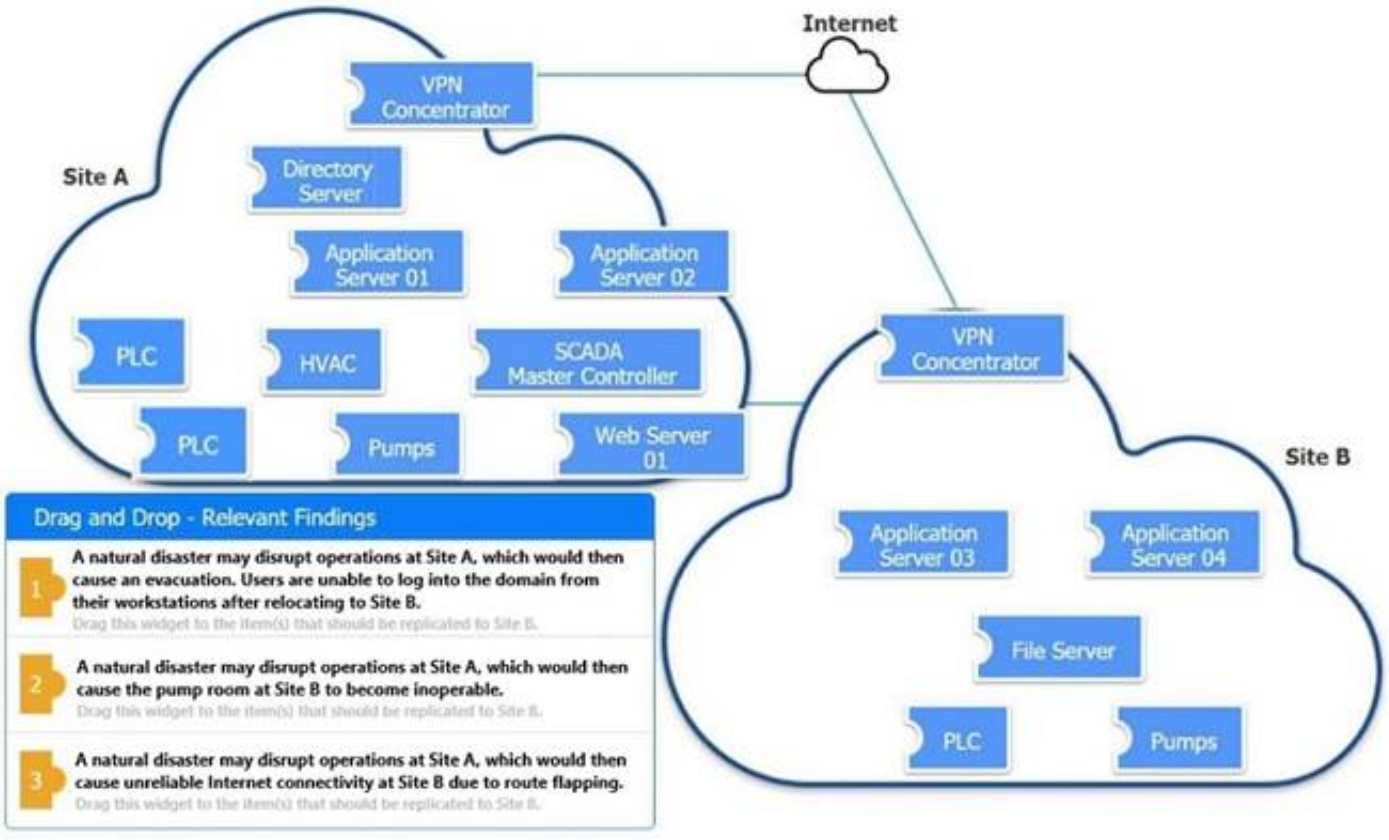
```
SELECT *
from ACCOUNTS
where * regexp '^[0-9]{4}[-]+[0-9]{4}[-]+[0-9]{4}[-]+[0-9]{4}$'
```

Assuming this query was used to acquire and exfiltrate data, which of the following types of
data was compromised, and what steps should the incident response plan contain?
A) Personal health information: Inform the human resources department of the breach and review the DLP logs.
) Account history; Inform the relationship managers of the breach and create new accounts for the affected users.
C) Customer IDs: Inform the customer service department of the breach and work to change the account numbers.
D) PAN: Inform the legal department of the breach and look for this data in dark web monitoring.

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

Answer: D

NEW QUESTION 6
DRAG DROP

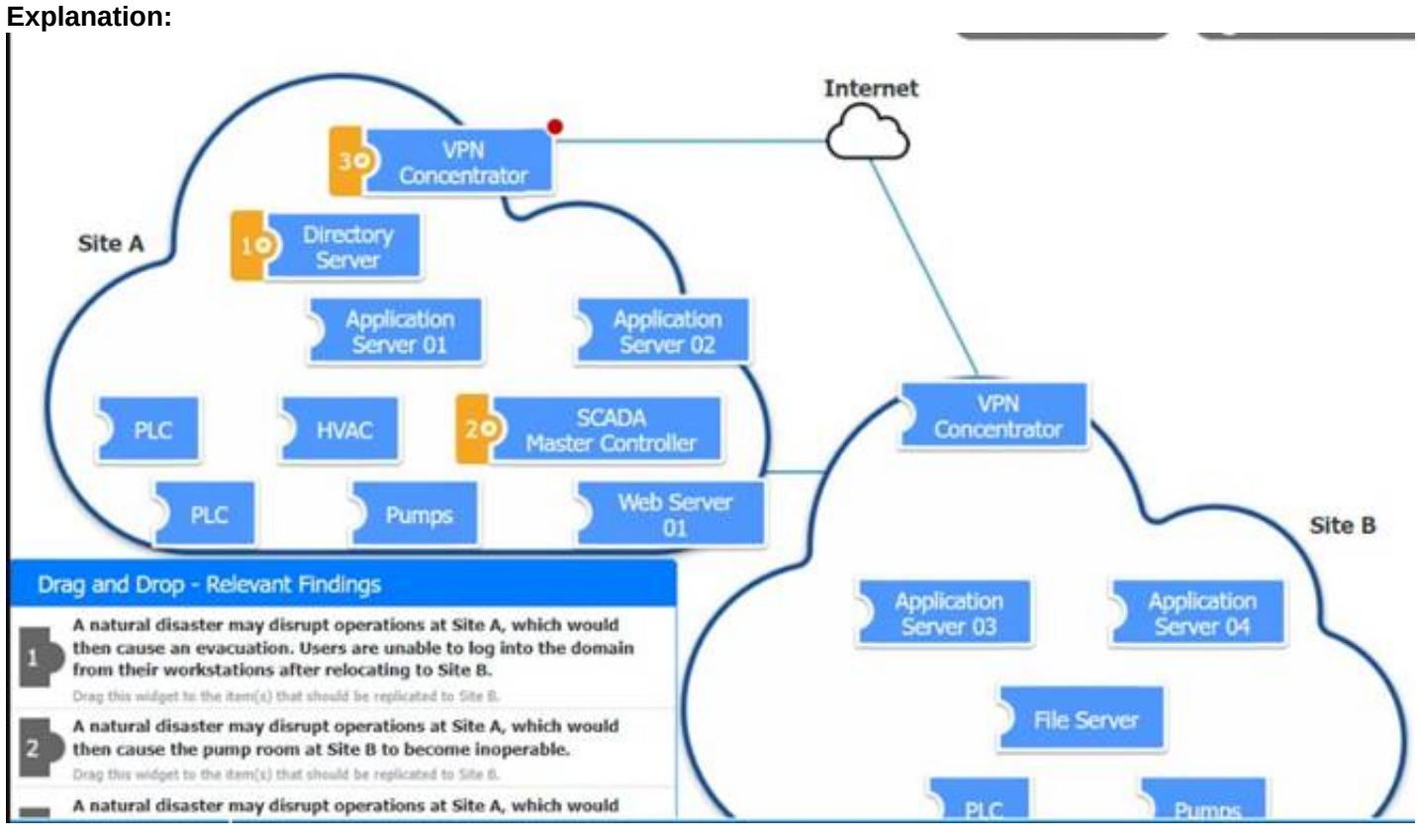


An organization is planning for disaster recovery and continuity of operations. INSTRUCTIONS
Review the following scenarios and instructions. Match each relevant finding to the affected host.
After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 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
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

An enterprise is undergoing an audit to review change management activities when promoting code to production. The audit reveals the following:
• Some developers can directly publish code to the production environment.
• Static code reviews are performed adequately.
• Vulnerability scanning occurs on a regularly scheduled basis per policy.
Which of the following should be noted as a recommendation within the audit report?

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

Answer: D

NEW QUESTION 10
An organization established an agreement with a partner company for specialized help desk services. A senior security officer within the organization Is tasked with providing documentation required to set up a dedicated VPN between the two entities. Which of the following should be required?

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

Answer: B

Explanation:
An ISA, or interconnection security agreement, is a document that should be required to set up a dedicated VPN between two entities that provide specialized help desk services. An ISA defines the technical and security requirements for establishing, operating, and maintaining a secure connection between two or more organizations. An ISA also specifies the roles and responsibilities of each party, the security controls and policies to be implemented, the data types and classifications to be exchanged, and the incident response procedures to be followed.
References: [CompTIA CASP+ Study Guide, Second Edition, page 36]

NEW QUESTION 15
A security operations center analyst is investigating anomalous activity between a database server and an unknown external IP address and gathered the following data:
• dbadmin last logged in at 7:30 a.m. and logged out at 8:05 a.m.
• A persistent TCP/6667 connection to the external address was established at 7:55 a.m. The connection is still active.
• Other than bytes transferred to keep the connection alive, only a few kilobytes of data transfer every hour since the start of the connection.
• A sample outbound request payload from PCAP showed the ASCII content: "JOIN
#community".
Which of the following is the MOST likely root cause?

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

Answer: D

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

NEW QUESTION 18
Users are claiming that a web server is not accessible. A security engineer logs for the site. The engineer connects to the server and runs netstat -an and receives the following output:

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

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

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

Answer: D

Explanation:
A denial of service (DoS) attack is a malicious attempt to disrupt the normal functioning of a server by overwhelming it with requests or traffic1. One possible indicator of a DoS attack is a large number of connections from a single source IP address1. In this case, the output of netstat -an shows that there are many connections from 213.37.55.67 with different port numbers and in TIME WAIT state23. This suggests that the attacker is sending many SYN packets to initiate connections but not completing them, thus exhausting the server's resources and preventing legitimate users from accessing it1.

NEW QUESTION 20
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 23
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 27
A company publishes several APIs for customers and is required to use keys to segregate customer data sets.
Which of the following would be BEST to use to store customer keys?

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

Answer: D

Explanation:
A public key infrastructure (PKI) is a system of certificates and keys that can provide encryption and authentication for APIs (application programming interfaces). A PKI can be used to store customer keys for accessing APIs and segregating customer data sets. A trusted platform module (TPM) is a hardware device that provides cryptographic functions and key storage, but it is not suitable for storing customer keys for APIs. A hardware security module (HSM) is similar to a TPM,

but it is used for storing keys for applications, not for APIs. A localized key store is a software component that stores keys locally, but it is not as secure or scalable as a PKI. Verified References: https://www.comptia.org/blog/what-is-pki https://partners.comptia.org/docs/default- source/resources/casp-content-guide

NEW QUESTION 29
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 32
A company just released a new video card. Due to limited supply and nigh demand, attackers are employing automated systems to purchase the device through the company's web store so they can resell it on the secondary market. The company's Intended customers are frustrated. A security engineer suggests implementing a CAPTCHA system on the web store to help reduce the number of video cards purchased through automated systems. Which of the following now describes the level of risk?

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

Answer: A

NEW QUESTION 37
A security auditor needs to review the manner in which an entertainment device operates. The auditor is analyzing the output of a port scanning tool to determine the next steps in the security review. Given the following log output.
The best option for the auditor to use NEXT is:

```
# nmap -F -T4 192.168.8.11
Starting Nmap 7.60
Nmap scan report for 192.168.8.11
Host is up (0.702s latency).
Not shown: 99 filtered ports
PORT    STATE   SERVICE
80/tcp  open    http
MAC Address: 04:18:18:E8:10:13 (CompTIA)
Nmap done: 1 IP address (1 host up) scanned in 3.18 seconds
```

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

Answer: A

NEW QUESTION 42
A development team created a mobile application that contacts a company’s back-end APIs housed in a PaaS environment. The APIs have been experiencing high processor utilization due to scraping activities. The security engineer needs to recommend a solution that will prevent and remedy the behavior.
Which of the following would BEST safeguard the APIs? (Choose two.)

A. Bot protection
B. OAuth 2.0
C. Input validation
D. Autoscaling endpoints
E. Rate limiting
F. CSRF protection

Answer: DE

Explanation:
Reference: https://stackoverflow.com/questions/3161548/how-do-i-prevent-site-scraping

NEW QUESTION 45
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 50
A security engineer estimates the company's popular web application experiences 100 attempted breaches per day. In the past four years, the company's data has been breached two times.
Which of the following should the engineer report as the ARO for successful breaches?

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

Answer: A

Explanation:
Reference: https://blog.netwrix.com/2020/07/24/annual-loss-expectancy-and-quantitative- risk-analysis/
The ARO (annualized rate of occurrence) for successful breaches is the number of times an event is expected to occur in a year. To calculate the ARO for successful breaches, the engineer can divide the number of breaches by the number of years. In this case, the company's data has been breached two times in four years, so the ARO is 2 / 4 = 0.5. The other options are incorrect calculations. Verified References: https://www.comptia.org/blog/what-is-risk-management https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 54
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 58
A company recently deployed a SIEM and began importing logs from a firewall, a file server, a domain controller a web server, and a laptop. A security analyst receives a series of SIEM alerts and prepares to respond. The following is the alert information:

Severity	Source device	Event info	Time (UTC)
Medium	abc-usa-fw01	RDP (3389) traffic from abc-admin-lp01 to abc-usa-fs1	1020:08
Low	abc-ger-dc1	Successful logon event for user jdoe on abc-usa-fs1	1020:34
Medium	abc-ger-fw01	RDP (3389) traffic from abc-usa-fs1 to abc-ger-fs1	1021:02
Low	abc-usa-fw01	SMB (445) traffic from abc-usa-fs1 to abc-web01	1020:51
Low	abc-usa-dc1	Successful logon event for user jdoe on abc-ger-fs1	1024:55
High	abc-usa-fw01	FTP (21) traffic from abc-ger-fs1 to abc-web01	1025:16
High	abc-web01	Successful logon event for user Administrator	1126:40

Which of the following should the security analyst do FIRST?

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

Answer: C

Explanation:
Based on the SIEM alerts, the security analyst should first disable the jdoe account, as it is likely compromised by an attacker. The alerts show that the jdoe account successfully logged on to the abc-usa-fsl server, which is a file server, and then initiated SMB (445) traffic to the abc-web01 server, which is a web server. This indicates that the attacker may be trying to exfiltrate data from the file server to the web server. Disabling the jdoe account would help stop this unauthorized activity and prevent further damage.
Disabling Administrator on abc-usa-fsl, the local account is compromised, is not the first action to take, as it is not clear from the alerts if the local account is compromised or not. The alert shows that there was a successful logon event for Administrator on abc-usa-fsl, but it does not specify if it was a local or domain account, or if it was authorized or not. Moreover, disabling the local account would not stop the SMB traffic from jdoe to abc- web01.
Shutting down the abc-usa-fsl server, a plaintext credential is being used, is not the first action to take, as it is not clear from the alerts if a plaintext credential is being used or not. The alert shows that there was RDP (3389) traffic from abc-admin1-logon to abc-usa-fsl, but it does not specify if the credential was encrypted or not. Moreover, shutting down the file server would disrupt its normal operations and affect other users.
Shutting down abc-usa-fw01; the remote access VPN vulnerability is exploited, is not the first action to take, as it is not clear from the alerts if the remote access VPN vulnerability is exploited or not. The alert shows that there was FTP (21) traffic from abc-usa-dcl to abc- web01, but it does not specify if it was related to the VPN or not. Moreover, shutting down the firewall would expose the network to other threats and affect other
services. References: What is SIEM? | Microsoft Security, What is a SIEM Alert? | Cofense

NEW QUESTION 59
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 63
An organization is deploying a new, online digital bank and needs to ensure availability and performance. The cloud-based architecture is deployed using PaaS and SaaS solutions, and it was designed with the following considerations:
- Protection from DoS attacks against its infrastructure and web applications is in place.
- Highly available and distributed DNS is implemented.
- Static content is cached in the CDN.
- A WAF is deployed inline and is in block mode.
- Multiple public clouds are utilized in an active-passive architecture.
With the above controls in place, the bank is experiencing a slowdown on the unauthenticated payments page. Which of the following is the MOST likely cause?

A. The public cloud provider is applying QoS to the inbound customer traffic.
B. The API gateway endpoints are being directly targeted.
C. The site is experiencing a brute-force credential attack.
D. A DDoS attack is targeted at the CDN.

Answer: A

NEW QUESTION 68
A networking team asked a security administrator to enable Flash on its web browser. The networking team explained that an important legacy embedded system gathers SNMP information from various devices. The system can only be managed through a web browser running Flash. The embedded system will be replaced within the year but is still critical at the moment.
Which of the following should the security administrator do to mitigate the risk?

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

Answer: D

NEW QUESTION 72
As part of its risk strategy, a company is considering buying insurance for cybersecurity incidents.
Which of the following BEST describes this kind of risk response?

A. Risk rejection
B. Risk mitigation
C. Risk transference

D. Risk avoidance

Answer: C

NEW QUESTION 73
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 78
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 80
A help desk technician just informed the security department that a user downloaded a suspicious file from internet explorer last night. The user confirmed accessing all the files and folders before going home from work. the next morning, the user was no longer able to boot the system and was presented a screen with a phone number. The technician then
tries to boot the computer using wake-on-LAN, but the system would not come up. which of the following explains why the computer would not boot?

A. The operating system was corrupted.
B. SElinux was in enforced status.
C. A secure boot violation occurred.
D. The disk was encrypted.

Answer: A

NEW QUESTION 81
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 83
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 85
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 89
A cybersecurity engineer analyst a system for vulnerabilities. The tool created an OVAL. Results document as output. Which of the following would enable the engineer to interpret the results in a human readable form? (Select TWO.)

A. Text editor
B. OOXML editor
C. Event Viewer
D. XML style sheet
E. SCAP tool
F. Debugging utility

Answer: BD

NEW QUESTION 94
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 99
Which of the following is the MOST important security objective when applying cryptography to control messages that tell an ICS how much electrical power to output?

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

Answer: D

Explanation:
Assuring the integrity of messages is the most important security objective when applying cryptography to control messages that tell an ICS (industrial control system) how much electrical power to output. Integrity is the security objective that ensures the accuracy and completeness of data or information, preventing unauthorized modifications or tampering. Assuring the integrity of messages can prevent malicious or accidental changes to the control messages that could affect the operation or safety of the ICS or the electrical power output. Importing the availability of messages is not a security objective when applying cryptography, but a security objective that ensures the accessibility and usability of data or information, preventing unauthorized denial or disruption of service.
Ensuring non-repudiation of messages is not a security objective when applying cryptography, but a security objective that ensures the authenticity and accountability of data or information, preventing unauthorized denial or dispute of actions or transactions. Enforcing protocol conformance for messages is not a security objective when applying cryptography, but a security objective that ensures the compliance and consistency of data or information, preventing unauthorized deviations or violations of rules or standards. Verified References: https://www.comptia.org/blog/what-is-integrity

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

NEW QUESTION 103
A security architect was asked to modify an existing internal network design to accommodate the following requirements for RDP:
• Enforce MFA for RDP
• Ensure RDP connections are only allowed with secure ciphers.
The existing network is extremely complex and not well segmented. Because of these limitations, the company has requested that the connections not be restricted by network- level firewalls Of ACLs.
Which of the following should the security architect recommend to meet these requirements?

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

Answer: C

Explanation:
A remote desktop gateway server is a solution that allows users to connect to remote desktops or applications over the internet using the Remote Desktop Protocol (RDP). A remote desktop gateway server can enforce MFA for RDP by integrating with Azure AD MFA using the Network Policy Server (NPS) extension. The NPS extension can send an OTP (one-time password) to the user's phone or mobile app as a second factor of authentication. A remote desktop gateway server can also enforce secure ciphers by
configuring the SSL Cipher Suite Order Group Policy setting to specify the preferred order of cipher suites for TLS/SSL connections. Verified References:
? https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-plan-access-from-anywhere
? https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa- nps-extension-rdg
? https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry- settings#ssl-cipher-suite-order

NEW QUESTION 108
A systems administrator is in the process of hardening the host systems before connecting to the network. The administrator wants to add protection to the boot loader to ensure the hosts are secure before the OS fully boots.
Which of the following would provide the BEST boot loader protection?

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

Answer: A

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

NEW QUESTION 113
A company plans to build an entirely remote workforce that utilizes a cloud-based infrastructure. The Chief Information Security Officer asks the security engineer to design connectivity to meet the following requirements:
Only users with corporate-owned devices can directly access servers hosted by the cloud provider.
The company can control what SaaS applications each individual user can access. User browser activity can be monitored.
Which of the following solutions would BEST meet these requirements?

A. IAM gateway, MDM, and reverse proxy
B. VPN, CASB, and secure web gateway
C. SSL tunnel, DLP, and host-based firewall
D. API gateway, UEM, and forward proxy

Answer: B

Explanation:
A VPN (virtual private network) can provide secure connectivity for remote users to access servers hosted by the cloud provider. A CASB (cloud access security broker) can enforce policies and controls for accessing SaaS applications. A secure web gateway can monitor and filter user browser activity to prevent malicious or unauthorized traffic. Verified References: https://partners.comptia.org/docs/default- source/resources/casp-content-guide https://www.comptia.org/blog/what-is-a-vpn

NEW QUESTION 116
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 120
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 121
Leveraging cryptographic solutions to protect data that is in use ensures the data is encrypted:

A. when it is passed across a local network.
B. in memory during processing
C. when it is written to a system's solid-state drive.
D. by an enterprise hardware security module.

Answer: B

NEW QUESTION 126
An analyst received a list of IOCs from a government agency. The attack has the following characteristics:
* 1. The attack starts with bulk phishing.
* 2. If a user clicks on the link, a dropper is downloaded to the computer.
* 3. Each of the malware samples has unique hashes tied to the user.
The analyst needs to identify whether existing endpoint controls are effective. Which of the following risk mitigation techniques should the analyst use?

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

Answer: D

Explanation:
Detonating the malware in a sandbox is the best way to analyze its behavior and determine whether the existing endpoint controls are effective. A sandbox is an isolated environment that mimics a real system but prevents any malicious actions from affecting the actual system. By detonating the malware in a sandbox, the analyst can observe how it interacts with the system, what files it creates or modifies, what network connections it establishes, and what indicators of compromise it exhibits. This can help the analyst identify the malware's capabilities, objectives, and weaknesses. A sandbox can also help the analyst compare different malware samples and determine if they are related or part of the same campaign.
* A. Updating the incident response plan is not a risk mitigation technique, but rather a proactive measure to prepare for potential incidents. It does not help the analyst identify whether existing endpoint controls are effective against the malware.
* B. Blocklisting the executable is a risk mitigation technique that can prevent the malware from running on the system, but it does not help the analyst analyze its behavior or determine whether existing endpoint controls are effective. Moreover, blocklisting may not be feasible if each malware sample has a unique hash tied to the user.
* C. Deploying a honeypot onto the laptops is a risk mitigation technique that can lure attackers away from the real systems and collect information about their activities, but it does not help the analyst analyze the malware's behavior or determine whether existing endpoint controls are effective. A honeypot is also more suitable for detecting network- based attacks rather than endpoint-based attacks.

NEW QUESTION 128
A bank hired a security architect to improve its security measures against the latest threats The solution must meet the following requirements
• Recognize and block fake websites
• Decrypt and scan encrypted traffic on standard and non-standard ports
• Use multiple engines for detection and prevention
• Have central reporting
Which of the following is the BEST solution the security architect can propose?

A. CASB
B. Web filtering
C. NGFW
D. EDR

Answer: C

Explanation:
A next-generation firewall (NGFW) is a device or software that provides advanced network security features beyond the traditional firewall functions. A NGFW can provide the following capabilities:
? Recognize and block fake websites, using URL filtering and reputation-based
analysis
? Decrypt and scan encrypted traffic on standard and non-standard ports, using SSL/TLS inspection and deep packet inspection
? Use multiple engines for detection and prevention, such as antivirus, intrusion prevention system (IPS), application control, and sandboxing
? Have central reporting, using a unified management console and dashboard A cloud access security broker (CASB) is a device or software that acts as an intermediary between cloud service users and cloud service providers. A CASB can provide various security functions such as visibility, compliance, data security, and threat protection, but it does not provide all the capabilities of a NGFW. Web filtering is a technique that blocks or allows web access based on predefined criteria such as categories, keywords, or reputation. Web filtering can help recognize and block fake websites, but it does not provide all the capabilities of a NGFW. Endpoint detection and response (EDR) is a technology that monitors and analyzes the activity and behavior of endpoints such as computers or mobile devices. EDR can help detect and respond to advanced threats, but it does not provide all the capabilities of a NGFW. References: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise
Security Architecture, Objective 2.2: Select appropriate hardware and software solutions

NEW QUESTION 131
Which of the following agreements includes no penalties and can be signed by two entities that are working together toward the same goal?

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

Answer: A

NEW QUESTION 133
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 135
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 137
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 142
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 146
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 148
An organization is establishing a new software assurance program to vet applications before they are introduced into the production environment, Unfortunately. many Of the applications are provided only as compiled binaries. Which Of the following should the organization use to analyze these applications? (Select TWO).

A. Regression testing
B. SAST
C. Third-party dependency management
D. IDE SAST
E. Fuzz testing
F. IAST

Answer: DE

NEW QUESTION 153
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 158
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 160
A forensic investigator would use the foremost command for:

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

Answer: C

NEW QUESTION 163
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 164
A cybersecurity analyst discovered a private key that could have been exposed.
Which of the following is the BEST way for the analyst to determine if the key has been compromised?

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

Answer: C

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

NEW QUESTION 168
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 169
An organization is implementing a new identity and access management architecture with the following objectives:
Supporting MFA against on-premises infrastructure
Improving the user experience by integrating with SaaS applications Applying risk-based policies based on location
Performing just-in-time provisioning
Which of the following authentication protocols should the organization implement to support these requirements?

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

Answer: C

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

NEW QUESTION 170
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 174
A security engineer needs to implement a solution to increase the security posture of user endpoints by providing more visibility and control over local administrator accounts. The endpoint security team is overwhelmed with alerts and wants a solution that has minimal operational burdens. Additionally, the solution must maintain a positive user experience after implementation.
Which of the following is the BEST solution to meet these objectives?

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

Answer: B

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

NEW QUESTION 178
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 179
A company created an external application for its customers. A security researcher now reports that the application has a serious LDAP injection vulnerability that could be leveraged to bypass authentication and authorization.
Which of the following actions would BEST resolve the issue? (Choose two.)

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

Answer: AE

Explanation:
A WAF protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, and prevents any unauthorized data from leaving the app. It does this by adhering to a set of policies that help determine what traffic is malicious and what traffic is safe.
According to OWASP, LDAP injection is an attack that exploits web applications that construct LDAP statements based on user input without proper validation or sanitization.
LDAP injection can result in unauthorized access, data modification, or denial of service. To prevent LDAP injection, OWASP recommends conducting input sanitization by escaping special characters in user input and deploying a web application firewall (WAF) that can detect and block malicious LDAP queries.45

NEW QUESTION 184
A software company wants to build a platform by integrating with another company's established product. Which of the following provisions would be MOST important to include when drafting an agreement between the two companies?

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

Answer: B

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

NEW QUESTION 189
As part of the customer registration process to access a new bank account, customers are required to upload a number of documents, including their passports and driver's licenses. The process also requires customers to take a current photo of themselves to be compared against provided documentation.
Which of the following BEST describes this process?

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

Answer: C

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

NEW QUESTION 192
A company is implementing SSL inspection. During the next six months, multiple web applications that will be separated out with subdomains will be deployed.
Which of the following will allow the inspection of the data without multiple certificate deployments?

A. Include all available cipher suites.
B. Create a wildcard certificate.
C. Use a third-party CA.
D. Implement certificate pinning.

Answer: B

Explanation:
A wildcard certificate is a certificate that can be used for multiple subdomains of a domain, such as *.example.com. This would allow the inspection of the data without multiple certificate deployments, as one wildcard certificate can cover all the subdomains that will be separated out with subdomains. Including all available cipher suites may not help with inspecting the data without multiple certificate deployments, as cipher suites are used for negotiating encryption and authentication algorithms, not for verifying certificates. Using a third-party CA (certificate authority) may not help with inspecting the data without multiple certificate deployments, as a third-party CA is an entity that issues and validates certificates, not a type of certificate. Implementing certificate pinning may not help with inspecting the data without multiple certificate deployments, as certificate pinning is a technique that hardcodes the expected certificate or public key in the application code, not a type of certificate. Verified References: https://www.comptia.org/blog/what-is-a-wildcard- certificate https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 194
A developer implement the following code snippet.

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

Which of the following vulnerabilities does the code snippet resolve?

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

Answer: A

Explanation:
SQL injection is a type of vulnerability that allows an attacker to execute malicious SQL commands on a database by inserting them into an input field. The code

snippet resolves this vulnerability by using parameterized queries, which prevent the input from being interpreted as part of the SQL command. Verified References:
https://www.comptia.org/training/books/casp-cas-004-study-guide , https://owasp.org/www- community/attacks/SQL_Injection

NEW QUESTION 198
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 200
A Chief Information Security Officer (CISO) is concerned that a company's current data disposal procedures could result in data remanence. The company uses only SSDs. Which of the following would be the MOST secure way to dispose of the SSDs given the CISO's concern?

A. Degaussing
B. Overwiting
C. Shredding
D. Formatting
E. Incinerating

Answer: C

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

NEW QUESTION 203
A network administrator who manages a Linux web server notices the following traffic: http://corr.ptia.org/.../.../.../... /etc./shadow
Which of the following Is the BEST action for the network administrator to take to defend against this type of web attack?

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

Answer: B

Explanation:
The network administrator is noticing a web attack that attempts to access the /etc/shadow file on a Linux web server. The /etc/shadow file contains the encrypted passwords of all users on the system and is a common target for attackers. The attack uses a technique called directory traversal, which exploits a vulnerability in the web application that allows an attacker to access files or directories outside of the intended scope by manipulating the file path.
Validating the server input and appending the input to the base directory path would be the best action for the network administrator to take to defend against this type of web attack, because it would:
? Check the user input for any errors, malicious data, or unexpected values before
processing it by the web application.
? Prevent directory traversal by ensuring that the user input is always relative to the base directory path of the web application, and not absolute to the root directory of the web server.
? Deny access to any files or directories that are not part of the web application’s scope or functionality.

NEW QUESTION 207
A security architect is implementing a web application that uses a database back end. Prior to the production, the architect is concerned about the possibility of XSS attacks and wants to identify security controls that could be put in place to prevent these attacks.
Which of the following sources could the architect consult to address this security concern?

A. SDLC

B. OVAL
C. IEEE
D. OWASP

Answer: D

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

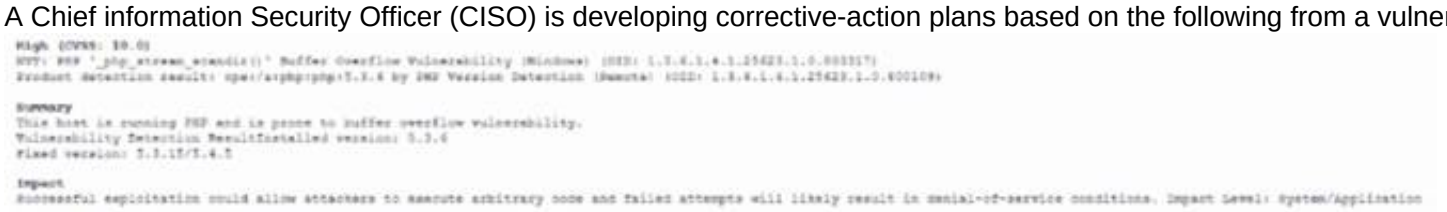
NEW QUESTION 209
A security manager has written an incident response playbook for insider attacks and is ready to begin testing it. Which of the following should the manager conduct to test the playbook?

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 214
A Chief information Security Officer (CISO) is developing corrective-action plans based on the following from a vulnerability scan of internal hosts:



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

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

Answer: A

NEW QUESTION 217
Company A acquired Company . During an audit, a security engineer found Company B's environment was inadequately patched. In response, Company A placed a firewall between the two environments until Company B's infrastructure could be integrated into Company A's security program.
Which of the following risk-handling techniques was used?

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

Answer: D

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

NEW QUESTION 221
A company based in the United States holds insurance details of EU citizens. Which of the following must be adhered to when processing EU citizens' personal, private, and confidential data?

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

Answer: A

NEW QUESTION 222

A vulnerability assessment endpoint generated a report of the latest findings. A security analyst needs to review the report and create a priority list of items that must be addressed. Which of the following should the analyst use to create the list quickly?

A. Business impact rating
B. CVE dates
C. CVSS scores
D. OVAL

Answer: A

NEW QUESTION 226
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 227
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 230
A company is migrating from company-owned phones to a BYOD strategy for mobile devices. The pilot program will start with the executive management team and be rolled out to the rest of the staff in phases. The company's Chief Financial Officer loses a phone multiple times a year.
Which of the following will MOST likely secure the data on the lost device?

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

Answer: C

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

NEW QUESTION 231
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 235
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 238
A company's claims processed department has a mobile workforce that receives a large number of email submissions from personal email addresses. An employees recently received an email that approved to be claim form, but it installed malicious software on the employee's laptop when was opened.

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

Answer: C

Explanation:
Implementing cloud-based content filtering with sandboxing capabilities is the best solution for preventing malicious software installation on the employee's laptop due to opening an email attachment that appeared to be a claim form. Cloud-based content filtering is a technique that uses a cloud service to filter or block web traffic based on predefined rules or policies, preventing unauthorized or malicious access to web resources or services. Cloud-based content filtering can prevent malicious software installation on the employee's laptop due to opening an email attachment that appeared to be a claim form, as it can scan or analyze email attachments before they reach the mailbox and block or quarantine them if they are malicious. Sandboxing is a technique that uses an isolated or virtualized environment to execute or test suspicious or untrusted code or applications, preventing them from affecting the host system or network. Sandboxing can prevent malicious software installation on the employee's laptop due to opening an email attachment that appeared to be a claim form, as it can run or detonate email attachments in a safe environment and observe their behavior or impact before allowing them to reach the mailbox. Implementing application whitelisting and adding only the email client to the whitelist for laptops in the claims processing department is not a good solution for preventing malicious software installation on the employee's laptop due to opening an email attachment that appeared to be a claim form, as it could affect the usability or functionality of other applications on the laptops that may be needed for work purposes, as well as not prevent malicious software from running within the email client. Requiring all laptops to connect to the VPN (virtual private network) before accessing email is not a good solution for preventing malicious software installation on the employee's laptop due to opening an email attachment that appeared to be a claim form, as it could introduce latency or performance issues for accessing email, as well as not prevent malicious software from reaching or executing on the laptops. Installing a mail gateway to scan incoming messages and strip attachments before they reach the mailbox is not a good solution for preventing malicious software installation on the employee's laptop due to opening an email attachment that appeared to be a claim form, as it could affect the normal operations or functionality of email communication, as well as not prevent legitimate attachments from reaching the mailbox. Verified References: https://www.comptia.org/blog/what-is-cloud- based-content-filtering https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 243
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 246
An organization is referencing NIST best practices for BCP creation while reviewing current internal organizational processes for mission-essential items. Which of the following phases establishes the identification and prioritization of critical systems and functions?

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

Answer: C

Explanation:
Reference: https://itsm.ucsf.edu/business-impact-analysis-bia-0
According to NIST SP 800-34 Rev. 1, a business impact analysis (BIA) is a process that identifies and evaluates the potential effects of natural and man-made events on organizational operations. The BIA enables an organization to determine which systems and processes are essential to the organization's mission and prioritize their recovery time objectives (RTOs) and recovery point objectives (RPOs).12

NEW QUESTION 249
A security analyst wants to keep track of alt outbound web connections from workstations. The analyst's company uses an on-premises web filtering solution that forwards the outbound traffic to a perimeter firewall. When the security analyst gets the connection events from the firewall, the source IP of the outbound web traffic is the translated IP of the web filtering solution. Considering this scenario involving source NAT. which of the following would be the BEST option to inject in the HTTP header to include the real source IP from workstations?

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

Answer: B

NEW QUESTION 253
FILL IN THE BLANK
A company's finance department acquired a new payment system that exports data to an unencrypted file on the system. The company implemented controls on the file so only appropriate personnel are allowed access. Which of the following risk techniques did the department use in this situation?

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

Answer: D

NEW QUESTION 256
A major broadcasting company that requires continuous availability to streaming content needs to be resilient against DDoS attacks Which of the following is the MOST important infrastructure security design element to prevent an outage7

A. Supporting heterogeneous architecture
B. Leveraging content delivery network across multiple regions
C. Ensuring cloud autoscaling is in place
D. Scaling horizontally to handle increases in traffic

Answer: B

Explanation:
A content delivery network (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 availability and performance of web applications 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 application availability. Supporting heterogeneous architecture means using different types of hardware, software, or platforms in an IT environment. This can help improve resilience by reducing single points of failure and increasing compatibility, but it does not directly prevent DDoS attacks. Ensuring cloud autoscaling is in place means using cloud services that automatically adjust the amount of resources allocated to an application based on the demand or load. This can help improve scalability and performance by providing more resources when needed, but it does not directly prevent
DDoS attacks. Scaling horizontally means adding more servers or nodes to an IT environment to increase its capacity or throughput. This can help improve scalability and performance by distributing the load across multiple servers, but it does not directly prevent DDoS attacks. References: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.4: Select controls based on systems security evaluation models

NEW QUESTION 257
A financial services company wants to migrate its email services from on-premises servers to a cloud-based email solution. The Chief information Security Officer (CISO) must brief board of directors on the potential security concerns related to this migration. The board is concerned about the following.
* Transactions being required by unauthorized individual
* Complete discretion regarding client names, account numbers, and investment information.
* Malicious attacker using email to distribute malware and ransom ware.
* Exfiltration of sensitivity company information.
The cloud-based email solution will provide an6-malware, reputation-based scanning, signature-based scanning, and sandboxing. Which of the following is the BEST option to resolve the board's concerns for this email migration?

A. Data loss prevention

B. Endpoint detection response
C. SSL VPN
D. Application whitelisting

Answer: A

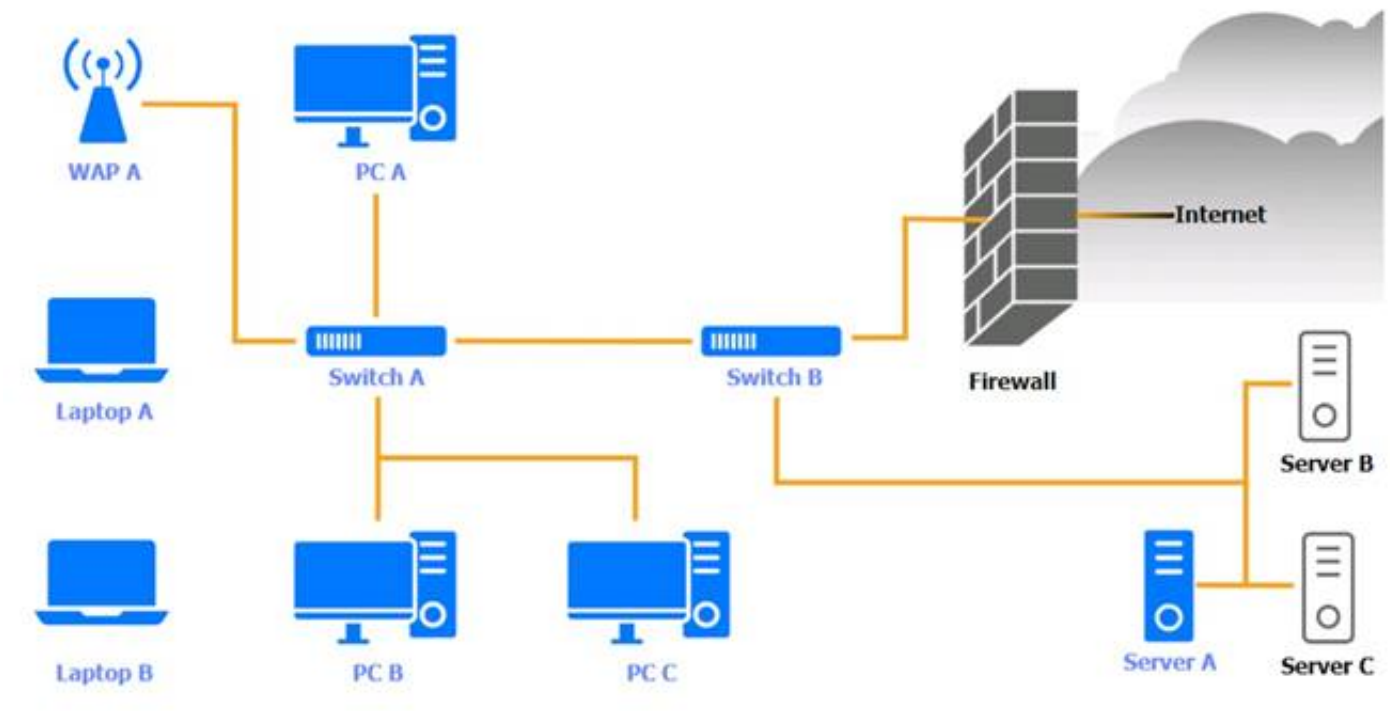
Explanation:
Data loss prevention (DLP) is the best option to resolve the board's concerns for this email migration. DLP is a set of tools and policies that aim to prevent unauthorized access, disclosure, or exfiltration of sensitive data. DLP can monitor, filter, encrypt, or block email messages based on predefined rules and criteria, such as content, sender, recipient, attachment, etc. DLP can help protect transactions, customer data, and company information from being compromised by malicious actors or accidental leaks. Verified References: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://www.csoonline.com/article/3245746/what-is-dlp-data-loss-prevention-and-how- does-it-work.html

NEW QUESTION 261
The OS on several servers crashed around the same time for an unknown reason. The servers were restored to working condition, and all file integrity was verified. Which of the following should the incident response team perform to understand the crash and prevent it in the future?

A. Root cause analysis
B. Continuity of operations plan
C. After-action report
D. Lessons learned

Answer: A

NEW QUESTION 266
SIMULATION
A security engineer needs to review the configurations of several devices on the network to meet the following requirements:
• The PostgreSQL server must only allow connectivity in the 10.1.2.0/24 subnet.
• The SSH daemon on the database server must be configured to listen to port 4022.
• The SSH daemon must only accept connections from a Single workstation.
• All host-based firewalls must be disabled on all workstations.
• All devices must have the latest updates from within the past eight days.
• All HDDs must be configured to secure data at rest.
• Cleartext services are not allowed.
• All devices must be hardened when possible.
Instructions:
Click on the various workstations and network devices to review the posture assessment results. Remediate any possible issues or indicate that no issue is found.
Click on Server A to review output data. Select commands in the appropriate tab to remediate connectivity problems to the pOSTGREsql DATABASE VIA ssh



WAP A

WAP A

Finding	Status	Remediation
Firmware	Updated 5 days ago	☑ No issue
Top 5 used ports	22, 80, 443, 123, 53	☐ Patch management
SSID broadcast	Disabled	☐ Update endpoint protection
Default admin account	Default password has been changed	☐ Enabled disk encryption
HTTP server	Disabled	☐ Enable port security on network device
		☐ Enable password complexity
		☐ Enable host-based firewall to block all traffic
		☐ Antivirus scan
		☐ Change default administrative password
		☐ Disable unneeded services
		☐ Enable all connectivity settings

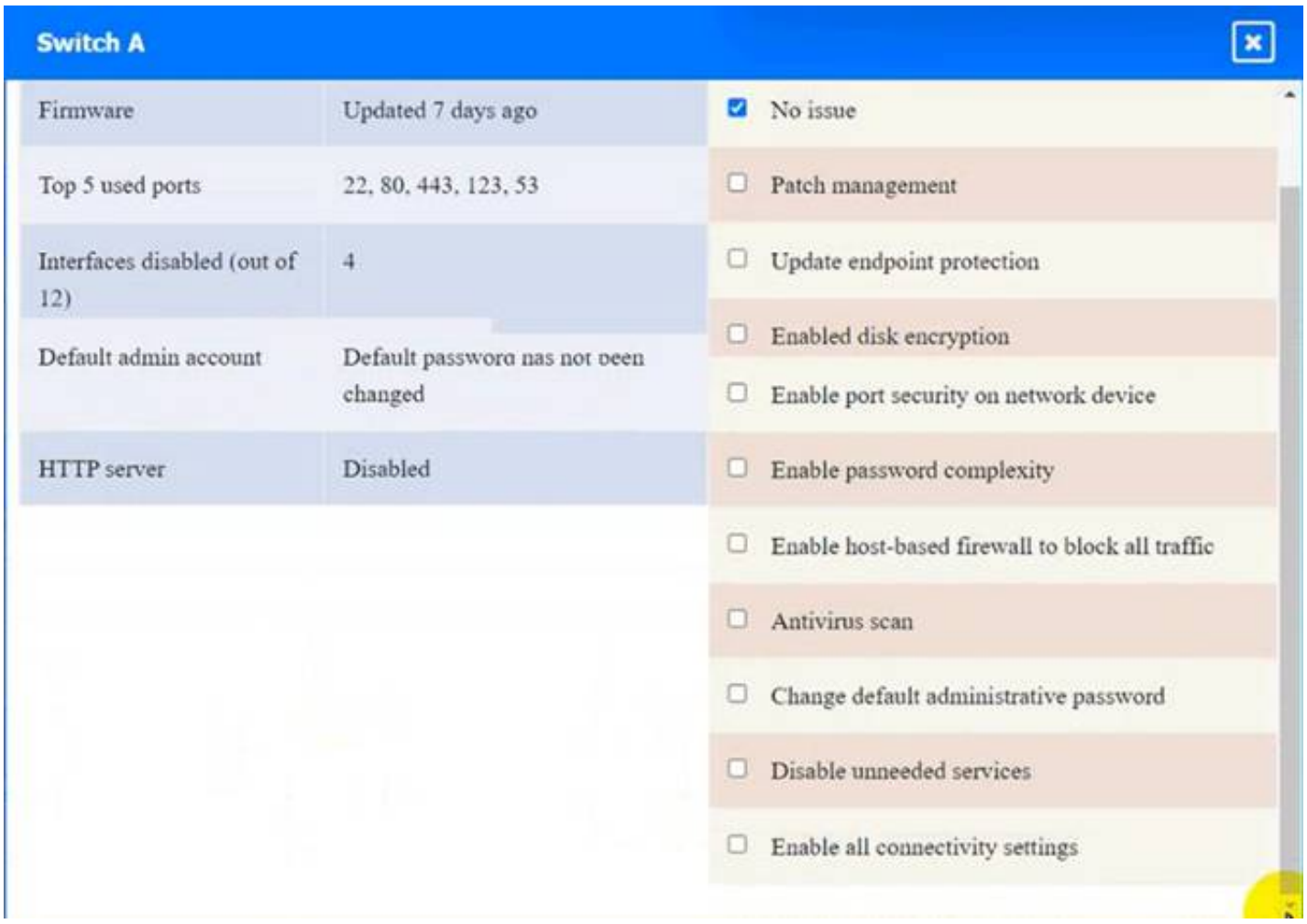
PC A

PC A

OS updates	Updated 2 days ago, last checked 5:08 a.m.	☑ No issue
Endpoint protection	Last checked 6:11 a.m.	☐ Patch management
Browser version	91.2.5 (7/31/2023)	☐ Update endpoint protection
Disk encryption	Enabled	☐ Enabled disk encryption
Password complexity	Enabled	☐ Enable port security on network device
Host-based firewall	Disabled	☐ Enable password complexity
CPU & memory usage	Normal	☐ Enable host-based firewall to block all traffic
Screensaver	Enabled	☐ Antivirus scan
Top 5 used ports	22, 80, 443, 389, 53	☐ Change default administrative password
Wireless	Disabled	☐ Disable unneeded services
		☐ Enable all connectivity settings

Laptop A

Switch A



Switch B:

Switch B

Firmware	Updated 7 days ago
Top 5 used ports	22, 80, 443, 123, 53
Interfaces disabled (out of 6)	1
Default admin account	Default password has been changed
HTTP server	Disabled

- [x] No issue
- [ ] Patch management
- [ ] Update endpoint protection
- [ ] Enabled disk encryption
- [ ] Enable port security on network device
- [ ] Enable password complexity
- [ ] Enable host-based firewall to block all traffic
- [ ] Antivirus scan
- [ ] Change default administrative password
- [ ] Disable unneeded services
- [ ] Enable all connectivity settings

Laptop B

Laptop B

OS updates	Updated 3 days ago, last checked 8:08 a.m.
Endpoint protection	Last checked in 8:11 a.m.
Browser version	81.2.5 (7/31/2023)
Disk encryption	Disabled
Password Complexity	Enabled
Host-based firewall	Disabled
CPU & memory usage	Normal
Screensaver	Enabled
Top 5 used ports	22, 80, 443, 8080, 53
Wireless	Enabled

- [x] No issue
- [ ] Patch management
- [ ] Update endpoint protection
- [ ] Enabled disk encryption
- [ ] Enable port security on network device
- [ ] Enable password complexity
- [ ] Enable host-based firewall to block all traffic
- [ ] Antivirus scan
- [ ] Change default administrative password
- [ ] Disable unneeded services
- [ ] Enable all connectivity settings

PC B

PC B

OS updates	Updated 2 days ago, last checked 5:10 a.m.	☑ No issue
Endpoint protection	Last checked in 6:13 a.m.	☐ Patch management
Browser version	91.2.5 (7/31/2023)	☐ Update endpoint protection
Disk encryption	Enabled	☐ Enabled disk encryption
Password complexity	Enabled	☐ Enable port security on network device
Host-based firewall	Disabled	☐ Enable password complexity
CPU & memory usage	Medium	☐ Enable host-based firewall to block all traffic
Screensaver	Enabled	☐ Antivirus scan
Top 5 used ports	22, 80, 443, 389, 53	☐ Change default administrative password
Wireless	Disabled	☐ Disable unneeded services
		☐ Enable all connectivity settings

PC C

PC C

OS updates	Updated 22 days ago	☑ No issue
Endpoint protection	Last checked 6:19 a.m.	☐ Patch management
Browser version	91.2.5 (7/18/2022)	☐ Update endpoint protection
Disk encryption	Enabled	☐ Enabled disk encryption
Password complexity	Enabled	☐ Enable port security on network device
Host-based firewall	Disabled	☐ Enable password complexity
CPU & memory usage	High	☐ Enable host-based firewall to block all traffic
Screensaver	Enabled	☐ Antivirus scan
Top 5 used ports	22, 80, 443, 23, 53	☐ Change default administrative password
Wireless	Disabled	☐ Disable unneeded services
		☐ Enable all connectivity settings

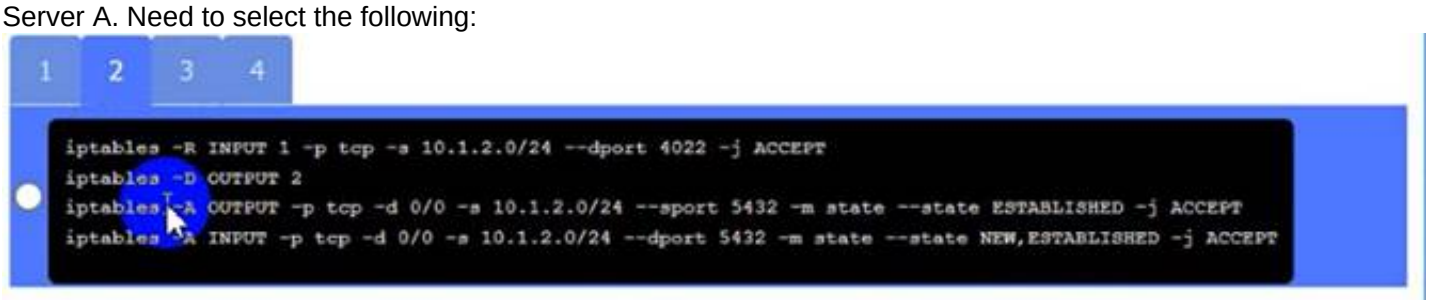
Server A

A. Mastered
B. Not Mastered

Answer: A

Explanation:
WAP A: No issue found. The WAP A is configured correctly and meets the requirements. PC A = Enable host-based firewall to block all traffic
This option will turn off the host-based firewall and allow all traffic to pass through. This will comply with the requirement and also improve the connectivity of PC A to other devices on the network. However, this option will also reduce the security of PC A and make it more vulnerable to attacks. Therefore, it is recommended to use other security measures, such as antivirus, encryption, and password complexity, to protect PC A from potential threats.
Laptop A: Patch management
This option will install the updates that are available for Laptop A and ensure that it has the most recent security patches and bug fixes. This will comply with the requirement and also improve the performance and stability of Laptop A. However, this option may also require a reboot of Laptop A and some downtime during the update process. Therefore, it is recommended to backup any important data and close any open applications before applying the updates.
Switch A: No issue found. The Switch A is configured correctly and meets the requirements.
Switch B: No issue found. The Switch B is configured correctly and meets the requirements.
Laptop B: Disable unneeded services

This option will stop and disable the telnet service that is using port 23 on Laptop B. Telnet is a cleartext service that transmits data in plain text over the network, which exposes it to eavesdropping, interception, and modification by attackers. By disabling the telnet service, you will comply with the requirement and also improve the security of Laptop B. However, this option may also affect the functionality of Laptop B if it needs to use telnet for remote administration or other purposes. Therefore, it is recommended to use a secure alternative to telnet, such as SSH or HTTPS, that encrypts the data in transit.
PC B: Enable disk encryption
This option will encrypt the HDD of PC B using a tool such as BitLocker or VeraCrypt. Disk encryption is a technique that protects data at rest by converting it into an unreadable format that can only be decrypted with a valid key or password. By enabling disk encryption, you will comply with the requirement and also improve the confidentiality and integrity of PC B's data. However, this option may also affect the performance and usability of PC B, as it requires additional processing time and user authentication to access the encrypted data. Therefore, it is recommended to backup any important data and choose a strong key or password before encrypting the disk.
PC C: Disable unneeded services
This option will stop and disable the SSH daemon that is using port 22 on PC C. SSH is a secure service that allows remote access and command execution over an encrypted channel. However, port 22 is the default and well-known port for SSH, which makes it a common target for brute-force attacks and port scanning. By disabling the SSH daemon on port 22, you will comply with the requirement and also improve the security of PC C. However, this option may also affect the functionality of PC C if it needs to use SSH for remote administration or other purposes. Therefore, it is recommended to enable the SSH daemon on a different port, such as 4022, by editing the configuration file using the following command:
sudo nano /etc/ssh/sshd_config
Server A. Need to select the following:



A black and white screen with white text
Description automatically generated

NEW QUESTION 271
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 276
A security architect works for a manufacturing organization that has many different branch offices. The architect is looking for a way to reduce traffic and ensure the branch offices receive the latest copy of revoked certificates issued by the CA at the organization's headquarters location. The solution must also have the lowest power requirement on the CA.
Which of the following is the BEST solution?

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

Answer: C

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

NEW QUESTION 280

A recent data breach revealed that a company has a number of files containing customer data across its storage environment. These files are individualized for each employee and are used in tracking various customer orders, inquiries, and issues. The files are not encrypted and can be accessed by anyone. The senior management team would like to address these issues without interrupting existing processes.
Which of the following should a security architect recommend?

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

Answer: D

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

NEW QUESTION 281
A vulnerability scanner detected an obsolete version of an open-source file-sharing application on one of a company's Linux servers. While the software version is no longer supported by the OSS community, the company's Linux vendor backported fixes, applied them for all current vulnerabilities, and agrees to support the software in the future.
Based on this agreement, this finding is BEST categorized as a:

A. true positive.
B. true negative.
C. false positive.
D. false negative.

Answer: C

NEW QUESTION 286
A bank is working with a security architect to find the BEST solution to detect database management system compromises. The solution should meet the following requirements:
Work at the application layer
Send alerts on attacks from both privileged and malicious users Have a very low false positive
Which of the following should the architect recommend?

A. FIM
B. WAF
C. NIPS
D. DAM
E. UTM

Answer: D

NEW QUESTION 287
A company is moving most of its customer-facing production systems to the cloud-facing production systems to the cloud. IaaS is the service model being used. The Chief Executive Officer is concerned about the type of encryption available and requires the solution must have the highest level of security.
Which of the following encryption methods should the cloud security engineer select during the implementation phase?

A. Instance-based
B. Storage-based
C. Proxy-based
D. Array controller-based

Answer: B

Explanation:
We recommend that you encrypt your virtual hard disks (VHDs) to help protect your boot volume and data volumes at rest in storage, along with your encryption keys and secrets. Azure Disk Encryption helps you encrypt your Windows and Linux IaaS virtual machine disks. Azure Disk Encryption uses the industry-standard BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the OS and the data disks. The solution is integrated with Azure Key Vault to help you control and manage the disk-encryption keys and secrets in your key vault subscription. The solution also ensures that all data on the virtual machine disks are encrypted at rest in Azure Storage. https://docs.microsoft.com/en-us/azure/security/fundamentals/iaas

NEW QUESTION 288
A significant weather event caused all systems to fail over to the disaster recovery site successfully. However, successful data replication has not occurred in the last six months, which has resulted in the service being unavailable. V•Vh1ch of the following would BEST prevent this scenario from happening again?

A. Performing routine tabletop exercises
B. Implementing scheduled, full interruption tests
C. Backing up system log reviews
D. Performing department disaster recovery walk-throughs

Answer: B

NEW QUESTION 292
An organization is moving its intellectual property data from on premises to a CSP and wants to secure the data from theft. Which of the following can be used to mitigate this risk?

A. An additional layer of encryption
B. A third-party data integrity monitoring solution
C. A complete backup that is created before moving the data
D. Additional application firewall rules specific to the migration

Answer: A

Explanation:
The company should use an additional layer of encryption to secure the data from theft when moving to a CSP. Encryption is a process of transforming data into an unreadable format using a secret key. Encryption can protect the data from unauthorized access or modification during transit and at rest. Encryption can be applied at different levels, such as disk, file, or application. An additional layer of encryption can provide an extra security measure on top of the encryption provided by the CSP. Verified References:

- https://learn.microsoft.com/en-us/partner-center/transition-seat-based-services
- https://cloud.google.com/architecture/patterns-for-connecting-other-csps-with-gcp

NEW QUESTION 296
A consultant needs access to a customer's cloud environment. The customer wants to enforce the following engagement requirements:
• All customer data must remain under the control of the customer at all times.
• Third-party access to the customer environment must be controlled by the customer.
• Authentication credentials and access control must be under the customer's control.
Which of the following should the consultant do to ensure all customer requirements are satisfied when accessing the cloud environment?

A. use the customer's SSO with read-only credentials and share data using the customer's provisioned secure network storage
B. use the customer-provided VDI solution to perform work on the customer's environment.
C. Provide code snippets to the customer and have the customer run code and securely deliver its output
D. Request API credentials from the customer and only use API calls to access the customer's environmen

Answer: B

Explanation:
The consultant should use the customer-provided VDI solution to perform work on the customer’s environment. VDI stands for virtual desktop infrastructure, which is a technology that allows users to access a virtual desktop hosted on a remote server. VDI can help meet the customer’s requirements by ensuring that all customer data remains under the customer’s control at all times, that third-party access to the customer environment is controlled by the customer, and that authentication credentials and access control are under the customer’s control. Verified References:

- https://www.kaspersky.com/resource-center/threats/how-to-avoid-social-engineering-attacks
- https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/understanding-preventing-social-engin
- https://www.indusface.com/blog/10-ways-businesses-can-prevent-social-engineering-attacks/

NEW QUESTION 298
A network administrator receives a ticket regarding an error from a remote worker who is trying to reboot a laptop. The laptop has not yet loaded the operating system, and the user is unable to continue the boot process. The administrator is able to provide the user with a recovery PIN, and the user is able to reboot the system and access the device as needed. Which of the following is the MOST likely cause of the error?

A. Lockout of privileged access account
B. Duration of the BitLocker lockout period
C. Failure of the Kerberos time drift sync
D. Failure of TPM authentication

Answer: D

Explanation:
The most likely cause of the error is the failure of TPM authentication. TPM stands for Trusted Platform Module, which is a hardware component that stores encryption keys and other security information. TPM can be used by BitLocker to protect the encryption keys and verify the integrity of the boot process. If TPM fails to authenticate the laptop, BitLocker will enter recovery mode and ask for a recovery PIN, which is a 48-digit numerical password that can be used to unlock the system. The administrator should check the TPM status and configuration and make sure it is working properly. Verified References:

- https://support.microsoft.com/en-us/windows/finding-your-bitlocker-recovery-key-in-windows-6b71ad27-
- https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/bi
- https://docs.sophos.com/esg/sgn/8-1/user/win/en-us/esg/SafeGuard-Enterprise/tasks/BitLockerRecoveryK

NEW QUESTION 301
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CAS-004 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CAS-004 Product From:

https://www.2passeasy.com/dumps/CAS-004/

Money Back Guarantee

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