



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

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

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

Answer: B

NEW QUESTION 3

A network architect is designing a new SD-WAN architecture to connect all local sites to a central hub site. The hub is then responsible for redirecting traffic to public cloud and datacenter applications. The SD-WAN routers are managed through a SaaS, and the same security policy is applied to staff whether working in the office or at a remote location. The main requirements are the following:

- * 1. The network supports core applications that have 99.99% uptime.
- * 2. Configuration updates to the SD-WAN routers can only be initiated from the management service.
- * 3. Documents downloaded from websites must be scanned for malware.

Which of the following solutions should the network architect implement to meet the requirements?

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

Answer: C

NEW QUESTION 4

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

Which of the following BEST describes the type of malware the solution should protect against?

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

Answer: C

NEW QUESTION 5

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 6

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 7

An organization is prioritizing efforts to remediate or mitigate risks identified during the latest assessment. For one of the risks, a full remediation was not possible,

but the organization was able to successfully apply mitigations to reduce the likelihood of impact. Which of the following should the organization perform NEXT?

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

Answer: A

NEW QUESTION 8

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 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

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

- A. NIST SP 800-53
- B. MITRE ATT&CK
- C. The Cyber Kill Chain
- D. The Diamond Model of Intrusion Analysis

Answer: A

NEW QUESTION 10

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.

Answer: A

NEW QUESTION 14

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.

Answer: A

NEW QUESTION 16

A software house is developing a new application. The application has the following requirements: Reduce the number of credential requests as much as possible
Integrate with social networks
Authenticate users

Which of the following is the BEST federation method to use for the application?

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

Answer: D

NEW QUESTION 18

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 21

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

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

Answer: C

NEW QUESTION 22

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

Answer: ACE

NEW QUESTION 26

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

Answer: C

NEW QUESTION 29

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

- A. Biometric authenticators are immutable.
- B. The likelihood of account compromise is reduced.

- C. Zero trust is achieved.
- D. Privacy risks are minimized.

Answer: B

NEW QUESTION 34

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

Answer: A

NEW QUESTION 37

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 40

A company created an external application for its customers. A security researcher now reports that the application has a serious LDAP injection vulnerability that could be leveraged to bypass authentication and authorization.

Which of the following actions would BEST resolve the issue? (Choose two.)

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

Answer: AE

Explanation:

A WAF protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, and prevents any unauthorized data from leaving the app. It does this by adhering to a set of policies that help determine what traffic is malicious and what traffic is safe.

NEW QUESTION 44

A systems administrator is preparing to run a vulnerability scan on a set of information systems in the organization. The systems administrator wants to ensure that the targeted systems produce accurate information especially regarding configuration settings.

Which of the following scan types will provide the systems administrator with the MOST accurate information?

- A. A passive, credentialed scan
- B. A passive, non-credentialed scan
- C. An active, non-credentialed scan
- D. An active, credentialed scan

Answer: D

NEW QUESTION 45

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 46

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 50

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

Based on RPO requirements, which of the following recommendations should the management team make?

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

Answer: C

NEW QUESTION 52

Which of the following technologies allows CSPs to add encryption across multiple data storages?

- A. Symmetric encryption
- B. Homomorphic encryption
- C. Data dispersion
- D. Bit splitting

Answer: D

NEW QUESTION 57

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 59

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 61

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

Answer: C

NEW QUESTION 66

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.

Answer: D

NEW QUESTION 71

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 sealed container.
- D. A duplicate copy of the image must be maintained

Answer: B

NEW QUESTION 73

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 77

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 78

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

Answer: C

NEW QUESTION 83

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

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

Which of the following would BEST mitigate this vulnerability?

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

Answer: B

NEW QUESTION 86

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 87

An enterprise is undergoing an audit to review change management activities when promoting code to production. The audit reveals the following:

- Some developers can directly publish code to the production environment.
- Static code reviews are performed adequately.
- Vulnerability scanning occurs on a regularly scheduled basis per policy.

Which of the following should be noted as a recommendation within the audit report?

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

Answer: D

NEW QUESTION 90

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 92

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 93

A security engineer was auditing an organization's current software development practice and discovered that multiple open-source libraries were integrated into the organization's software. The organization currently performs SAST and DAST on the software it develops.

Which of the following should the organization incorporate into the SDLC to ensure the security of the open-source libraries?

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

Answer: D

NEW QUESTION 95

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. PaaS solution in a multi-tenancy cloud
- C. SaaS solution in a community cloud
- D. Private SaaS solution in a single-tenancy cloud.

Answer: D

NEW QUESTION 99

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

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

Answer: A

NEW QUESTION 104

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 library 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. Web application firewall

Answer: B

NEW QUESTION 106

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 110

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 113

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

Which of the following is the BEST solution?

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

Answer: C

NEW QUESTION 114

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

Answer: A

NEW QUESTION 119

A company's product site recently had failed API calls, resulting in customers being unable to check out and purchase products. This type of failure could lead to the loss of customers and damage to the company's reputation in the market.

Which of the following should the company implement to address the risk of system unavailability?

- A. User and entity behavior analytics
- B. Redundant reporting systems
- C. A self-healing system
- D. Application controls

Answer: D

NEW QUESTION 123

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 126

A security analyst sees that a hacker has discovered some keys and they are being made available on a public website. The security analyst is then able to successfully decrypt the data using the keys from the website. Which of the following should the security analyst recommend to protect the affected data?

- A. Key rotation
- B. Key revocation
- C. Key escrow
- D. Zeroization
- E. Cryptographic obfuscation

Answer: E

NEW QUESTION 130

A company undergoing digital transformation is reviewing the resiliency of a CSP and is concerned about meeting SLA requirements in the event of a CSP incident.

Which of the following would be BEST to proceed with the transformation?

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

Answer: C

Explanation:

An active-active cluster does nothing if the cloud provider goes down. One of the main features of multi-cloud is redundancy.

<https://www.cloudflare.com/learning/cloud/what-is-multicloud/>

NEW QUESTION 134

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 136

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

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

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

- A. TLS_AES_128_CCM_8_SHA256
- B. TLS_DHE_DSS_WITH_RC4_128_SHA
- C. TLS_CHACHA20_POLY1305_SHA256
- D. TLS_AES_128_GCM_SHA256

Answer: B

NEW QUESTION 141

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

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

Answer: D

NEW QUESTION 145

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 147

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

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

Answer: A

NEW QUESTION 148

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
DocumentRoot /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.

Answer: A

NEW QUESTION 151

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

Which of the following is the BEST solution to meet these objectives?

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

D. Implement EDR, keep users in the local administrators group, and enable user behavior analytics.

Answer: B

NEW QUESTION 155

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

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

Answer: D

NEW QUESTION 160

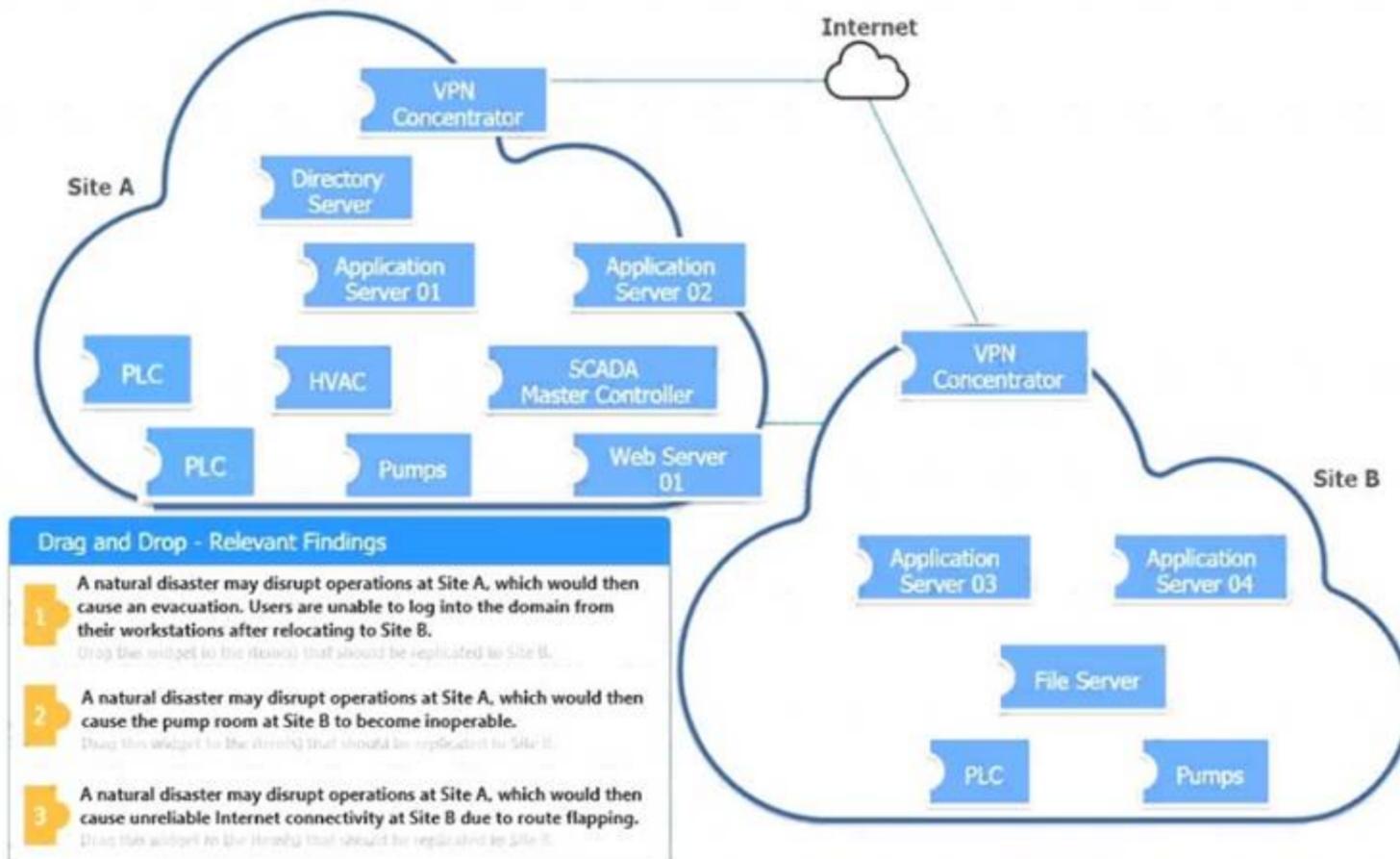
An organization is planning for disaster recovery and continuity of operations. INSTRUCTIONS

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:

Drag and Drop - Relevant Findings

- 1 A natural disaster may disrupt operations at Site A, which would then cause an evacuation. Users are unable to log into the domain from their workstations after relocating to Site B.
Drag this widget to the item(s) that should be replicated to Site B.
- 2 A natural disaster may disrupt operations at Site A, which would then cause the pump room at Site B to become inoperable.
Drag this widget to the item(s) that should be replicated to Site B.

Corrective Action

Modify the BGP configuration

NEW QUESTION 163

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 164

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 Decompiler
- B. Network enurrerator
- C. Log reduction and analysis tool
- D. Static code analysis

Answer: D

NEW QUESTION 166

An energy company is required to report the average pressure of natural gas used over the past quarter. A PLC sends data to a historian server that creates the required reports. Which of the following historian server locations will allow the business to get the required reports in an and IT environment?

- A. In the environment, use a VPN from the IT environment into the environment.
- B. In the environment, allow IT traffic into the environment.
- C. In the IT environment, allow PLCs to send data from the environment to the IT environment.
- D. Use a screened subnet between the and IT environments.

Answer: C

NEW QUESTION 167

A company was recently infected by malware. During the root cause analysis. the company determined that several users were installing their own applications. TO prevent further compromises, the company has decided it will only allow authorized applications to run on its systems. Which Of the following should the company implement?

- A. Signing
- B. Access control

- C. HIPS
- D. Permit listing

Answer: D

NEW QUESTION 170

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 173

An organization requires a contractual document that includes

- An overview of what is covered
- Goals and objectives
- Performance metrics for each party
- A review of how the agreement is managed by all parties

Which of the following BEST describes this type of contractual document?

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

Answer: A

NEW QUESTION 178

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 183

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

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

Answer: A

NEW QUESTION 187

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. Multitenancy SaaS
- C. Single-tenancy SaaS
- D. On-premises cloud service model

Answer: A

NEW QUESTION 192

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

```
0x014435a5 <+7>: mov 0x0(%ebp),%eax
0x014435a8 <+10>: movl $0xffffffff,-0x1c(%ebp) //Tester note, start
0x014435af <+17>: mov %eax,%edx
0x014435b1 <+19>: mov $0x0,%eax
0x014435b8 <+24>: mov -0x1c(%ebp),%ecx
0x014435bd <+27>: mov %edx,%edx
0x014435bb <+29>: testl $0x0,%edi,%edi
0x014435bd <+31>: mov %ecx,%eax
0x014435bf <+33>: not %eax
0x014435c1 <+35>: sub $0x1,%eax //Tester note, end
0x014435c4 <+38>: mov %al,-0x5(%ebp)
0x014435c7 <+41>: cmpl $0x3,-0x9(%ebp) //Tester note <=4
0x014435cb <+45>: jbe 0x1443500 <validate_passwd+36>
0x014435cd <+47>: cmpl $0x5,-0x9(%ebp) //Tester note >=8
0x014435d1 <+51>: ja 0x1443500 <validate_passwd+98>
0x014435d3 <+53>: movl $0x1443560,(%esp)
0x014435d8 <+60>: call 0x14433a0 <puts@plt>
0x014435df <+65>: mov 0x1443020,%eax
0x014435e6 <+70>: mov %eax,(%esp)
0x014435e7 <+73>: call 0x1443380 <fflush@plt>
0x014435ec <+78>: mov 0x0(%ebp),%eax
0x014435ef <+81>: mov %eax,0x4(%esp)
0x014435f3 <+85>: lea -0x14(%ebp),%eax
0x014435f8 <+88>: mov %eax,(%esp)
0x014435f9 <+91>: call 0x1443390 <entropy@plt> //Tester note, breakpoint
0x014435fe <+96>: jmp 0x1443510 <validate_passwd+127>
0x01443500 <+98>: movl $0x144356f,(%esp)
```

The penetration testers MOST likely took advantage of:

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

Answer: A

NEW QUESTION 195

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 200

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

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

Answer: DE

NEW QUESTION 202

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

Answer: BC

NEW QUESTION 206

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 210

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 214

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 217

An organization recently experienced a ransomware attack. The security team leader is concerned about the attack reoccurring. However, no further security measures have been implemented.

Which of the following processes can be used to identify potential prevention recommendations?

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

Answer: A

NEW QUESTION 218

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 220

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

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

Answer: A

NEW QUESTION 224

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 226

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

- A. Log collection
- B. Reverse proxy
- C. A WAF
- D. API mode

Answer: A

NEW QUESTION 231

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 232

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

```
High (CVSS: 10.0)
NVT: FTP '_php_errors_stderr()' Buffer Overflow Vulnerability (Windows) (OID: 1.3.6.1.4.1.25623.1.1.933317)
Product detection result: open/arpip/php:5.3.6 by ZMS Version Detection (Remote: (OID: 1.3.6.1.4.1.25623.1.1.933317))
```

```
Summary
This host is running FTP and is prone to buffer overflow vulnerability.
Vulnerability Detection Result: installed version: 5.3.6
Fixed version: 5.3.17/5.4.7
```

```
Impact
Successful exploitation could allow attackers to execute arbitrary code and failed attempts will likely result in denial-of-service conditions. Impact Level: system/application
```

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

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

Answer: A

NEW QUESTION 237

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 238

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 240

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 244

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

```
http://www.safelibrary.com/search.asp?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 249

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 253

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 256

A Chief Information Officer (CIO) wants to implement a cloud solution that will satisfy the following requirements:
Support all phases of the SDLC. Use tailored website portal software.
Allow the company to build and use its own gateway software. Utilize its own data management platform.
Continue using agent-based security tools.
Which of the following cloud-computing models should the CIO implement?

- A. SaaS
- B. PaaS
- C. MaaS
- D. IaaS

Answer: D

NEW QUESTION 260

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

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

Answer: B

NEW QUESTION 264

An organization is developing a disaster recovery plan that requires data to be backed up and available at a moment's notice. Which of the following should the organization consider FIRST to address this requirement?

- A. Implement a change management plan to ensure systems are using the appropriate versions.
- B. Hire additional on-call staff to be deployed if an event occurs.
- C. Design an appropriate warm site for business continuity.
- D. Identify critical business processes and determine associated software and hardware requirements.

Answer: D

NEW QUESTION 267

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

Answer: A

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.

NEW QUESTION 271

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

Answer: B

NEW QUESTION 274

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

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

Answer: B

NEW QUESTION 278

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 280

A shipping company that is trying to eliminate entire classes of threats is developing an SELinux policy to ensure its custom Android devices are used exclusively for package tracking.

After compiling and implementing the policy, in which of the following modes must the company ensure the devices are configured to run?

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

Answer: C

NEW QUESTION 284

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 286

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 288

A SOC analyst is reviewing malicious activity on an external, exposed web server. During the investigation, the analyst determines specific traffic is not being logged, and there is no visibility from the WAF for the web application.

Which of the following is the MOST likely cause?

- A. The user agent client is not compatible with the WAF.

- B. A certificate on the WAF is expired.
- C. HTTP traffic is not forwarding to HTTPS to decrypt.
- D. Old, vulnerable cipher suites are still being used.

Answer: D

NEW QUESTION 292

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.

Answer: AC

NEW QUESTION 296

An organization developed a social media application that is used by customers in multiple remote geographic locations around the world. The organization's headquarters and only datacenter are located in New York City. The Chief Information Security Officer wants to ensure the following requirements are met for the social media application:

- Low latency for all mobile users to improve the users' experience
- SSL offloading to improve web server performance
- Protection against DoS and DDoS attacks
- High availability

Which of the following should the organization implement to BEST ensure all requirements are met?

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

Answer: B

NEW QUESTION 300

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 304

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

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

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

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

Answer: C

NEW QUESTION 308

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 312

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: 04:15:18:EB:1D:13 (CompuEIA)
Nmap done: 1 IP address (1 host up) scanned in 3.18 seconds
```

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

Answer: A

NEW QUESTION 316

.....

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](#)