

## CAS-004 Dumps

### CompTIA Advanced Security Practitioner (CASP+) Exam

<https://www.certleader.com/CAS-004-dumps.html>



**NEW QUESTION 1**

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 2**

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 3**

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 4**

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 5**

A security engineer is hardening a company's multihomed SFTP server. When scanning a public-facing network interface, the engineer finds the following ports are open:

- 22
- 25
- 110
- 137
- 138
- 139
- 445

Internal Windows clients are used to transferring files to the server to stage them for customer download as part of the company's distribution process. Which of the following would be the BEST solution to harden the system?

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

**Answer:** A

**NEW QUESTION 6**

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 7**

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 8**

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 9**

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 10**

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 10**

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

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

**Answer: BF**

**NEW QUESTION 13**

Device event logs sources from MDM software as follows:

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

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

**Answer: A**

**NEW QUESTION 18**

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:

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 22**

Leveraging cryptographic solutions to protect data that is in use ensures the data is encrypted:

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

**Answer: B**

**NEW QUESTION 25**

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 27**

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 32**

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 37**

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 42**

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 44**

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 48**

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 53**

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 56**

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

Which of the following should the security team recommend FIRST?

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

**Answer: A**

**NEW QUESTION 59**

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 60**

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 65**

A company security engineer arrives at work to face the following scenario:

- 1) Website defacement
  - 2) Calls from the company president indicating the website needs to be fixed immediately because it is damaging the brand
  - 3) A job offer from the company's competitor
  - 4) A security analyst's investigative report, based on logs from the past six months, describing how lateral movement across the network from various IP addresses originating from a foreign adversary country resulted in exfiltrated data
- Which of the following threat actors is MOST likely involved?

- A. Organized crime
- B. Script kiddie
- C. APT/nation-state
- D. Competitor

**Answer: C**

**NEW QUESTION 67**

**SIMULATION**

You are a security analyst tasked with interpreting an Nmap scan output from company's privileged network. The company's hardening guidelines indicate the following:

There should be one primary server or service per device. Only default ports should be used.

Non-secure protocols should be disabled. **INSTRUCTIONS**

Using the Nmap output, identify the devices on the network and their roles, and any open ports that should be closed.

For each device found by Nmap, add a device entry to the Devices Discovered list, with the following information:

The IP address of the device

The primary server or service of the device (Note that each IP should be associated with one service/port only) The protocol(s) that should be disabled based on the hardening guidelines (Note that multiple ports may need to be closed to comply with the hardening guidelines)

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:**

- \* 10.1.45.65 SFTP Server Disable 8080
- \* 10.1.45.66 Email Server Disable 415 and 443
- \* 10.1.45.67 Web Server Disable 21, 80
- \* 10.1.45.68 UTM Appliance Disable 21

**NEW QUESTION 70**

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 71**

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 72**

A security architect needs to implement a CASB solution for an organization with a highly distributed remote workforce. One Of the requirements for the implementation includes the capability to discover SaaS applications and block access to those that are unapproved or identified as risky. Which of the following would BEST achieve this objective?

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

**Answer: C**

**NEW QUESTION 77**

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 78**

Given the following log snippet from a web server:

Which of the following BEST describes this type of attack?

- A. SQL injection
- B. Cross-site scripting
- C. Brute-force
- D. Cross-site request forgery

**Answer: A**

**NEW QUESTION 79**

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

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

**Answer: C**

**NEW QUESTION 81**

A security analyst is investigating a possible buffer overflow attack. The following output was found on a user's workstation:  
graphic.linux\_randomization.prg

Which of the following technologies would mitigate the manipulation of memory segments?

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

**Answer:** B

**Explanation:**

<https://eklitzke.org/memory-protection-and-aslr>

**NEW QUESTION 85**

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 88**

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 89**

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 92**

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 94**

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 95**

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 97

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 102

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 105

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 107

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

Which of the following solutions should the security architect recommend?

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

**Answer: A**

#### NEW QUESTION 108

Which of the following allows computation and analysis of data within a ciphertext without knowledge of the plaintext?

- A. Lattice-based cryptography
- B. Quantum computing
- C. Asymmetric cryptography
- D. Homomorphic encryption

**Answer: D**

#### NEW QUESTION 109

Based on PCI DSS v3.4, one particular database field can store data, but the data must be unreadable. Which of the following data objects meets this requirement?

- A. PAN
- B. CVV2
- C. Cardholder name
- D. Expiration date

**Answer: A**

**NEW QUESTION 113**

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 116**

Over the last 90 days, many storage services has been exposed in the cloud services environments, and the security team does not have the ability to see is creating these instance. Shadow IT is creating data services and instances faster than the small security team can keep up with them. The Chief information security Officer (CIASO) has asked the security officer (CISO) has asked the security lead architect to architect to recommend solutions to this problem. Which of the following BEST addresses the problem best address the problem with the least amount of administrative effort?

- A. Compile a list of firewall requests and compare than against interesting cloud services.
- B. Implement a CASB solution and track cloud service use cases for greater visibility.
- C. Implement a user-behavior system to associate user events and cloud service creation events.
- D. Capture all log and feed then to a SIEM and then for cloud service events

**Answer:** C

**NEW QUESTION 117**

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 119**

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 123**

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 128**

A security analyst is reviewing the following output:

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 133**

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

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

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

**Answer: C**

**NEW QUESTION 135**

A customer reports being unable to connect to a website at [www.test.com](http://www.test.com) to consume services. The customer notices the web application has the following published cipher suite:

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 137**

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 141**

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 142**

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 143**

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 147**

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

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

**Answer: A**

**NEW QUESTION 150**

A penetration tester obtained root access on a Windows server and, according to the rules of engagement, is permitted to perform post-exploitation for persistence.

Which of the following techniques would BEST support this?

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

**Answer: B**

**NEW QUESTION 155**

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 156**

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

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

**Answer: A**

**NEW QUESTION 157**

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

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

**Answer: B**

**NEW QUESTION 159**

Which of the following is a benefit of using steganalysis techniques in forensic response?

- A. Breaking a symmetric cipher used in secure voice communications
- B. Determining the frequency of unique attacks against DRM-protected media
- C. Maintaining chain of custody for acquired evidence
- D. Identifying least significant bit encoding of data in a .wav file

**Answer: B**

**NEW QUESTION 160**

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 164**

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 168**

A company's Chief Information Security Officer is concerned that the company's proposed move to the cloud could lead to a lack of visibility into network traffic flow logs within the VPC.

Which of the following compensating controls would be BEST to implement in this situation?

- A. EDR
- B. SIEM
- C. HIDS
- D. UEBA

**Answer: B**

**NEW QUESTION 171**

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:

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 172**

An organization's assessment of a third-party, non-critical vendor reveals that the vendor does not have cybersecurity insurance and IT staff turnover is high. The organization uses the vendor to move customer office equipment from one service location to another. The vendor acquires customer data and access to the business via an API.

Given this information, which of the following is a noted risk?

- A. Feature delay due to extended software development cycles
- B. Financial liability from a vendor data breach
- C. Technical impact to the API configuration

D. The possibility of the vendor's business ceasing operations

**Answer:** A

**NEW QUESTION 173**

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 176**

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 177**

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

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

**Answer:** C

**NEW QUESTION 178**

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

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

**Answer:** E

**NEW QUESTION 179**

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**

Clients are reporting slowness when attempting to access a series of load-balanced APIs that do not require authentication. The servers that host the APIs are showing heavy CPU utilization. No alerts are found on the WAFs sitting in front of the APIs.

Which of the following should a security engineer recommend to BEST remedy the performance issues in a timely manner?

- A. Implement rate limiting on the API.
- B. Implement geoblocking on the WAF.
- C. Implement OAuth 2.0 on the API.
- D. Implement input validation on the API.

**Answer:** A

**NEW QUESTION 185**

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 187**

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 191**

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

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

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

**Answer:** A

**NEW QUESTION 195**

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 197**

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 199**

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 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 204**

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 208**

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 210**

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

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

**Answer:** B

**NEW QUESTION 215**

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 217**

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 221**

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 222**

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

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

**Answer: C**

**NEW QUESTION 227**

A financial institution has several that currently employ the following controls:

- \* The servers follow a monthly patching cycle.
- \* All changes must go through a change management process.
- \* Developers and systems administrators must log into a jumpbox to access the servers hosting the data using two-factor authentication.
- \* The servers are on an isolated VLAN and cannot be directly accessed from the internal production network. An outage recently occurred and lasted several days due to an upgrade that circumvented the approval process.

Once the security team discovered an unauthorized patch was installed, they were able to resume operations within an hour. Which of the following should the security administrator recommend to reduce the time to resolution if a similar incident occurs in the future?

- A. Require more than one approver for all change management requests.
- B. Implement file integrity monitoring with automated alerts on the servers.
- C. Disable automatic patch update capabilities on the servers
- D. Enhanced audit logging on the jump servers and ship the logs to the SIEM.

**Answer: B**

**NEW QUESTION 229**

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 232**

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 237**

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 239**

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

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

**Answer: C**

**NEW QUESTION 242**

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

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

**Answer: B**

**NEW QUESTION 243**

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 246**

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 251**

Due to internal resource constraints, the management team has asked the principal security architect to recommend a solution that shifts partial responsibility for application-level controls to the cloud provider. In the shared responsibility model, which of the following levels of service meets this requirement?

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

**Answer: D**

**NEW QUESTION 255**

A security analyst is reviewing the following vulnerability assessment report:

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 256**

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 261**

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

- A. The system logs rotated prematurely.
- B. The disk utilization alarms are higher than what the service restarts require.
- C. The number of nodes in the self-healing cluster was healthy,

D. Conditional checks prior to the service restart succeeded.

**Answer:** D

**NEW QUESTION 262**

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 263**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your CAS-004 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/CAS-004-dumps.html>