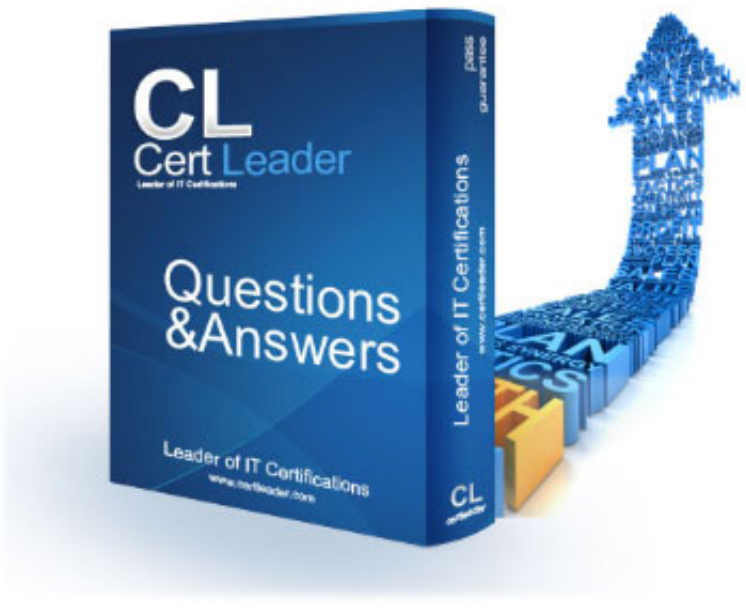
CAS-004 Dumps

CompTIA Advanced Security Practitioner (CASP+) Exam

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



NEW QUESTION 1
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: D

NEW QUESTION 2
A security architect works for a manufacturing organization that has many different branch offices. The architect is looking for a way to reduce traffic and ensure the branch offices receive the latest copy of revoked certificates issued by the CA at the organization's headquarters location. The solution must also have the lowest power requirement on the CA.
Which of the following is the BEST solution?

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

Answer: C

Explanation:
Reference: https://www.sciencedirect.com/topics/computer-science/revoke-certificate

NEW QUESTION 3
A high-severity vulnerability was found on a web application and introduced to the enterprise. The vulnerability could allow an unauthorized user to utilize an open-source library to view privileged user information. The enterprise is unwilling to accept the risk, but the developers cannot fix the issue right away. Which of the following should be implemented to reduce the risk to an acceptable level until the issue can be fixed?

A. Scan the code with a static code analyzer, change privileged user passwords, and provide security training.
B. Change privileged usernames, review the OS logs, and deploy hardware tokens.
C. Implement MFA, review the application logs, and deploy a WAF.
D. Deploy a VPN, configure an official open-source library repository, and perform a full application review for vulnerabilities.

Answer: D

Explanation:
Reference: https://www.microfocus.com/en-us/what-is/sast

NEW QUESTION 4
A company's SOC has received threat intelligence about an active campaign utilizing a specific vulnerability. The company would like to determine whether it is vulnerable to this active campaign.
Which of the following should the company use to make this determination?

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

Answer: B

NEW QUESTION 5
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

Explanation:
Reference: https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

NEW QUESTION 6
During a system penetration test, a security engineer successfully gained access to a shell on a Linux host as a standard user and wants to elevate the privilege levels.
Which of the following is a valid Linux post-exploitation method to use to accomplish this goal?

A. Spawn a shell using sudo and an escape string such as sudo vim -c '!sh'.
B. Perform ASIC password cracking on the host.
C. Read the /etc/passwd file to extract the usernames.
D. Initiate unquoted service path exploits.
E. Use the UNION operator to extract the database schema.

Answer: C

Explanation:
Reference: https://docs.rapid7.com/insightvm/elevating-permissions/

NEW QUESTION 7
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: B

Explanation:
Reference: https://source.android.com/security/selinux/customize

1. Use the latest Android kernel.
2. Adopt the principle of least privilege.
3. Address only your own additions to Android. The default policy works with the Android Open Source Project codebase automatically.
4. Compartmentalize software components into modules that conduct singular tasks.
5. Create SELinux policies that isolate those tasks from unrelated functions.
6. Put those policies in `*.te` files (the extension for SELinux policy source files) within the `/device/manufacturer/device-name/sepolicy` directory and use `BOARD_SEPOLICY` variables to include them in your build.
7. Make new domains permissive initially. This is done by using a permissive declaration in the domain's `.te` file.
8. Analyze results and refine your domain definitions.
9. Remove the permissive declaration when no further denials appear in userdebug builds.

NEW QUESTION 8
An organization is implementing a new identity and access management architecture with the following objectives: Supporting MFA against on-premises infrastructure
Improving the user experience by integrating with SaaS applications
Applying risk-based policies based on location Performing just-in-time provisioning Which of the following authentication protocols should the organization implement to support these requirements?

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

Answer: A

Explanation:
Reference: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/migrate-application-authentication-toazure-active-directory

Manage cost

Your organization may have multiple Identity Access Management (IAM) solutions in place. Migrating to one Azure AD infrastructure is an opportunity to reduce dependencies on IAM licenses (on-premises or in the cloud) and infrastructure costs. In cases where you may have already paid for Azure AD via Microsoft 365 licenses, there is no reason to pay the added cost of another IAM solution.

With Azure AD, you can reduce infrastructure costs by:

- Providing secure remote access to on-premises apps using Azure AD Application Proxy.
- Decoupling apps from the on-prem credential approach in your tenant by setting up Azure AD as the trusted universal identity provider.

NEW QUESTION 9
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: A

Explanation:
Reference: https://www.cyberark.com/what-is/privileged-access-management/

NEW QUESTION 10
A company is moving most of its customer-facing production systems to the cloud-facing production systems to the cloud.
IaaS is the service model being used. The Chief Executive Officer is concerned about the type of encryption available and requires the solution must have the highest level of security.
Which of the following encryption methods should the cloud security engineer select during the implementation phase?

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

Answer: A

NEW QUESTION 10
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 TLSprotected 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: A

Explanation:
Reference: https://www.internetsociety.org/deploy360/tls/basics/

NEW QUESTION 14
A home automation company just purchased and installed tools for its SOC to enable incident identification and response on software the company develops. The company would like to prioritize defenses against the following attack scenarios:
Unauthorized insertions into application development environments
Authorized insiders making unauthorized changes to environment configurations Which of the following actions will enable the data feeds needed to detect these types of attacks on development environments? (Choose two.)

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

Answer: CD

NEW QUESTION 15
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 20
A security engineer thinks the development team has been hard-coding sensitive environment variables in its code. Which of the following would BEST secure the company's CI/CD pipeline?

A. Utilizing a trusted secrets manager

B. Performing DAST on a weekly basis
C. Introducing the use of container orchestration
D. Deploying instance tagging

Answer: A

Explanation:
Reference: https://about.gitlab.com/blog/2021/04/09/demystifying-ci-cd-variables/

When creating a CI/CD variable in the settings, GitLab gives the user more configuration options for the variable. Use these extra configuration options for stricter control over more sensitive variables:

1. **Environment scope**: If a variable only ever needs to be used in one specific environment, set it to only ever be available in that environment. For example, you can set a deploy token to only be available in the `production` environment.
2. **Protected variables**: Similar to the environment scope, you can set a variable to be available only when the pipeline runs on a protected branch, like your default branch.
3. **Masked**: Variables that contain secrets should always be masked. This lets you use the variable in job scripts without the risk of exposing the value of the variable. If someone tries to output it in a job log with a command like `echo $VARIABLE`, the job log will only show `echo [masked]`. There are limits to the types of values that can be masked.

NEW QUESTION 24
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: D

NEW QUESTION 27
A junior developer is informed about the impact of new malware on an Advanced RISC Machine (ARM) CPU, and the code must be fixed accordingly. Based on the debug, the malware is able to insert itself in another process memory location.
Which of the following technologies can the developer enable on the ARM architecture to prevent this type of malware?

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

Answer: A

Explanation:
Reference: https://developer.arm.com/documentation/102433/0100/Stack-smashing-and-execution-permissions

NEW QUESTION 29
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

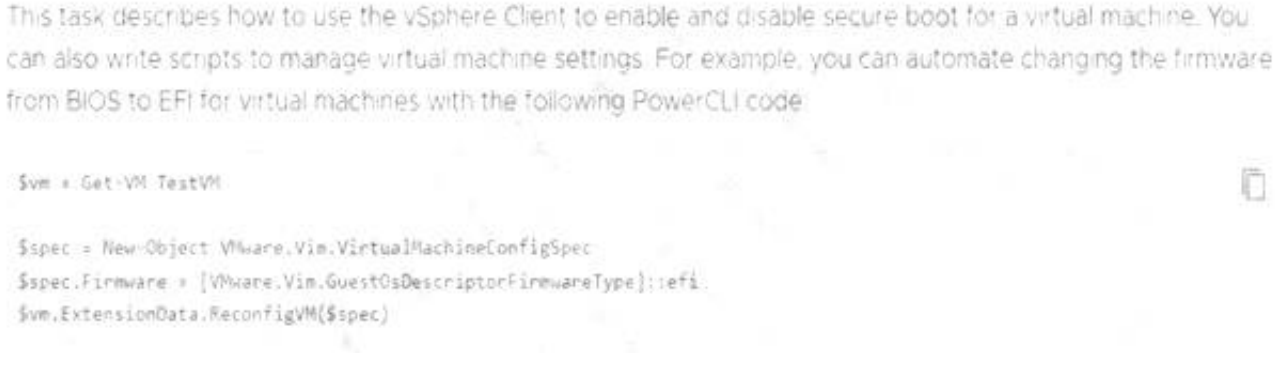
Answer: C

NEW QUESTION 30
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

Explanation:
Reference: https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-898217D4-689D-4EB5-866C-888353FE241C.html



NEW QUESTION 33
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

Explanation:
Reference: https://www.cynet.com/network-attacks/network-attacks-and-network-security-threats/

NEW QUESTION 38
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: B

NEW QUESTION 41
A small company recently developed prototype technology for a military program. The company's security engineer is concerned about potential theft of the newly developed, proprietary information.
Which of the following should the security engineer do to BEST manage the threats proactively?

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

Answer: D

NEW QUESTION 42
A security engineer was auditing an organization's current software development practice and discovered that multiple opensource 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: B

Explanation:

Reference: https://www.whitesourcesoftware.com/resources/blog/application-security-best-practices/

NEW QUESTION 44
A company is preparing to deploy a global service.
Which of the following must the company do to ensure GDPR compliance? (Choose two.)

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

Answer: AB

Explanation:
Reference: https://gdpr.eu/compliance-checklist-us-companies/

- Conduct an information audit for EU personal data

Confirm that your organization needs to comply with the GDPR. First, determine what personal data you process and whether any of it belongs to people in the EU. If you do process such data, determine whether "the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment." Recital 23 can help you clarify whether your activities qualify as subject to the GDPR. If you are subject to the GDPR, continue to the next steps.

- Inform your customers why you're processing their data

NEW QUESTION 47
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 48
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.

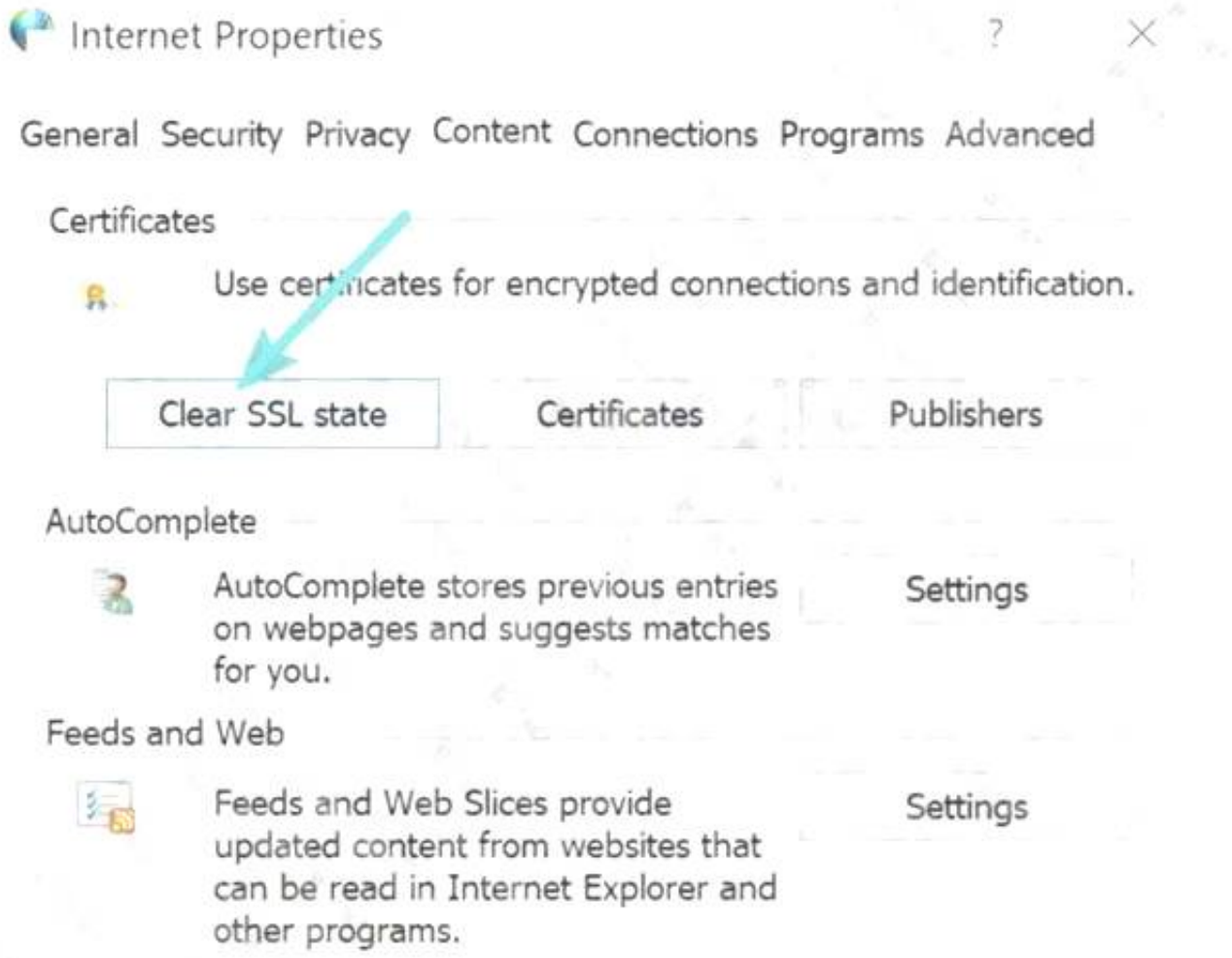
Answer: A

NEW QUESTION 53
An application server was recently upgraded to prefer TLS 1.3, and now users are unable to connect their clients to the server. Attempts to reproduce the error are confirmed, and clients are reporting the following:
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
Which of the following is MOST likely the root cause?

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

Answer: C

Explanation:
Reference: https://kinsta.com/knowledgebase/err_ssl_version_or_cipher_mismatch/

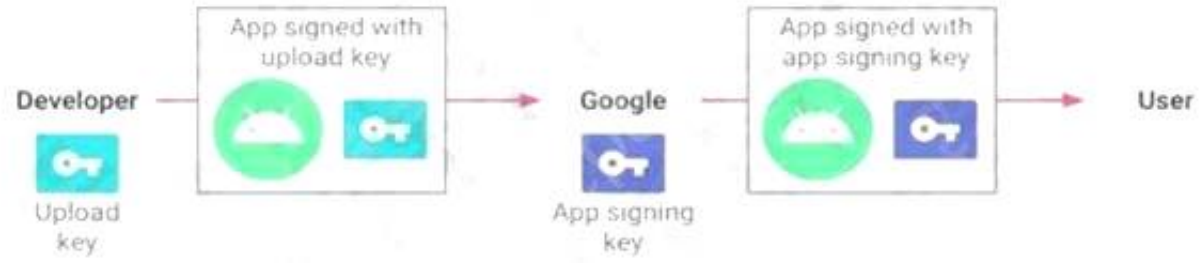


NEW QUESTION 57
A company publishes several APIs for customers and is required to use keys to segregate customer data sets. Which of the following would be BEST to use to store customer keys?

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

Answer: C

Explanation:
Reference: https://developer.android.com/studio/publish/app-signing



NEW QUESTION 61
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: C

NEW QUESTION 63
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

Explanation:
Reference: https://www.govinfo.gov/content/pkg/GOVPUB-C13-9ecd8eae582935c93d7f410e955dabb6/pdf/GOVPUB-C13-9ecd8eae582935c93d7f410e955dabb6.pdf (p.12)

NEW QUESTION 64
A security engineer needs to recommend a solution that will meet the following requirements: Identify sensitive data in the provider's network
Maintain compliance with company and regulatory guidelines
Detect and respond to insider threats, privileged user threats, and compromised accounts Enforce datacentric security, such as encryption, tokenization, and access control Which of the following solutions should the security engineer recommend to address these requirements?

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

Answer: A

NEW QUESTION 66
A small business requires a low-cost approach to theft detection for the audio recordings it produces and sells. Which of the following techniques will MOST likely meet the business's needs?

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

Answer: C

Explanation:
Reference: https://portswigger.net/daily-swig/what-is-steganography-a-complete-guide-to-the-ancient-art-of-concealingmessages

How does steganography work?

Steganography works by hiding information in a way that doesn't arouse suspicion. One of the most popular techniques is 'least significant bit (LSB) steganography. In this type of steganography, the information hider embeds the secret information in the least significant bits of a media file.

For instance, in an image file each pixel is comprised of three bytes of data corresponding to the colors red, green, and blue (some image formats allocate an additional fourth byte to transparency, or 'alpha').

LSB steganography changes the last bit of each of those bytes to hide one bit of data. So, to hide one megabyte of data using this method, you'll need an eight-megabyte image file.

Since modifying the last bit of the pixel value doesn't result in a visually perceptible change to the picture, a person viewing the original and the steganographically modified images won't be able to tell the difference.

NEW QUESTION 70
A company's claims processed department has a mobile workforce that receives a large number of email submissions from personal email addresses. An employees recently received an email that approved to be claim form, but it installed malicious software on the employee's laptop when was opened.

A. Impalement application whitelisting and add only the email client to the whitelist for laptop in the claims processing department.
B. Required all laptops to connect to the VPN before accessing email.
C. Implement cloud-based content filtering with sandboxing capabilities.
D. Install a mail gateway to scan incoming messages and strip attachments before they reach the mailbox.

Answer: C

NEW QUESTION 74
.....

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