CompTIA.Premium.CAS-004.by.VCEplus.83q

Number: CAS-004
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

Exam Code: CAS-004
Exam Name: CompTIA Advanced Security Practitioner (CASP+) CAS-004
Certification Provider: CompTIA
Corresponding Certification: CASP
Website: www.vceplus.com - www.vceplus.co - www.vceplus.io
Free Exam: https://vceplus.com/exam-cas-004/

Questions & Answers Exam Engine is rigorously checked before being put up for sale. We make sure there is nothing irrelevant in CAS-004 exam products and you get latest questions. We strive to deliver the best CAS-004 exam product for top grades in your first attempt.

QUESTION 1
Which of the following are risks associated with vendor lock-in? (Choose two.)

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://www.cloudflare.com/learning/cloud/what-is-vendor-lockin/#:~:text=Vendor%20lock%2Din%20can%20become,may%20involve%20reformatting%20the%20data

QUESTION 2
A security analyst receives an alert from the SIEM regarding unusual activity on an authorized public SSH jump server. To further investigate, the analyst pulls the event logs directly from /var/log/ auth.log: graphic.ssh_auth_log.
Which of the following actions would BEST address the potential risks by the activity in the logs?

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

Correct Answer: C
Section: (none)
Explanation

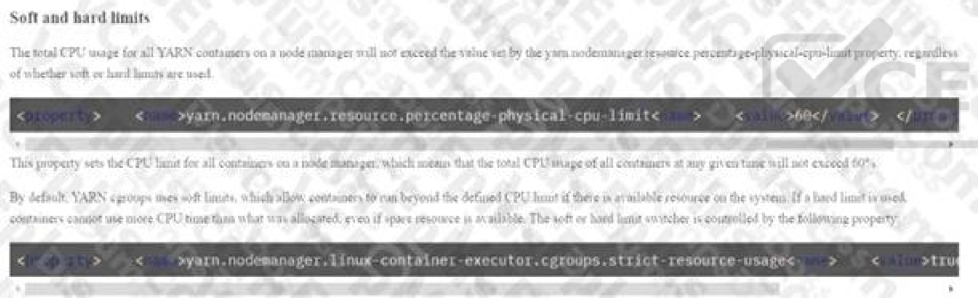
Explanation/Reference:
Explanation:
Reference: https://www.rapid7.com/blog/post/2017/10/04/how-to-secure-ssh-server-using-port-knocking-on-ubuntu-linux/

QUESTION 3
A security analyst is researching containerization concepts for an organization. The analyst is concerned about potential resource exhaustion scenarios on the Docker host due to a single application that is overconsuming available resources.
Which of the following core Linux concepts BEST reflects the ability to limit resource allocation to containers?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://www.ibm.com/support/pages/deep-dive-yarn-cgroups-hadoop-dev



Soft and hard limits

The total CPU usage for all YARN containers on a node manager will not exceed the value set by the yarn.nodemanager.resource.percentage-physical-cpu-limit property, regardless of whether soft or hard limits are used.

```
<property>    <name>yarn.nodemanager.resource.percentage-physical-cpu-limit</name>    <value>60</value>  </prope
```

This property sets the CPU limit for all containers on a node manager, which means that the total CPU usage of all containers at any given time will not exceed 60%.

By default, YARN cgroups uses soft limits, which allow containers to run beyond the defined CPU limit if there is available resource on the system. If a hard limit is used, containers cannot use more CPU time than what was allocated, even if spare resource is available. The soft or hard limit switcher is controlled by the following property:

```
<property>    <name>yarn.nodemanager.linux-container-executor.cgroups.strict-resource-usage</name>    <value>tru
```

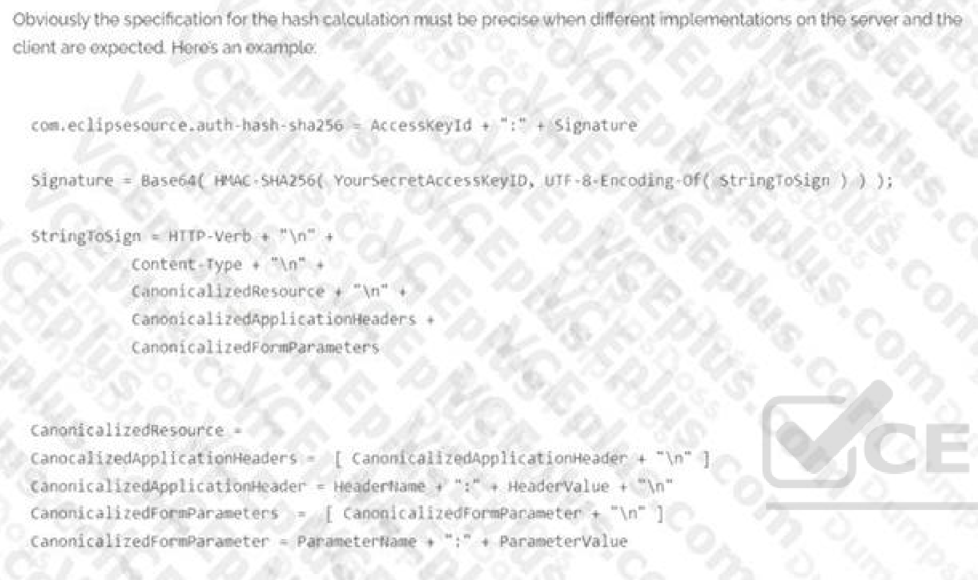
QUESTION 4
An enterprise is deploying APIs that utilize a private key and a public key to ensure the connection string is protected. To connect to the API, customers must use the private key.
Which of the following would BEST secure the REST API connection to the database while preventing the use of a hardcoded string in the request string?

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://eclipsesource.com/blogs/2016/07/06/keyed-hash-message-authentication-code-in-rest-apis/



Obviously the specification for the hash calculation must be precise when different implementations on the server and the client are expected. Here's an example:

```
com.eclipsesource.auth-hash-sha256 = AccessKeyId + ":" + Signature

Signature = Base64( HMAC-SHA256( YourSecretAccessKeyID, UTF-8-Encoding-Of( StringToSign ) ) );

StringToSign = HTTP-Verb + "\n" +
          Content-Type + "\n" +
          CanonicalizedResource + "\n" +
          CanonicalizedApplicationHeaders +
          CanonicalizedFormParameters


CanonicalizedResource =
CanocalizedApplicationHeaders =  [ CanonicalizedApplicationHeader + "\n" ]
CanonicalizedApplicationHeader = HeaderName + ":" + HeaderValue + "\n"
CanonicalizedFormParameters  =  [ CanonicalizedFormParameter + "\n" ]
CanonicalizedFormParameter = ParameterName + ":" + ParameterValue
```

QUESTION 5
A company undergoing digital transformation is reviewing the resiliency of a CSP and is concerned about meeting SLA requirements in the event of a CSP incident.
Which of the following would be BEST to proceed with the transformation?

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

Correct Answer: D
Section: (none)
Explanation

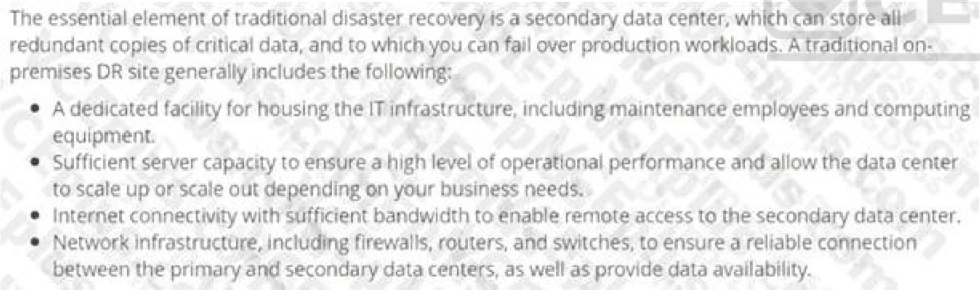
Explanation/Reference:

QUESTION 6
A disaster recovery team learned of several mistakes that were made during the last disaster recovery parallel test.
Computational resources ran out at 70% of restoration of critical services.
Which of the following should be modified to prevent the issue from reoccurring?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://www.nakivo.com/blog/disaster-recovery-in-cloud-computing/



The essential element of traditional disaster recovery is a secondary data center, which can store all redundant copies of critical data, and to which you can fail over production workloads. A traditional on-premises DR site generally includes the following:

- A dedicated facility for housing the IT infrastructure, including maintenance employees and computing equipment.
- Sufficient server capacity to ensure a high level of operational performance and allow the data center to scale up or scale out depending on your business needs.
- Internet connectivity with sufficient bandwidth to enable remote access to the secondary data center.
- Network infrastructure, including firewalls, routers, and switches, to ensure a reliable connection between the primary and secondary data centers, as well as provide data availability.

QUESTION 7
A company processes data subject to NDAs with partners that define the processing and storage constraints for the covered data. The agreements currently do not permit moving the covered data to the cloud, and the company would like to renegotiate the terms of the agreements.
Which of the following would MOST likely help the company gain consensus to move the data to the cloud?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
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.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 9
An IT administrator is reviewing all the servers in an organization and notices that a server is missing crucial practice against a recent exploit that could gain root access.
Which of the following describes the administrator's discovery?

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

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:
Reference: https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

QUESTION 11
A high-severity vulnerability was found on a web application and introduced to the enterprise. The vulnerability could allow an unauthorized user to utilize an open-source library to view privileged user information. The enterprise is unwilling to accept the risk, but the developers cannot fix the issue right away.
Which of the following should be implemented to reduce the risk to an acceptable level until the issue can be fixed?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

QUESTION 12
In preparation for the holiday season, a company redesigned the system that manages retail sales and moved it to a cloud service provider. The new infrastructure did not meet the company's availability requirements. During a postmortem analysis, the following issues were highlighted:
1. International users reported latency when images on the web page were initially loading.
2. During times of report processing, users reported issues with inventory when attempting to place orders.3. Despite the fact that ten new API servers were added, the load across servers was heavy at peak times.
Which of the following infrastructure design changes would be BEST for the organization to implement to avoid these issues in the future?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
A security architect is implementing a web application that uses a database back end. Prior to the production, the architect is concerned about the possibility of XSS attacks and wants to identify security controls that could be put in place to prevent these attacks.
Which of the following sources could the architect consult to address this security concern?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://dzone.com/articles/what-is-oval-a-community-driven-vulnerability-mana

QUESTION 14
A company has decided to purchase a license for software that is used to operate a mission-critical process. The third-party developer is new to the industry but is delivering what the company needs at this time.
Which of the following BEST describes the reason why utilizing a source code escrow will reduce the operational risk to the company if the third party stops supporting the application?

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

B. The company will be able to force the third-party developer to continue support.

C. The company will be able to manage the third-party developer's development process.

D. The company will be paid by the third-party developer to hire a new development team.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
A SOC analyst is reviewing malicious activity on an external, exposed web server. During the investigation, the analyst determines specific traffic is not being logged, and there is no visibility from the WAF for the web application.
Which of the following is the MOST likely cause?

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

B. A certificate on the WAF is expired.

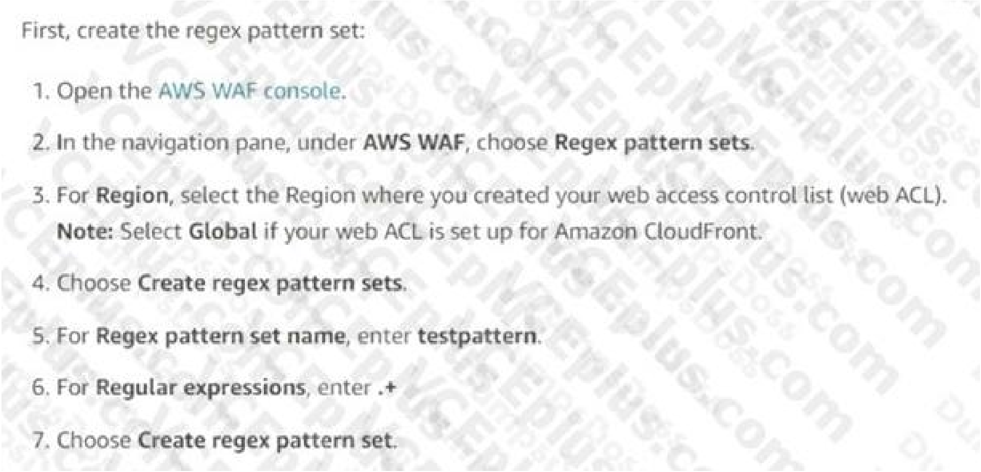
C. HTTP traffic is not forwarding to HTTPS to decrypt.

D. Old, vulnerable cipher suites are still being used.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Reference: https://aws.amazon.com/premiumsupport/knowledge-center/waf-block-http-requests-no-user-agent/



First, create the regex pattern set:

1. Open the AWS WAF console.
2. In the navigation pane, under **AWS WAF**, choose **Regex pattern sets**.
3. For **Region**, select the Region where you created your web access control list (web ACL).
   Note: Select **Global** if your web ACL is set up for Amazon CloudFront.
4. Choose **Create regex pattern sets**.
5. For **Regex pattern set name**, enter **testpattern**.
6. For **Regular expressions**, enter **.+**
7. Choose **Create regex pattern set**.

QUESTION 16

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

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

A. Distributed connection allocation

B. Local caching

C. Content delivery network

D. SD-WAN vertical heterogeneity

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

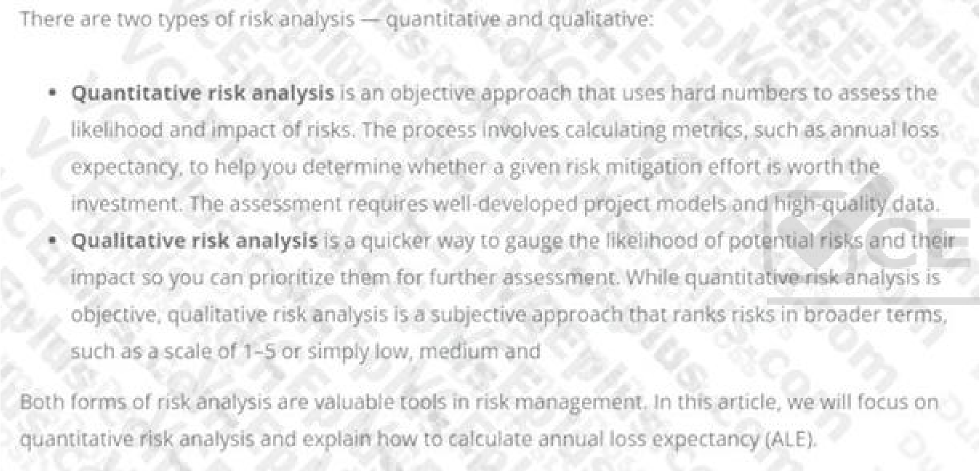
A security engineer estimates the company's popular web application experiences 100 attempted breaches per day. In the past four years, the company's data has been breached two times.

Which of the following should the engineer report as the ARO for successful breaches?

A. 0.5
B. 8
C. 50
D. 36,500

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://blog.netwrix.com/2020/07/24/annual-loss-expectancy-and-quantitative-risk-analysis/



There are two types of risk analysis — quantitative and qualitative:

- **Quantitative risk analysis** is an objective approach that uses hard numbers to assess the likelihood and impact of risks. The process involves calculating metrics, such as annual loss expectancy, to help you determine whether a given risk mitigation effort is worth the investment. The assessment requires well-developed project models and high-quality data.
- **Qualitative risk analysis** is a quicker way to gauge the likelihood of potential risks and their impact so you can prioritize them for further assessment. While quantitative risk analysis is objective, qualitative risk analysis is a subjective approach that ranks risks in broader terms, such as a scale of 1–5 or simply low, medium and

Both forms of risk analysis are valuable tools in risk management. In this article, we will focus on quantitative risk analysis and explain how to calculate annual loss expectancy (ALE).

QUESTION 18
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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
An organization recently started processing, transmitting, and storing its customers' credit card information. Within a week of doing so, the organization suffered a massive breach that resulted in the exposure of the customers' information.
Which of the following provides the BEST guidance for protecting such information while it is at rest and in transit?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 20
During a system penetration test, a security engineer successfully gained access to a shell on a Linux host as a standard user and wants to elevate the privilege levels.
Which of the following is a valid Linux post-exploitation method to use to accomplish this goal?

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

Correct Answer: C
Section: (none)
Explanation

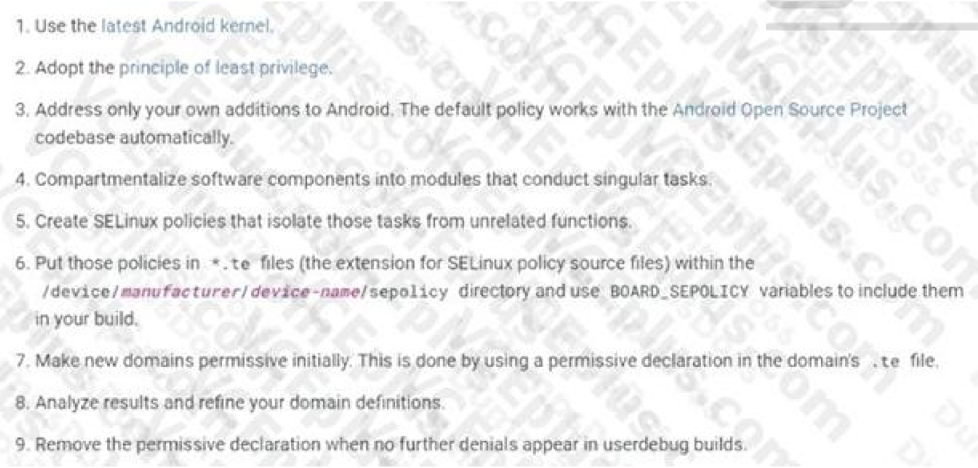
Explanation/Reference:
Explanation:
Reference: https://docs.rapid7.com/insightvm/elevating-permissions/

QUESTION 21
A shipping company that is trying to eliminate entire classes of threats is developing an SELinux policy to ensure its custom Android devices are used exclusively for package tracking.
After compiling and implementing the policy, in which of the following modes must the company ensure the devices are configured to run?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

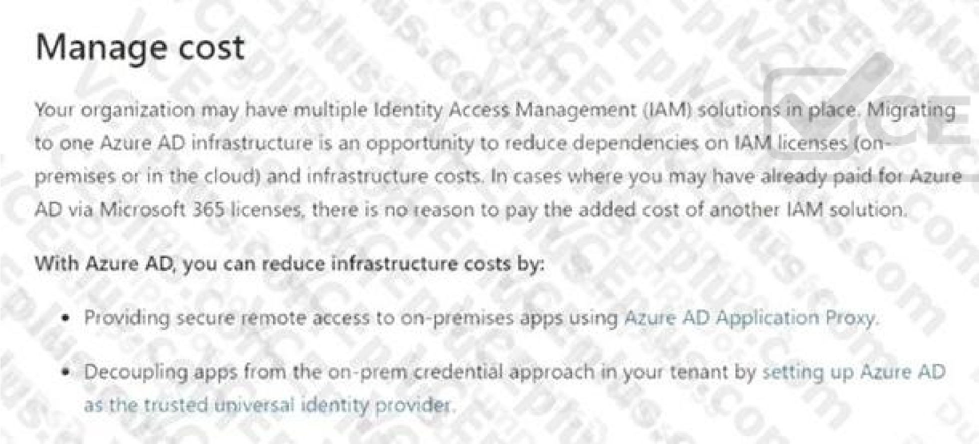
QUESTION 22
An organization is implementing a new identity and access management architecture with the following objectives:
Supporting MFA against on-premises infrastructure

Improving the user experience by integrating with SaaS applications
Applying risk-based policies based on location Performing just-in-time provisioning Which of the following authentication protocols should the organization implement to support these requirements?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 23
An e-commerce company is running a web server on premises, and the resource utilization is usually less than 30%. During the last two holiday seasons, the server experienced performance issues because of too many connections, and several customers were not able to finalize purchase orders. The company is looking to change the server configuration to avoid this kind of performance issue.
Which of the following is the MOST cost-effective solution?

A. Move the server to a cloud provider.
B. Change the operating system.

C. Buy a new server and create an active-active cluster.

D. Upgrade the server with a new one.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24

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.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 25

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

A. Instance-based

B. Storage-based

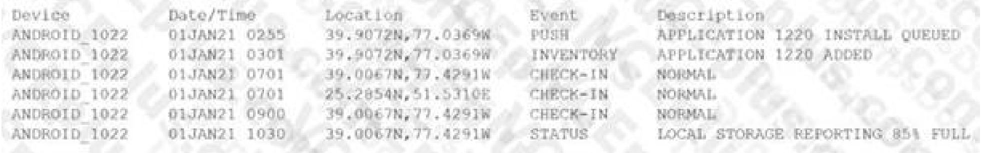
C. Proxy-based

D. Array controller-based

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Device event logs sources from MDM software as follows:



```
Device          Date/Time       Location              Event       Description
ANDROID_1022    01JAN21 0255    39.9072N,77.0369W     PUSH        APPLICATION 1220 INSTALL QUEUED
ANDROID_1022    01JAN21 0301    39.9072N,77.0369W     INVENTORY   APPLICATION 1220 ADDED
ANDROID_1022    01JAN21 0701    39.0067N,77.4291W     CHECK-IN    NORMAL
ANDROID_1022    01JAN21 0701    25.2854N,51.5310E     CHECK-IN    NORMAL
ANDROID_1022    01JAN21 0900    39.0067N,77.4291W     CHECK-IN    NORMAL
ANDROID_1022    01JAN21 1030    39.0067N,77.4291W     STATUS      LOCAL STORAGE REPORTING 85% FULL
```

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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

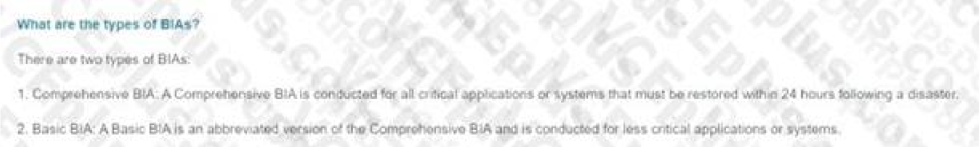
QUESTION 27
An organization is referencing NIST best practices for BCP creation while reviewing current internal organizational processes for mission-essential items.
Which of the following phases establishes the identification and prioritization of critical systems and functions?

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

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://itsm.ucsf.edu/business-impact-analysis-bia-0



What are the types of BIAs?

There are two types of BIAs:

1. Comprehensive BIA: A Comprehensive BIA is conducted for all critical applications or systems that must be restored within 24 hours following a disaster.

2. Basic BIA: A Basic BIA is an abbreviated version of the Comprehensive BIA and is conducted for less critical applications or systems.

QUESTION 28
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.

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 29
A home automation company just purchased and installed tools for its SOC to enable incident identification and response on software the company develops. The company would like to prioritize defenses against the following attack scenarios:
Unauthorized insertions into application development environments
Authorized insiders making unauthorized changes to environment configurations Which of the following actions will enable the data feeds needed to detect these types of attacks on development environments? (Choose two.)

A. Perform static code analysis of committed code and generate summary reports.

B. Implement an XML gateway and monitor for policy violations.

C. Monitor dependency management tools and report on susceptible third-party libraries.

D. Install an IDS on the development subnet and passively monitor for vulnerable services.

E. Model user behavior and monitor for deviations from normal.

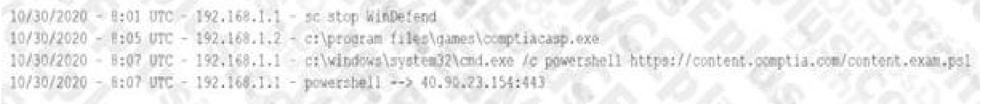
F. Continuously monitor code commits to repositories and generate summary logs.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30

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



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

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

A. Disable powershell.exe on all Microsoft Windows endpoints.

B. Restart Microsoft Windows Defender.

C. Configure the forward proxy to block 40.90.23.154.

D. Disable local administrator privileges on the endpoints.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31

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

A. Monitor camera footage corresponding to a valid access request.

B. Require both security and management to open the door.

C. Require department managers to review denied-access requests.

D. Issue new entry badges on a weekly basis.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://www.getkisi.com/access-control

QUESTION 32
Ransomware encrypted the entire human resources fileshare for a large financial institution. Security operations personnel were unaware of the activity until it was too late to stop it. The restoration will take approximately four hours, and the last backup occurred 48 hours ago. The management team has indicated that the RPO for a disaster recovery event for this data classification is 24 hours.
Based on RPO requirements, which of the following recommendations should the management team make?

A. Leave the current backup schedule intact and pay the ransom to decrypt the data.

B. Leave the current backup schedule intact and make the human resources fileshare read-only.

C. Increase the frequency of backups and create SIEM alerts for IOCs.

D. Decrease the frequency of backups and pay the ransom to decrypt the data.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
A security engineer thinks the development team has been hard-coding sensitive environment variables in its code.
Which of the following would BEST secure the company's CI/CD pipeline?

A. Utilizing a trusted secrets manager

B. Performing DAST on a weekly basis

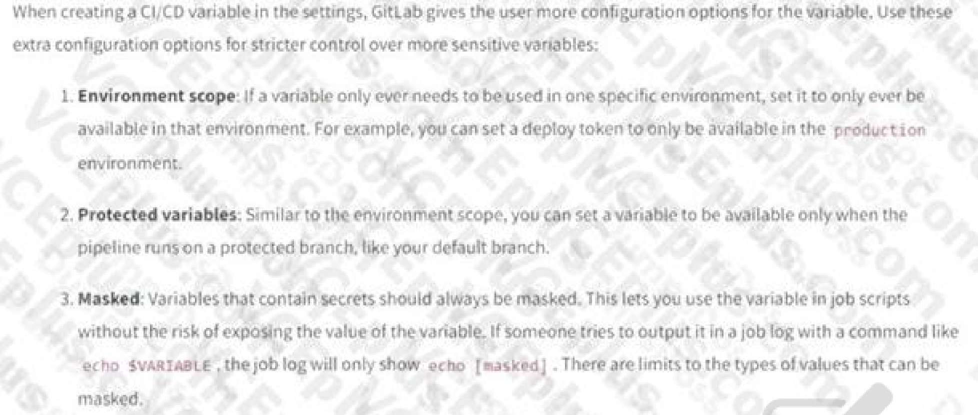
C. Introducing the use of container orchestration

D. Deploying instance tagging

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 34
A vulnerability analyst identified a zero-day vulnerability in a company's internally developed software. Since the current vulnerability management system does not have any checks for this vulnerability, an engineer has been asked to create one.
Which of the following would be BEST suited to meet these requirements?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Which of the following terms refers to the delivery of encryption keys to a CASB or a third-party entity?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://www.open.edu/openlearn/ocw/mod/oucontent/view.php?id=48322§ion=1.3

QUESTION 36
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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 37
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
A developer is creating a new mobile application for a company. The application uses REST API and TLS 1.2 to communicate securely with the external back-end server. Due to this configuration, the company is concerned about HTTPS interception attacks.
Which of the following would be the BEST solution against this type of attack?

A. Cookies

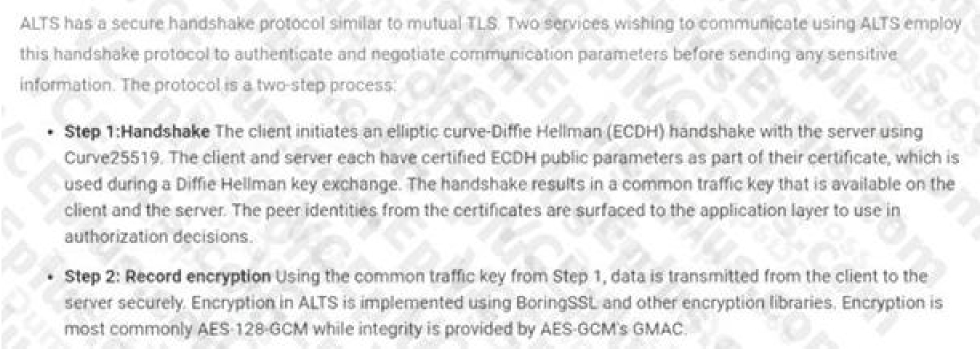
B. Wildcard certificates

C. HSTS

D. Certificate pinning

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://cloud.google.com/security/encryption-in-transit



ALTS has a secure handshake protocol similar to mutual TLS. Two services wishing to communicate using ALTS employ this handshake protocol to authenticate and negotiate communication parameters before sending any sensitive information. The protocol is a two-step process:

- **Step 1:Handshake** The client initiates an elliptic curve-Diffie Hellman (ECDH) handshake with the server using Curve25519. The client and server each have certified ECDH public parameters as part of their certificate, which is used during a Diffie Hellman key exchange. The handshake results in a common traffic key that is available on the client and the server. The peer identities from the certificates are surfaced to the application layer to use in authorization decisions.
- **Step 2: Record encryption** Using the common traffic key from Step 1, data is transmitted from the client to the server securely. Encryption in ALTS is implemented using BoringSSL and other encryption libraries. Encryption is most commonly AES-128-GCM while integrity is provided by AES-GCM's GMAC.

QUESTION 39

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

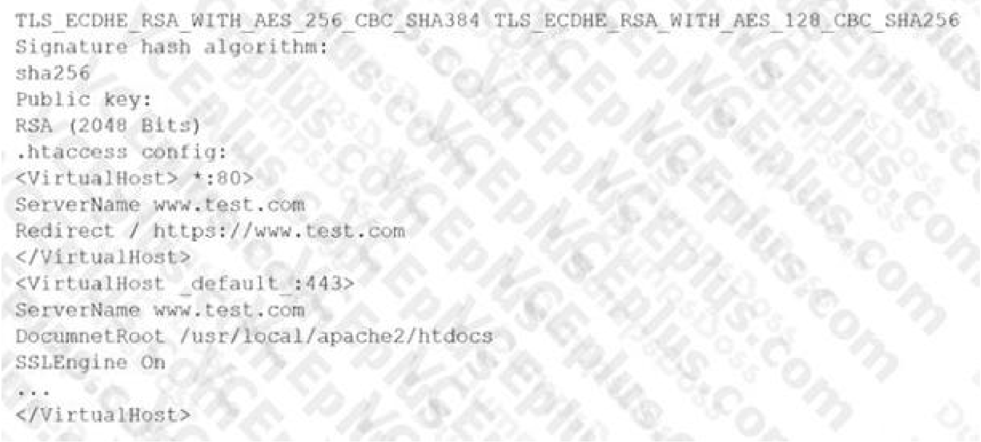
QUESTION 40
A company hired a third party to develop software as part of its strategy to be quicker to market. The company's policy outlines the following requirements:
The credentials used to publish production software to the container registry should be stored in a secure location.
Access should be restricted to the pipeline service account, without the ability for the third-party developer to read the credentials directly.
Which of the following would be the BEST recommendation for storing and monitoring access to these shared credentials?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/tpm-fundamentals

QUESTION 41
A customer reports being unable to connect to a website at www.test.com to consume services. The customer notices the web application has the following published cipher suite:



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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://security.stackexchange.com/questions/23383/ssh-key-type-rsa-dsa-ecdsa-are-there-easy-answers-forwhich-to-choose-when

QUESTION 42
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
A Chief Information Officer is considering migrating all company data to the cloud to save money on expensive SAN storage.
Which of the following is a security concern that will MOST likely need to be addressed during migration?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

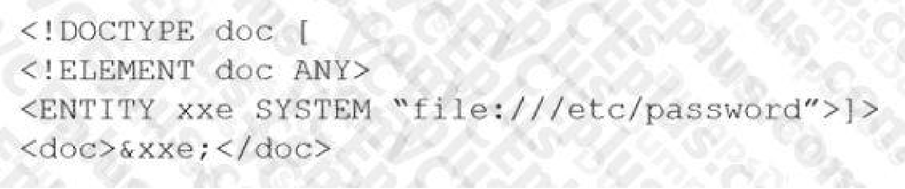
QUESTION 44
A developer wants to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users. Which of the following would be BEST for the developer to perform? (Choose two.)

A. Utilize code signing by a trusted third party.
B. Implement certificate-based authentication.
C. Verify MD5 hashes.
D. Compress the program with a password.
E. Encrypt with 3DES.
F. Make the DACL read-only.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
A security analyst discovered that the company's WAF was not properly configured. The main web server was breached, and the following payload was found in one of the malicious requests:



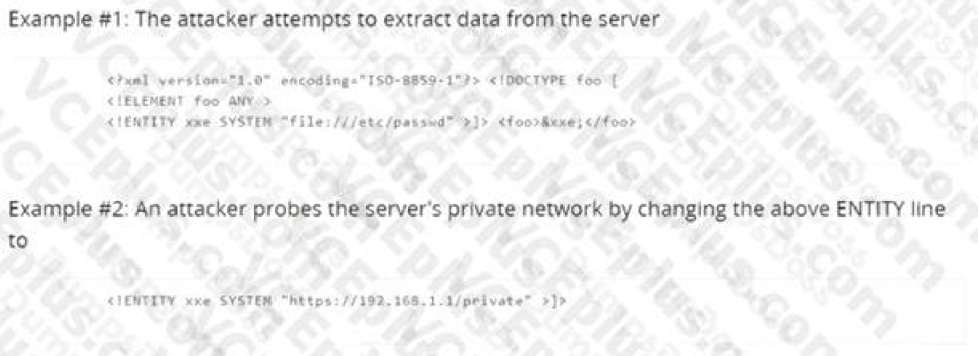
```
<!DOCTYPE doc [
<!ELEMENT doc ANY>
<ENTITY xxe SYSTEM "file:///etc/password">]>
<doc>&xxe;</doc>
```

Which of the following would BEST mitigate this vulnerability?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://hdivsecurity.com/owasp-xml-external-entities-xxe



Example #1: The attacker attempts to extract data from the server

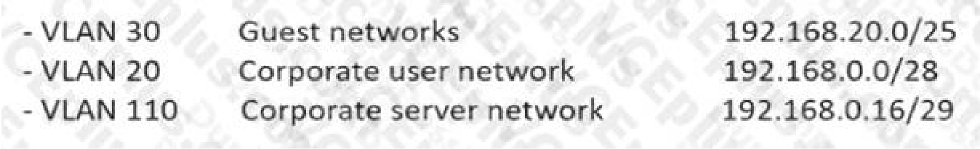
```
<?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE foo [
<!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]> <foo>&xxe;</foo>
```

Example #2: An attacker probes the server's private network by changing the above ENTITY line to

```
<!ENTITY xxe SYSTEM "https://192.168.1.1/private" >]>
```

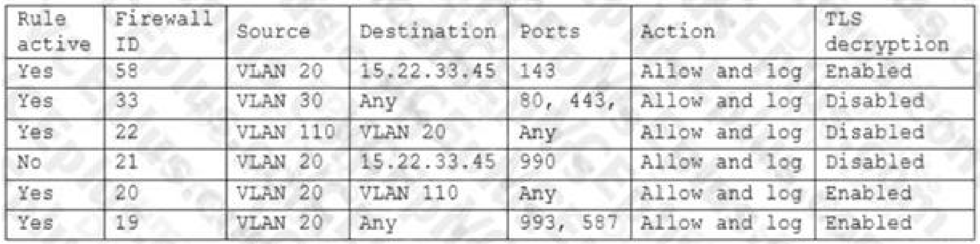
QUESTION 46
A security engineer has been asked to close all non-secure connections from the corporate network. The engineer is attempting to understand why the corporate

UTM will not allow users to download email via IMAPS. The engineer formulates a theory and begins testing by creating the firewall ID 58, and users are able to download emails correctly by using IMAP instead. The network comprises three VLANs:



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

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



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

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

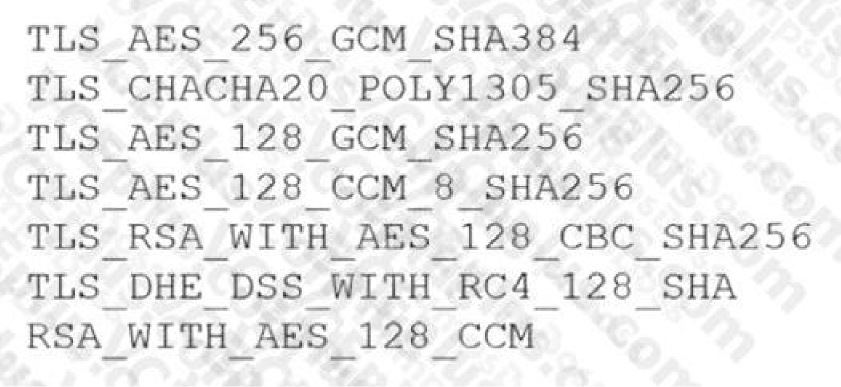
A. Contact the email service provider and ask if the company IP is blocked.
B. Confirm the email server certificate is installed on the corporate computers.
C. Make sure the UTM certificate is imported on the corporate computers.
D. Create an IMAPS firewall rule to ensure email is allowed.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
A security analyst is performing a vulnerability assessment on behalf of a client. The analyst must define what constitutes a risk to the organization.
Which of the following should be the analyst’s FIRST action?

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

Correct Answer: C
Section: (none)
Explanation

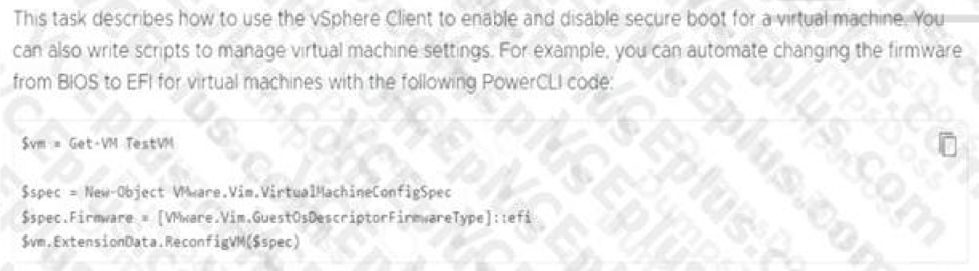
Explanation/Reference:

QUESTION 49
A systems administrator is in the process of hardening the host systems before connecting to the network. The administrator wants to add protection to the boot loader to ensure the hosts are secure before the OS fully boots.
Which of the following would provide the BEST boot loader protection?

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

Correct Answer: D
Section: (none)
Explanation

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



This task describes how to use the vSphere Client to enable and disable secure boot for a virtual machine. You can also write scripts to manage virtual machine settings. For example, you can automate changing the firmware from BIOS to EFI for virtual machines with the following PowerCLI code:

```
$vm = Get-VM TestVM

$spec = New-Object VMware.Vim.VirtualMachineConfigSpec
$spec.Firmware = [VMware.Vim.GuestOsDescriptorFirmwareType]::efi
$vm.ExtensionData.ReconfigVM($spec)
```

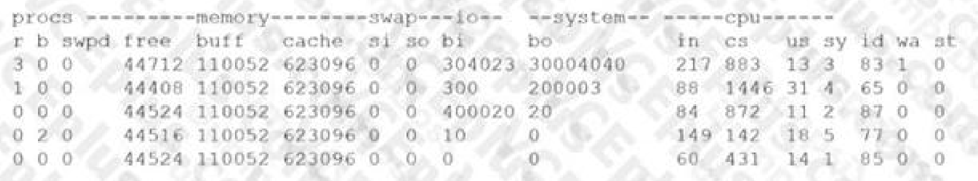
QUESTION 50
An organization’s hunt team thinks a persistent threats exists and already has a foothold in the enterprise network.
Which of the following techniques would be BEST for the hunt team to use to entice the adversary to uncover malicious activity?

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.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 51
A security analyst is concerned that a malicious piece of code was downloaded on a Linux system. After some research, the analyst determines that the suspected piece of code is performing a lot of input/ output (I/O) on the disk drive.



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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
All staff at a company have started working remotely due to a global pandemic. To transition to remote work, the company has migrated to SaaS collaboration tools. The human resources department wants to use these tools to process sensitive information but is concerned the data could be:
Leaked to the media via printing of the documents
Sent to a personal email address
Accessed and viewed by systems administrators Uploaded to a file storage site Which of the following would mitigate the department’s concerns?

A. Data loss detection, reverse proxy, EDR, and PGP

B. VDI, proxy, CASB, and DRM
C. Watermarking, forward proxy, DLP, and MFA
D. Proxy, secure VPN, endpoint encryption, and AV

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
A security analyst is reviewing network connectivity on a Linux workstation and examining the active TCP connections using the command line.
Which of the following commands would be the BEST to run to view only active Internet connections?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://www.codegrepper.com/code-examples/shell/netstat+find+port

QUESTION 54
A small company recently developed prototype technology for a military program. The company’s security engineer is concerned about potential theft of the newly developed, proprietary information.
Which of the following should the security engineer do to BEST manage the threats proactively?

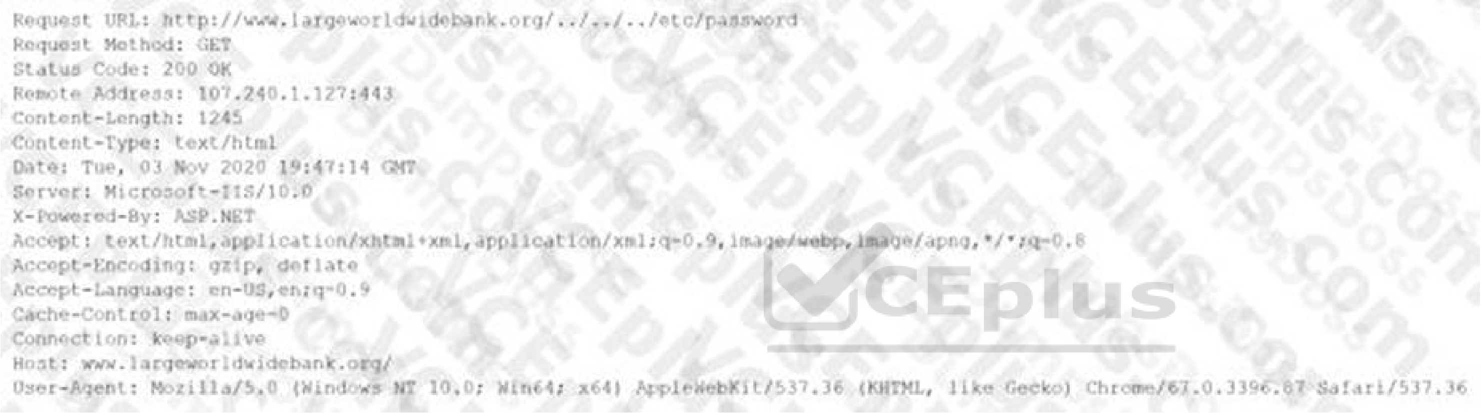
A. Join an information-sharing community that is relevant to the company.
B. Leverage the MITRE ATT&CK framework to map the TTR.
C. Use OSINT techniques to evaluate and analyze the threats.

D. Update security awareness training to address new threats, such as best practices for data security.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
A security analyst is reviewing the following output:



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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56

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.

Correct Answer: B
Section: (none)
Explanation

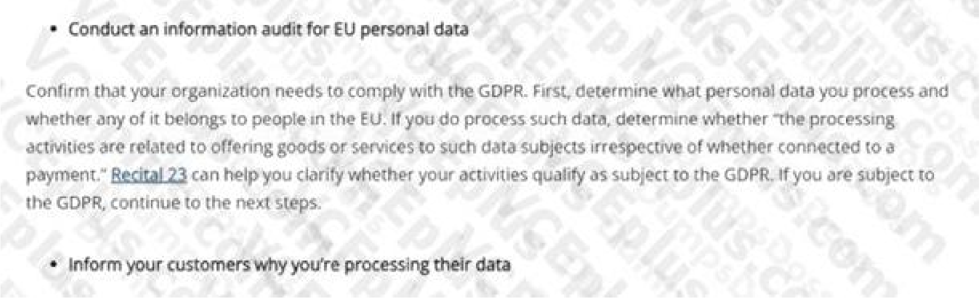
Explanation/Reference:
Explanation:
Reference: https://www.whitesourcesoftware.com/resources/blog/application-security-best-practices/

QUESTION 57
A company is preparing to deploy a global service.
Which of the following must the company do to ensure GDPR compliance? (Choose two.)

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 58
A company is looking to fortify its cybersecurity defenses and is focusing on its network infrastructure. The solution cannot affect the availability of the company's services to ensure false positives do not drop legitimate traffic.
Which of the following would satisfy the requirement?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://subscription.packtpub.com/book/networking-and-servers/9781782174905/5/ch05lvl1sec38/differentiatingbetween-nids-and-nips

QUESTION 59
Which of the following is the MOST important security objective when applying cryptography to control messages that tell an ICS how much electrical power to output?

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 60

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61

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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which of the following allows computation and analysis of data within a ciphertext without knowledge of the plaintext?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://searchsecurity.techtarget.com/definition/cryptanalysis

QUESTION 63
A security analyst is investigating a possible buffer overflow attack. The following output was found on a user's workstation: graphic.linux_randomization.prg
Which of the following technologies would mitigate the manipulation of memory segments?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: http://webpages.eng.wayne.edu/~fy8421/19sp-csc5290/labs/lab2-instruction.pdf (3)

QUESTION 64
An organization is considering a BYOD standard to support remote working. The first iteration of the solution will utilize only approved collaboration applications and the ability to move corporate data between those applications. The security team has concerns about the following:

Unstructured data being exfiltrated after an employee leaves the organization Data being exfiltrated as a result of compromised credentials Sensitive information in emails being exfiltrated Which of the following solutions should the security team implement to mitigate the risk of data loss?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://www.garykessler.net/library/fsc_stego.html

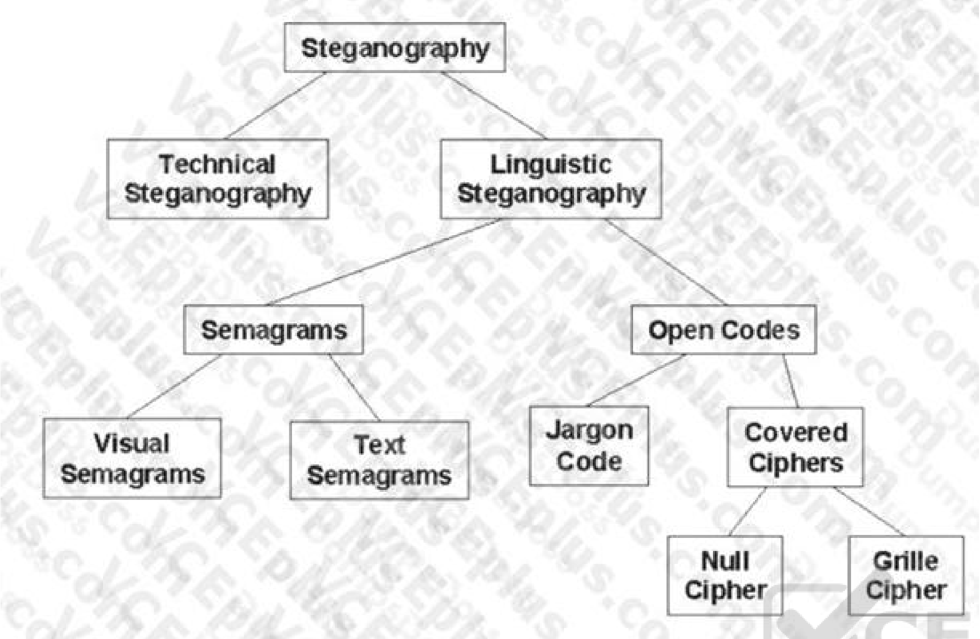


Figure 1. Classification of Steganography Techniques (Adapted from Bauer 2002).

QUESTION 66

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

A. Peer-to-peer secure communications enabled by mobile applications

B. Proxied application data connections enabled by API gateways

C. Microsegmentation enabled by software-defined networking

D. VLANs enabled by network infrastructure devices

Correct Answer: C
Section: (none)
Explanation

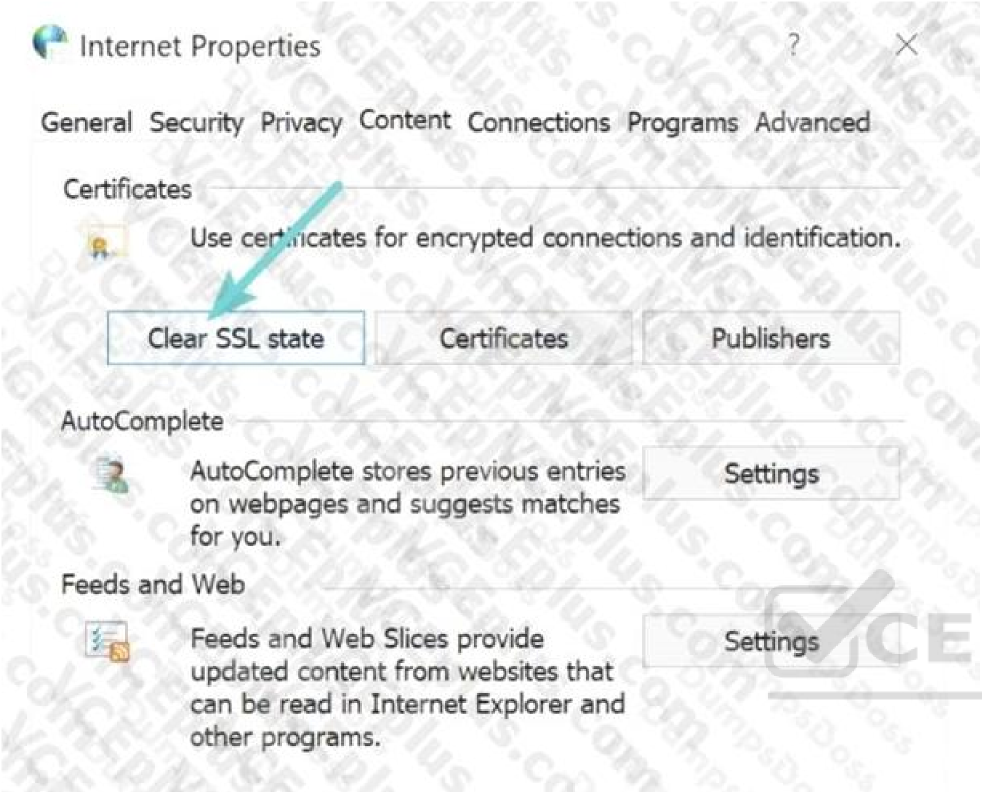
Explanation/Reference:

QUESTION 67
An application server was recently upgraded to prefer TLS 1.3, and now users are unable to connect their clients to the server. Attempts to reproduce the error are confirmed, and clients are reporting the following:
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
Which of the following is MOST likely the root cause?

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

Correct Answer: C
Section: (none)
Explanation

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



Use certificates for encrypted connections and identification.

AutoComplete stores previous entries on webpages and suggests matches for you.

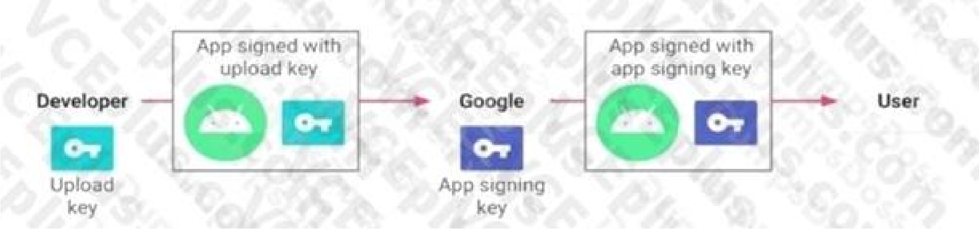
Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.

QUESTION 68
A company publishes several APIs for customers and is required to use keys to segregate customer data sets.
Which of the following would be BEST to use to store customer keys?

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

Correct Answer: C
Section: (none)
Explanation

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



QUESTION 69
A university issues badges through a homegrown identity management system to all staff and students. Each week during the summer, temporary summer school students arrive and need to be issued a badge to access minimal campus resources.
The security team received a report from an outside auditor indicating the homegrown system is not consistent with best practices in the security field and leaves the institution vulnerable.
Which of the following should the security team recommend FIRST?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
A satellite communications ISP frequently experiences outages and degraded modes of operation over one of its legacy satellite links due to the use of deprecated hardware and software. Three days per week, on average, a contracted company must follow a checklist of 16 different high-latency commands that must be run in serial to restore nominal performance. The ISP wants this process to be automated.
Which of the following techniques would be BEST suited for this requirement?

A. Deploy SOAR utilities and runbooks.
B. Replace the associated hardware.
C. Provide the contractors with direct access to satellite telemetry data.

D. Reduce link latency on the affected ground and satellite segments.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
A company plans to build an entirely remote workforce that utilizes a cloud-based infrastructure. The Chief Information Security Officer asks the security engineer to design connectivity to meet the following requirements:
Only users with corporate-owned devices can directly access servers hosted by the cloud provider. The company can control what SaaS applications each individual user can access. User browser activity can be monitored.
Which of the following solutions would BEST meet these requirements?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
An organization recently experienced a ransomware attack. The security team leader is concerned about the attack reoccurring. However, no further security measures have been implemented.
Which of the following processes can be used to identify potential prevention recommendations?

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
A company created an external application for its customers. A security researcher now reports that the application has a serious LDAP injection vulnerability that could be leveraged to bypass authentication and authorization.
Which of the following actions would BEST resolve the issue? (Choose two.)

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
A company has hired a security architect to address several service outages on the endpoints due to new malware. The Chief Executive Officer's laptop was impacted while working from home. The goal is to prevent further endpoint disruption.
The edge network is protected by a web proxy.
Which of the following solutions should the security architect recommend?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77

DRAG DROP

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

INSTRUCTIONS

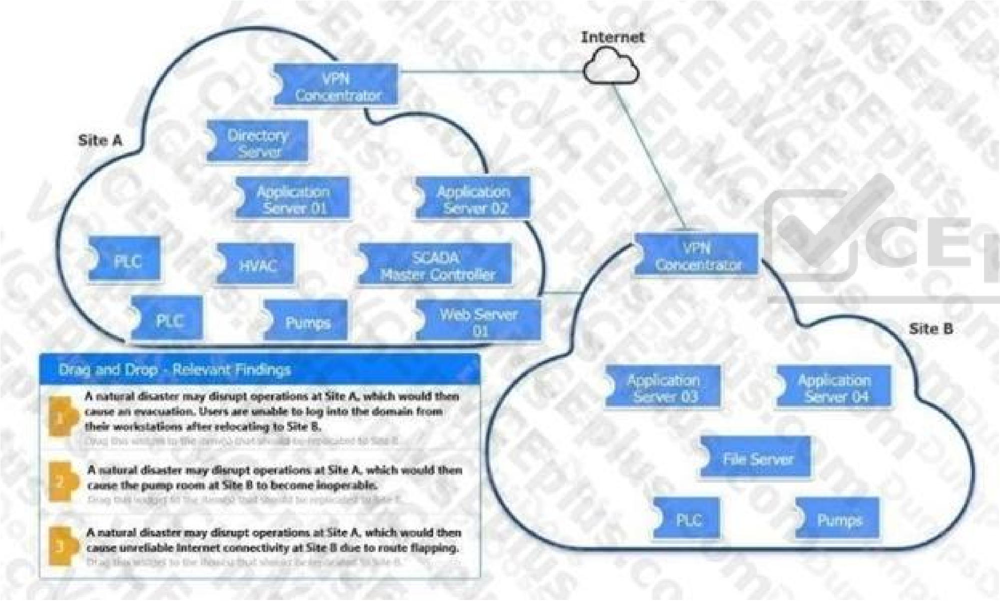
Review the following scenarios and instructions. Match each relevant finding to the affected host.

After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective action for that finding.

Each finding may be used more than once.

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

Select and Place:



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 device(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 device(s) that should be replicated to Site B.

3 A natural disaster may disrupt operations at Site A, which would then cause unreliable Internet connectivity at Site B due to route flapping.
Drag this widget to the device(s) that should be replicated to Site B.

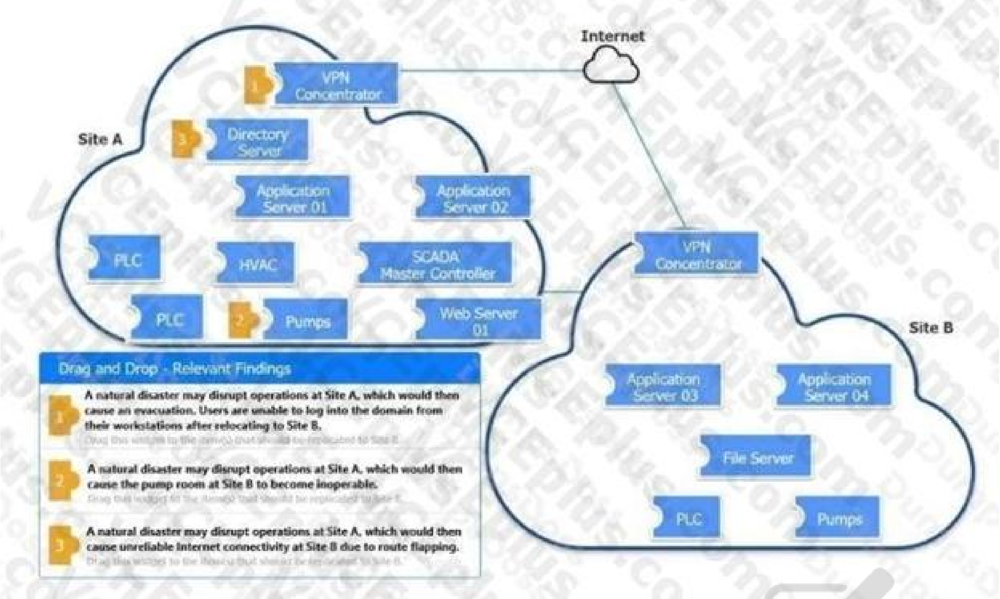
A.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



Drag and Drop - Relevant Findings

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 device(s) that should be replicated to Site B.

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 device(s) that should be replicated to Site B.

A natural disaster may disrupt operations at Site A, which would then cause unreliable Internet connectivity at Site B due to route flapping.
Drag this widget to the device(s) that should be replicated to Site B.

Explanation:

QUESTION 78

An organization is preparing to migrate its production environment systems from an on-premises environment to a cloud service. The lead security architect is concerned that the organization's current methods for addressing risk may not be possible in the cloud environment.

Which of the following BEST describes the reason why traditional methods of addressing risk may not be possible in the cloud?

A. Migrating operations assumes the acceptance of all risk.

B. Cloud providers are unable to avoid risk.

C. Specific risks cannot be transferred to the cloud provider.

D. Risks to data in the cloud cannot be mitigated.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Reference: https://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf

QUESTION 79
After a security incident, a network security engineer discovers that a portion of the company's sensitive external traffic has been redirected through a secondary ISP that is not normally used.
Which of the following would BEST secure the routes while allowing the network to function in the event of a single provider failure?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
A business stores personal client data of individuals residing in the EU in order to process requests for mortgage loan approvals.
Which of the following does the business's IT manager need to consider?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://gdpr.eu/right-to-beforgotten/#:~:text=Also%20known%20as%20the%20right,to%20delete%20their%20personal%20data.&text=The%20General%20Data%20Protection%20Regulation,collected%2C%20processed%2C%20and%20erased

QUESTION 81
An organization wants to perform a scan of all its systems against best practice security configurations.
Which of the following SCAP standards, when combined, will enable the organization to view each of the configuration checks in a machine-readable checklist format for fill automation? (Choose two.)

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

Correct Answer: BF
Section: (none)
Explanation

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

QUESTION 82
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

Correct Answer: A
Section: (none)
Explanation

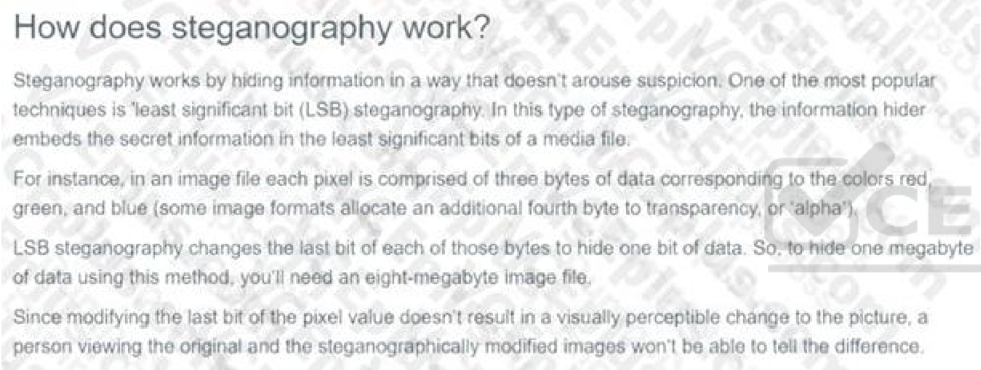
Explanation/Reference:

QUESTION 83
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.