# Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

**https://www.2passeasy.com/dumps/CAS-004/**

**NEW QUESTION 1**
Which of the following BEST sets expectation between the security team and business units within an organization?

A. Risk assessment
B. Memorandum of understanding
C. Business impact analysis
D. Business partnership agreement
E. Services level agreement

**Answer:** C

**NEW QUESTION 2**
A company is looking for a solution to hide data stored in databases. The solution must meet the following requirements:
- Be efficient at protecting the production environment
- Not require any change to the application
- Act at the presentation layer

Which of the following techniques should be used?

A. Masking
B. Tokenization
C. Algorithmic
D. Random substitution

**Answer:** A

**NEW QUESTION 3**
Which of the following is the BEST disaster recovery solution when resources are running in a cloud environment?

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

**Answer:** B

**NEW QUESTION 4**
A security analyst detected a malicious PowerShell attack on a single server. The malware used the
Invoke-Expression function to execute an external malicious script. The security analyst scanned the disk with an antivirus application and did not find any IOCs.
The security analyst now needs to deploy a protection solution against this type of malware.
Which of the following BEST describes the type of malware the solution should protect against?

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

**Answer:** C

**NEW QUESTION 5**
A security consultant needs to protect a network of electrical relays that are used for monitoring and controlling the energy used in a manufacturing facility.
Which of the following systems should the consultant review before making a recommendation?

A. CAN
B. ASIC
C. FPGA
D. SCADA

**Answer:** D

**NEW QUESTION 6**
A company wants to quantify and communicate the effectiveness of its security controls but must establish measures. Which of the following is MOST likely to be included in an effective assessment roadmap for these controls?

A. Create a change management process.
B. Establish key performance indicators.
C. Create an integrated master schedule.
D. Develop a communication plan.
E. Perform a security control assessment.

**Answer:** C

**NEW QUESTION 7**
An organization is prioritizing efforts to remediate or mitigate risks identified during the latest assessment. For one of the risks, a full remediation was not possible, but the organization was able to successfully apply mitigations to reduce the likelihood of impact.

Which of the following should the organization perform NEXT?

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

**Answer:** A

**NEW QUESTION 8**
A threat hunting team receives a report about possible APT activity in the network. Which of the following threat management frameworks should the team implement?

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

**Answer:** A

**NEW QUESTION 9**
A company is outsourcing to an MSSP that performs managed detection and response services. The MSSP requires a server to be placed inside the network as a log aggregate and allows remote access to MSSP analyst. Critical devices send logs to the log aggregator, where data is stored for 12 months locally before being archived to a multitenant cloud. The data is then sent from the log aggregate to a public IP address in the MSSP datacenter for analysis.
A security engineer is concerned about the security of the solution and notes the following.
* The critical devise send cleartext logs to the aggregator.
* The log aggregator utilize full disk encryption.
* The log aggregator sends to the analysis server via port 80.
* MSSP analysis utilize an SSL VPN with MFA to access the log aggregator remotely.
* The data is compressed and encrypted prior to being achieved in the cloud. Which of the following should be the engineer's GREATEST concern?

A. Hardware vulnerabilities introduced by the log aggregate server
B. Network bridging from a remote access VPN
C. Encryption of data in transit
D. Multinancy and data remnants in the cloud

**Answer:** C

**NEW QUESTION 10**
An e-commerce company is running a web server on premises, and the resource utilization is usually less than 30%. During the last two holiday seasons, the server experienced performance issues because of too many connections, and several customers were not able to finalize purchase orders. The company is looking to change the server configuration to avoid this kind of performance issue.
Which of the following is the MOST cost-effective solution?

A. Move the server to a cloud provider.
B. Change the operating system.
C. Buy a new server and create an active-active cluster.
D. Upgrade the server with a new one.

**Answer:** A

**NEW QUESTION 10**
A security analyst is performing a vulnerability assessment on behalf of a client. The analyst must define what constitutes a risk to the organization.
Which of the following should be the analyst's FIRST action?

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

**Answer:** A

**NEW QUESTION 11**
A software house is developing a new application. The application has the following requirements: Reduce the number of credential requests as much as possible Integrate with social networks Authenticate users
Which of the following is the BEST federation method to use for the application?

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

**Answer:** D

**NEW QUESTION 15**
Which of the following is the MOST important security objective when applying cryptography to control messages that tell an ICS how much electrical power to output?

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

**Answer:** D

**NEW QUESTION 16**
Device event logs sources from MDM software as follows:

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

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

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

**Answer:** A

**NEW QUESTION 20**
A healthcare system recently suffered from a ransomware incident As a result the board of directors decided to hire a security consultant to improve existing network security. The security consultant found that the healthcare network was completely flat, had no privileged access limits and had open RDP access to servers with personal health information. As the consultant builds the remediation plan, which of the following solutions would BEST solve these challenges? (Select THREE).

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

**Answer:** ACE

**NEW QUESTION 25**
A high-severity vulnerability was found on a web application and introduced to the enterprise. The vulnerability could allow an unauthorized user to utilize an open-source library to view privileged user information. The enterprise is unwilling to accept the risk, but the developers cannot fix the issue right away.
Which of the following should be implemented to reduce the risk to an acceptable level until the issue can be fixed?

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

**Answer:** C

**NEW QUESTION 30**
During a system penetration test, a security engineer successfully gained access to a shell on a Linux host as a standard user and wants to elevate the privilege levels.
Which of the following is a valid Linux post-exploitation method to use to accomplish this goal?

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

**Answer:** A

**NEW QUESTION 32**
Leveraging cryptographic solutions to protect data that is in use ensures the data is encrypted:

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

**Answer:** B

**NEW QUESTION 35**
An organization is considering a BYOD standard to support remote working. The first iteration of the solution will utilize only approved collaboration applications and the ability to move corporate data between those applications. The security team has concerns about the following:
Unstructured data being exfiltrated after an employee leaves the organization Data being exfiltrated as a result of compromised credentials
Sensitive information in emails being exfiltrated
Which of the following solutions should the security team implement to mitigate the risk of data loss?

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

**Answer:** A

**NEW QUESTION 36**
A large telecommunications equipment manufacturer needs to evaluate the strengths of security controls in a new telephone network supporting first responders.
Which of the following techniques would the company use to evaluate data confidentiality controls?

A. Eavesdropping
B. On-path
C. Cryptanalysis
D. Code signing
E. RF sidelobe sniffing

**Answer:** A

**NEW QUESTION 40**
Which of the following represents the MOST significant benefit of implementing a passwordless authentication solution?

A. Biometric authenticators are immutable.
B. The likelihood of account compromise is reduced.
C. Zero trust is achieved.
D. Privacy risks are minimized.

**Answer:** B

**NEW QUESTION 44**
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 Of 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.

**Answer:** A

**NEW QUESTION 47**
A security engineer at a company is designing a system to mitigate recent setbacks caused competitors that are beating the company to market with the new products. Several of the products incorporate propriety enhancements developed by the engineer's company. The network already includes a SEIM and a NIPS and requires 2FA for all user access. Which of the following system should the engineer consider NEXT to mitigate the associated risks?

A. DLP
B. Mail gateway
C. Data flow enforcement
D. UTM

**Answer:** A

**NEW QUESTION 48**
A systems administrator is preparing to run a vulnerability scan on a set of information systems in the organization. The systems administrator wants to ensure that the targeted systems produce accurate information especially regarding configuration settings.
Which of the following scan types will provide the systems administrator with the MOST accurate information?

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

**Answer:** D

**NEW QUESTION 53**
A security engineer needs to recommend a solution that will meet the following requirements: Identify sensitive data in the provider's network

Maintain compliance with company and regulatory guidelines
Detect and respond to insider threats, privileged user threats, and compromised accounts Enforce datacentric security, such as encryption, tokenization, and access control
Which of the following solutions should the security engineer recommend to address these requirements?

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

**Answer:** B

**Explanation:**
https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/what-is-a-casb.html

**NEW QUESTION 58**
A cybersecurity analyst discovered a private key that could have been exposed.
Which of the following is the BEST way for the analyst to determine if the key has been compromised?

A. HSTS
B. CRL
C. CSRs
D. OCSP

**Answer:** C

**NEW QUESTION 61**
Ransomware encrypted the entire human resources fileshare for a large financial institution. Security operations personnel were unaware of the activity until it was too late to stop it. The restoration will take approximately four hours, and the last backup occurred 48 hours ago. The management team has indicated that the RPO for a disaster recovery event for this data classification is 24 hours.
Based on RPO requirements, which of the following recommendations should the management team make?

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

**Answer:** C

**NEW QUESTION 62**
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.

**Answer:** D

**NEW QUESTION 63**
Which of the following technologies allows CSPs to add encryption across multiple data storages?

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

**Answer:** D

**NEW QUESTION 68**
A company provides guest WiFi access to the internet and physically separates the guest network from the company's internal WIFI. Due to a recent incident in which an attacker gained access to the compay's intend WIFI, the company plans to configure WPA2 Enterprise in an EAP- TLS configuration. Which of the following must be installed on authorized hosts for this new configuration to work properly?

A. Active Directory OPOs
B. PKI certificates
C. Host-based firewall
D. NAC persistent agent

**Answer:** B

**NEW QUESTION 73**
A company security engineer arrives at work to face the following scenario:
1) Website defacement
2) Calls from the company president indicating the website needs to be fixed Immediately because It Is damaging the brand
3) A Job offer from the company's competitor
4) A security analyst's investigative report, based on logs from the past six months, describing how lateral movement across the network from various IP addresses originating from a foreign adversary country resulted in exfiltrated data
Which of the following threat actors Is MOST likely involved?

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

**Answer:** C

**NEW QUESTION 74**
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

**Answer:** D

**NEW QUESTION 75**
An administrator at a software development company would like to protect the integrity Of the company's applications with digital signatures. The developers report that the signing process keeps failing on all applications. The same key pair used for signing, however, is working properly on the website, is valid, and is issued by a trusted CA. Which of the following is MOST likely the cause of the signature failing?

A. The NTP server is set incorrectly for the developers.
B. The CA has included the certificate in its CRL_
C. The certificate is set for the wrong key usage.
D. Each application is missing a SAN or wildcard entry on the certificate.

**Answer:** C

**NEW QUESTION 78**
An organization is preparing to migrate its production environment systems from an on-premises environment to a cloud service. The lead security architect is concerned that the organization's current methods for addressing risk may not be possible in the cloud environment.
Which of the following BEST describes the reason why traditional methods of addressing risk may not be possible in the cloud?

A. Migrating operations assumes the acceptance of all risk.
B. Cloud providers are unable to avoid risk.
C. Specific risks cannot be transferred to the cloud provider.
D. Risks to data in the cloud cannot be mitigated.

**Answer:** D

**NEW QUESTION 82**
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

**Answer:** A

**NEW QUESTION 84**
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.

**Answer:** BD

**NEW QUESTION 89**
A recent data breach stemmed from unauthorized access to an employee's company account with a cloud-based productivity suite. The attacker exploited excessive permissions granted to a third-party OAuth application to collect sensitive information. Which of the following BEST mitigates inappropriate access and permissions issues?

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

**Answer:** C

**NEW QUESTION 92**
A security analyst discovered that the company's WAF was not properly configured. The main web server was breached, and the following payload was found in one of the malicious requests:

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

Which of the following would BEST mitigate this vulnerability?

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

**Answer:** B

**NEW QUESTION 96**
A forensic investigator would use the foremost command for:

A. cloning disks.
B. analyzing network-captured packets.

C. recovering lost files.
D. extracting features such as email addresses

**Answer:** C

**NEW QUESTION 97**
A recent data breach revealed that a company has a number of files containing customer data across its storage environment. These files are individualized for each employee and are used in tracking various customer orders, inquiries, and issues. The files are not encrypted and can be accessed by anyone. The senior management team would like to address these issues without interrupting existing processes.
Which of the following should a security architect recommend?

A. A DLP program to identify which files have customer data and delete them
B. An ERP program to identify which processes need to be tracked
C. A CMDB to report on systems that are not configured to security baselines
D. A CRM application to consolidate the data and provision access based on the process and need

**Answer:** D

**NEW QUESTION 98**
A health company has reached the physical and computing capabilities in its datacenter, but the computing demand continues to increase. The infrastructure is fully virtualized and runs custom and commercial healthcare application that process sensitive health and payment information. Which of the following should the company implement to ensure it can meet the computing demand while complying with healthcare standard for virtualization and cloud computing?

A. Hybrid IaaS solution in a single-tenancy cloud
B. Pass solution in a multinency cloud
C. SaaS solution in a community cloud
D. Private SaaS solution in a single tenancy cloud.

**Answer:** D

**NEW QUESTION 103**
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

**Answer:** C

**Explanation:**
WPA3 SAE prevents brute-force attacks.
“WPA3 Personal (WPA-3 SAE) Mode is a static passphrase-based method. It provides better security than what WPA2 previously provided, even when a non-complex password is used, thanks to Simultaneous Authentication of Equals (SAE), the personal authentication process of WPA3.”

**NEW QUESTION 108**
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 horary 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 exfilltrate the data without detection.
Which of the following is the BEST solution to help prevent this type of attack from being successful in the future?

A. Dynamic analysis
B. Secure web gateway
C. Software composition analysis
D. User behavior analysis
E. Web application firewall

**Answer:** B

**NEW QUESTION 113**
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.
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

**Answer:** B

**NEW QUESTION 118**

A company is looking at sending historical backups containing customer PII to a cloud service provider to save on storage costs. Which of the following is the MOST important consideration before making this decision?

A. Availability
B. Data sovereignty
C. Geography
D. Vendor lock-in

**Answer:** B

**NEW QUESTION 120**
An organization is assessing the security posture of a new SaaS CRM system that handles sensitive Pll and identity information, such as passport numbers. The SaaS CRM system does not meet the organization's current security standards. The assessment identifies the following:
* 1- There will be a $20,000 per day revenue loss for each day the system is delayed going into production. * 2- The inherent risk is high.
* 3- The residual risk is low.
* 4- There will be a staged deployment to the solution rollout to the contact center.
Which of the following risk-handling techniques will BEST meet the organization's requirements?

A. Apply for a security exemption, as the risk is too high to accept.
B. Transfer the risk to the SaaS CRM vendor, as the organization is using a cloud service.
C. Accept the risk, as compensating controls have been implemented to manage the risk.
D. Avoid the risk by accepting the shared responsibility model with the SaaS CRM provider.

**Answer:** A

**NEW QUESTION 123**
Which of the following allows computation and analysis of data within a ciphertext without knowledge of the plaintext?

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

**Answer:** D

**NEW QUESTION 128**
Based on PCI DSS v3.4, One Particular database field can store data, but the data must be unreadable. which of the following data objects meets this requirement?

A. PAN
B. CVV2
C. Cardholder name
D. expiration date

**Answer:** A

**NEW QUESTION 131**
A security architect works for a manufacturing organization that has many different branch offices. The architect is looking for a way to reduce traffic and ensure the branch offices receive the latest copy of revoked certificates issued by the CA at the organization’s headquarters location. The solution must also have the lowest power requirement on the CA.
Which of the following is the BEST solution?

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

**Answer:** C

**NEW QUESTION 136**
Over the last 90 days, many storage services has been exposed in the cloud services environments, and the security team does not have the ability to see is creating these instance. Shadow IT is creating data services and instances faster than the small security team can keep up with them. The Chief information security Officer (CIASO) has asked the security officer (CISO) has asked the security lead architect to architect to recommend solutions to this problem.
Which of the following BEST addresses the problem best address the problem with the least amount of administrative effort?

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

**Answer:** C

**NEW QUESTION 137**
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

**Answer:** C

**NEW QUESTION 142**
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.

**Answer:** D

**NEW QUESTION 145**
A security analyst is validating the MAC policy on a set of Android devices. The policy was written to ensure non-critical applications are unable to access certain resources. When reviewing dmesg, the analyst notes many entries such as:
Despite the deny message, this action was still permit following is the MOST likely fix for this issue?

A. Add the objects of concern to the default context.
B. Set the devices to enforcing
C. Create separate domain and context files for irc.
D. Rebuild the policy, reinstall, and test.

**Answer:** B

**NEW QUESTION 149**
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

**Answer:** A

**Explanation:**
The concern is users operating in a spit tunnel config which is what is being described. Using a Full Tunnel would route traffic from all applications through a single tunnel.
https://cybernews.com/what-is-vpn/split-tunneling/

**NEW QUESTION 154**
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

**Answer:** C

**NEW QUESTION 156**
A cybersecurity analyst receives a ticket that indicates a potential incident is occurring. There has been a large in log files generated by a generated by a website

containing a ‘’Contact US’’ form. The analyst must determine if the increase in website traffic is due to a recent marketing campaign of if this is a potential incident. Which of the following would BEST assist the analyst?

A. Ensuring proper input validation is configured on the ‘’Contact US’’ form
B. Deploy a WAF in front of the public website
C. Checking for new rules from the inbound network IPS vendor
D. Running the website log files through a log reduction and analysis tool

**Answer:** D

**NEW QUESTION 158**
A company has decided to purchase a license for software that is used to operate a mission-critical process. The third-party developer is new to the industry but is delivering what the company needs at this time.
Which of the following BEST describes the reason why utilizing a source code escrow will reduce the operational risk to the company if the third party stops supporting the application?

A. The company will have access to the latest version to continue development.
B. The company will be able to force the third-party developer to continue support.
C. The company will be able to manage the third-party developer’s development process.
D. The company will be paid by the third-party developer to hire a new development team.

**Answer:** A

**NEW QUESTION 161**
The Chief information Officer (CIO) wants to establish a non-banding agreement with a third party that outlines the objectives of the mutual arrangement dealing with data transfers between both organizations before establishing a format partnership. Which of the follow would MOST likely be used?

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

**Answer:** A

**NEW QUESTION 166**
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.

**Answer:** A

**NEW QUESTION 167**
A cybersecurity engineer analyst a system for vulnerabilities. The tool created an OVAL. Results document as output. Which of the following would enable the engineer to interpret the results in a human readable form? (Select TWO.)

A. Text editor
B. OOXML editor
C. Event Viewer
D. XML style sheet
E. SCAP tool
F. Debugging utility

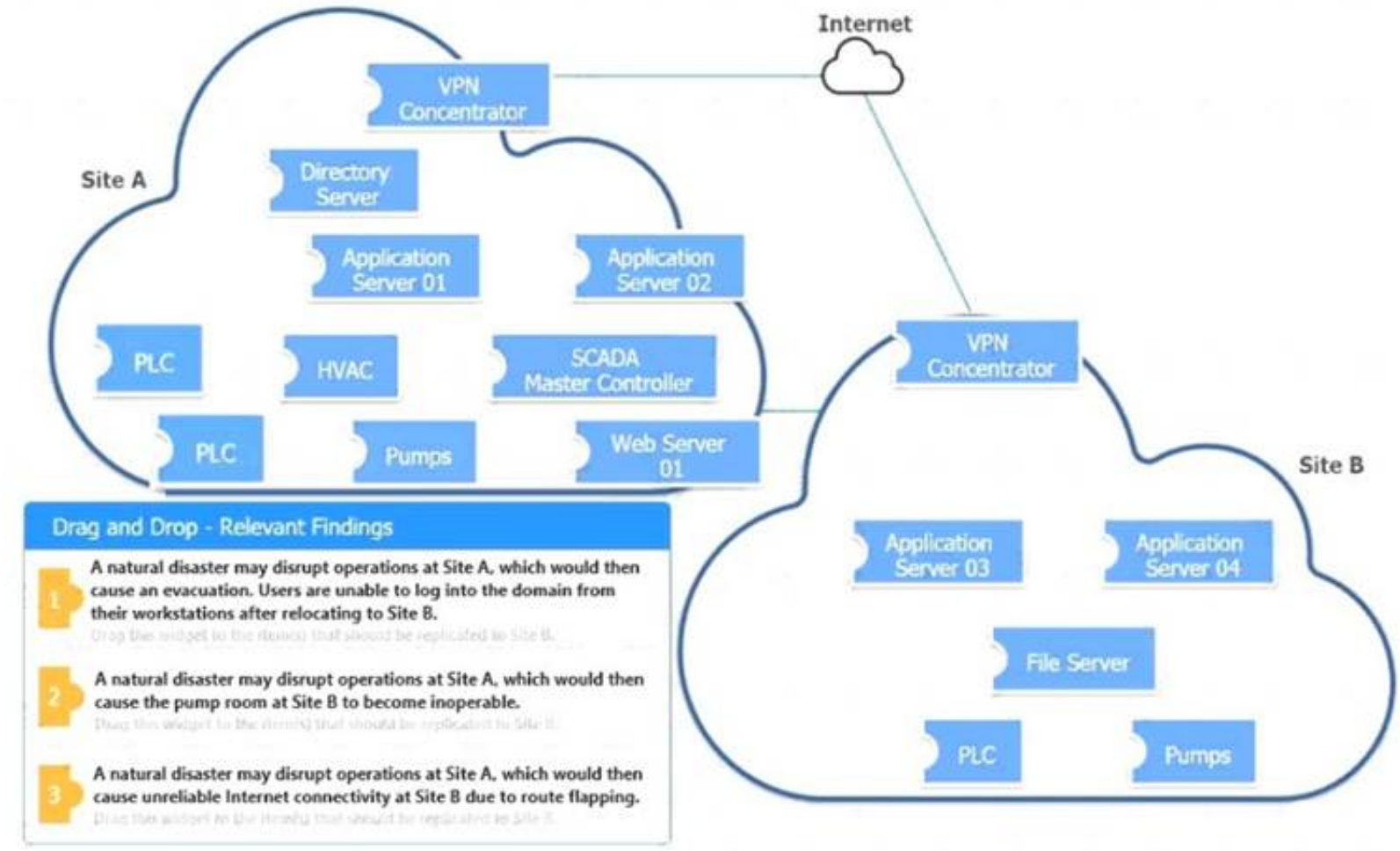
**Answer:** BD

**NEW QUESTION 170**
A company's finance department acquired a new payment system that exports data to an unencrypted file on the system. The company implemented controls on the file so only appropriate personnel are allowed access. Which of the following risk techniques did the department use in this situation?

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

**Answer:** D

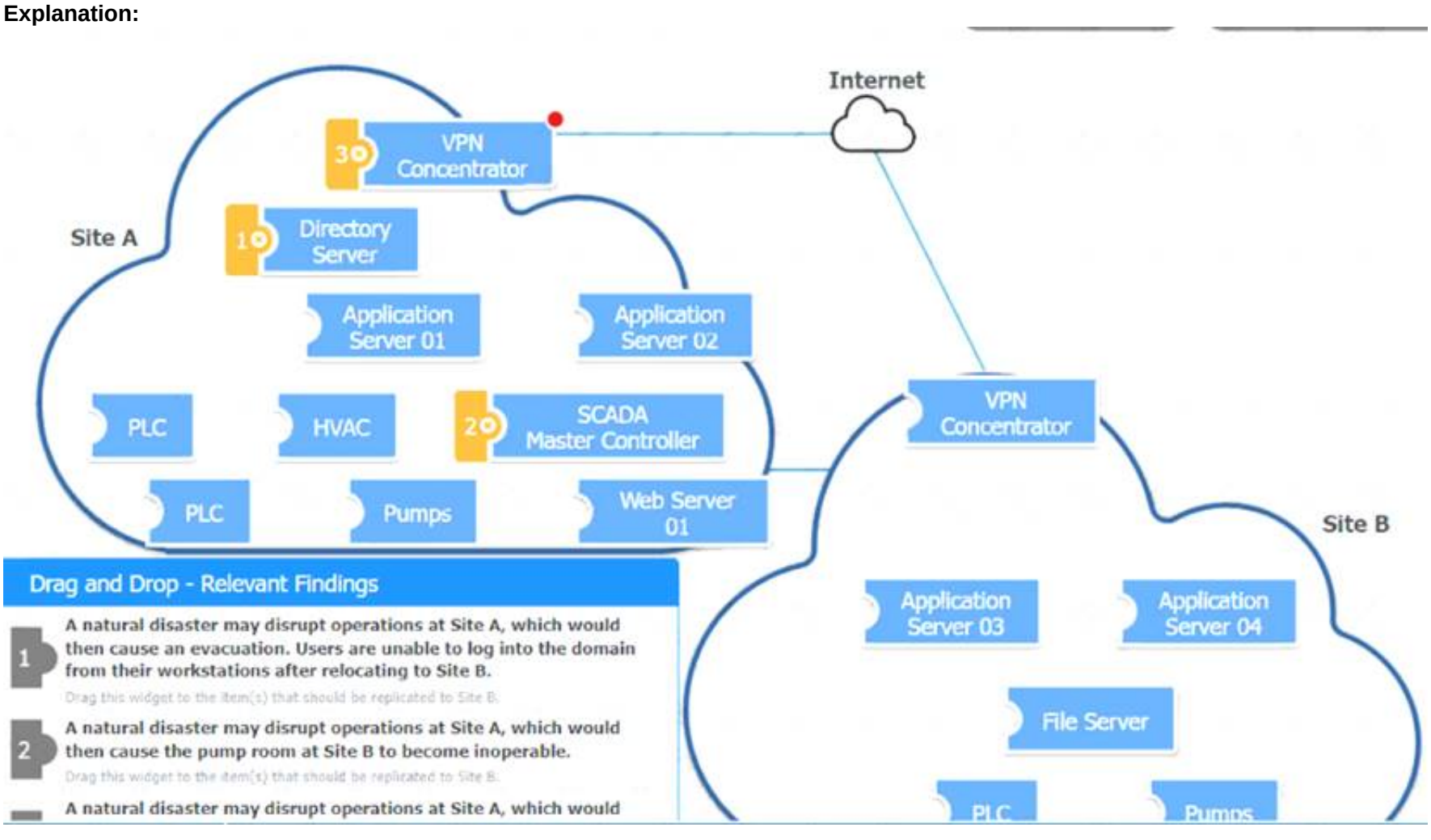
**NEW QUESTION 173**
An organization is planning for disaster recovery and continuity of operations. INSTRUCTIONS
Review the following scenarios and instructions. Match each relevant finding to the affected host.
After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective action for that finding.
Each finding may be used more than once.
If at any time you would like to bring back the initial state of the simul-ation, please click the Reset All button.




A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**




**NEW QUESTION 176**
A security engineer thinks the development team has been hard-coding sensitive environment variables in its code.
Which of the following would BEST secure the company's CI/CD pipeline?

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

**Answer:** A

**NEW QUESTION 177**
A penetration tester obtained root access on a Windows server and, according to the rules of engagement, is permitted to perform post-exploitation for persistence.
Which of the following techniques would BEST support this?

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

**Answer:** B

**NEW QUESTION 181**
An energy company is required to report the average pressure of natural gas used over the past quarter. A PLC sends data to a historian server that creates the required reports.
Which of the following historian server locations will allow the business to get the required reports in an and IT environment?

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

**Answer:** C

**NEW QUESTION 182**
An organization is researching the automation capabilities for systems within an OT network. A security analyst wants to assist with creating secure coding practices and would like to learn about the programming languages used on the PLCs. Which of the following programming languages is the MOST relevant for PLCs?

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

**Answer:** A

**NEW QUESTION 186**
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

**Answer:** C

**NEW QUESTION 187**
Which of the following is required for an organization to meet the ISO 27018 standard?

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

**Answer:** A

**NEW QUESTION 191**
A security architect is tasked with scoping a penetration test that will start next month. The architect wants to define what security controls will be impacted. Which of the following would be the BEST document to consult?

A. Rules of engagement
B. Master service agreement
C. Statement of work
D. Target audience

**Answer:** C

**NEW QUESTION 196**
Which of the following is a benefit of using steganalysis techniques in forensic response?

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

**Answer:** B

**NEW QUESTION 198**
A company launched a new service and created a landing page within its website network for users to access the service. Per company policy, all websites must utilize encryption for any authentication pages. A junior network administrator proceeded to use an outdated procedure to order new certificates. Afterward, customers are reporting the following error when accessing a new web page: NET:ERR_CERT_COMMON_NAME_INVALID. Which of the following BEST describes what the administrator should do NEXT?

A. Request a new certificate with the correct subject alternative name that includes the new websites.
B. Request a new certificate with the correct organizational unit for the company's website.
C. Request a new certificate with a stronger encryption strength and the latest cipher suite.
D. Request a new certificate with the same information but including the old certificate on the CRL.

**Answer:** D

**NEW QUESTION 200**
A company’s Chief Information Security Officer is concerned that the company’s proposed move to the cloud could lead to a lack of visibility into network traffic flow logs within the VPC.
Which of the following compensating controls would be BEST to implement in this situation?

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

**Answer:** B

**NEW QUESTION 203**
A developer wants to develop a secure external-facing web application. The developer is looking for an online community that produces tools, methodologies, articles, and documentation in the field of
web-application security Which of the following is the BEST option?

A. ICANN
B. PCI DSS
C. OWASP
D. CSA
E. NIST

**Answer:** C

**NEW QUESTION 205**
An organization’s assessment of a third-party, non-critical vendor reveals that the vendor does not have cybersecurity insurance and IT staff turnover is high. The organization uses the vendor to move customer office equipment from one service location to another. The vendor acquires customer data and access to the business via an API.
Given this information, which of the following is a noted risk?

A. Feature delay due to extended software development cycles
B. Financial liability from a vendor data breach
C. Technical impact to the API configuration
D. The possibility of the vendor’s business ceasing operations

**Answer:** A

**NEW QUESTION 209**

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

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

**Answer:** C

**NEW QUESTION 213**
An organization decided to begin issuing corporate mobile device users microSD HSMs that must be installed in the mobile devices in order to access corporate resources remotely. Which of the following features of these devices MOST likely led to this decision? (Select TWO.)

A. Software-backed keystore
B. Embedded cryptoprocessor
C. Hardware-backed public key storage
D. Support for stream ciphers
E. Decentralized key management
F. TPM 2.0 attestation services

**Answer:** BC

**NEW QUESTION 217**
While investigating a security event, an analyst finds evidence that a user opened an email attachment from an unknown source. Shortly after the user opened the attachment, a group of servers experienced a large amount of network and resource activity. Upon investigating the servers, the analyst discovers the servers were encrypted by ransomware that is demanding payment within 48 hours or all data will be destroyed. The company has no response plans for ransomware.
Which of the following is the NEXT step the analyst should take after reporting the incident to the management team?

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

**Answer:** B

**NEW QUESTION 220**
A company just released a new video card. Due to limited supply and nigh demand, attackers are employing automated systems to purchase the device through the company's web store so they can resell it on the secondary market. The company's Intended customers are frustrated. A security engineer suggests implementing a CAPTCHA system on the web store to help reduce the number of video cards purchased through automated systems. Which of the following now describes the level of risk?

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

**Answer:** A

**NEW QUESTION 223**
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 t he NEXT step of the incident response plan?

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

**Answer:** B

**NEW QUESTION 224**
A bank is working with a security architect to find the BEST solution to detect database management system compromises. The solution should meet the following requirements:
Work at the application layer
Send alerts on attacks from both privileged and malicious users Have a very low false positive
Which of the following should the architect recommend?

A. FIM
B. WAF
C. NIPS
D. DAM
E. UTM

**Answer:** D

**NEW QUESTION 228**
An organization recently experienced a ransomware attack. The security team leader is concerned about the attack reoccurring. However, no further security measures have been implemented.
Which of the following processes can be used to identify potential prevention recommendations?

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

**Answer:** A

**NEW QUESTION 229**
A large number of emails have been reported, and a security analyst is reviewing the following information from the emails:

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

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

A. Block the email address carl b@comptia1 com, as it is sending spam to subject matter experts
B. Validate the final "Received" header against the DNS entry of the domain.
C. Compare the 'Return-Path" and "Received" fields.
D. Ignore the emails, as SPF validation is successful, and it is a false positive

**Answer:** C

**NEW QUESTION 232**
A company's claims processed department has a mobile workforce that receives a large number of email submissions from personal email addresses. An employees recently received an email that approved to be claim form, but it installed malicious software on the employee's laptop when was opened.

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

**Answer:** C

**NEW QUESTION 236**
A DevOps team has deployed databases, event-driven services, and an API gateway as PaaS solution that will support a new billing system. Which of the following security responsibilities will the DevOps team need to perform?

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

**Answer:** A

**NEW QUESTION 237**
A security engineer needs 10 implement a CASB to secure employee user web traffic. A Key requirement is mat relevant event data must be collected from existing on-premises infrastructure components and consumed by me CASB to expand traffic visibility. The solution must be nighty resilient to network outages.
Which of the following architectural components would BEST meet these requirements?

A. Log collection
B. Reverse proxy
C. AWAF
D. API mode

**Answer:** A

**NEW QUESTION 238**
A company is moving most of its customer-facing production systems to the cloud-facing production systems to the cloud. IaaS is the service model being used. The Chief Executive Officer is concerned about the type of encryption available and requires the solution must have the highest level of security.
Which of the following encryption methods should the cloud security engineer select during the implementation phase?

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

**Answer:** B

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

**NEW QUESTION 239**
Company A acquired Company . 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

**Answer:** D

**NEW QUESTION 240**
An IT administrator is reviewing all the servers in an organization and notices that a server is missing crucial practice against a recent exploit that could gain root access.
Which of the following describes the administrator's discovery?

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

**Answer:** A

**NEW QUESTION 243**
Which of the following controls primarily detects abuse of privilege but does not prevent it?

A. Off-boarding
B. Separation of duties
C. Least privilege
D. Job rotation

**Answer:** A

**NEW QUESTION 245**
An auditor needs to scan documents at rest for sensitive text. These documents contain both text and Images. Which of the following software functionalities must be enabled in the DLP solution for the auditor to be able to fully read these documents? (Select TWO).

A. Document interpolation
B. Regular expression pattern matching
C. Optical character recognition functionality
D. Baseline image matching
E. Advanced rasterization
F. Watermarking

**Answer:** AC

**NEW QUESTION 247**
A company that uses AD is migrating services from LDAP to secure LDAP. During the pilot phase, services are not connecting properly to secure LDAP. Block is an except of output from the troubleshooting session:

```
openssl s_client -host ldap1.comptia.com -port 636

CONNECTED(00000003)
...
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
Subject=/CN=*.comptia.com
Issuer=/DC=com/DC=danville/CN=chicago
```

Which of the following BEST explains why secure LDAP is not working? (Select TWO.)

A. The clients may not trust idapt by default.
B. The secure LDAP service is not started, so no connections can be made.
C. Danvills.com is under a DDoS-inator attack and cannot respond to OCSP requests.
D. Secure LDAP should be running on UDP rather than TCP.
E. The company is using the wrong por
F. It should be using port 389 for secure LDAP.
G. Secure LDAP does not support wildcard certificates.
H. The clients may not trust Chicago by default.

**Answer:** BE

**NEW QUESTION 251**
An engineering team is developing and deploying a fleet of mobile devices to be used for specialized inventory management purposes. These devices should:
* Be based on open-source Android for user familiarity and ease.
* Provide a single application for inventory management of physical assets.
* Permit use of the camera be only the inventory application for the purposes of scanning
* Disallow any and all configuration baseline modifications.
* Restrict all access to any device resource other than those requirement ?

A. Set an application wrapping policy, wrap the application, distributes the inventory APK via the MAM tool, and test the application restrictions.
B. Write a MAC sepolicy that defines domains with rules, label the inventory application, build the policy, and set to enforcing mode.
C. Swap out Android Linux kernel version for >2,4,0, but the internet build Android, remove unnecessary functions via MDL, configure to block network access, and perform integration testing
D. Build and install an Android middleware policy with requirements added, copy the file into/ user/init, and then built the inventory application.

**Answer:** A

**NEW QUESTION 252**
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.

**Answer:** D

**NEW QUESTION 254**
A financial services company wants to migrate its email services from on-premises servers to a cloud-based email solution. The Chief information Security Officer (CISO) must brief board of directors on the potential security concerns related to this migration. The board is concerned about the following.
* Transactions being required by unauthorized individual
* Complete discretion regarding client names, account numbers, and investment information.
* Malicious attacker using email to distribute malware and ransom ware.
* Exfiltration of sensitivity company information.
The cloud-based email solution will provide an6-malware, reputation-based scanning, signature-based scanning, and sandboxing. Which of the following is the BEST option to resolve the board's concerns for this email migration?

A. Data loss prevention
B. Endpoint detection response
C. SSL VPN
D. Application whitelisting

**Answer:** A

**NEW QUESTION 259**
A systems administrator is in the process of hardening the host systems before connecting to the network. The administrator wants to add protection to the boot loader to ensure the hosts are secure before the OS fully boots.
Which of the following would provide the BEST boot loader protection?
A. TPM
B. HSM
C. PKI
D. UEFI/BIOS

**Answer:** D

**NEW QUESTION 264**
A Chief Information Officer (CIO) wants to implement a cloud solution that will satisfy the following requirements:
Support all phases of the SDLC. Use tailored website portal software.
Allow the company to build and use its own gateway software. Utilize its own data management platform.
Continue using agent-based security tools.
Which of the following cloud-computing models should the CIO implement?

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

**Answer:** D

**NEW QUESTION 265**
A home automation company just purchased and installed tools for its SOC to enable incident identification and response on software the company develops. The

company would like to prioritize defenses against the following attack scenarios:
Unauthorized insertions into application development environments
Authorized insiders making unauthorized changes to environment configurations
Which of the following actions will enable the data feeds needed to detect these types of attacks on development environments? (Choose two.)

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

**Answer:** AF

**NEW QUESTION 269**
An organization recently started processing, transmitting, and storing its customers' credit card information. Within a week of doing so, the organization suffered a massive breach that resulted in the exposure of the customers' information.
Which of the following provides the BEST guidance for protecting such information while it is at rest and in transit?

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

**Answer:** C

**NEW QUESTION 271**
A company processes data subject to NDAs with partners that define the processing and storage constraints for the covered data. The agreements currently do not permit moving the covered data to the cloud, and the company would like to renegotiate the terms of the agreements.
Which of the following would MOST likely help the company gain consensus to move the data to the cloud?

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

**Answer:** D

**NEW QUESTION 274**
A company recently acquired a SaaS provider and needs to integrate its platform into the company's existing infrastructure without impact to the customer's experience. The SaaS provider does not have a mature security program A recent vulnerability scan of the SaaS provider's systems shows multiple critical vulnerabilities attributed to very old and outdated Oss. Which of the following solutions would prevent these vulnerabilities from being introduced into the company's existing infrastructure?

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

**Answer:** B

**NEW QUESTION 277**
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

**Answer:** C

**NEW QUESTION 278**
All staff at a company have started working remotely due to a global pandemic. To transition to remote work, the company has migrated to SaaS collaboration tools. The human resources department wants to use these tools to process sensitive information but is concerned the data could be:
Leaked to the media via printing of the documents Sent to a personal email address
Accessed and viewed by systems administrators Uploaded to a file storage site
Which of the following would mitigate the department's concerns?

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

**Answer:** C

**NEW QUESTION 280**
A company is preparing to deploy a global service.
Which of the following must the company do to ensure GDPR compliance? (Choose two.)

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

**Answer:** AC

**Explanation:**
The main rights for individuals under the GDPR are to: allow subject access
have inaccuracies corrected have information erased prevent direct marketing
prevent automated decision-making and profiling allow data portability (as per the paragraph above)
source: https://www.clouddirect.net/11-things-you-must-do-now-for-gdpr-compliance/

**NEW QUESTION 281**
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 intelligence
B. e-discovery.
C. due care.
D. legal hold.

**Answer:** A

**NEW QUESTION 282**
A company's SOC has received threat intelligence about an active campaign utilizing a specific vulnerability. The company would like to determine whether it is vulnerable to this active campaign.
Which of the following should the company use to make this determination?

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

**Answer:** A

**NEW QUESTION 286**
A vulnerability analyst identified a zero-day vulnerability in a company's internally developed software. Since the current vulnerability management system does not have any checks for this vulnerability, an engineer has been asked to create one.
Which of the following would be BEST suited to meet these requirements?

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

**Answer:** B

**NEW QUESTION 288**
A security analyst receives an alert from the SIEM regarding unusual activity on an authorized public SSH jump server. To further investigate, the analyst pulls the event logs directly from /var/log/auth.log: graphic.ssh_auth_log.
Which of the following actions would BEST address the potential risks by the activity in the logs?

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

**Answer:** B

**NEW QUESTION 293**
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?

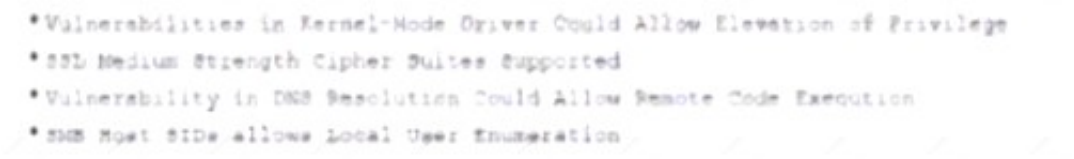
A. Adding a second redundant layer of alternate vendor VPN concentrators
B. Using Base64 encoding within the existing site-to-site VPN connections
C. Distributing security resources across VPN sites
D. Implementing IDS services with each VPN concentrator

E. Transitioning to a container-based architecture for site-based services

**Answer:** A

**Explanation:**
If on VPN concentrator goes down due to a zero day threat, having a redundant VPN concentrator of a different vendor should keep you going.

**NEW QUESTION 296**
An analyst execute a vulnerability scan against an internet-facing DNS server and receives the following report:




Which of the following tools should the analyst use FIRST to validate the most critical vulnerability?

A. Password cracker
B. Port scanner
C. Account enumerator
D. Exploitation framework

**Answer:** A

**NEW QUESTION 301**
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

**Answer:** B

**NEW QUESTION 303**
A developer wants to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users.
Which of the following would be BEST for the developer to perform? (Choose two.)

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

**Answer:** AC

**NEW QUESTION 304**
An organization mat provides a SaaS solution recently experienced an incident involving customer data loss. The system has a level of sell-healing that includes monitoring performance and available resources. When me system detects an issue, the self-healing process is supposed to restart pans of me software. During the incident, when me 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 me system as fully operational. Which of the following BEST describes me reason why the silent failure occurred?

A. The system logs rotated prematurely.
B. The disk utilization alarms are higher than what me service restarts require.
C. The number of nodes in me self-healing cluster was healthy,
D. Conditional checks prior to the service restart succeeded.

**Answer:** D

**NEW QUESTION 305**
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

**Answer:** B

**NEW QUESTION 308**
A security analyst is investigating a series of suspicious emails by employees to the security team. The email appear to come from a current business partner and do not contain images or URLs. No images or URLs were stripped from the message by the security tools the company uses instead, the emails only include the

following in plain text.




Which of the following should the security analyst perform?

A. Contact the security department at the business partner and alert them to the email event.
B. Block the IP address for the business partner at the perimeter firewall.
C. Pull the devices of the affected employees from the network in case they are infected with a zero-day virus.
D. Configure the email gateway to automatically quarantine all messages originating from the business partner.

**Answer:** A

**NEW QUESTION 310**
An attacker infiltrated the code base of a hardware manufacturer and inserted malware before the code was compiled. The malicious code is now running at the hardware level across a number of industries and sectors. Which of the following categories BEST describes this type of vendor risk?

A. SDLC attack
B. Side-load attack
C. Remote code signing
D. Supply chain attack

**Answer:** D

**NEW QUESTION 312**
.....

# THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CAS-004 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CAS-004 Product From:

**https://www.2passeasy.com/dumps/CAS-004/**

## Money Back Guarantee

## CAS-004 Practice Exam Features:

* CAS-004 Questions and Answers Updated Frequently

* CAS-004 Practice Questions Verified by Expert Senior Certified Staff

* CAS-004 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CAS-004 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year