Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam

https://www.2passeasy.com/dumps/CS0-003/

NEW QUESTION 1
- (Exam Topic 1)
Which of the following is the use of tools to simulate the ability for an attacker to gain access to a specified network?

A. Reverse engineering
B. Fuzzing
C. Penetration testing
D. Network mapping

Answer: C

NEW QUESTION 2
- (Exam Topic 1)
A company recently experienced a break-in whereby a number of hardware assets were stolen through unauthorized access at the back of the building. Which of the following would BEST prevent this type of theft from occurring in the future?

A. Motion detection
B. Perimeter fencing
C. Monitored security cameras
D. Badged entry

Answer: A

NEW QUESTION 3
- (Exam Topic 1)
An analyst is investigating an anomalous event reported by the SOC. After reviewing the system logs the analyst identifies an unexpected addition of a user with root-level privileges on the endpoint. Which of the following data sources will BEST help the analyst to determine whether this event constitutes an incident?

A. Patching logs
B. Threat feed
C. Backup logs
D. Change requests
E. Data classification matrix

Answer: D

NEW QUESTION 4
- (Exam Topic 1)
A developer wrote a script to make names and other Pll data unidentifiable before loading a database export into the testing system Which of the following describes the type of control that is being used?

A. Data encoding
B. Data masking
C. Data loss prevention
D. Data classification

Answer: C

NEW QUESTION 5
- (Exam Topic 1)
Which of the following policies would state an employee should not disable security safeguards, such as host firewalls and antivirus on company systems?

A. Code of conduct policy
B. Account management policy
C. Password policy
D. Acceptable use policy

Answer: D

NEW QUESTION 6
- (Exam Topic 1)
A security analyst discovers a vulnerability on an unpatched web server that is used for testing machine learning on Bing Data sets. Exploitation of the vulnerability could cost the organization $1.5 million in lost productivity. The server is located on an isolated network segment that has a 5% chance of being compromised. Which of the following is the value of this risk?

A. $75.000
B. $300.000
C. $1.425 million
D. $1.5 million

Answer: A

NEW QUESTION 7
- (Exam Topic 1)
An organization developed a comprehensive modern response policy Executive management approved the policy and its associated procedures. Which of the

following activities would be MOST beneficial to evaluate personnel's familiarity with incident response procedures?

A. A simulated breach scenario evolving the incident response team
B. Completion of annual information security awareness training by ail employees
C. Tabtetop activities involving business continuity team members
D. Completion of lessons-learned documentation by the computer security incident response team
E. External and internal penetration testing by a third party

Answer: A

NEW QUESTION 8
- (Exam Topic 1)
An organization that handles sensitive financial information wants to perform tokenization of data to enable the execution of recurring transactions. The organization is most interested m a secure, built-in device to
support its solution. Which of the following would MOST likely be required to perform the desired function?

A. TPM
B. eFuse
C. FPGA
D. HSM
E. UEFI

Answer: D

NEW QUESTION 9
- (Exam Topic 1)
A company's marketing emails are either being found in a spam folder or not being delivered at all. The security analyst investigates the issue and discovers the emails in question are being sent on behalf of the company by a third party in1marketingpartners.com Below is the exiting SPP word:

Which of the following updates to the SPF record will work BEST to prevent the emails from being marked as spam or blocked?
A)

B)

C)

D)

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

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
An analyst has been asked to provide feedback regarding the control required by a revised regulatory framework At this time, the analyst only needs to focus on the technical controls. Which of the following should the analyst provide an assessment of?

A. Tokenization of sensitive data
B. Establishment o' data classifications
C. Reporting on data retention and purging activities
D. Formal identification of data ownership
E. Execution of NDAs

Answer: A

NEW QUESTION 10

- (Exam Topic 1)
A security analyst implemented a solution that would analyze the attacks that the organization’s firewalls failed to prevent. The analyst used the existing systems to enact the solution and executed the following command.
S sudo nc -1 -v -c maildemon . py 25 caplog, txt
Which of the following solutions did the analyst implement?

A. Log collector
B. Crontab mail script
C. Snikhole
D. Honeypot

Answer: A

NEW QUESTION 15
- (Exam Topic 1)
The help desk provided a security analyst with a screenshot of a user's desktop:

For which of the following is aircrack-ng being used?

A. Wireless access point discovery
B. Rainbow attack
C. Brute-force attack
D. PCAP data collection

Answer: B

NEW QUESTION 16
- (Exam Topic 1)
A team of security analysis has been alerted to potential malware activity. The initial examination indicates one of the affected workstations on beaconing on TCP port 80 to five IP addresses and attempting to spread across the network over port 445. Which of the following should be the team's NEXT step during the detection phase of this response process?

A. Escalate the incident to management ,who will then engage the network infrastructure team to keep them informed
B. Depending on system critically remove each affected device from the network by disabling wired and wireless connections
C. Engage the engineering team to block SMB traffic internally and outbound HTTP traffic to the five IP addressesIdentify potentially affected systems by creating a correlation
D. Identify potentially affected system by creating a correlation search in the SIEM based on the network traffic.

Answer: D

NEW QUESTION 21
- (Exam Topic 1)
A security analyst is conducting a post-incident log analysis to determine which indicators can be used to detect further occurrences of a data exfiltration incident. The analyst determines backups were not performed during this time and reviews the following:

Which of the following should the analyst review to find out how the data was exfilltrated?

A. Monday's logs
B. Tuesday's logs
C. Wednesday's logs
D. Thursday's logs

Answer: D

NEW QUESTION 23

- (Exam Topic 1)
An organization has several systems that require specific logons Over the past few months, the security analyst has noticed numerous failed logon attempts followed by password resets. Which of the following should the analyst do to reduce the occurrence of legitimate failed logons and password resets?

A. Use SSO across all applications
B. Perform a manual privilege review
C. Adjust the current monitoring and logging rules
D. Implement multifactor authentication

Answer: A

NEW QUESTION 28
- (Exam Topic 1)
The security team at a large corporation is helping the payment-processing team to prepare for a regulatory compliance audit and meet the following objectives:

Reduce the number of potential findings by the auditors.
Limit the scope of the audit to only devices used by the payment-processing team for activities directly impacted by the regulations.
Prevent the external-facing web infrastructure used by other teams from coming into scope.
Limit the amount of exposure the company will face if the systems used by the payment-processing team are compromised.
Which of the following would be the MOST effective way for the security team to meet these objectives?

A. Limit the permissions to prevent other employees from accessing data owned by the business unit.
B. Segment the servers and systems used by the business unit from the rest of the network.
C. Deploy patches to all servers and workstations across the entire organization.
D. Implement full-disk encryption on the laptops used by employees of the payment-processing team.

Answer: B

NEW QUESTION 33
- (Exam Topic 1)
A security analyst wants to identify which vulnerabilities a potential attacker might initially exploit if the network is compromised Which of the following would provide the BEST results?

A. Baseline configuration assessment
B. Uncredentialed scan
C. Network ping sweep
D. External penetration test

Answer: D

NEW QUESTION 36
- (Exam Topic 1)
An executive assistant wants to onboard a new cloud based product to help with business analytics and dashboarding. When of the following would be the BEST integration option for the service?

A. Manually log in to the service and upload data files on a regular basis.
B. Have the internal development team script connectivity and file translate to the new service.
C. Create a dedicated SFTP sue and schedule transfers to ensue file transport security
D. Utilize the cloud products API for supported and ongoing integrations

Answer: D

NEW QUESTION 38
- (Exam Topic 1)

A cybersecurity analyst is contributing to a team hunt on an organization's endpoints. Which of the following should the analyst do FIRST?

A. Write detection logic.
B. Establish a hypothesis.
C. Profile the threat actors and activities.
D. Perform a process analysis.

Answer: C

Explanation:
Reference: https://www.cybereason.com/blog/blog-the-eight-steps-to-threat-hunting

NEW QUESTION 41
- (Exam Topic 1)
An employee in the billing department accidentally sent a spreadsheet containing payment card data to a recipient outside the organization The employee intended to send the spreadsheet to an internal staff member with a similar name and was unaware of the mistake until the recipient replied to the message In addition to retraining the employee, which of the following would prevent this from happening in the future?

A. Implement outgoing filter rules to quarantine messages that contain card data
B. Configure the outgoing mail filter to allow attachments only to addresses on the whitelist
C. Remove all external recipients from the employee's address book
D. Set the outgoing mail filter to strip spreadsheet attachments from all messages.

Answer: B

NEW QUESTION 44
- (Exam Topic 1)
While preparing of an audit of information security controls in the environment an analyst outlines a framework control that has the following requirements:
• All sensitive data must be classified
• All sensitive data must be purged on a quarterly basis
• Certificates of disposal must remain on file for at least three years This framework control is MOST likely classified as:

A. prescriptive
B. risk-based
C. preventive
D. corrective

Answer: A

Explanation:
prescrcriptiveitive. now look at definition of prescriptive. The definition of prescriptive is the imposition of rules, or something that has become established because it has been going on a long time and has become customary. A handbook dictating the rules for proper behavior is an example of something that would be described as a prescriptive handbookules are being implimented.
Preventative controls describe any security measure that’s designed to stop unwanted or unauthorized activity from occurring. Examples include physical controls such as fences, locks, and alarm systems; technical controls such as antivirus software, firewalls, and IPSs; and administrative controls like separation of duties, data classification, and auditing. https://www.f5.com/labs/articles/education/what-are-security-controls

NEW QUESTION 48
- (Exam Topic 1)
Which of the following attacks can be prevented by using output encoding?

A. Server-side request forgery
B. Cross-site scripting
C. SQL injection
D. Command injection
E. Cross-site request forgery
F. Directory traversal

Answer: B

NEW QUESTION 49
- (Exam Topic 1)
A security analyst has discovered suspicious traffic and determined a host is connecting to a known malicious website. The MOST appropriate action for the analyst to take would be lo implement a change request to:

A. update the antivirus software
B. configure the firewall to block traffic to the domain
C. add the domain to the blacklist
D. create an IPS signature for the domain

Answer: B

NEW QUESTION 50
- (Exam Topic 1)
A cybersecurity analyst is reading a daily intelligence digest of new vulnerabilities The type of vulnerability that should be disseminated FIRST is one that:

A. enables remote code execution that is being exploited in the wild.
B. enables data leakage but is not known to be in the environment

C. enables lateral movement and was reported as a proof of concept
D. affected the organization in the past but was probably contained and eradicated

Answer: C

NEW QUESTION 52
- (Exam Topic 1)
A product manager is working with an analyst to design a new application that will perform as a data analytics platform and will be accessible via a web browser. The product manager suggests using a PaaS provider to host the application.
Which of the following is a security concern when using a PaaS solution?

A. The use of infrastructure-as-code capabilities leads to an increased attack surface.
B. Patching the underlying application server becomes the responsibility of the client.
C. The application is unable to use encryption at the database level.
D. Insecure application programming interfaces can lead to data compromise.

Answer: D

NEW QUESTION 55
- (Exam Topic 1)
A cybersecurity analyst is supporting an incident response effort via threat intelligence. Which of the following is the analyst MOST likely executing?

A. Requirements analysis and collection planning
B. Containment and eradication
C. Recovery and post-incident review
D. Indicator enrichment and research pivoting

Answer: A

NEW QUESTION 57
- (Exam Topic 1)
Which of the following technologies can be used to house the entropy keys for task encryption on desktops and laptops?

A. Self-encrypting drive
B. Bus encryption
C. TPM
D. HSM

Answer: A

NEW QUESTION 62
- (Exam Topic 1)
An information security analyst is compiling data from a recent penetration test and reviews the following output:

The analyst wants to obtain more information about the web-based services that are running on the target. Which of the following commands would MOST likely provide the needed information?

A. ping -t 10.79.95.173.rdns.datacenters.com
B. telnet 10.79.95.173 443
C. ftpd 10.79.95.173.rdns.datacenters.com 443
D. tracert 10.79.95.173

Answer: B

NEW QUESTION 66
- (Exam Topic 1)
Which of the following software security best practices would prevent an attacker from being able to run arbitrary SQL commands within a web application? (Choose two.)

A. Parameterized queries
B. Session management
C. Input validation
D. Output encoding
E. Data protection
F. Authentication

Answer: AC

Explanation:
Reference: https://www.ptsecurity.com/ww-en/analytics/knowledge-base/how-to-prevent-sql-injection-attacks/

NEW QUESTION 67
- (Exam Topic 1)
Which of the following MOST accurately describes an HSM?

A. An HSM is a low-cost solution for encryption.
B. An HSM can be networked based or a removable USB

C. An HSM is slower at encrypting than software
D. An HSM is explicitly used for MFA

Answer: B

NEW QUESTION 70
- (Exam Topic 1)
Which of the following BEST describes the process by which code is developed, tested, and deployed in small batches?

A. Agile
B. Waterfall
C. SDLC
D. Dynamic code analysis

Answer: A

Explanation:
Reference: https://www.cleverism.com/software-development-life-cycle-sdlc-methodologies/

NEW QUESTION 72
- (Exam Topic 1)
A cyber-incident response analyst is investigating a suspected cryptocurrency miner on a company's server. Which of the following is the FIRST step the analyst should take?

A. Create a full disk image of the server's hard drive to look for the file containing the malware.
B. Run a manual antivirus scan on the machine to look for known malicious software.
C. Take a memory snapshot of the machine to capture volatile information stored in memory.
D. Start packet capturing to look for traffic that could be indicative of command and control from the miner.

Answer: D

NEW QUESTION 76
- (Exam Topic 1)
Which of the following BEST articulates the benefit of leveraging SCAP in an organization’s cybersecurity analysis toolset?

A. It automatically performs remedial configuration changes to enterprise security services
B. It enables standard checklist and vulnerability analysis expressions for automation
C. It establishes a continuous integration environment for software development operations
D. It provides validation of suspected system vulnerabilities through workflow orchestration

Answer: B

NEW QUESTION 80
- (Exam Topic 1)
An analyst is working with a network engineer to resolve a vulnerability that was found in a piece of legacy hardware, which is critical to the operation of the organization's production line. The legacy hardware does not have third-party support, and the OEM manufacturer of the controller is no longer in operation. The analyst documents the activities and verifies these actions prevent remote exploitation of the vulnerability.
Which of the following would be the MOST appropriate to remediate the controller?

A. Segment the network to constrain access to administrative interfaces.
B. Replace the equipment that has third-party support.
C. Remove the legacy hardware from the network.
D. Install an IDS on the network between the switch and the legacy equipment.

Answer: A

NEW QUESTION 81
- (Exam Topic 1)
A system’s authority to operate (ATO) is set to expire in four days. Because of other activities and limited staffing, the organization has neglected to start reauthentication activities until now. The cybersecurity group just performed a vulnerability scan with the partial set of results shown below:

Based on the scenario and the output from the vulnerability scan, which of the following should the security team do with this finding?

A. Remediate by going to the web config file, searching for the enforce HTTP validation setting, and manually updating to the correct setting.
B. Accept this risk for now because this is a “high” severity, but testing will require more than the four days available, and the system ATO needs to be competed.
C. Ignore i
D. This is false positive, and the organization needs to focus its efforts on other findings.
E. Ensure HTTP validation is enabled by rebooting the server.

Answer: A

NEW QUESTION 83
- (Exam Topic 1)
A user's computer has been running slowly when the user tries to access web pages. A security analyst runs the command netstat -aon from the command line and receives the following output:

Which of the following lines indicates the computer may be compromised?

A. Line 1
B. Line 2
C. Line 3
D. Line 4
E. Line 5
F. Line 6

Answer: D

NEW QUESTION 88
- (Exam Topic 1)
A cybersecurity analyst has access to several threat feeds and wants to organize them while simultaneously comparing intelligence against network traffic. Which of the following would BEST accomplish this goal?

A. Continuous integration and deployment
B. Automation and orchestration
C. Static and dynamic analysis
D. Information sharing and analysis

Answer: B

NEW QUESTION 91
- (Exam Topic 1)
A security analyst is investigating a malware infection that occurred on a Windows system. The system was not connected to a network and had no wireless capability Company policy prohibits using portable media or mobile storage The security analyst is trying to determine which user caused the malware to get onto the system Which of the following registry keys would MOST likely have this information?

A. HKEY_USERS\<user SID>\Software\Microsoft\Windows\CurrentVersion\Run
B. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
C. HKEY_USERS\<user SID>\Software\Microsoft\Windows\explorer\MountPoints2
D. HKEY_USERS\<user SID>\Software\Microsoft\Internet Explorer\Typed URLs
E. HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\System\iusb3hub

Answer: E

NEW QUESTION 94
- (Exam Topic 1)
A security analyst gathered forensics from a recent intrusion in preparation for legal proceedings. The analyst used EnCase to gather the digital forensics. cloned the hard drive, and took the hard drive home for further analysis. Which of the following of the security analyst violate?

A. Cloning procedures
B. Chain of custody
C. Hashing procedures
D. Virtualization

Answer: B

NEW QUESTION 95
- (Exam Topic 1)
A security analyst is investigating malicious traffic from an internal system that attempted to download proxy avoidance software as identified from the firewall logs but the destination IP is blocked and not captured. Which of the following should the analyst do?

A. Shut down the computer
B. Capture live data using Wireshark
C. Take a snapshot
D. Determine if DNS logging is enabled.
E. Review the network logs.

Answer: D

Explanation:
The DNS debug log provides extremely detailed data about all DNS information that is sent and received by the DNS server, similar to the data that can be gathered using packet capture tools such as network monitor.
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn80066

NEW QUESTION 98
- (Exam Topic 1)
An organization developed a comprehensive incident response policy. Executive management approved the policy and its associated procedures. Which of the following activities would be MOST beneficial to evaluate personnel’s familiarity with incident response procedures?

A. A simulated breach scenario involving the incident response team
B. Completion of annual information security awareness training by all employees
C. Tabletop activities involving business continuity team members
D. Completion of lessons-learned documentation by the computer security incident response team
E. External and internal penetration testing by a third party

Answer: A

NEW QUESTION 99
- (Exam Topic 1)
While planning segmentation for an ICS environment, a security engineer determines IT resources will need access to devices within the ICS environment without compromising security.
To provide the MOST secure access model in this scenario, the jumpbox should be.

A. placed in an isolated network segment, authenticated on the IT side, and forwarded into the ICS network.
B. placed on the ICS network with a static firewall rule that allows IT network resources to authenticate.
C. bridged between the IT and operational technology networks to allow authenticated access.
D. placed on the IT side of the network, authenticated, and tunneled into the ICS environment.

Answer: A

NEW QUESTION 103
- (Exam Topic 1)
As part of an exercise set up by the information security officer, the IT staff must move some of the network systems to an off-site facility and redeploy them for testing. All staff members must ensure their respective systems can power back up and match their gold image. If they find any inconsistencies, they must formally document the information.
Which of the following BEST describes this test?

A. Walk through
B. Full interruption
C. Simulation
D. Parallel

Answer: C

NEW QUESTION 105
- (Exam Topic 1)
During a routine log review, a security analyst has found the following commands that cannot be identified from the Bash history log on the root user.

Which of the following commands should the analyst investigate FIRST?

A. Line 1
B. Line 2
C. Line 3
D. Line 4
E. Line 5
F. Line 6

Answer: B

NEW QUESTION 106
- (Exam Topic 1)
A security analyst is investigating a compromised Linux server. The analyst issues the ps command and receives the following output.

Which of the following commands should the administrator run NEXT to further analyze the compromised system?

A. strace /proc/1301
B. rpm -V openash-server
C. /bin/la -1 /proc/1301/exe
D. kill -9 1301

Answer: A

NEW QUESTION 107
- (Exam Topic 1)
An organization needs to limit its exposure to accidental disclosure when employees send emails that contain personal information to recipients outside the company Which of the following technical controls would BEST accomplish this goal?

A. DLP
B. Encryption
C. Data masking
D. SPF

Answer: C

NEW QUESTION 108
- (Exam Topic 1)

Which of the following technologies can be used to store digital certificates and is typically used in high-security implementations where integrity is paramount?

A. HSM
B. eFuse
C. UEFI
D. Self-encrypting drive

Answer: A

NEW QUESTION 112
- (Exam Topic 1)
A security analyst is supporting an embedded software team. Which of the following is the BEST recommendation to ensure proper error handling at runtime?

A. Perform static code analysis.
B. Require application fuzzing.
C. Enforce input validation
D. Perform a code review

Answer: B

NEW QUESTION 116
- (Exam Topic 1)
A hybrid control is one that:

A. is implemented differently on individual systems
B. is implemented at the enterprise and system levels
C. has operational and technical components
D. authenticates using passwords and hardware tokens

Answer: B

NEW QUESTION 121
- (Exam Topic 1)
An audit has revealed an organization is utilizing a large number of servers that are running unsupported operating systems.
As part of the management response phase of the audit, which of the following would BEST demonstrate senior management is appropriately aware of and addressing the issue?

A. Copies of prior audits that did not identify the servers as an issue
B. Project plans relating to the replacement of the servers that were approved by management
C. Minutes from meetings in which risk assessment activities addressing the servers were discussed
D. ACLs from perimeter firewalls showing blocked access to the servers
E. Copies of change orders relating to the vulnerable servers

Answer: B

NEW QUESTION 125
- (Exam Topic 1)
A security analyst reviews the following aggregated output from an Nmap scan and the border firewall ACL:

Which of the following should the analyst reconfigure to BEST reduce organizational risk while maintaining current functionality?

A. PC1
B. PC2
C. Server1
D. Server2
E. Firewall

Answer: B

NEW QUESTION 128
- (Exam Topic 2)
A contained section of a building is unable to connect to the Internet A security analyst. A security analyst investigates me issue but does not see any connections to the corporate web proxy However the analyst does notice a small spike in traffic to the Internet. The help desk technician verifies all users are connected to the connect SSID. but there are two of the same SSIDs listed in the network connections. Which of the following BEST describes what is occurring?

A. Bandwidth consumption
B. Denial of service
C. Beaconing
D. Rogue device on the network

Answer: A

NEW QUESTION 132
- (Exam Topic 2)
Which of the following threat classifications would MOST likely use polymorphic code?

A. Known threat

B. Zero-day threat
C. Unknown threat
D. Advanced persistent threat

Answer: D

NEW QUESTION 136
- (Exam Topic 2)
When reviewing a compromised authentication server, a security analyst discovers the following hidden file:

Further analysis shows these users never logged in to the server. Which of the following types of attacks was used to obtain the file and what should the analyst recommend to prevent this type of attack from reoccurring?

A. A rogue LDAP server is installed on the system and is connecting password
B. The analyst should recommend wiping and reinstalling the server.
C. A password spraying attack was used to compromise the password
D. The analyst should recommend that all users receive a unique password.
E. A rainbow tables attack was used to compromise the account
F. The analyst should recommend that future password hashes contains a salt.
G. A phishing attack was used to compromise the accoun
H. The analyst should recommend users install endpoint protection to disable phishing links.

Answer: B

NEW QUESTION 139
- (Exam Topic 2)
Portions of a legacy application are being refactored to discontinue the use of dynamic SQL Which of the following would be BEST to implement in the legacy application?

A. Multifactor authentication
B. Web-application firewall
C. SQL injection
D. Parameterized queries
E. Input validation

Answer: A

NEW QUESTION 143
- (Exam Topic 2)
An information security analyst on a threat-hunting team Is working with administrators to create a hypothesis related to an internally developed web application The working hypothesis is as follows:
• Due to the nature of the industry, the application hosts sensitive data associated with many clients and Is a significant target.
• The platform Is most likely vulnerable to poor patching and Inadequate server hardening, which expose vulnerable services.
• The application is likely to be targeted with SQL injection attacks due to the large number of reporting capabilities within the application.
As a result, the systems administrator upgrades outdated service applications and validates the endpoint configuration against an industry benchmark. The analyst suggests developers receive additional training on implementing identity and access management, and also implements a WAF to protect against SQL injection attacks Which of the following BEST represents the technique in use?

A. Improving detection capabilities

B. Bundling critical assets
C. Profiling threat actors and activities
D. Reducing the attack surface area

Answer: D

NEW QUESTION 145
- (Exam Topic 2)
A security analyst receives an alert from the SIEM about a possible attack happening on the network The analyst opens the alert and sees the IP address of the suspected server as 192.168.54.66. which is part of the network 192 168 54 0/24. The analyst then pulls all the command history logs from that server and sees the following

Which of the following activities is MOST likely happening on the server?

A. A MITM attack
B. Enumeration
C. Fuzzing
D. A vulnerability scan

Answer: A

NEW QUESTION 147
- (Exam Topic 2)
A security analyst is reviewing vulnerability scan results and notices new workstations are being flagged as having outdated antivirus signatures. The analyst observes the following plugin output:
The analyst uses the vendor's website to confirm the oldest supported version is correct. Which of the following BEST describes the situation?

A. This is a false positive and the scanning plugin needs to be updated by the vendor
B. This is a true negative and the new computers have the correct version of the software
C. This is a true positive and the new computers were imaged with an old version of the software
D. This is a false negative and the new computers need to be updated by the desktop team

Answer: C

NEW QUESTION 148
- (Exam Topic 2)
A cybersecurity analyst needs to determine whether a large file named access log from a web server contains the following loC:
../../../../bin/bash
Which of the following commands can be used to determine if the string is present in the log?

A. echo access.log | grep "../../../../bin/bash"
B. grep "../../../../bin/bash" 1 cat access.log
C. grep "../../../. ./bin/bash" < access.log
D. cat access.log > grep "../../../ ../bin/bash"

Answer: C

NEW QUESTION 153
- (Exam Topic 2)

Which of the following sources will provide the MOST relevant threat intelligence data to the security team of a dental care network?

A. Open threat exchange
B. H-ISAC
C. Dark web chatter
D. Dental forums

Answer: B

NEW QUESTION 158
- (Exam Topic 2)
An organisation is assessing risks so it can prioritize its mitigation actions. Following are the risks and their probability and impact:

Which of the following is the order of priority for risk mitigation from highest to lowest?

A. A, B, C, D
B. A, D, B, C
C. B, C, A, D
D. C, B, D, A
E. D, A, C, B

Answer: A

NEW QUESTION 159
- (Exam Topic 2)
A security analyst reviews the latest reports from the company's vulnerability scanner and discovers the following:
Which of the following changes should the analyst recommend FIRST?

A. Configuring SSL ciphers to use different encryption blocks
B. Programming changes to encode output
C. Updating the 'mod_status' module
D. Disabling HTTP connection debugging commands

Answer: C

NEW QUESTION 162
- (Exam Topic 2)
The management team assigned the following values to an inadvertent breach of privacy regulations during the original risk assessment:
Probability = 25%
Magnitude = $1,015 per record Total records = 10,000
Two breaches occurred during the fiscal year. The first compromised 35 records, and the second compromised 65 records. Which of the following is the value of the records that were compromised?

A. $10,150
B. $25,375
C. $101,500
D. $2,537,500

Answer: A

NEW QUESTION 163
- (Exam Topic 2)
An organization's network administrator uncovered a rogue device on the network that is emulating the charactenstics of a switch. The device is trunking protocols and inserting tagging va the flow of traffic at the data link layer
Which of the following BEST describes this attack?

A. VLAN hopping
B. Injection attack
C. Spoofing
D. DNS pharming

Answer: A

NEW QUESTION 168
- (Exam Topic 2)
Following a recent security breach, a company decides to investigate account usage to ensure privileged accounts are only being utilized during typical business hours. During the investigation, a security analyst determines an account was consistently utilized in the middle of the night.
Which of the following actions should the analyst take NEXT?

A. Initiate the incident response plan.
B. Disable the privileged account
C. Report the discrepancy to human resources.
D. Review the activity with the user.

Answer: D

NEW QUESTION 170
- (Exam Topic 2)
A company has contracted with a software development vendor to design a web portal for customers to access a medical records database. Which of the following should the security analyst recommend to BEST control the unauthorized disclosure of sensitive data when sharing the development database with the vendor?

A. Establish an NDA with the vendor.
B. Enable data masking of sensitive data tables in the database.
C. Set all database tables to read only.
D. Use a de-identified data process for the development database.

Answer: B

NEW QUESTION 171
- (Exam Topic 2)
The steering committee for information security management annually reviews the security incident register for the organization to look for trends and systematic issues The steering committee wants to rank the risks based on past incidents to improve the security program for next year Below is the incident register for the organization.

Which of the following should the organization consider investing in FIRST due to the potential impact of availability?

A. Hire a managed service provider to help with vulnerability management
B. Build a warm site in case of system outages
C. Invest in a failover and redundant system, as necessary
D. Hire additional staff for the IT department to assist with vulnerability management and log review

Answer: C

Explanation:
Both on July 31 and November 24, the organization could not restore multiple days due to missing disaster recovery plan. Therefore, failover systems are very important for this organization.

NEW QUESTION 175
- (Exam Topic 2)
A security analyst inspects the header of an email that is presumed to be malicious and sees the following:

Which of the following is inconsistent with the rest of the header and should be treated as suspicious?

A. The subject line
B. The sender's email address
C. The destination email server
D. The use of a TLS cipher

Answer: C

NEW QUESTION 180
- (Exam Topic 2)
A security analyst reviews a recent network capture and notices encrypted inbound traffic on TCP port 465 was coming into the company's network from a database server. Which of the following will the security analyst MOST likely identify as the reason for the traffic on this port?

A. The server is receiving a secure connection using the new TLS 1.3 standard
B. Someone has configured an unauthorized SMTP application over SSL
C. The traffic is common static data that Windows servers send to Microsoft

D. A connection from the database to the web front end is communicating on the port

Answer: B

NEW QUESTION 185
- (Exam Topic 2)
A security analyst received a series of antivirus alerts from a workstation segment, and users reported ransomware messages. During lessons- learned activities, the analyst determines the antivirus was able to alert to abnormal behavior but did not stop this newest variant of ransomware. Which of the following actions should be taken to BEST mitigate the effects of this type of threat in the future?

A. Enabling application blacklisting
B. Enabling sandboxing technology
C. Purchasing cyber insurance
D. Installing a firewall between the workstations and Internet

Answer: B

NEW QUESTION 190
- (Exam Topic 2)
Which of the following session management techniques will help to prevent a session identifier from being stolen via an XSS attack?

A. Ensuring the session identifier length is sufficient
B. Creating proper session identifier entropy
C. Applying a secure attribute on session cookies
D. Utilizing transport layer encryption on all requests
E. Implementing session cookies with the HttpOnly flag

Answer: B

NEW QUESTION 195
- (Exam Topic 2)
A Chief Security Officer (CSO) is working on the communication requirements (or an organization's incident response plan. In addition to technical response activities, which of the following is the main reason why communication must be addressed in an effective incident response program?

A. Public relations must receive information promptly in order to notify the community.
B. Improper communications can create unnecessary complexity and delay response actions.
C. Organizational personnel must only interact with trusted members of the law enforcement community.
D. Senior leadership should act as the only voice for the incident response team when working with forensics teams.

Answer: B

NEW QUESTION 197
- (Exam Topic 2)
The SFTP server logs show thousands of failed login attempts from hundreds of IP addresses worldwide. Which of the following controls would BEST protect the service?

A. Whitelisting authorized IP addresses
B. Enforcing more complex password requirements
C. Blacklisting unauthorized IP addresses
D. Establishing a sinkhole service

Answer: C

NEW QUESTION 202
- (Exam Topic 2)
A company's legal department is concerned that its incident response plan does not cover the countless ways security incidents can occur They have asked a security analyst to help tailor the response plan to provide broad coverage for many situations. Which of the following is the BEST way to achieve this goal?

A. Focus on incidents that may require law enforcement support.
B. Focus on common attack vectors first.
C. Focus on incidents that have a high chance of reputation harm.
D. Focus on incidents that affect critical systems.

Answer: D

NEW QUESTION 206
- (Exam Topic 2)
A user reports a malware alert to the help desk A technician verifies the alert, determines the workstation is classified as a low-severity device, and uses network controls to block access The technician then assigns the ticket to a security analyst who will complete the eradication and recovery processes. Which of the following should the security analyst do NEXT?

A. Document the procedures and walk through the incident training guide.
B. Sanitize the workstation and verify countermeasures are restored
C. Reverse engineer the malware to determine its purpose and risk to the organization.
D. Isolate the workstation and issue a new computer to the user.

Answer: B

NEW QUESTION 211
- (Exam Topic 2)
A custom script currently monitors real-time logs of a SAMIL authentication server to mitigate brute-force attacks. Which of the following is a concern when moving authentication to a cloud service?

A. Logs may contain incorrect information.
B. SAML logging is not supported for cloud-based authentication.
C. Access to logs may be delayed for some time.
D. Log data may be visible to other customers.

Answer: C

Explanation:
Threats & Vulnerabilities Associated with the Cloud, Subsection "Logging and Monitoring"
"Because the responsibility of protecting portions of the stack falls to the service provider, it does sometimes mean the organization loses monitoring capabilities, for better or worse."
CompTIA CySA+ Cybersecurity Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002) (p. 158).

NEW QUESTION 212
- (Exam Topic 2)
A company recently experienced multiple DNS DDoS attacks, and the information security analyst must provide a DDoS solution to deploy in the company's datacenter Which of the following would BEST prevent future attacks?

A. Configure a sinkhole on the router.
B. Buy a UTM to block the number of requests.
C. Route the queries on the DNS server to 127.0.0.1.
D. Call the Internet service provider to block the attack.

Answer: A

NEW QUESTION 217
- (Exam Topic 2)
A software development team asked a security analyst to review some code for security vulnerabilities. Which of the following would BEST assist the security analyst while performing this task?

A. Static analysis
B. Dynamic analysis
C. Regression testing
D. User acceptance testing

Answer: C

NEW QUESTION 220
- (Exam Topic 2)
The Chief Information Officer (CIO) for a large manufacturing organization has noticed a significant number of unknown devices with possible malware infections are on the organization's corporate network.
Which of the following would work BEST to prevent the issue?

A. Reconfigure the NAC solution to prevent access based on a full device profile and ensure antivirus is installed.
B. Segment the network to isolate all systems that contain highly sensitive information, such as intellectual property.
C. Implement certificate validation on the VPN to ensure only employees with the certificate can access the company network.
D. Update the antivirus configuration to enable behavioral and real-time analysis on all systems within the network.

Answer: A

NEW QUESTION 221
- (Exam Topic 2)
A host is spamming the network unintentionally. Which of the following control types should be used to address this situation?

A. Operational
B. Corrective
C. Managerial
D. Technical

Answer: B

NEW QUESTION 223
- (Exam Topic 2)
A user reports the system is behaving oddly following the installation of an approved third-party software application. The application executable was sourced from an internal repository Which of the following will ensure the application is valid?

A. Ask the user to refresh the existing definition file for the antivirus software
B. Perform a malware scan on the file in the internal repository
C. Hash the application's installation file and compare it to the hash provided by the vendor
D. Remove the user's system from the network to avoid collateral contamination

Answer: C

NEW QUESTION 227
- (Exam Topic 2)
While analyzing network traffic, a security analyst discovers several computers on the network are connecting to a malicious domain that was blocked by a DNS sinkhole. A new private IP range is now visible, but no change requests were made to add it. Which of the following is the BEST solution for the security analyst to implement?

A. Block the domain IP at the firewall.
B. Blacklist the new subnet
C. Create an IPS rule.
D. Apply network access control.

Answer: A

NEW QUESTION 231
- (Exam Topic 2)
A company wants to reduce the cost of deploying servers to support increased network growth. The company is currently unable to keep up with the demand, so it wants to outsource the infrastructure to a cloud-based solution.
Which of the following is the GREATEST threat for the company to consider when outsourcing its infrastructure?

A. The cloud service provider is unable to provide sufficient logging and monitoring.
B. The cloud service provider is unable to issue sufficient documentation for configurations.
C. The cloud service provider conducts a system backup each weekend and once a week during peak business times.
D. The cloud service provider has an SLA for system uptime that is lower than 99 9%.

Answer: B

NEW QUESTION 234
- (Exam Topic 2)
A security analyst is auditing firewall rules with the goal of scanning some known ports to check the firewall's behavior and responses. The analyst executes the following commands:

The analyst then compares the following results for port 22: nmap returns "Closed"
hping3 returns "flags=RA"
Which of the following BEST describes the firewall rule?

A. DNAT –-to-destination 1.1.1.1:3000
B. REJECT with –-tcp-reset
C. LOG –-log-tcp-sequence
D. DROP

Answer: B

Explanation:
No doubt does the nmap result mean its being rejected as it returns closed. However, what threw me for a loop was the hping3 response. After further web surfing I found that the "flag=RA" means actually means "flag= RST, ACK" which means that it too was rejected.

NEW QUESTION 236
- (Exam Topic 2)
An analyst is reviewing the following code output of a vulnerability scan:

Which of the following types of vulnerabilities does this MOST likely represent?

A. A insecure direct object reference vulnerability
B. An HTTP response split vulnerability
C. A credential bypass vulnerability
D. A XSS vulnerability

Answer: C

NEW QUESTION 239
- (Exam Topic 2)
An employee was found to have performed fraudulent activities. The employee was dismissed, and the employee's laptop was sent to the IT service desk to undergo a data sanitization procedure. However, the security analyst responsible for the investigation wants to avoid data sanitization. Which of the following can the security analyst use to justify the request?

A. Data retention
B. Evidence retention
C. GDPR
D. Data correlation procedure

Answer: A

NEW QUESTION 243
- (Exam Topic 2)
Which of the following BEST describes the primary role ol a risk assessment as it relates to compliance with risk-based frameworks?

A. It demonstrates the organization's mitigation of risks associated with internal threats.
B. It serves as the basis for control selection.
C. It prescribes technical control requirements.
D. It is an input to the business impact assessment.

Answer: A

NEW QUESTION 248
- (Exam Topic 2)
A security analyst is reviewing the following requirements (or new time clocks that will be installed in a shipping warehouse:
• The clocks must be configured so they do not respond to ARP broadcasts.
• The server must be configured with static ARP entries for each clock.
Which of the following types of attacks will this configuration mitigate?

A. Spoofing
B. Overflows
C. Rootkits
D. Sniffing

Answer: A

NEW QUESTION 252
- (Exam Topic 2)
A security analyst for a large pharmaceutical company was given credentials from a threat intelligence resources organisation for Internal users, which contain usernames and valid passwords for company accounts. Which of the following is the FIRST action the analyst should take as part of security operations monitoring?

A. Run scheduled antivirus scans on all employees' machines to look for malicious processes.
B. Reimage the machines of all users within the group in case of a malware infection.
C. Change all the user passwords to ensure the malicious actors cannot use them.
D. Search the event logs for event identifiers that indicate Mimikatz was used.

Answer: D

NEW QUESTION 257
- (Exam Topic 2)
Which of the following is a best practice when sending a file/data to another individual in an organization?

A. Encrypt the file but do not compress it.
B. When encrypting, split the file: and then compress each file.
C. Compress and then encrypt the file.
D. Encrypt and then compress the file.

Answer: C

NEW QUESTION 259
- (Exam Topic 2)
A security team identified some specific known tactics and techniques to help mitigate repeated credential access threats, such as account manipulation and brute forcing. Which of the following frameworks or models did the security team MOST likely use to identify the tactics and techniques'?

A. Kill chain
B. Diamond Model of Intrusion Analysis
C. MITRE ATT&CK
D. ITIL

Answer: C

NEW QUESTION 263
- (Exam Topic 2)
Given the Nmap request below:

Which of the following actions will an attacker be able to initiate directly against this host?

A. Password sniffing
B. ARP spoofing
C. A brute-force attack
D. An SQL injection

Answer: C

NEW QUESTION 268
- (Exam Topic 3)
Which of the following APT adversary archetypes represent non-nation-state threat actors? (Select TWO)

A. Kitten
B. Panda
C. Tiger
D. Jackal
E. Bear
F. Spider

Answer: CD

NEW QUESTION 270
- (Exam Topic 3)
A company wants to ensure confidential data from its storage media files is sanitized so the drives cannot oe reused. Which of the following is the BEST approach?

A. Degaussing
B. Shredding
C. Formatting
D. Encrypting

Answer: B

Explanation:
https://legalshred.com/degaussing-vs-hard-drive-shredding/
The best and most secure method of rendering hard drive information completely unusable is to completely destroy it through hard drive shredding

NEW QUESTION 274
- (Exam Topic 3)
A security analyst is reviewing a firewall usage report that contains traffic generated over the last 30 minutes in order to locate unusual traffic patterns:

Which of the following source IP addresses does the analyst need to investigate further?

A. 10.18.76.179
B. 10.50.180.49
C. 192.168.48.147
D. 192.168.100.5

Answer: C

NEW QUESTION 276
- (Exam Topic 3)
While implementing a PKI for a company, a security analyst plans to utilize a dedicated server as the certAcate authority that is only used to sign intermediate certificates. Which of the following are the MOST secure states for the certificate authority server when it is not in use? (Select TWO)

A. On a private VLAN
B. Full disk encrypted
C. Powered off
D. Backed up hourly
E. VPN accessible only
F. Air gapped

Answer: EF

NEW QUESTION 280
- (Exam Topic 3)
A vulnerability assessment solution is hosted in the cloud This solution will be used as an accurate inventory data source for both the configuration management database and the governance nsk and compliance tool An analyst has been asked to automate the data acquisition Which of the following would be the BEST way to acqutre the data'

A. CSV export
B. SOAR
C. API
D. Machine learning

Answer: C

Explanation:
An example of API is google weather app, using the weather channel's API to collect accurate weather data and broadcast it on goggle weather app, so google doesn't have to do it their selves

NEW QUESTION 283
- (Exam Topic 3)
While conoXicting a cloud assessment, a security analyst performs a Prowler scan, which generates the following within the report:

Based on the Prowler report, which of the following is the BEST recommendation?

A. Delete Cloud Dev access key 1
B. Delete BusinessUsr access key 1.
C. Delete access key 1.
D. Delete access key 2.

Answer: D

NEW QUESTION 288
- (Exam Topic 3)
A company stores all of its data in the cloud. All company-owned laptops are currently unmanaged, and all users have administrative rights. The security team is having difficulty identifying a way to secure the environment. Which of the following would be the BEST method to protect the company's data?

A. Implement UEM on an systems and deploy security software.
B. Implement DLP on all workstations and block company data from being sent outside the company
C. Implement a CASB and prevent certain types of data from being downloaded to a workstation
D. Implement centralized monitoring and logging for an company systems.

Answer: C

Explanation:
Cloud Access Security Broker (CASB): An enterprise management software designed to mediate access to cloud services by users across all types of devices

NEW QUESTION 293
- (Exam Topic 3)
A new vanant of malware is spreading on ihe company network using TCP 443 to contact its
command-and-control server The domain name used for callback continues to change, and the analyst is unable to predict future domain name variance Which of the following actions should the analyst take to stop malicious communications with the LEAST disruption to service?

A. Implement a sinkhole with a high entropy level
B. Disable TCP/53 at the penmeter firewall
C. Block TCP/443 at the edge router
D. Configure the DNS forwarders to use recursion

Answer: D

NEW QUESTION 294

- (Exam Topic 3)
The majority of a company's employees have stated they are unable to perform their job duties due to outdated workstations, so the company has decided to institute BYOD. Which of the following would a security analyst MOST likely recommend for securing the proposed solution?

A. A Linux-based system and mandatory training on Linux for all BYOD users
B. A firewalled environment for client devices and a secure VDl for BYOO users
C. A standardized anti-malware platform and a unified operating system vendor
D. 802.1X lo enforce company policy on BYOD user hardware

Answer: B

Explanation:
VDI means virtual desktop interface. Using VDI, you can maintain a standard image and remove the threat of an infected machine plugging into your network.

NEW QUESTION 297
- (Exam Topic 3)
During an incident response procedure, a security analyst collects a hard drive to analyze a possible vector of compromise. There is a Linux swap partition on the hard drive that needs to be checked. Which of the following, should the analyst use to extract human-readable content from the partition?

A. strings
B. head
C. fsstat
D. dd

Answer: A

NEW QUESTION 300
- (Exam Topic 3)
An organization is experiencing security incidents in which a systems administrator is creating unauthorized user accounts A security analyst has created a script to snapshot the system configuration each day. Following iss one of the scripts:

This script has been running successfully every day. Which of the following commands would provide the analyst with additional useful information relevant to the above script?
A)

B)

C)

D)

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

Answer: B

NEW QUESTION 301
- (Exam Topic 3)
A small organization has proprietary software that is used internally. The system has not been wen maintained and cannot be updated with the rest or the environment. Which of the following is the BEST solution?

A. virtualize the system and decommission the physical machine.
B. Remove it from the network and require air gapping.
C. Implement privileged access management for identity access.
D. Implement MFA on the specific system.

Answer: B

NEW QUESTION 304
- (Exam Topic 3)
Which of the following BEST explains the function of trusted firmware updates as they relate to hardware assurance?

A. Trusted firmware updates provide organizations with development, compilation, remote access, and customization for embedded devices.
B. Trusted firmware updates provide organizations with security specifications, open-source libraries, and custom toots for embedded devices.
C. Trusted firmware updates provide organizations with remote code execution, distribution, maintenance, and extended warranties for embedded devices
D. Trusted firmware updates provide organizations with secure code signing, distribution, installatio
E. and attestation for embedded devices.

Answer: D

Explanation:
The CySA+ exam outline calls out “trusted firmware updates,” but trusted firmware itself is more commonly described as part of trusted execution environments (TEEs). Trusted firmware is signed by a chip vendor or other trusted party, and then used to access keys to help control access to hardware. TEEs like those used by ARM processors leverage these technologies to protect the hardware by preventing unsigned code from using privileged features."

NEW QUESTION 309
- (Exam Topic 3)
A company has alerted planning the implemented a vulnerability management procedure. However, to security maturity level is low, so there are some prerequisites to complete before risk calculation and prioritization. Which of the following should be completed FIRST?

A. A business Impact analysis
B. A system assessment
C. Communication of the risk factors
D. A risk identification process

Answer: D

NEW QUESTION 312
- (Exam Topic 3)
An analyst is reviewing the output from some recent network enumeration activities. The following entry relates to a target on the network:

Based on the above output, which Of the following tools or techniques is MOST likely being used?

A. Web application firewall
B. Port triggering
C. Intrusion prevention system
D. Port isolation
E. Port address translation

Answer: A

NEW QUESTION 313
- (Exam Topic 3)
A company's application development has been outsourced to a third-party development team. Based on the SLA. The development team must follow industry best practices for secure coding. Which of the following is the BEST way to verify this agreement?

A. Input validation
B. Security regression testing
C. Application fuzzing
D. User acceptance testing
E. Stress testing

Answer: C

Explanation:
Fuzzing or fuzz testing is a dynamic application security testing technique for negative testing. Fuzzing aims to detect known, unknown, and zero-day vulnerabilities
https://brightsec.com/blog/fuzzing/

NEW QUESTION 318
- (Exam Topic 3)
After detecting possible malicious external scanning, an internal vulnerability scan was performed, and a critical server was found with an outdated version of JBoss. A legacy application that is running depends on that version of JBoss. Which of the following actions should be taken FIRST to prevent server compromise and business disruption at the same time?

A. Make a backup of the server and update the JBoss server that is running on it.
B. Contact the vendor for the legacy application and request an updated version.
C. Create a proper DMZ for outdated components and segregate the JBoss server.
D. Apply visualization over the server, using the new platform to provide the JBoss service for the legacy application as an external service.

Answer: C

Explanation:
What is that application for? "The DMZ is a special network zone designed to house systems that receive connections from the outside world, such as web and email servers. Sound firewall designs place these systems on an isolated network where, if they become compromised, they pose little threat to the internal network because connections between the DMZ and the internal network must still pass through the firewall and are subject to its security policy"

NEW QUESTION 323
- (Exam Topic 3)
An organization wants to implement a privileged access management solution to belter manage the use ot emergency and privileged service accounts Which of the following would BEST satisfy the organization's goal?

A. Access control lists
B. Discretionary access controls
C. Policy-based access controls
D. Credential vaulting

Answer: C

NEW QUESTION 327
- (Exam Topic 3)
An organization has the following policy statements:
• All emails entering or leaving the organization will be subject to inspection for malware, policy violations, and unauthorized coolant.
•AM network activity will be logged and monitored.
• Confidential data will be tagged and tracked
• Confidential data must never be transmitted in an unencrypted form.
• Confidential data must never be stored on an unencrypted mobile device. Which of the following is the organization enforcing?

A. Acceptable use policy
B. Data privacy policy
C. Encryption policy
D. Data management, policy

Answer: B

NEW QUESTION 329
- (Exam Topic 3)
A routine vulnerability scan detected a known vulnerability in a critical enterprise web application. Which of the following would be the BEST next step?

A. Submit a change request to have the system patched
B. Evaluate the risk and criticality to determine it further action is necessary
C. Notify a manager of the breach and initiate emergency procedures.
D. Remove the application from production and Inform the users.

Answer: A

NEW QUESTION 334
- (Exam Topic 3)
An organization has the following risk mitigation policies
• Risks without compensating controls will be mitigated first it the nsk value is greater than $50,000
• Other nsk mitigation will be pnontized based on risk value. The following risks have been identified:
Which of the following is the ordei of priority for risk mitigation from highest to lowest?

A. A, C, D, B
B. B, C, D, A
C. C, B, A, D
D. D, A, B
E. D, C, B, A

Answer: D

NEW QUESTION 336
- (Exam Topic 3)
An organization has the following policies:
*Services must run on standard ports.
*Unneeded services must be disabled.
The organization has the following servers:
*192.168.10.1 - web server
*192.168.10.2 - database server
A security analyst runs a scan on the servers and sees the following output:

Which of the following actions should the analyst take?

A. Disable HTTPS on 192.168.10.1.
B. Disable IIS on 192.168.10.1.
C. Disable DNS on 192.168.10.2.
D. Disable MSSQL on 192.168.10.2.

E. Disable SSH on both servers.

Answer: C

NEW QUESTION 340
- (Exam Topic 3)
An organization wants to ensure the privacy of the data that is on its systems Full disk encryption and DLP are already in use Which of the following is the BEST option?

A. Require all remote employees to sign an NDA
B. Enforce geofencmg to limit data accessibility
C. Require users to change their passwords more frequently
D. Update the AUP to restrict data sharing

Answer: A

NEW QUESTION 341
- (Exam Topic 3)
A company's domain has been spooled in numerous phishing campaigns. An analyst needs to determine the company is a victim of domain spoofing, despite having a DMARC record that should tell mailbox providers to ignore any email that fails DMARC upon review of the record, the analyst finds the following:

Which of the following BEST explains the reason why the company's requirements are not being processed correctly by mailbox providers?

A. The DMARC record's DKIM alignment tag Is incorrectly configured.
B. The DMARC record's policy tag is incorrectly configured.
C. The DMARC record does not have an SPF alignment tag.
D. The DMARC record's version tag is set to DMARC1 instead of the current version, which is DMARC3.

Answer: C

NEW QUESTION 345
- (Exam Topic 3)
Which of the following BEST describes HSM?

A. A computing device that manages cryptography, decrypts traffic, and maintains library calls
B. A computing device that manages digital keys, performs encryption/decryption functions, and maintains other cryptographic functions
C. A computing device that manages physical keys, encrypts devices, and creates strong cryptographic functions
D. A computing device that manages algorithms, performs entropy functions, and maintains digital signatures

Answer: B

NEW QUESTION 349
- (Exam Topic 3)
A Chief Executive Officer (CEO) is concerned the company will be exposed lo data sovereignty issues as a result of some new privacy regulations to help mitigate this risk. The Chief Information Security Officer (CISO) wants to implement an appropriate technical control. Which of the following would meet the requirement?

A. Data masking procedures
B. Enhanced encryption functions
C. Regular business impact analysis functions
D. Geographic access requirements

Answer: B

NEW QUESTION 351
- (Exam Topic 3)
A company’s Chief Information Security Officer (CISO) published an Internet usage policy that prohibits employees from accessing unauthorized websites. The IT department whitelisted websites used for business needs. The CISO wants the security analyst to recommend a solution that would improve security and support employee morale. Which of the following security recommendations would allow employees to browse non-business-related websites?

A. Implement a virtual machine alternative.
B. Develop a new secured browser.
C. Configure a personal business VLAN.
D. Install kiosks throughout the building.

Answer: C

NEW QUESTION 354
- (Exam Topic 3)
A company uses an FTP server to support its critical business functions The FTP server is configured as follows:
• The FTP service is running with (he data duectory configured in /opt/ftp/data.
• The FTP server hosts employees' home aVectories in /home
• Employees may store sensitive information in their home directories
An loC revealed that an FTP director/ traversal attack resulted in sensitive data loss Which of the following should a server administrator implement to reduce the risk of current and future directory traversal attacks targeted at the FTP server?

A. Implement file-level encryption of sensitive files
B. Reconfigure the FTP server to support FTPS
C. Run the FTP server n a chroot environment
D. Upgrade the FTP server to the latest version

Answer: C

NEW QUESTION 357
- (Exam Topic 3)
A security analyst performs various types of vulnerability scans. Review the vulnerability scan results to determine the type of scan that was executed and if a false positive occurred for each device.
Instructions:
Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan.
For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.
Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results. The Linux Web Server, File-Print Server and Directory Server are draggable.
If at any time you would like to bring back the initial state of the simulation, please select the Reset All button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 358
- (Exam Topic 3)
A security administrator needs to provide access from partners to an Isolated laboratory network inside an organization that meets the following requirements:
• The partners' PCs must not connect directly to the laboratory network.
• The tools the partners need to access while on the laboratory network must be available to all partners
• The partners must be able to run analyses on the laboratory network, which may take hours to complete Which of the following capabilities will MOST likely meet the security objectives of the request?

A. Deployment of a jump box to allow access to the laboratory network and use of VDI in persistent mode to provide the necessary tools for analysis
B. Deployment of a firewall to allow access to the laboratory network and use of VDI in non-persistent mode to provide the necessary tools tor analysis
C. Deployment of a firewall to allow access to the laboratory network and use of VDI In persistent mode to provide the necessary tools for analysis
D. Deployment of a jump box to allow access to the Laboratory network and use of VDI in non-persistent mode to provide the necessary tools for analysis

Answer: C

NEW QUESTION 363
- (Exam Topic 3)
The incident response team is working with a third-party forensic specialist to investigate the root cause of a recent intrusion An analyst was asked to submit sensitive network design details for review The forensic specialist recommended electronic delivery for efficiency but email was not an approved communication channel to send network details Which of the following BEST explains the importance of using a secure method of communication during incident response?

A. To prevent adversaries from intercepting response and recovery details

B. To ensure intellectual property remains on company servers
C. To have a backup plan in case email access is disabled
D. To ensure the management team has access to all the details that are being exchanged

Answer: B

NEW QUESTION 365
- (Exam Topic 3)
A code review reveals a web application is using lime-based cookies for session management. This is a security concern because lime-based cookies are easy to:

A. parameterize.
B. decode.
C. guess.
D. decrypt.

Answer: A

NEW QUESTION 370
- (Exam Topic 3)
Which of the following BEST identifies the appropriate use of threat intelligence as a function of detection and response?

A. To identify weaknesses in an organization's security posture
B. To identify likely attack scenarios within an organization
C. To build a business security plan for an organization
D. To build a network segmentation strategy

Answer: B

NEW QUESTION 372
- (Exam Topic 3)
An organization's internal department frequently uses a cloud provider to store large amounts of sensitive data. A threat actor has deployed a virtual machine to at the use of the cloud hosted hypervisor, the threat actor has escalated the access rights. Which of the following actions would be BEST to remediate the vulnerability?

A. Sandbox the virtual machine.
B. Implement an MFA solution.
C. Update lo the secure hypervisor version.
D. Implement dedicated hardware for each customer.

Answer: C

Explanation:
MFA can be used to reduce the likelihood that the attacker gains access to the VM, however, the scenario specifically states that the attacker was able to escalate rights and the question asks what can be done to remediate the vulnerability. the vulnerability in this case would be the ability to escalate rights.

NEW QUESTION 373
- (Exam Topic 3)
An analyst is responding to an incident within a cloud infrastructure Based on the logs and traffic analysis, the analyst thinks a container has been compromised Which of the following should Ihe analyst do FIRST?

A. Perform threat hunting in other areas of the cloud infrastructure
B. Contact law enforcement to report the incident
C. Perform a root cause analysis on the container and the service logs
D. Isolate the container from production using a predefined policy template

Answer: A

NEW QUESTION 375
- (Exam Topic 3)
An online gaming company was impacted by a ransomware attack. An employee opened an attachment that was received via an SMS attack on a company-issue firewall. Which following actions would help during the forensic analysis of the mobile device? (Select TWO).

A. Resetting the phone to factory settings
B. Rebooting the phone and installing the latest security updates
C. Documenting the respective chain of custody
D. Uninstalling any potentially unwanted programs
E. Performing a memory dump of the mobile device for analysis
F. Unlocking the device by blowing the eFuse

Answer: AE

NEW QUESTION 377
- (Exam Topic 3)
A security analyst notices the following entry while reviewing the server togs
OR 1=1' ADD USER attacker' PW 1337password' ---- Which of the following events occurred?

A. CSRF

B. XSS
C. SQLi
D. RCE

Answer: C

NEW QUESTION 379
- (Exam Topic 3)
A security learn implemented a SCM as part for its security-monitoring program there is a requirement to integrate a number of sources Into the SIEM to provide better context relative to the events being processed. Which of the following B€ST describes the result the security learn hopes to accomplish by adding these sources?

A. Data enrichment
B. Continuous integration
C. Machine learning
D. Workflow orchestration

Answer: A

NEW QUESTION 380
- (Exam Topic 3)
A security analyst is scanning the network to determine if a critical security patch was applied to all systems in an enterprise. The Organization has a very low tolerance for risk when it comes to resource availability. Which of the following is the BEST approach for configuring and scheduling the scan?

A. Make sure the scan is credentialed, covers at hosts in the patch management system, and is scheduled during business hours so it can be terminated if it affects business operations.
B. Make sure the scan is uncredentialed, covers at hosts in the patch management system, and Is scheduled during of business hours so it has the least impact on operations.
C. Make sure the scan is credentialed, has the latest software and signature versions, covers all external hosts in the patch management system and is scheduled during off-business hours so it has the least impact on operations.
D. Make sure the scan is credentialed, uses a ironed plug-in set, scans all host IP addresses in the enterprise, and is scheduled during off-business hours so it has the least impact on operations.

Answer: D

NEW QUESTION 385
- (Exam Topic 3)
A security analyst is performing a Diamond Model analysis of an incident the company had last quarter. A potential benefit of this activity is that it can identify:

A. detection and prevention capabilities to improve.
B. which systems were exploited more frequently.
C. possible evidence that is missing during forensic analysis.
D. which analysts require more training.
E. the time spent by analysts on each of the incidents.

Answer: A

NEW QUESTION 386
- (Exam Topic 3)
A security analyst is investigating a reported phishing attempt that was received by many users throughout the company The text of one of the emails is shown below:
Office 365 User.
It looks like you account has been locked out Please click this link and follow the pfompts to restore access Regards. Security Team
Due to the size of the company and the high storage requirements, the company does not log DNS requests or perform packet captures of network traffic, but rt does log network flow data Which of the following commands will the analyst most likely execute NEXT?

A. telnet office365.com 25
B. tracert 122.167.40.119
C. curl http:// accountfix-office365.com/logi
D. php
E. nslookup accountfix-office365.com

Answer: D

NEW QUESTION 390
- (Exam Topic 3)
Which of the following BEST describes how logging and monitoring work when entering into a public cloud relationship with a service provider?

A. Logging and monitoring are not needed in a public cloud environment
B. Logging and monitoring are done by the data owners
C. Logging and monitoring duties are specified in the SLA and contract
D. Logging and monitoring are done by the service provider

Answer: D

Explanation:

When transitioning over to a cloud solution, an organization may lose visibility of certain points on the technology stack, particularly if it's subscribing to PaaS or SaaS solutions. Because the responsibility of protecting portions of the stack falls to the service provider, it does sometimes mean the organization loses monitoring capabilities, for better or worse. Chapman, Brent; Maymi, Fernando. CompTIA CySA+ Cybersecurity Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002) (p. 158). McGraw Hill LLC. Kindle Edition.

NEW QUESTION 392
- (Exam Topic 3)
Which of me following are reasons why consumer IoT devices should be avoided in an enterprise environment? (Select TWO)

A. Message queuing telemetry transport does not support encryption.
B. The devices may have weak or known passwords.
C. The devices may cause a dramatic Increase in wireless network traffic.
D. The devices may utilize unsecure network protocols.
E. Multiple devices may interface with the functions of other loT devices.
F. The devices are not compatible with TLS 12.

Answer: BD

NEW QUESTION 394
- (Exam Topic 3)
Which of the following factors would determine the regulations placed on data under data sovereignty laws?

A. What the company intends to do with the data it owns
B. The company's data security policy
C. The type of data the company stores
D. The data laws of the country in which the company is located

Answer: D

NEW QUESTION 395
- (Exam Topic 3)
A security analyst is reviewing the output of tcpdump to analyze the type of activity on a packet capture:

Which of the following generated the above output?

A. A port scan
B. A TLS connection
C. A vulnerability scan
D. A ping sweep

Answer: A

Explanation:
Port scan againts 442-446 ports. For port 443 the scanner closed the connection after SYN-ACK.

NEW QUESTION 396
- (Exam Topic 3)
A security officer needs lo find Ihe mosl cos!-effective solution lo the cunent data pnvacy and protection gap found in the last security assessment Which of the following is the BEST recommendation?

A. Require users to sign NDAs
B. Create a data minimization plan.
C. Add access control requirements
D. Implement a data loss prevention solution

Answer: A

NEW QUESTION 400
- (Exam Topic 3)
A security analyst is reviewing the following server statistics:

Which of the following is MOST likely occurring?

A. Race condition
B. Privilege escalation
C. Resource exhaustion
D. VM escape

Answer: C

NEW QUESTION 403

- (Exam Topic 3)
Which of the following types of controls defines placing an ACL on a file folder?

A. Technical control
B. Confidentiality control
C. Managerial control
D. Operational control

Answer: A

Explanation:
"Technical controls enforce confidentiality, integrity, and availability in the digital space. Examples of technical security controls include firewall rules, access control lists, intrusion prevention systems, and encryption."

NEW QUESTION 408
- (Exam Topic 3)
An organization has a policy that requires servers to be dedicated to one function and unneeded services to be disabled. Given the following output from an Nmap scan of a web server:

Which of the following ports should be closed?

A. 22
B. 80
C. 443
D. 1433

Answer: D

NEW QUESTION 412
- (Exam Topic 3)
An incident response team detected malicious software that could have gained access to credit card data. The incident response team was able to mitigate significant damage and implement corrective actions. By having incident response mechanisms in place. Which of the following should be notified for lessons learned?

A. The human resources department
B. Customers
C. Company leadership
D. The legal team

Answer: D

NEW QUESTION 413
- (Exam Topic 3)
An analyst receives an alert from the continuous-monitoring solution about unauthorized changes to the firmware versions on several field devices. The asset owners confirm that no firmware version updates were performed by authorized technicians, and customers have not reported any performance issues or outages. Which Of the following actions would be BEST for the analyst to recommend to the asset owners to secure the devices from further exploitation?

A. Change the passwords on the devices.
B. Implement BIOS passwords.
C. Remove the assets from the production network for analysis.
D. Report the findings to the threat intel community.

Answer: C

Explanation:
If were referring to other devices, yes - Implement BIOS passwords before they are compromised. But the ones that were already compromised, they need to be removed from the system to avoid further exploitation. Plus, if you put a password on there, the attacker may now have your password.

NEW QUESTION 414
- (Exam Topic 3)
After examining a header and footer file, a security analyst begins reconstructing files by scanning the raw data bytes of a hard disk and rebuilding them. Which of the following techniques is the analyst using?

A. Header analysis
B. File carving
C. Metadata analysis
D. Data recovery

Answer: B

NEW QUESTION 415
- (Exam Topic 3)
A security analyst observes a large amount of scanning activity coming from an IP address outside the organization's environment. Which of the following should the analyst do to block this activity?

A. Create an IPS rule to block the subnet.
B. Sinkhole the IP address.
C. Create a firewall rule to block the IP address.
D. Close all unnecessary open ports.

Answer: C

NEW QUESTION 419
- (Exam Topic 3)
A security analyst identified some potentially malicious processes after capturing the contents of memory from a machine during incident response. Which of the following procedures is the NEXT step for further in investigation?

A. Data carving
B. Timeline construction
C. File cloning
D. Reverse engineering

Answer: C

NEW QUESTION 424
- (Exam Topic 3)
A security analyst identified one server that was compromised and used as a data making machine, and a few of the hard drive that was created. Which of the following will MOST likely provide information about when and how the machine was compromised and where the malware is located?

A. System timeline reconstruction
B. System registry extraction
C. Data carving
D. Volatile memory analysts

Answer: D

Explanation:
Information security professionals conduct memory forensics to investigate and identify attacks or malicious behaviors that do not leave easily detectable tracks on hard drive data.

NEW QUESTION 426
- (Exam Topic 3)
Forming a hypothesis, looking for indicators of compromise, and using the findings to proactively improve detection capabilities are examples of the value of:

A. vulnerability scanning.
B. threat hunting.
C. red learning.
D. penetration testing.

Answer: A

NEW QUESTION 429
- (Exam Topic 3)
When investigating a report of a system compromise, a security analyst views the following /var/log/secure log file:

Which of the following can the analyst conclude from viewing the log file?

A. The comptia user knows the sudo password.
B. The comptia user executed the sudo su command.
C. The comptia user knows the root password.
D. The comptia user added himself or herself to the /etc/sudoers file.

Answer: C

Explanation:

the user is not in the sudoers file. you use your own password for that. the user used the su command to switch user accounts. when no user is specified, the su command defaults to the root account. the user is now logged into the root account. you need to know the root password to log into the root account.

NEW QUESTION 432
- (Exam Topic 3)
Which of the following describes the mam difference between supervised and unsupervised machine-learning algorithms that are used in cybersecurity applications?

A. Supervised algorithms can be used to block attacks, while unsupervised algorithms cannot.
B. Supervised algorithms require security analyst feedback, while unsupervised algorithms do not.
C. Unsupervised algorithms are not suitable for IDS systems, white supervised algorithms are
D. Unsupervised algorithms produce more false positive
E. Than supervised algorithms.

Answer: B

NEW QUESTION 434
- (Exam Topic 3)
A company recently experienced a breach of sensitive information that affects customers across multiple geographical regions. Which of the following roles would be BEST suited to determine the breach notification requirements?

A. Legal counsel
B. Chief Security Officer
C. Human resources
D. Law enforcement

Answer: A

NEW QUESTION 438
- (Exam Topic 3)
Due to continued support of legacy applications, an organization's enterprise password complexity rules are inadequate for its required security posture. Which of the following is the BEST compensating control to help reduce authentication compromises?

A. Smart cards
B. Multifactor authentication
C. Biometrics
D. Increased password-rotation frequency

Answer: D

NEW QUESTION 440
- (Exam Topic 3)
After a series of Group Policy Object updates, multiple services stopped functioning. The systems administrator believes the issue resulted from a Group Policy Object update but cannot validate which update caused the Issue. Which of the following security solutions would resolve this issue?

A. Privilege management
B. Group Policy Object management
C. Change management
D. Asset management

Answer: C

NEW QUESTION 445
- (Exam Topic 3)
The Chief information Officer of a large cloud software vendor reports that many employees are falling victim to phishing emails because they appear to come from other employees. Which of the following would BEST prevent this issue

A. Induce digital signatures on messages originating within the company.
B. Require users authenticate to the SMTP server
C. Implement DKIM to perform authentication that will prevent this Issue.
D. Set up an email analysis solution that looks for known malicious Iinks within the email.

Answer: C

NEW QUESTION 450
- (Exam Topic 3)
As part of the senior leadership team's ongoing nsk management activities the Chief Information Security Officer has tasked a security analyst with coordinating the right training and testing methodology to respond to new business initiatives or significant changes to existing ones The management team wants to examine a new business process that would use existing infrastructure to process and store sensitive data Which of the following would be appropnate for the security analyst to coordinate?

A. A black-box penetration testing engagement
B. A tabletop exercise
C. Threat modeling
D. A business impact analysis

Answer: D

NEW QUESTION 455
- (Exam Topic 3)
An analyst receives artifacts from a recent Intrusion and is able to pull a domain, IP address, email address, and software version. When of the following points of the Diamond Model of Intrusion Analysis does this intelligence represent?

A. Infrastructure
B. Capabilities
C. Adversary
D. Victims

Answer: C

NEW QUESTION 456
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CS0-003 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CS0-003 Product From:

https://www.2passeasy.com/dumps/CS0-003/

Money Back Guarantee

CS0-003 Practice Exam Features:

* CS0-003 Questions and Answers Updated Frequently

* CS0-003 Practice Questions Verified by Expert Senior Certified Staff

* CS0-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CS0-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year