CompTIA

Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam

NEW QUESTION 1
- (Exam Topic 1)
A security analyst is reviewing the following log from an email security service.

Which of the following BEST describes the reason why the email was blocked?

A. The To address is invalid.
B. The email originated from the www.spamfilter.org URL.
C. The IP address and the remote server name are the same.
D. The IP address was blacklisted.
E. The From address is invalid.

Answer: C

Explanation:
Reference: https://www.webopediA.com/TERM/R/RBL.html

NEW QUESTION 2
- (Exam Topic 1)
Which of the following types of policies is used to regulate data storage on the network?

A. Password
B. Acceptable use
C. Account management
D. Retention

Answer: D

Explanation:
Reference:
http://www.css.edu/administration/information-technologies/computing-policies/computer-and- network-policies.html

NEW QUESTION 3
- (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 4
- (Exam Topic 1)
A security analyst has been alerted to several emails that snow evidence an employee is planning malicious activities that involve employee PII on the network before leaving the organization. The security analysis BEST response would be to coordinate with the legal department and:

A. the public relations department

B. senior leadership
C. law enforcement
D. the human resources department

Answer: D

NEW QUESTION 5
- (Exam Topic 1)
A security analyst received an email with the following key: Xj3XJ3LLc
A second security analyst received an email with following key: 3XJ3xjcLLC
The security manager has informed the two analysts that the email they received is a key that allows access to the company's financial segment for maintenance.
This is an example of:

A. dual control
B. private key encryption
C. separation of duties
D. public key encryption
E. two-factor authentication

Answer: A

NEW QUESTION 6
- (Exam Topic 1)
Which of the following is the MOST important objective of a post-incident review?

A. Capture lessons learned and improve incident response processes
B. Develop a process for containment and continue improvement efforts
C. Identify new technologies and strategies to remediate
D. Identify a new management strategy

Answer: A

NEW QUESTION 7
- (Exam Topic 1)
A user receives a potentially malicious email that contains spelling errors and a PDF document. A security
analyst reviews the email and decides to download the attachment to a Linux sandbox for review. Which of the following commands would MOST likely indicate if the email is malicious?

A. sha256sum ~/Desktop/file.pdf
B. file ~/Desktop/file.pdf
C. strings ~/Desktop/file.pdf | grep "<script"
D. cat < ~/Desktop/file.pdf | grep -i .exe

Answer: A

NEW QUESTION 8
- (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 9
- (Exam Topic 1)
Which of the following technologies can be used to house the entropy keys for disk encryption on desktops and laptops?

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

Answer: A

NEW QUESTION 10
- (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 10
- (Exam Topic 1)
A security analyst has a sample of malicious software and needs to know what the sample does? The analyst runs the sample in a carefully controlled and monitored virtual machine to observe the software behavior. Which of the following malware analysis approaches is this?

A. White box testing
B. Fuzzing
C. Sandboxing
D. Static code analysis

Answer: C

NEW QUESTION 14
- (Exam Topic 1)
Which of the following are components of the intelligence cycle? (Select TWO.)

A. Collection
B. Normalization
C. Response
D. Analysis
E. Correction
F. Dissension

Answer: BE

NEW QUESTION 16
- (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 18
- (Exam Topic 1)
A pharmaceutical company's marketing team wants to send out notifications about new products to alert users of recalls and newly discovered adverse drug reactions. The team plans to use the names and mailing addresses that users have provided.
Which of the following data privacy standards does this violate?

A. Purpose limitation
B. Sovereignty
C. Data minimization
D. Retention

Answer: A

Explanation:
Reference:
http://www.isitethical.eu/portfolio-item/purpose-limitation/

NEW QUESTION 22
- (Exam Topic 1)
A finance department employee has received a message that appears to have been sent from the Chief Financial Officer (CFO) asking the employee to perform a wife transfer Analysis of the email shows the message came from an external source and is fraudulent. Which of the following would work BEST to improve the likelihood of employees quickly recognizing fraudulent emails?

A. Implementing a sandboxing solution for viewing emails and attachments
B. Limiting email from the finance department to recipients on a pre-approved whitelist
C. Configuring email client settings to display all messages in plaintext when read
D. Adding a banner to incoming messages that identifies the messages as external

Answer: D

NEW QUESTION 25
- (Exam Topic 1)
After a breach involving the exfiltration of a large amount of sensitive data a security analyst is reviewing the following firewall logs to determine how the breach occurred:

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

A. 192.168.1.1
B. 192.168.1.10
C. 192.168.1.12
D. 192.168.1.193

Answer: C

NEW QUESTION 30
- (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 32
- (Exam Topic 1)
The help desk noticed a security analyst that emails from a new email server are not being sent out. The new email server was recently added to the existing ones. The analyst runs the following command on the new server.

Given the output, which of the following should the security analyst check NEXT?

A. The DNS name of the new email server
B. The version of SPF that is being used
C. The IP address of the new email server
D. The DMARC policy

Answer: A

NEW QUESTION 36
- (Exam Topic 1)
A security analyst is reviewing the logs from an internal chat server. The chat.log file is too large to review manually, so the analyst wants to create a shorter log file that only includes lines associated with a user demonstrating anomalous activity. Below is a snippet of the log:

Which of the following commands would work BEST to achieve the desired result?

A. grep -v chatter14 chat.log
B. grep -i pythonfun chat.log
C. grep -i javashark chat.log
D. grep -v javashark chat.log
E. grep -v pythonfun chat.log
F. grep -i chatter14 chat.log

Answer: D

NEW QUESTION 37
- (Exam Topic 1)
A human resources employee sends out a mass email to all employees that contains their personnel records. A security analyst is called in to address the concern of the human resources director on how to prevent this from happening in the future.
Which of the following would be the BEST solution to recommend to the director?

A. Install a data loss prevention system, and train human resources employees on its us
B. Provide PII training to all employees at the compan
C. Encrypt PII information.
D. Enforce encryption on all emails sent within the compan
E. Create a PII program and policy on how to handle dat
F. Train all human resources employees.
G. Train all employee
H. Encrypt data sent on the company networ
I. Bring in privacy personnel to present a plan on how PII should be handled.
J. Install specific equipment to create a human resources policy that protects PII dat
K. Train company employees on how to handle PII dat
L. Outsource all PII to another compan
M. Send the human resourcesdirector to training for PII handling.

Answer: A

NEW QUESTION 39
- (Exam Topic 1)
During an investigation, a security analyst identified machines that are infected with malware the antivirus was unable to detect.
Which of the following is the BEST place to acquire evidence to perform data carving?

A. The system memory
B. The hard drive
C. Network packets
D. The Windows Registry

Answer: A

Explanation:
Reference: https://resources.infosecinstitute.com/memory-forensics/#gref https://www.computerhope.com/jargon/d/data-carving.htm

NEW QUESTION 43
- (Exam Topic 1)
Which of the following is the BEST way to share incident-related artifacts to provide non-repudiation?

A. Secure email
B. Encrypted USB drives
C. Cloud containers
D. Network folders

Answer: B

NEW QUESTION 48
- (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 51
- (Exam Topic 1)
A security manager has asked an analyst to provide feedback on the results of a penetration lest. After reviewing the results the manager requests information regarding the possible exploitation of vulnerabilities Much of the following information data points would be MOST useful for the analyst to provide to the security manager who would then communicate the risk factors to senior management? (Select TWO)

A. Probability
B. Adversary capability
C. Attack vector
D. Impact
E. Classification
F. Indicators of compromise

Answer: AD

NEW QUESTION 55
- (Exam Topic 1)
Which of the following will allow different cloud instances to share various types of data with a minimal amount of complexity?

A. Reverse engineering
B. Application log collectors
C. Workflow orchestration
D. API integration
E. Scripting

Answer: D

NEW QUESTION 60
- (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 63
- (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 65
- (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 70
- (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 71
- (Exam Topic 1)
During routine monitoring, a security analyst discovers several suspicious websites that are communicating with a local host. The analyst queries for IP 192.168.50.2 for a 24-hour period:

To further investigate, the analyst should request PCAP for SRC 192.168.50.2 and.

A. DST 138.10.2.5.
B. DST 138.10.25.5.
C. DST 172.10.3.5.
D. DST 172.10.45.5.
E. DST 175.35.20.5.

Answer: A

NEW QUESTION 73
- (Exam Topic 1)
The inability to do remote updates of certificates. keys software and firmware is a security issue commonly associated with:

A. web servers on private networks.
B. HVAC control systems
C. smartphones
D. firewalls and UTM devices

Answer: B

NEW QUESTION 77
- (Exam Topic 1)
Which of me following BEST articulates the benefit of leveraging SCAP in an organization's cybersecurity analysis toolset?

A. It automatically performs remedial configuration changes lo enterprise security services
B. It enables standard checklist and vulnerability analysis expressions for automaton
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 82
- (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 85
- (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 86
- (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 89
- (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 93
- (Exam Topic 1)
An organization has not had an incident for several month. The Chief information Security Officer (CISO) wants to move to proactive stance for security investigations. Which of the following would BEST meet that goal?

A. Root-cause analysis
B. Active response
C. Advanced antivirus
D. Information-sharing community
E. Threat hunting

Answer: E

NEW QUESTION 96
- (Exam Topic 1)
A security analyst needs to reduce the overall attack surface.
Which of the following infrastructure changes should the analyst recommend?

A. Implement a honeypot.
B. Air gap sensitive systems.
C. Increase the network segmentation.
D. Implement a cloud-based architecture.

Answer: C

Explanation:
Reference: https://www.securitymagazine.com/articles/89283-ways-to-reduce-your-attack-surface

NEW QUESTION 100
- (Exam Topic 1)
A security analyst conducted a risk assessment on an organization's wireless network and identified a high-risk element in the implementation of data confidentially protection. Which of the following is the BEST technical security control to mitigate this risk?

A. Switch to RADIUS technology
B. Switch to TACACS+ technology.
C. Switch to 802 IX technology
D. Switch to the WPA2 protocol.

Answer: D

NEW QUESTION 101
- (Exam Topic 1)
Ann, a user, reports to the security team that her browser began redirecting her to random sites while using her Windows laptop. Ann further reports that the OS shows the C: drive is out of space despite having plenty of space recently. Ann claims she not downloaded anything. The security team obtains the laptop and begins to investigate, noting the following:
File access auditing is turned off.
When clearing up disk space to make the laptop functional, files that appear to be cached web pages are immediately created in a temporary directory, filling up the available drive space.
All processes running appear to be legitimate processes for this user and machine.
Network traffic spikes when the space is cleared on the laptop.
No browser is open.
Which of the following initial actions and tools would provide the BEST approach to determining what is happening?

A. Delete the temporary files, run an Nmap scan, and utilize Burp Suite.
B. Disable the network connection, check Sysinternals Process Explorer, and review netstat output.
C. Perform a hard power down of the laptop, take a dd image, and analyze with FTK.
D. Review logins to the laptop, search Windows Event Viewer, and review Wireshark captures.

Answer: B

NEW QUESTION 102
- (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 106
- (Exam Topic 1)
Joe, a penetration tester, used a professional directory to identify a network administrator and ID administrator for a client's company. Joe then emailed the network administrator, identifying himself as the ID administrator, and asked for a current password as part of a security exercise. Which of the following techniques were used in this scenario?

A. Enumeration and OS fingerprinting
B. Email harvesting and host scanning
C. Social media profiling and phishing
D. Network and host scanning

Answer: C

NEW QUESTION 107
- (Exam Topic 1)
While analyzing logs from a WAF, a cybersecurity analyst finds the following:

Which of the following BEST describes what the analyst has found?

A. This is an encrypted GET HTTP request
B. A packet is being used to bypass the WAF
C. This is an encrypted packet
D. This is an encoded WAF bypass

Answer: D

NEW QUESTION 111
- (Exam Topic 1)
A small electronics company decides to use a contractor to assist with the development of a new FPGA-based device. Several of the development phases will occur off-site at the contractor's labs.
Which of the following is the main concern a security analyst should have with this arrangement?

A. Making multiple trips between development sites increases the chance of physical damage to the FPGAs.
B. Moving the FPGAs between development sites will lessen the time that is available for security testing.
C. Development phases occurring at multiple sites may produce change management issues.
D. FPGA applications are easily cloned, increasing the possibility of intellectual property theft.

Answer: D

Explanation:
Reference: https://www.eetimes.com/how-to-protect-intellectual-property-in-fpgas-devices-part-1/#

NEW QUESTION 114
- (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 119
- (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 121
- (Exam Topic 1)
Which of the following software assessment methods would be BEST for gathering data related to an application's availability during peak times?

A. Security regression testing
B. Stress testing
C. Static analysis testing
D. Dynamic analysis testing
E. User acceptance testing

Answer: B

NEW QUESTION 124
- (Exam Topic 1)
Which of the following roles is ultimately responsible for determining the classification levels assigned to specific data sets?

A. Data custodian
B. Data owner
C. Data processor
D. Senior management

Answer: B

Explanation:
Reference: https://www.pearsonitcertification.com/articles/article.aspx?p=2731933&seqNum=3

NEW QUESTION 125
- (Exam Topic 1)
During a cyber incident, which of the following is the BEST course of action?

A. Switch to using a pre-approved, secure, third-party communication system.
B. Keep the entire company informed to ensure transparency and integrity during the incident.
C. Restrict customer communication until the severity of the breach is confirmed.
D. Limit communications to pre-authorized parties to ensure response efforts remain confidential.

Answer: D

NEW QUESTION 128
- (Exam Topic 1)
A company was recently awarded several large government contracts and wants to determine its current risk from one specific APT.
Which of the following threat modeling methodologies would be the MOST appropriate to use during this analysis?

A. Attack vectors
B. Adversary capability
C. Diamond Model of Intrusion Analysis
D. Kill chain
E. Total attack surface

Answer: B

Explanation:
Reference: https://www.secureworks.com/blog/advanced-persistent-threats-apt-b

NEW QUESTION 132
- (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 135

- (Exam Topic 1)
An organization was alerted to a possible compromise after its proprietary data was found for sale on the Internet. An analyst is reviewing the logs from the next-generation UTM in an attempt to find evidence of this breach. Given the following output:

Which of the following should be the focus of the investigation?

A. webserver.org-dmz.org
B. sftp.org-dmz.org
C. 83hht23.org-int.org
D. ftps.bluemed.net

Answer: A

NEW QUESTION 138
- (Exam Topic 1)
A security analyst is investigating a system compromise. The analyst verities the system was up to date on OS patches at the time of the compromise. Which of the following describes the type of vulnerability that was MOST likely expiated?

A. Insider threat
B. Buffer overflow
C. Advanced persistent threat
D. Zero day

Answer: D

NEW QUESTION 142
- (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 146
- (Exam Topic 1)
A system administrator is doing network reconnaissance of a company's external network to determine the vulnerability of various services that are running. Sending some sample traffic to the external host, the administrator obtains the following packet capture:

Based on the output, which of the following services should be further tested for vulnerabilities?

A. SSH
B. HTTP
C. SMB

D. HTTPS

Answer: A

NEW QUESTION 150
- (Exam Topic 1)
Ransomware is identified on a company's network that affects both Windows and MAC hosts. The command and control channel for encryption for this variant uses TCP ports from 11000 to 65000. The channel goes to good1. Iholdbadkeys.com, which resolves to IP address 72.172.16.2.
Which of the following is the MOST effective way to prevent any newly infected systems from actually encrypting the data on connected network drives while causing the least disruption to normal Internet traffic?

A. Block all outbound traffic to web host good1 iholdbadkeys.com at the border gateway.
B. Block all outbound TCP connections to IP host address 172.172.16.2 at the border gateway.
C. Block all outbound traffic on TCP ports 11000 to 65000 at the border gateway.
D. Block all outbound traffic on TCP ports 11000 to 65000 to IP host address 172.172.16.2 at the border gateway.

Answer: A

NEW QUESTION 152
- (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 156
- (Exam Topic 1)
A SIEM solution alerts a security analyst of a high number of login attempts against the company's webmail portal. The analyst determines the login attempts used credentials from a past data breach.
Which of the following is the BEST mitigation to prevent unauthorized access?

A. Single sign-on
B. Mandatory access control
C. Multifactor authentication
D. Federation
E. Privileged access management

Answer: C

NEW QUESTION 157
- (Exam Topic 1)
Which of the following should be found within an organization's acceptable use policy?

A. Passwords must be eight characters in length and contain at least one special character.
B. Customer data must be handled properly, stored on company servers, and encrypted when possible
C. Administrator accounts must be audited monthly, and inactive accounts should be removed.
D. Consequences of violating the policy could include discipline up to and including termination.

Answer: D

NEW QUESTION 159
- (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 164
- (Exam Topic 1)
A security analyst, who is working for a company that utilizes Linux servers, receives the following results from a vulnerability scan:

Which of the following is MOST likely a false positive?

A. ICMP timestamp request remote date disclosure
B. Windows SMB service enumeration via \srvsvc

C. Anonymous FTP enabled
D. Unsupported web server detection

Answer: B

NEW QUESTION 168
- (Exam Topic 1)
A security analyst for a large financial institution is creating a threat model for a specific threat actor that is likely targeting an organization's financial assets. Which of the following is the BEST example of the level of sophistication this threat actor is using?

A. Social media accounts attributed to the threat actor
B. Custom malware attributed to the threat actor from prior attacks
C. Email addresses and phone numbers tied to the threat actor
D. Network assets used in previous attacks attributed to the threat actor
E. IP addresses used by the threat actor for command and control

Answer: B

NEW QUESTION 171
- (Exam Topic 1)
As a proactive threat-hunting technique, hunters must develop situational cases based on likely attack scenarios derived from the available threat intelligence information. After forming the basis of the scenario, which of the following may the threat hunter construct to establish a framework for threat assessment?

A. Critical asset list
B. Threat vector
C. Attack profile
D. Hypothesis

Answer: D

NEW QUESTION 175
- (Exam Topic 1)
An analyst is performing penetration testing and vulnerability assessment activities against a new vehicle automation platform. Which of the following is MOST likely an attack vector that is being utilized as part of the testing and assessment?

A. FaaS
B. RTOS
C. SoC
D. GPS
E. CAN bus

Answer: E

NEW QUESTION 177
- (Exam Topic 1)
A security analyst is reviewing the following web server log:

Which of the following BEST describes the issue?

A. Directory traversal exploit
B. Cross-site scripting
C. SQL injection
D. Cross-site request forgery

Answer: A

NEW QUESTION 178
- (Exam Topic 1)
Which of the following would MOST likely be included in the incident response procedure after a security breach of customer PII?

A. Human resources
B. Public relations
C. Marketing
D. Internal network operations center

Answer: B

NEW QUESTION 179
- (Exam Topic 1)
A security team wants to make SaaS solutions accessible from only the corporate campus Which of the following would BEST accomplish this goal?

A. Geofencing
B. IP restrictions
C. Reverse proxy
D. Single sign-on

Answer: A

Explanation:
Reference: https://bluedot.io/library/what-is-geofencing/

NEW QUESTION 183
- (Exam Topic 1)
Which of the following would a security engineer recommend to BEST protect sensitive system data from being accessed on mobile devices?

A. Use a UEFl boot password.
B. Implement a self-encrypted disk.
C. Configure filesystem encryption
D. Enable Secure Boot using TPM

Answer: C

NEW QUESTION 184
- (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 186
- (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 190
- (Exam Topic 1)
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:
Antivirus is installed on the remote host:
Installation path: C:\Program Files\AVProduct\Win32\ Product Engine: 14.12.101
Engine Version: 3.5.71
Scanner does not currently have information about AVProduct version 3.5.71. It may no longer be supported. The engine version is out of date. The oldest supported version from the vendor is 4.2.11.
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 193
- (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 196
- (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 199
- (Exam Topic 1)
A security analyst is responding to an incident on a web server on the company network that is making a large number of outbound requests over DNS Which of the following is the FIRST step the analyst should take to evaluate this potential indicator of compromise'?

A. Run an anti-malware scan on the system to detect and eradicate the current threat
B. Start a network capture on the system to look into the DNS requests to validate command and control traffic.
C. Shut down the system to prevent further degradation of the company network
D. Reimage the machine to remove the threat completely and get back to a normal running state.
E. Isolate the system on the network to ensure it cannot access other systems while evaluation is underway.

Answer: B

NEW QUESTION 200
- (Exam Topic 1)
A large software company wants to move «s source control and deployment pipelines into a cloud-computing environment. Due to the nature of the business management determines the recovery time objective needs to be within one hour. Which of the following strategies would put the company in the BEST position to achieve the desired recovery time?

A. Establish an alternate site with active replication to other regions
B. Configure a duplicate environment in the same region and load balance between both instances
C. Set up every cloud component with duplicated copies and auto scaling turned on
D. Create a duplicate copy on premises that can be used for failover in a disaster situation

Answer: A

NEW QUESTION 203
- (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 208
- (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 210
- (Exam Topic 1)
A security analyst recently discovered two unauthorized hosts on the campus's wireless network segment from a man-m-the-middle attack .The security analyst also verified that privileges were not escalated, and the two devices did not gain access to other network devices Which of the following would BEST mitigate and improve the security posture of the wireless network for this type of attack?

A. Enable MAC filtering on the wireless router and suggest a stronger encryption for the wireless network,
B. Change the SSID, strengthen the passcode, and implement MAC filtering on the wireless router.
C. Enable MAC filtering on the wireless router and create a whitelist that allows devices on the network
D. Conduct a wireless survey to determine if the wireless strength needs to be reduced.

Answer: A

NEW QUESTION 211
- (Exam Topic 1)
Risk management wants IT to implement a solution that will permit an analyst to intercept, execute, and analyze potentially malicious files that are downloaded from the Internet.
Which of the following would BEST provide this solution?

A. File fingerprinting
B. Decomposition of malware
C. Risk evaluation
D. Sandboxing

Answer: A

NEW QUESTION 214
- (Exam Topic 1)
A security technician is testing a solution that will prevent outside entities from spoofing the company's email domain, which is comptiA.org. The testing is successful, and the security technician is prepared to fully implement the solution.
Which of the following actions should the technician take to accomplish this task?

A. Add TXT @ "v=spf1 mx include:_spf.comptiA.org all" to the DNS record.
B. Add TXT @ "v=spf1 mx include:_spf.comptiA.org all" to the email server.
C. Add TXT @ "v=spf1 mx include:_spf.comptiA.org +all" to the domain controller.
D. Add TXT @ "v=spf1 mx include:_spf.comptiA.org +all" to the web server.

Answer: A

Explanation:
Reference: https://blog.finjan.com/email-spoofing/

NEW QUESTION 216
- (Exam Topic 1)
A malicious hacker wants to gather guest credentials on a hotel 802.11 network. Which of the following tools is the malicious hacker going to use to gain access to information found on the hotel network?

A. Nikto
B. Aircrak-ng
C. Nessus
D. tcpdump

Answer: B

NEW QUESTION 221
- (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 224
- (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 228
- (Exam Topic 1)
As part of a merger with another organization, a Chief Information Security Officer (CISO) is working with an assessor to perform a risk assessment focused on data privacy compliance. The CISO is primarily concerned with the potential legal liability and fines associated with data privacy. Based on the CISO's concerns, the assessor will MOST likely focus on:

A. qualitative probabilities.
B. quantitative probabilities.
C. qualitative magnitude.
D. quantitative magnitude.

Answer: D

NEW QUESTION 230
- (Exam Topic 1)
A storage area network (SAN) was inadvertently powered off while power maintenance was being performed in a datacenter. None of the systems should have lost all power during the maintenance. Upon review, it is discovered that a SAN administrator moved a power plug when testing the SAN's fault notification features.
Which of the following should be done to prevent this issue from reoccurring?

A. Ensure both power supplies on the SAN are serviced by separate circuits, so that if one circuit goes down, the other remains powered.
B. Install additional batteries in the SAN power supplies with enough capacity to keep the system powered on during maintenance operations.
C. Ensure power configuration is covered in the datacenter change management policy and have the SAN administrator review this policy.
D. Install a third power supply in the SAN so loss of any power intuit does not result in the SAN completely powering off.

Answer: A

NEW QUESTION 231
- (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 232
- (Exam Topic 1)
A company wants to establish a threat-hunting team. Which of the following BEST describes the rationale for integration intelligence into hunt operations?

A. It enables the team to prioritize the focus area and tactics within the company’s environment.
B. It provide critically analyses for key enterprise servers and services.
C. It allow analysis to receive updates on newly discovered software vulnerabilities.
D. It supports rapid response and recovery during and followed an incident.

Answer: A

NEW QUESTION 234
- (Exam Topic 1)
A new on-premises application server was recently installed on the network. Remote access to the server was enabled for vendor support on required ports, but recent security reports show large amounts of data are being sent to various unauthorized networks through those ports. Which of the following configuration changes must be implemented to resolve this security issue while still allowing remote vendor access?

A. Apply a firewall application server rule.
B. Whitelist the application server.
C. Sandbox the application server.
D. Enable port security.
E. Block the unauthorized networks.

Answer: B

NEW QUESTION 239
- (Exam Topic 1)
A security analyst is reviewing a web application. If an unauthenticated user tries to access a page in the application, the user is redirected to the login page. After successful authentication, the user is then redirected back to the original page. Some users have reported receiving phishing emails with a link that takes them to the application login page but then redirects to a fake login page after successful authentication.
Which of the following will remediate this software vulnerability?

A. Enforce unique session IDs for the application.
B. Deploy a WAF in front of the web application.
C. Check for and enforce the proper domain for the redirect.

D. Use a parameterized query to check the credentials.
E. Implement email filtering with anti-phishing protection.

Answer: C

NEW QUESTION 242
- (Exam Topic 1)
A security analyst suspects a malware infection was caused by a user who downloaded malware after clicking http://<malwaresource>/A.php in a phishing email.
To prevent other computers from being infected by the same malware variation, the analyst should create a rule on the.

A. email server that automatically deletes attached executables.
B. IDS to match the malware sample.
C. proxy to block all connections to <malwaresource>.
D. firewall to block connection attempts to dynamic DNS hosts.

Answer: C

NEW QUESTION 246
- (Exam Topic 1)
A security administrator needs to create an IDS rule to alert on FTP login attempts by root. Which of the following rules is the BEST solution?

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

Answer: B

NEW QUESTION 247
- (Exam Topic 1)
Data spillage occurred when an employee accidentally emailed a sensitive file to an external recipient.
Which of the following controls would have MOST likely prevented this incident?

A. SSO
B. DLP
C. WAF
D. VDI

Answer: B

Explanation:
Reference: https://greenlightcorp.com/blog/cyber-security-solutions-data-spillage-and-how-to-create-an-after- incident-to-do-list/

NEW QUESTION 248
- (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 250
- (Exam Topic 1)
A system is experiencing noticeably slow response times, and users are being locked out frequently. An analyst asked for the system security plan and found the system comprises two servers: an application server in the DMZ and a database server inside the trusted domain. Which of the following should be performed NEXT to investigate the availability issue?

A. Review the firewall logs.
B. Review syslogs from critical servers.
C. Perform fuzzing.
D. Install a WAF in front of the application server.

Answer: B

NEW QUESTION 252
- (Exam Topic 1)
A security analyst is attempting to utilize the blowing threat intelligence for developing detection capabilities:

In which of the following phases is this APT MOST likely to leave discoverable artifacts?

A. Data collection/exfiltration
B. Defensive evasion
C. Lateral movement
D. Reconnaissance

Answer: A

NEW QUESTION 255
- (Exam Topic 1)
A company's modem response team is handling a threat that was identified on the network Security analysts have as at remote sites. Which of the following is the MOST appropriate next step in the incident response plan?

A. Quarantine the web server
B. Deploy virtual firewalls
C. Capture a forensic image of the memory and disk
D. Enable web server containerization

Answer: B

NEW QUESTION 256
- (Exam Topic 1)
A security analyst is trying to determine if a host is active on a network. The analyst first attempts the following:

The analyst runs the following command next:

Which of the following would explain the difference in results?

A. ICMP is being blocked by a firewall.
B. The routing tables for ping and hping3 were different.
C. The original ping command needed root permission to execute.
D. hping3 is returning a false positive.

Answer: A

NEW QUESTION 260
- (Exam Topic 1)
An information security analyst is working with a data owner to identify the appropriate controls to preserve the confidentiality of data within an enterprise environment One of the primary concerns is exfiltration of data by malicious insiders Which of the following controls is the MOST appropriate to mitigate risks?

A. Data deduplication
B. OS fingerprinting
C. Digital watermarking
D. Data loss prevention

Answer: D

NEW QUESTION 261
- (Exam Topic 2)
A company's security officer needs to implement geographical IP blocks for nation-state actors from a foreign country On which of the following should the blocks be implemented'?

A. Web content filter
B. Access control list
C. Network access control
D. Data loss prevention

Answer: B

NEW QUESTION 266
- (Exam Topic 2)
Which of the following is the BEST security practice to prevent ActiveX controls from running malicious code on a user's web application?

A. Configuring a firewall to block traffic on ports that use ActiveX controls
B. Adjusting the web-browser settings to block ActiveX controls
C. Installing network-based IPS to block malicious ActiveX code
D. Deploying HIPS to block malicious ActiveX code

Answer: B

NEW QUESTION 270
- (Exam Topic 2)
Malware is suspected on a server in the environment.
The analyst is provided with the output of commands from servers in the environment and needs to review all output files in order to determine which process running on one of the servers may be malware.
INSTRUCTIONS
Servers 1, 2, and 4 are clickable. Select the Server and the process that host the malware.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Server 4 192.168.50.6 Windows, svchost.exe

NEW QUESTION 272
- (Exam Topic 2)
To prioritize the morning's work, an analyst is reviewing security alerts that have not yet been investigated. Which of the following assets should be investigated FIRST?

A. The workstation of a developer who is installing software on a web server
B. A new test web server that is in the process of initial installation
C. The laptop of the vice president that is on the corporate LAN
D. An accounting supervisor's laptop that is connected to the VPN

Answer: C

NEW QUESTION 274
- (Exam Topic 2)
A security analyst is generating a list of recommendations for the company's insecure API. Which of the following is the BEST parameter mitigation rec

A. Implement parameterized queries.
B. Use effective authentication and authorization methods.
C. Validate all incoming data.
D. Use TLs for all data exchanges.

Answer: D

NEW QUESTION 277
- (Exam Topic 2)
An information security analyst discovered a virtual machine server was compromised by an attacker. Which of the following should be the FIRST step to confirm

and respond to the incident?

A. Pause the virtual machine.
B. Shut down the virtual machine.
C. Take a snapshot of the virtual machine.
D. Remove the NIC from the virtual machine.

Answer: A

NEW QUESTION 282
- (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 283
- (Exam Topic 2)
A cybersecurity analyst is establishing a threat hunting and intelligence group at a growing organization. Which of the following is a collaborative resource that would MOST likely be used for this purpose?

A. Scrum
B. loC feeds
C. ISAC
D. VSS scores

Answer: C

NEW QUESTION 285
- (Exam Topic 2)
A security analyst needs to perform a search for connections with a suspicious IP on the network traffic. The company collects full packet captures at the Internet gateway and retains them for one week. Which of the following will enable the analyst to obtain the BEST results?

A. tcpdump –n –r internet.pcap host <suspicious ip>
B. strings internet.pcap | grep <suspicious ip>
C. grep –a <suspicious ip> internet.pcap
D. npcapd internet.pcap | grep <suspicious ip>

Answer: A

NEW QUESTION 289
- (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 290
- (Exam Topic 2)
A small marketing firm uses many SaaS applications that hold sensitive information The firm has discovered terminated employees are retaining access to systems for many weeks after their end date. Which of the following would BEST resolve the issue of lingering access?

A. Configure federated authentication with SSO on cloud provider systems.
B. Perform weekly manual reviews on system access to uncover any issues.
C. Implement MFA on cloud-based systems.
D. Set up a privileged access management tool that can fully manage privileged account access.

Answer: D

NEW QUESTION 293
- (Exam Topic 2)
During the forensic analysis of a compromised machine, a security analyst discovers some binaries that are exhibiting abnormal behaviors. After extracting the strings, the analyst finds unexpected content Which of the following is the NEXT step the analyst should take?

A. Only allow whitelisted binaries to execute.
B. Run an antivirus against the binaries to check for malware.
C. Use file integrity monitoring to validate the digital signature.
D. Validate the binaries' hashes from a trusted source.

Answer: B

NEW QUESTION 297
- (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 299
- (Exam Topic 2)
A threat intelligence analyst has received multiple reports that are suspected to be about the same advanced persistent threat. To which of the following steps in the intelligence cycle would this map?

A. Dissemination
B. Analysis
C. Feedback
D. Requirements
E. Collection

Answer: E

NEW QUESTION 304
- (Exam Topic 2)
While investigating an incident in a company's SIEM console, a security analyst found hundreds of failed SSH login attempts, which all occurred in rapid succession. The failed attempts were followed by a successful login on the root user Company policy allows systems administrators to manage their systems only from the company's internal network using their assigned corporate logins. Which of the following are the BEST actions the analyst can take to stop any further compromise? (Select TWO).

A. Configure /etc/sshd_config to deny root logins and restart the SSHD service.
B. Add a rule on the network IPS to block SSH user sessions
C. Configure /etc/passwd to deny root logins and restart the SSHD service.
D. Reset the passwords for all accounts on the affected system.
E. Add a rule on the perimeter firewall to block the source IP address.
F. Add a rule on the affected system to block access to port TCP/22.

Answer: CE

NEW QUESTION 305
- (Exam Topic 2)
Which of the following secure coding techniques can be used to prevent cross-site request forgery attacks?

A. Input validation
B. Output encoding
C. Parameterized queries

D. Tokenization

Answer: D

NEW QUESTION 306
- (Exam Topic 2)
A large insurance company wants to outsource its claim-handling operations to an overseas third-party organization Which of the following would BEST help to reduce the chance of highly sensitive data leaking?

A. Configure a VPN between the third party organization and the internal company network
B. Set up a VDI that the third party must use to interact with company systems.
C. Use MFA to protect confidential company information from being leaked.
D. Implement NAC to ensure connecting systems have malware protection
E. Create jump boxes that are used by the third-party organization so it does not connect directly.

Answer: D

NEW QUESTION 309
- (Exam Topic 2)
A security analyst is investigating an incident that appears to have started with SOL injection against a publicly available web application. Which of the following is the FIRST step the analyst should take to prevent future attacks?

A. Modify the IDS rules to have a signature for SQL injection.
B. Take the server offline to prevent continued SQL injection attacks.
C. Create a WAF rule In block mode for SQL injection
D. Ask the developers to implement parameterized SQL queries.

Answer: A

NEW QUESTION 313
- (Exam Topic 2)
A security analyst is reviewing the following log entries to identify anomalous activity:

Which of the following attack types is occurring?

A. Directory traversal
B. SQL injection
C. Buffer overflow
D. Cross-site scripting

Answer: A

NEW QUESTION 318
- (Exam Topic 2)
The Cruel Executive Officer (CEO) of a large insurance company has reported phishing emails that contain malicious links are targeting the entire organza lion Which of the following actions would work BEST to prevent against this type of attack?

A. Turn on full behavioral analysis to avert an infection
B. Implement an EDR mail module that will rewrite and analyze email links.
C. Reconfigure the EDR solution to perform real-time scanning of all files
D. Ensure EDR signatures are updated every day to avert infection.
E. Modify the EDR solution to use heuristic analysis techniques for malware.

Answer: B

Explanation:
If you’re concerned about spear phishing and other advanced threats that may impact your organization, a next-gen EDR endpoint protection platform offers a lot of advantages over traditional antivirus.

NEW QUESTION 322
- (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 325
- (Exam Topic 2)
A security analyst receives an alert to expect increased and highly advanced cyberattacks originating from a foreign country that recently had sanctions implemented. Which of the following describes the type of threat actors that should concern the security analyst?

A. Hacktivist
B. Organized crime
C. Insider threat
D. Nation-state

Answer: D

NEW QUESTION 330
- (Exam Topic 2)
An organization is upgrading its network and all of its workstations. The project will occur in phases, with infrastructure upgrades each month and workstation installs every other week. The schedule should accommodate the enterprise-wide changes, while minimizing the impact to the network. Which of the following schedules BEST addresses these requirements?

A. Monthly topology scans, biweekly host discovery scans, weekly vulnerability scans
B. Monthly vulnerability scans, biweekly topology scans, daily host discovery scans
C. Monthly host discovery scans; biweekly vulnerability scans, monthly topology scans
D. Monthly topology scans, biweekly host discovery scans, monthly vulnerability scans

Answer: D

NEW QUESTION 332
- (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 336
- (Exam Topic 2)
During an investigation, an analyst discovers the following rule in an executive's email client: IF * TO <executive@anycompany.com> THEN mailto: <someaddress@domain.com> SELECT FROM 'sent' THEN DELETE FROM <executive@anycompany.com>
The executive is not aware of this rule. Which of the following should the analyst do FIRST to evaluate the potential impact of this security incident?

A. Check the server logs to evaluate which emails were sent to <someaddress@domain.com>
B. Use the SIEM to correlate logging events from the email server and the domain server
C. Remove the rule from the email client and change the password
D. Recommend that management implement SPF and DKIM

Answer: A

NEW QUESTION 337
- (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 340
- (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 341
- (Exam Topic 2)
A security analyst is researching an incident and uncovers several details that may link to other incidents. The security analyst wants to determine if other incidents are related to the current incident Which of the followinq threat research methodoloqies would be MOST appropriate for the analyst to use?

A. Reputation data
B. CVSS score
C. Risk assessment
D. Behavioral analysis

Answer: D

NEW QUESTION 346
- (Exam Topic 2)
An organization that uses SPF has been notified emails sent via its authorized third-party partner are getting rejected A security analyst reviews the DNS entry and sees the following:
v=spf1 ip4:180.10.6.5 ip4:180.10.6.10 include:robustmail.com –all
The organization's primary mail server IP is 180.10 6.6, and the secondary mail server IP is 180.10.6.5. The organization's third-party mail provider is "Robust Mail" with the domain name robustmail.com.
Which of the following is the MOST likely reason for the rejected emails?

A. The wrong domain name is in the SPF record.
B. The primary and secondary email server IP addresses are out of sequence.
C. SPF version 1 does not support third-party providers
D. An incorrect IP version is being used.

Answer: A

NEW QUESTION 348
- (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 353
- (Exam Topic 2)
A remote code execution vulnerability was discovered in the RDP. An organization currently uses RDP for remote access to a portion of its VDI environment. The analyst verified network-level
authentication is enabled
Which of the following is the BEST remediation for this vulnerability?

A. Verify the latest endpoint-protection signature is in place.
B. Verify the corresponding patch for the vulnerability is installed^
C. Verify the system logs do not contain indicator of compromise.
D. Verify the threat intelligence feed is updated with the latest solutions

Answer: A

NEW QUESTION 357
- (Exam Topic 2)
Employees of a large financial company are continuously being Infected by strands of malware that are not detected by EDR tools. When of the following Is the BEST security control to implement to reduce corporate risk while allowing employees to exchange files at client sites?

A. MFA on the workstations
B. Additional host firewall rules
C. VDI environment
D. Hard drive encryption
E. Network access control
F. Network segmentation

Answer: C

NEW QUESTION 362
- (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 363
- (Exam Topic 2)
A security analyst needs to identify possible threats to a complex system a client is developing. Which of the following methodologies would BEST address this task?

A. Open Source Security Information Management (OSSIM)
B. Software Assurance Maturity Model (SAMM)
C. Open Web Application Security Project (OWASP)
D. Spoofing, Tamperin
E. Repudiation, Information disclosur
F. Denial of service, Elevation of privileges (STRIDE)

Answer: C

NEW QUESTION 366
- (Exam Topic 2)
An organization supports a large number of remote users. Which of the following is the BEST option to protect the data on the remote users1 laptops?

A. Use whole disk encryption.
B. Require the use of VPNs.
C. Require employees to sign an NDA.
D. implement a DLP solution.

Answer: D

NEW QUESTION 369
- (Exam Topic 2)
During an incident investigation, a security analyst acquired a malicious file that was used as a backdoor but was not detected by the antivirus application. After performing a reverse-engineering procedure, the analyst found that part of the code was obfuscated to avoid signature detection. Which of the following types of instructions should the analyst use to understand how the malware was obfuscated and to help deobfuscate it?

A. MOV
B. ADD
C. XOR
D. SUB
E. MOVL

Answer: C

NEW QUESTION 372
- (Exam Topic 2)
An analyst wants to identify hosts that are connecting to the external FTP servers and what, if any, passwords are being used. Which of the following commands should the analyst use?

A. tcpdump –X dst port 21
B. ftp ftp.server –p 21
C. nmap –o ftp.server –p 21
D. telnet ftp.server 21

Answer: A

NEW QUESTION 375
- (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 377
- (Exam Topic 2)
An organization wants to mitigate against risks associated with network reconnaissance. ICMP is already blocked at the firewall; however, a penetration testing team has been able to perform reconnaissance against the organization’s network and identify active hosts. An analyst sees the following output from a packet capture:

Which of the following phrases from the output provides information on how the testing team is successfully getting around the ICMP firewall rule?

A. flags=RA indicates the testing team is using a Christmas tree attack
B. ttl=64 indicates the testing team is setting the time to live below the firewall’s threshold

C. 0 data bytes indicates the testing team is crafting empty ICMP packets
D. NO FLAGS are set indicates the testing team is using hping

Answer: D

NEW QUESTION 381
- (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 382
- (Exam Topic 2)
A general contractor has a list of contract documents containing critical business data that are stored at a public cloud provider. The organization's security analyst recently reviewed some of the storage containers and discovered most of the containers are not encrypted. Which of the following configurations will provide the MOST security to resolve the vulnerability?

A. Upgrading TLS 1.2 connections to TLS 1.3
B. Implementing AES-256 encryption on the containers
C. Enabling SHA-256 hashing on the containers
D. Implementing the Triple Data Encryption Algorithm at the file level

Answer: C

NEW QUESTION 383
- (Exam Topic 2)
A malicious artifact was collected during an incident response procedure. A security analyst is unable to run it in a sandbox to understand its features and method of operation. Which of the following procedures is the BEST approach to perform a further analysis of the malware's capabilities?

A. Reverse engineering
B. Dynamic analysis
C. Strings extraction
D. Static analysis

Answer: D

NEW QUESTION 384
- (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 386
- (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 391
- (Exam Topic 2)
A company creates digitally signed packages for its devices. Which of the following BEST describes the method by which the security packages are delivered to the company's customers?

A. Trusted firmware updates
B. SELinux
C. eFuse
D. Anti-tamper mechanism

Answer: A

NEW QUESTION 393
- (Exam Topic 2)
An organization has been seeing increased levels of malicious traffic. A security analyst wants to take a more proactive approach to identify the threats that are acting against the organization's network. Which of the following approaches should the security analyst recommend?

A. Use the MITRE ATT&CK framework to develop threat models.
B. Conduct internal threat research and establish indicators of compromise.
C. Review the perimeter firewall rules to ensure rule-set accuracy.
D. Use SCAP scans to monitor for configuration changes on the network.

Answer: D

NEW QUESTION 398
- (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 400
- (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 403
- (Exam Topic 2)
A newly appointed Chief Information Security Officer (CISO) has completed a risk assessment review of the organization and wants to reduce the numerous risks that were identified. Which of the following will provide a trend of risk mitigation?

A. Risk response
B. Risk analysis
C. Planning
D. Oversight
E. Continuous monitoring

Answer: A

NEW QUESTION 404
- (Exam Topic 2)
A company's Chief Information Security Officer (CISO) is concerned about the integrity of some highly confidential files. Any changes to these files must be tied back to a specific authorized user's activity session. Which of the following is the BEST technique to address the CISO's concerns?

A. Configure DLP to reject all changes to the files without pre-authorizatio
B. Monitor the files for unauthorized changes.
C. Regularly use SHA-256 to hash the directory containing the sensitive informatio
D. Monitor the files for unauthorized changes.
E. Place a legal hold on the file
F. Require authorized users to abide by a strict time context access policy.Monitor the files for unauthorized changes.
G. Use Wireshark to scan all traffic to and from the director
H. Monitor the files for unauthorized changes.

Answer: AC

NEW QUESTION 405
- (Exam Topic 2)
A security analyst recently used Arachni to perform a vulnerability assessment of a newly developed web application. The analyst is concerned about the following output:

Which of the following is the MOST likely reason for this vulnerability?

A. The developer set input validation protection on the specific field of search.aspx.
B. The developer did not set proper cross-site scripting protections in the header.
C. The developer did not implement default protections in the web application build.

D. The developer did not set proper cross-site request forgery protections.

Answer: A

NEW QUESTION 409
- (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 412
- (Exam Topic 3)
A security analyst needs to determine the best method for securing access to a top-secret datacenter Along
with an access card and PIN code, which of the following additional authentication methods would be BEST to enhance the datacenter's security?

A. Physical key
B. Retinal scan
C. Passphrase
D. Fingerprint

Answer: D

NEW QUESTION 414
- (Exam Topic 3)
A business recently acquired a software company. The software company's security posture is unknown. However, based on an assessment, there are limited security controls. No significant security monitoring exists. Which of the following is the NEXT step that should be completed to obtain information about the software company's security posture?

A. Develop an asset inventory to determine the systems within the software company
B. Review relevant network drawings, diagrams and documentation
C. Perform penetration tests against the software company's Internal and external networks
D. Baseline the software company's network to determine the ports and protocols in use.

Answer: A

NEW QUESTION 417
- (Exam Topic 3)
A security officer needs to find the most cost-effective solution to the current data privacy 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: B

NEW QUESTION 418
- (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 420
- (Exam Topic 3)
A Chief Executive Officer (CEO) is concerned about the company’s intellectual property being leaked to competitors. The security team performed an extensive review but did not find any indication of an outside breach. The data sets are currently encrypted using the Triple Data Encryption Algorithm. Which of the following courses of action is appropriate?

A. Limit all access to the sensitive data based on geographic access requirements with strict role-based access controls.
B. Enable data masking and reencrypt the data sets using AES-256.
C. Ensure the data is correctly classified and labeled, and that DLP rules are appropriate to prevent disclosure.
D. Use data tokenization on sensitive fields, reencrypt the data sets using AES-256, and then create an MD5 hash.

Answer: C

NEW QUESTION 421
- (Exam Topic 3)
A help desk technician inadvertently sent the credentials of the company's CRM n clear text to an employee's personal email account. The technician then reset the employee's account using the appropriate process and the employee's corporate email, and notified the security team of the incident According to the incident response procedure, which of the following should the security team do NEXT?

A. Contact the CRM vendor.
B. Prepare an incident summary report.
C. Perform postmortem data correlation.
D. Update the incident response plan.

Answer: C

NEW QUESTION 422
- (Exam Topic 3)
An internally developed file-monitoring system identified the following except as causing a program to crash often:

Which of the following should a security analyst recommend to fix the issue?

A. Open the access.log file ri read/write mode.
B. Replace the strcpv function.
C. Perform input samtizaton
D. Increase the size of the file data buffer

Answer: A

NEW QUESTION 427
- (Exam Topic 3)
A company is experiencing a malware attack within its network. A security engineer notices many of the impacted assets are connecting outbound to a number of remote destinations and exfiltrating data. The security engineer also see that deployed, up-to-date antivirus signatures are ineffective. Which of the following is the BEST approach to prevent any impact to the company from similar attacks in the future?

A. IDS signatures
B. Data loss prevention
C. Port security
D. Sinkholing

Answer: B

Explanation:
"Preventing data exfiltration is possible with security solutions that ensure data loss and leakage prevention. For example, firewalls can block unauthorized access to resources and systems storing sensitive information. On the other hand, a security information and event management system (SIEM) can secure data in motion, in use, and at rest, secure endpoints, and identify suspicious data transfers" https://www.fortinet.com/resources/cyberglossary/data-exfiltration

NEW QUESTION 428
- (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 432
- (Exam Topic 3)
Which of the following is a difference between SOAR and SCAP?

A. SOAR can be executed taster and with fewer false positives than SCAP because of advanced heunstics
B. SOAR has a wider breadth of capability using orchestration and automation, while SCAP is more limited in scope
C. SOAR is less expensive because process and vulnerability remediation is more automated than what SCAP does
D. SOAR eliminates the need for people to perform remediation, while SCAP relies heavily on security analysts

Answer: D

NEW QUESTION 436
- (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 440
- (Exam Topic 3)
Which of the following is MOST dangerous to the client environment during a vulnerability assessment penetration test?

A. There is a longer period of time to assess the environment.
B. The testing is outside the contractual scope
C. There is a shorter period of time to assess the environment
D. No status reports are included with the assessment.

Answer: B

NEW QUESTION 445
- (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 447
- (Exam Topic 3)
A security analyst is looking at the headers of a few emails that appear to be targeting all users at an organization:

Which of the following technologies would MOST likely be used to prevent this phishing attempt?

A. DNSSEC
B. DMARC
C. STP
D. S/IMAP

Answer: B

NEW QUESTION 449
- (Exam Topic 3)
A threat hurting team received a new loC from an ISAC that follows a threat actor's profile and activities. Which of the following should be updated NEXT?

A. The whitelist
B. The DNS
C. The blocklist
D. The IDS signature

Answer: D

NEW QUESTION 453
- (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 458
- (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 462
- (Exam Topic 3)
A security analyst is handling an incident in which ransomware has encrypted the disks of several company workstations. Which of the following would work BEST to prevent this type of Incident in the future?

A. Implement a UTM instead of a stateful firewall and enable gateway antivirus.
B. Back up the workstations to facilitate recovery and create a gold Image.
C. Establish a ransomware awareness program and implement secure and verifiable backups.
D. Virtualize all the endpoints with dairy snapshots of the virtual machines.

Answer: A

NEW QUESTION 467
- (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 469
- (Exam Topic 3)
An organization prohibits users from logging in to the administrator account. If a user requires elevated permissions. the user's account should be part of an administrator group, and the user should escalate permission only as needed and on a temporary basis. The organization has the following reporting priorities when reviewing system activity:
• Successful administrator login reporting priority - high
• Failed administrator login reporting priority - medium
• Failed temporary elevated permissions - low

• Successful temporary elevated permissions - non-reportable
A security analyst is reviewing server syslogs and sees the following: Which of the following events is the HIGHEST reporting priority?

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

Answer: A

NEW QUESTION 473
- (Exam Topic 3)
During a review of recent network traffic, an analyst realizes the team has seen this same traffic multiple times in the past three weeks, and it resulted in confirmed malware activity The analyst also notes there is no other alert in place for this traffic After resolving the security incident, which of the following would be the BEST action for the analyst to take to increase the chance of detecting this traffic in the future?

A. Share details of the security incident with the organization's human resources management team
B. Note the security incident so other analysts are aware the traffic is malicious
C. Communicate the security incident to the threat team for further review and analysis
D. Report the security incident to a manager for inclusion in the daily report

Answer: C

NEW QUESTION 475
- (Exam Topic 3)
An organization is focused on restructuring its data governance programs and an analyst has been Tasked with surveying sensitive data within the organization. Which of the following is the MOST accurate method for the security analyst to complete this assignment?

A. Perform an enterprise-wide discovery scan.
B. Consult with an internal data custodian.
C. Review enterprise-wide asset Inventory.
D. Create a survey and distribute it to data owners.

Answer: D

NEW QUESTION 480
- (Exam Topic 3)
A company's legal and accounting teams have decided it would be more cost-effective to offload the risks of data storage to a third party. The IT management team has decided to implement a cloud model and has asked the security team for recommendations. Which of the following will allow all data to be kept on the third-party network?

A. VDI
B. SaaS
C. CASB
D. FaaS

Answer: B

NEW QUESTION 485
- (Exam Topic 3)
A developer downloaded and attempted to install a file transfer application in which the installation package is bundled with acKvare. The next-generation antivirus software prevented the file from executing, but it did not remove the file from the device. Over the next few days, more developers tried to download and execute the offending file. Which of the following changes should be made to the security tools to BEST remedy the issue?

A. Blacklist the hash in the next-generation antivirus system.
B. Manually delete the file from each of the workstations.
C. Remove administrative rights from all developer workstations.
D. Block the download of the fie via the web proxy

Answer: A

NEW QUESTION 490
- (Exam Topic 3)
A security is reviewing a vulnerability scan report and notes the following finding:

As part of the detection and analysis procedures, which of the following should the analyst do NEXT?

A. Patch or reimage the device to complete the recovery
B. Restart the antiviruses running processes
C. Isolate the host from the network to prevent exposure
D. Confirm the workstation's signatures against the most current signatures.

Answer: D

NEW QUESTION 491
- (Exam Topic 3)
An organization has specific technical nsk mitigation configurations that must be implemented before a new server can be approved for production Several critical servers were recently deployed with the antivirus missing unnecessary ports disabled and insufficient password complexity Which of the following should the analyst recommend to prevent a recurrence of this risk exposure?

A. Perform password-cracking attempts on all devices going into production
B. Perform an Nmap scan on all devices before they are released to production
C. Perform antivirus scans on all devices before they are approved for production
D. Perform automated security controls testing of expected configurations pnor to production

Answer: D

NEW QUESTION 493
- (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 496
- (Exam Topic 3)
A development team has asked users to conduct testing to ensure an application meets the needs of the business. Which of the fallowing types of testing docs This describe?

A. Acceptance testing
B. Stress testing
C. Regression testing
D. Penetration testing

Answer: A

NEW QUESTION 498
- (Exam Topic 3)
In response to an audit finding, a company's Chief information Officer (CIO) instructed the security department to Increase the security posture of the vulnerability management program. Currency, the company's vulnerability management program has the following attributes:
Which of the following would BEST Increase the security posture of the vulnerably management program?

A. Expand the ports Being scanned lo Include al ports increase the scan interval to a number the business win accept without causing service interruptio
B. Enable authentication and perform credentialed scans
C. Expand the ports being scanned to Include all port
D. Keep the scan interval at its current level Enable authentication and perform credentialed scans.
E. Expand the ports being scanned to Include at ports increase the scan interval to a number the business will accept without causing service Interruptio
F. Continue unauthenticated scans.
G. Continue scanning the well-known ports increase the scan interval to a number the business will accept without causing service Interruptio
H. Enable authentication and perform credentialed scans.

Answer: A

NEW QUESTION 501
- (Exam Topic 3)
In SIEM software, a security analysis selected some changes to hash signatures from monitored files during the night followed by SMB brute-force attacks against the file servers Based on this behavior, which of the following actions should be taken FIRST to prevent a more serious compromise?

A. Fully segregate the affected servers physically in a network segment, apart from the production network.
B. Collect the network traffic during the day to understand if the same activity is also occurring during business hours
C. Check the hash signatures, comparing them with malware databases to verify if the files are infected.
D. Collect all the files that have changed and compare them with the previous baseline

Answer: A

NEW QUESTION 506
- (Exam Topic 3)
A SIEM analyst receives an alert containing the following URL:

Which of the following BEST describes the attack?

A. Password spraying
B. Buffer overflow
C. insecure object access
D. Directory traversal

Answer: D

NEW QUESTION 508
- (Exam Topic 3)
A security analyst is deploying a new application in the environment. The application needs to be integrated with several existing applications that contain SPI Pnor to the deployment, the analyst should conduct:

A. a tabletop exercise
B. a business impact analysis
C. a PCI assessment
D. an application stress test.

Answer: B

NEW QUESTION 512
- (Exam Topic 3)
A company wants to configure the environment to allow passive network monitonng. To avoid disrupting the sensitive network, which of the following must be supported by the scanner's NIC to assist with the company's request?

A. Port bridging
B. Tunnel all mode
C. Full-duplex mode
D. Port mirroring
E. Promiscuous mode

Answer: D

NEW QUESTION 516
- (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 520
- (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 521
- (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 526
- (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 530
- (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 531
- (Exam Topic 3)
A software developer is correcting the error-handling capabilities of an application following the initial coding of the fix. Which of the following would the software developer MOST likely performed to validate the code poor to pushing it to production?

A. Web-application vulnerability scan
B. Static analysis
C. Packet inspection
D. Penetration test

Answer: B

NEW QUESTION 536
- (Exam Topic 3)
A security analyst discovers suspicious host activity while performing monitoring activities. The analyst pulls a packet capture for the activity and sees the following:

Which of the following describes what has occurred?

A. The host attempted to download an application from utoftor.com.
B. The host downloaded an application from utoftor.com.

C. The host attempted to make a secure connection to utoftor.com.
D. The host rejected the connection from utoftor.co

Answer: D

NEW QUESTION 539
- (Exam Topic 3)
An organization recently discovered that spreadsheet files containing sensitive financial data were improperly stored on a web server. The management team wants to find out if any of these files were downloaded by pubic users accessing the server. The results should be written to a text file and should induce the date. time, and IP address associated with any spreadsheet downloads. The web server's log file Is named webserver log, and the report We name should be accessreport.txt. Following is a sample of the web servefs.log file:
2017-0-12 21:01:12 GET /index.htlm - @4..102.33.7 - return=200 1622
Which of the following commands should be run if an analyst only wants to include entries in which spreadsheet was successfully downloaded?

A. more webserver.log | grep * xIs > accessreport.txt
B. more webserver.log > grep ''xIs > egrep -E 'success' > accessreport.txt
C. more webserver.log | grep ' -E ''return=200 | accessreport.txt
D. more webserver.log | grep -A *.xIs < accessreport.txt

Answer: C

NEW QUESTION 540
- (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 544
- (Exam Topic 3)
A security analyst found an old version of OpenSSH running on a DMZ server and determined the following piece of code could have led to a command execution through an integer overflow;

Which of the following controls must be in place to prevent this vulnerability?

A. Convert all integer numbers in strings to handle the memory buffer correctly.
B. Implement float numbers instead of integers to prevent integer overflows.
C. Use built-in functions from libraries to check and handle long numbers properly.
D. Sanitize user inputs, avoiding small numbers that cannot be handled in the memory.

Answer: C

NEW QUESTION 547
- (Exam Topic 3)
A security analyst is researching ways to improve the security of a company's email system to mitigate emails that are impersonating company executives. Which of the following would be BEST for the analyst to configure to achieve this objective?

A. A TXT record on the name server for SPF
B. DNSSEC keys to secure replication
C. Domain Keys identified Man
D. A sandbox to check incoming mad

Answer: B

NEW QUESTION 550
- (Exam Topic 3)
A small business does not have enough staff in the accounting department to segregate duties. The controller writes the checks for the business and reconciles them against the ledger. To ensure there is no fraud occurring, the business conducts quarterly reviews in which a different officer in the business compares all the cleared checks against the ledger. Which of the following BEST describes this type of control?

A. Deterrent
B. Preventive
C. Compensating
D. Detective

Answer: C

Explanation:
A compensating control, also called an alternative control, is a mechanism that is put in place to satisfy the requirement for a security measure that is deemed too difficult or impractical to implement at the present time.

NEW QUESTION 552
- (Exam Topic 3)
A forensics investigator is analyzing a compromised workstation. The investigator has cloned the hard drive and needs to verify that a bit-level image copy of a hard drive is an exact clone of the original hard drive that was collected as evidence. Which of the following should the investigator do?

A. Insert the hard drive on a test computer and boot the computer.
B. Record the serial numbers of both hard drives.
C. Compare the file-directory "sting of both hard drives.
D. Run a hash against the source and the destination.

Answer: D

NEW QUESTION 553
- (Exam Topic 3)
Which of the following is MOST important when developing a threat hunting program?

A. Understanding penetration testing techniques
B. Understanding how to build correlation rules within a SIEM
C. Understanding security software technologies
D. Understanding assets and categories of assets

Answer: C

Explanation:
https://www.stickmancyber.com/cybersecurity-blog/7-threat-hunting-misconceptions https://www.simplilearn.com/skills-to-become-threat-hunter-article

NEW QUESTION 555
- (Exam Topic 3)
An analyst determines a security incident has occurred Which of the following is the most appropnate NEXT step in an incident response plan?

A. Consult the malware analysis process
B. Consult the disaster recovery plan
C. Consult the data classification process
D. Consult the communications plan

Answer: D

NEW QUESTION 560
- (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 564
- (Exam Topic 3)
An IT security analyst has received an email alert regarding vulnerability within the new fleet of vehicles the company recently purchased. Which of the following attack vectors is the vulnerability MOST likely targeting?

A. SCADA
B. CAN bus
C. Modbus
D. loT

Answer: D

NEW QUESTION 568
- (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 570
- (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 572
- (Exam Topic 3)
An organization has the following risk mitigation policy:
Risks with a probability of 95% or greater will be addressed before all others regardless of the impact. All other prioritization will be based on risk value.
The organization has identified the following risks:

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

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

Answer: D

NEW QUESTION 573
- (Exam Topic 3)
Which of the following incident response components can identify who is the llaison between multiple lines of business and the pubic?

A. Red-team analysis
B. Escalation process and procedures
C. Triage and analysis

D. Communications plan

Answer: C

NEW QUESTION 577
- (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 582
- (Exam Topic 3)
A security analyst needs to provide the development learn with secure connectivity from the corporate network to a three-tier cloud environment. The developers require access to servers in all three tiers in order to perform various configuration tasks. Which of the following technologies should the analyst implement to provide secure transport?

A. CASB
B. VPC
C. Federation
D. VPN

Answer: D

Explanation:
What is the difference between VPN and VPC?
Just as a virtual private network (VPN) provides secure data transfer over the public Internet, a VPC provides secure data transfer between a private enterprise and a public cloud provider.

NEW QUESTION 586
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

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