CompTIA

Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

NEW QUESTION 1
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: C

Explanation:
A PCI assessment should be conducted prior to the deployment of a new application that contains SPI (Sensitive Personal Information). A PCI assessment is an evaluation of how well an organization complies with the Payment Card Industry Data Security Standard (PCI DSS), which is a set of requirements for protecting cardholder data. PCI DSS applies to any organization that stores, processes, or transmits cardholder data, such as credit card numbers, expiration dates, or security codes4. A PCI assessment can help identify and remediate any gaps or weaknesses in the security controls of an application that handles cardholder data.

NEW QUESTION 2
An organization wants to collect loCs from multiple geographic regions so it can sell the information to its customers. Which of the following should the organization deploy to accomplish this task?

A. A honeypot
B. A bastion host
C. A proxy server
D. A Jumpbox

Answer: A

Explanation:
A honeypot is a decoy system that is designed to attract and trap attackers, by mimicking a real system or network, but containing fake or harmless data. A honeypot can be used to collect IoCs from multiple geographic regions, by deploying it in different locations or networks, and monitoring the activities or attacks that target it. A honeypot can also provide valuable threat intelligence data that can be sold to customers.

NEW QUESTION 3
A company is aiming to test a new incident response plan. The management team has made it clear that the initial test should have no impact on the environment. The company has limited
resources to support testing. Which of the following exercises would be the best approach?

A. Tabletop scenarios
B. Capture the flag
C. Red team v
D. blue team
E. Unknown-environment penetration test

Answer: A

Explanation:
A tabletop scenario is an informal, discussion-based session in which a team discusses their roles and responses during an emergency, walking through one or more example scenarios. A tabletop scenario is the best approach for a company that wants to test a new incident response plan without impacting the environment or using many resources. A tabletop scenario can help the company identify strengths and weaknesses in their plan, clarify roles and responsibilities, and improve communication and coordination among team members. The other options are more intensive and disruptive exercises that involve simulating a real incident or attack. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 16; https://www.linkedin.com/pulse/tabletop-exercises-explained-matt-lemon-phd

NEW QUESTION 4
A company's threat team has been reviewing recent security incidents and looking for a common theme. The team discovered the incidents were caused by incorrect configurations on the impacted systems. The issues were reported to support teams, but no action was taken. Which of the following is the next step the company should take to ensure any future issues are remediated?

A. Require support teams to develop a corrective control that ensures security failures are addressed once they are identified.
B. Require support teams to develop a preventive control that ensures new systems are built with the required security configurations.
C. Require support teams to develop a detective control that ensures they continuously assess systems for configuration errors.
D. Require support teams to develop a managerial control that ensures systems have a documented configuration baseline.

Answer: A

Explanation:
Requiring support teams to develop a corrective control that ensures security failures are addressed once they are identified is the best step to prevent future issues from being remediated. Corrective controls are actions or mechanisms that are implemented after a security incident or failure has occurred to fix or restore the normal state of the system or network. Corrective controls can include patching, updating, repairing, restoring, or reconfiguring systems or components that were affected by the incident or failure .

NEW QUESTION 5
A manufacturing company has joined the information sharing and analysis center for its sector. As a benefit, the company will receive structured loC data contributed by other members. Which of the following best describes the utility of this data?

A. Other members will have visibility into Instances o' positive loC identification within me manufacturing company's corporate network.
B. The manufacturing company will have access to relevant malware samples from all other manufacturing sector members.
C. Other members will automatically adjust their security postures lo defend the manufacturing company's processes.
D. The manufacturing company can automatically generate security configurations for all of Its Infrastructure.

Answer: B

Explanation:
This best describes the utility of the structured loC data contributed by other members of the information sharing and analysis center (ISAC) for its sector. loC stands for indicator of compromise, which is a piece of information that suggests a potential intrusion or attack, such as an IP address, a file hash, a domain name, or a malware signature. By sharing loC data, the ISAC members can benefit from each other's threat intelligence and improve their security defenses.

NEW QUESTION 6
A security operations manager wants some recommendations for improving security monitoring. The security team currently uses past events to create an IOC list for monitoring.
Which of the following is the best suggestion for improving monitoring capabilities?

A. Update the IPS and IDS with the latest rule sets from the provider.
B. Create an automated script to update the IPS and IDS rule sets.
C. Use an automated subscription to select threat feeds for IDS.
D. Implement an automated malware solution on the IPS.

Answer: C

Explanation:
Threat feeds are sources of information that provide timely and relevant data about current or emerging cyber threats, such as indicators of compromise (IOCs), tactics, techniques, and procedures (TTPs), or threat actors. An IDS, or intrusion detection system, is a tool that monitors network traffic and detects malicious or anomalous activities based on predefined or custom rules. Using an automated subscription to select threat feeds for IDS can help to improve security monitoring capabilities by providing the security team with up-to-date and actionable intelligence that can enhance the detection and response to cyberattacks

NEW QUESTION 7
An analyst reviews the most recent vulnerability management report and notices a firewall with 99.98% required uptime is reporting different firmware versions on scans than were reported in previous scans. The vendor released new firewall firmware a few months ago. Which of the following will the analyst most likely do next given the requirements?

A. Request to route traffic through a secondary firewall
B. Check for change tickets.
C. Perform a credentialed scan
D. Request an exception to the uptime policy.

Answer: B

Explanation:
The analyst should check for change tickets as the next step, given that the firewall is reporting different firmware versions on scans than were reported in previous scans. Change tickets are records of any authorized changes made to a system or a network, such as updating firmware, installing patches, or modifying configurations. Checking for change tickets can help verify if the firmware change was intentional and approved, or if it was unauthorized or malicious.

NEW QUESTION 8
A cybersecunty analyst needs to harden a server that is currently being used as a web server The server needs to be accessible when entenng www company com into the browser Additionally web pages require frequent updates which are performed by a remote contractor Given the following output:

```
Starting Nmap 7.12 ( https://nmap.org ) at 2020-08-25 11:44
Nmap scan report for finance-server (72.56.70.94)
Host is up (0.000060s latency).
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
23/tcp    open     telnet
53/tcp    open     domain
80/tcp    open     http
443/tcp   open     https
```

Which of the following should the cybersecunty analyst recommend to harden the server? (Select TWO).

A. Uninstall the DNS service
B. Perform a vulnerability scan
C. Change the server's IP to a private IP address
D. Disable the Telnet service
E. Block port 80 with the host-based firewall
F. Change the SSH port to a non-standard port

Answer: DF

Explanation:
Disabling the Telnet service would harden the server by removing an insecure protocol that transmits data in cleartext and could allow unauthorized access to the server. Changing the SSH port to a non-standard port would harden the server by reducing the exposure to brute-force attacks or port scans that target the default SSH port (22). Uninstalling the DNS service, performing a vulnerability scan, changing the server's IP to a private IP address, or blocking port 80 with the host-based firewall would not harden the server or could affect its functionality as a web server. Reference:
https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

NEW QUESTION 9
An organization is concerned about the security posture of vendors with access to its facilities and systems. The organization wants to implement a vendor review process to ensure \hi> policies implemented by vendors are in line with its own. Which of the following will provide the highest assurance of compliance?

A. An in-house red-team report
B. A vendor self-assessment report
C. An independent third-party audit report
D. Internal and external scans from an approved third-party vulnerability vendor

Answer: C

Explanation:
An independent third-party audit report can provide the highest assurance of compliance with the organization's policies by vendors, as it involves an objective and unbiased evaluation of the vendor's security posture and practices by an external auditor who follows established standards and criteria. An independent third-party audit report can help verify if the vendor meets the organization's requirements and expectations, as well as identify any gaps or weaknesses that need to be addressed.

NEW QUESTION 10
An analyst is reviewing the following output as part of an incident:

```
ICMP ECHO REQUEST 192.168.1.10 -> 10.20.30.40 Length=10 ABCDEFGHIJ
ICMP ECHO REPLY 10.20.30.40 -> 192.168.1.10 Length=10 ABCDEFGHIJ
ICMP ECHO REQUEST 192.168.1.10 -> 10.20.30.40 Length=15 ABCDEFGHIJ
ICMP ECHO REPLY 10.20.30.40 -> 192.168.1.10 Length=15 ABCDEFGHIJ[]8fd
ICMP ECHO REQUEST 192.168.1.10 -> 10.20.30.40 Length=20 ABCDEFGHIJ1234567890
ICMP ECHO REPLY 10.20.30.40 -> 192.168.1.10 Length=20 ABCDEFGHIJ1234567890
```

Which of the Wowing is MOST likely happening?

A. The hosts are part of a reflective denial -of -service attack.
B. Information is leaking from the memory of host 10.20 30.40
C. Sensitive data is being exfilltrated by host 192.168.1.10.
D. Host 291.168.1.10 is performing firewall port knocking.

Answer: A

Explanation:
The hosts are most likely part of a reflective denial-of-service attack. A reflective denial-of-service attack is a technique that allows attackers to both magnify the amount of malicious traffic they can generate and obscure the sources of the attack traffic. This type of distributed denial-of-service (DDoS) attack overwhelms the target, causing disruption or outage of systems and services. A reflective denial-of-service attack works by spoofing the target's IP address and sending requests to vulnerable servers that will respond to the target. The servers act as reflectors that bounce back the responses to the target, amplifying the attack volume and hiding the attacker's identity1. The output shows that host 10.20.30.40 is sending requests with a spoofed source IP address of 192.168.1.10 to host 203.0.113.15 on port 123, which is used by the Network Time Protocol (NTP). NTP is a common protocol used for reflection/amplification attacks, as it can generate large responses to small requests2.

NEW QUESTION 10
Some hard disks need to be taken as evidence for further analysis during an incident response. Which of the following procedures must be completed FIRST for this type of evidence acquisition?

A. Extract the hard drives from the compromised machines and then plug them into a forensics machine to apply encryption over the stored data to protect it from nonauthorized access.
B. Build the chain-of-custody document, noting the media model, serial number, size, vendor, date, and time of acquisition.
C. Perform a disk sanitization using the command #dd if=/dev/zero of=/dev/sdc bs=1M over the media that will receive a copy of the collected data.
D. Execute the command #dd if-/dev/sda of=/dev/sdc bs=512 to clone the evidence data to external media to prevent any further change.

Answer: B

Explanation:
Building the chain-of-custody document is the procedure that must be completed first for this type of evidence acquisition. The chain-of-custody document is a record that tracks the handling and custody of digital evidence from the time it is collected until it is presented in court. The chain-of-custody document should include information such as the media model, serial number, size, vendor, date, and time of acquisition, as well as the names and signatures of the persons who handled, transferred, or examined the evidence. The chain-of-custody document helps to preserve the integrity and admissibility of the evidence by preventing tampering, alteration, or loss1.

NEW QUESTION 15
Which of the following should a database administrator for an analytics firm implement to best protect PII from an insider threat?

A. Data deidentification
B. Data encryption
C. Data auditing
D. Data minimization

Answer: C

Explanation:
Data auditing is the most essential and effective method to protect PII from an insider threat. Data auditing is the process of monitoring and recording the activities and events related to data access and usage. Data
auditing can help detect and prevent any suspicious or anomalous behavior by an insider threat who tries to
access or manipulate PII.
Data auditing can provide several benefits for data protection, such as:
>

It can provide accountability and transparency for data access and usage, which can deter potential insider threats from abusing their privileges or violating policies.

- It can provide evidence and traceability for data incidents, which can help investigate and respond to data breaches or leaks by insider threats.
- It can provide feedback and insights for data security improvement, which can help identify and address any gaps or weaknesses in data protection measures.

Data auditing can be done by using tools such as logs, alerts, reports, or dashboards. These tools can help security analysts track and analyze data activity and identify any patterns or anomalies that indicate a possible insider threat.

NEW QUESTION 16
While reviewing abnormal user activity, a security analyst notices a user has the following fileshare activities:

Server	Share	Action
Server001	Confidential	Deny
Server001	HumanResources	Deny
Server002	Temporary	Permit
Server002	Installs	Permit
Server003	Payroll	Deny
Server003	W9Docs	Deny

Which of the following should the analyst do first?

A. Initiate the security incident response process for unauthorized access.
B. Shut down the servers while the access is investigated.
C. Remove the user's access for all fileshares.
D. Lock the user account until the access can be explained.

Answer: A

Explanation:
The security incident response process is a set of procedures and guidelines that define how to identify, contain, analyze, and recover from security incidents that compromise the confidentiality, integrity, or availability of an organization’s assets or operations. Initiating the security incident response process for unauthorized access is the first and most appropriate action that the analyst should take, as it would allow the analyst to follow a structured and consistent approach to handle the situation and mitigate the impact of the incident1.

NEW QUESTION 18
A financial institution's business unit plans to deploy a new technology in a manner that violates existing information security standards. Which of the following actions should the Chief Information Security Officer (CISO) take to manage any type of violation?

A. Enforce the existing security standards and controls.
B. Perform a risk analysis and qualify the risk with legal.
C. Perform research and propose a better technology.
D. Enforce the standard permits.

Answer: B

Explanation:
The International Standards Organization, or ISO, develops standards for businesses around the world so that they may operate using a uniform set of best practices. These standards are not enforceable laws, but companies who choose to follow them stand to gain international credibility from their compliance; standards are set as guidance for best practices but are not enforceable laws

NEW QUESTION 19
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

Explanation:
The security team should perform postmortem data correlation next after receiving notification of the incident from the help desk technician. Postmortem data correlation is an activity that involves analyzing data from various sources (such as logs, alerts, reports, etc.) to identify root causes, impacts, indicators of compromise (IoCs), lessons learned, and recommendations for improvement after an incident3. Postmortem data correlation can help the security team to:

- Determine how the incident occurred and how it was detected and resolved
- Identify any gaps or weaknesses in security controls or processes that contributed to the incident
- Develop action plans or remediation strategies to prevent recurrence or mitigate future incidents

NEW QUESTION 24
During a review of SIEM alerts, a securrty analyst discovers the SIEM is receiving many alerts per day from the file-integrity monitoring toot about files from a newly deployed application that should not change. Which of the following steps should the analyst complete FIRST to respond to the issue7

A. Warn the incident response team that the server can be compromised
B. Open a ticket informing the development team about the alerts
C. Check if temporary files are being monitored
D. Dismiss the alert, as the new application is still being adapted to the environment

Answer: C

Explanation:
The analyst should check if temporary files are being monitored first to respond to the issue. Temporary files are files that are created and used by applications for various purposes, such as storing data temporarily or caching data for faster access. However, temporary files are not meant to be permanent and are usually deleted when they are no longer needed or when the application is closed. Therefore, monitoring temporary files can generate many alerts from the file-integrity monitoring tool that are not relevant or useful for security purposes. The analyst should check if temporary files are being monitored and exclude them from the monitoring scope to reduce the number of alerts and focus on the files that should not change.

NEW QUESTION 29
A security analyst is concerned about sensitive data living on company file servers following a zero-day attack that nearly resulted in a breach of millions of customer records. The after action report indicates a lack of controls around the file servers that contain sensitive data. Which of the following DLP considerations would best help the analyst to classify and address the sensitive data on the file servers?

A. Implement a CASB device and connect the SaaS applications.
B. Deploy network DLP appliances pointed to all file servers.
C. Use data-at-rest scans to locate and identify sensitive data.
D. Install endpoint DLP agents on all computing resources.

Answer: C

Explanation:
Use data-at-rest scans to locate and identify sensitive data. This option is the best DLP consideration for addressing the sensitive data on the file servers. Data-at-rest scans are performed on data that is stored on a device or a network, such as file servers, and can help identify and classify sensitive data based on predefined policies or rules. The other options are not relevant for this scenario, as they either deal with data in transit (network DLP appliances), data in use (endpoint DLP agents), or cloud-based data (CASB device).

NEW QUESTION 31
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: B

Explanation:
A routine vulnerability scan is a process of identifying and assessing known vulnerabilities in a system or
network using automated tools or software3
A vulnerability scan does not necessarily mean that there is an active threat or exploit on the system or network, but rather that there are potential weaknesses that could be exploited by attackers. The best next step after a routine vulnerability scan detected a known vulnerability in a critical enterprise web application is to evaluate the risk and criticality of the vulnerability, which means assessing the likelihood and impact of an exploit on the web application, and prioritizing the remediation actions based on the severity and urgency of the vulnerability.

NEW QUESTION 32
A new prototype for a company's flagship product was leaked on the internet As a result, the management team has locked out all USB drives Optical drive writers are not present on company computers The sales team has been granted an exception to share sales presentation files with third parties Which of the following would allow the IT team to determine which devices are USB enabled?

A. Asset tagging
B. Device encryption
C. Data loss prevention
D. SIEMIogs

Answer: D

Explanation:
A security information and event management (SIEM) system is a tool that collects and analyzes log data from various sources and provides alerts and reports on security incidents and events. A SIEM system can help the IT team to determine which devices are USB enabled by querying the log data for events related to USB device insertion, removal, or usage. The other options are not relevant or effective for this purpose. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 15;
https://www.sans.org/reading-room/whitepapers/analyst/security-information-event-management-siem-impleme

NEW QUESTION 34
Which of the following BEST describes what an organizations incident response plan should cover regarding how the organization handles public or private disclosures of an incident?

A. The disclosure section should focus on how to reduce the likelihood customers will leave due to the incident.
B. The disclosure section should contain the organization's legal and regulatory requirements regardingdisclosures.
C. The disclosure section should include the names and contact information of key employees who are needed for incident resolution
D. The disclosure section should contain language explaining how the organization will reduce the likelihood of the incident from happening m the future.

Answer: B

Explanation:
The disclosure section of an organization's incident response plan should cover how the organization handles public or private disclosures of an incident. The disclosure section should contain the organization's legal and regulatory requirements regarding disclosures, such as the type, content, format, timing, and recipients of the disclosures. The disclosure section should also specify the roles and responsibilities of the personnel involved in the disclosure process, such as who is authorized to make or approve disclosures, who is responsible for communicating with internal and external stakeholders, and who is accountable for ensuring compliance with the disclosure requirements. The disclosure section should not focus on how to reduce the likelihood customers will leave due to the incident (A), as this is a business objective rather than a disclosure requirement. The disclosure section should not include the names and contact information of key employees who are needed for incident resolution ©, as this is an operational detail rather than a disclosure requirement. The disclosure section should not contain language explaining how the organization will reduce the likelihood of the incident from happening in the future (D), as this is a remediation action rather than a disclosure requirement.

NEW QUESTION 38
During a risk assessment, a senior manager inquires about what the cost would be if a unique occurrence would impact the availability of a critical service. The service generates $1 ,000 in revenue for the organization. The impact of the attack would affect 20% of the server's capacity to perform jobs. The organization expects that five out of twenty attacks would succeed during the year. Which of the following is the calculated single loss expectancy?

A. $200
B. $800
C. $5,000
D. $20,000

Answer: A

Explanation:
The single loss expectancy (SLE) is a measure of the monetary loss associated with a single occurrence of a risk. The SLE can be calculated by multiplying the asset value (AV) by the exposure factor (EF), which is the percentage of loss that the asset would suffer if the risk occurred. In this case, the asset value is the revenue generated by the service, which is $1,000. The exposure factor is the impact of the attack on the server's capacity, which is 20%. Therefore, the SLE is $1,000 x 0.2 = $2001.

NEW QUESTION 39
An organizational policy requires one person to input accounts payable and another to do accounts receivable. A separate control requires one person to write a check and another person to sign all checks greater than $5,000 and to get an additional signature for checks greater than $10,000. Which of the following controls has the organization implemented?

A. Segregation of duties
B. Job rotation
C. Non-repudiaton
D. Dual control

Answer: A

Explanation:
Segregation of duties is a security control that requires multiple people to be involved with completing a task. This helps prevent fraud, as it ensures that no one individual has the ability to commit fraud or make mistakes without other people being aware of it

NEW QUESTION 41
An organization wants to consolidate a number of security technologies throughout the organization and standardize a workflow for identifying security issues prioritizing the severity and automating a response Which of the following would best meet the organization's needs'?

A. MaaS
B. SIEM
C. SOAR
D. CI/CD

Answer: C

Explanation:
A security orchestration, automation, and response (SOAR) system is a solution that combines various security technologies and workflows to identify security issues, prioritize their severity, and automate a response. A SOAR system can help an organization consolidate its security tools and processes and standardize its workflow for incident response. The other options are not relevant or comprehensive for this purpose. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 15; https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-and-response-s

NEW QUESTION 42
An employee contacts the SOC to report a high-severity bug that was identified in a new, internally developed web application, which went live in production last week. The SOC staff did not receive contact details or escalation procedures to follow. Which of the following stages of the SDLC process was overlooked?

A. Input validation
B. Planning
C. Implementation and integration
D. Operations and maintenance

Answer: B

Explanation:
The planning stage of the SDLC process is when the project scope, objectives, requirements, risks, and deliverables are defined and agreed upon by all stakeholders. This stage also involves creating a project plan that outlines the tasks, resources, schedule, budget, and communication channels for the project. The planning stage is crucial for ensuring that the project is aligned with the business goals and customer needs, and that the project team has a clear vision and direction for the development process. By overlooking this stage, the SOC staff did not receive contact details or escalation procedures to follow in case of a high-

severity bug, which could have serious consequences for the security and functionality of the web application.

NEW QUESTION 45
During an incident response procedure, a security analyst extracted a binary file from the disk of a compromised server. Which of the following is the best approach for analyzing the file without executing it?

A. Memory analysis
B. Hash signature check
C. Reverse engineering
D. Dynamic analysis

Answer: C

Explanation:
Reverse engineering is the process of analyzing a binary file without executing it, by using tools such as disassemblers, debuggers, and decompilers. Reverse engineering can help identify the functionality, behavior, and purpose of a binary file, as well as any malicious code or vulnerabilities it may contain.

NEW QUESTION 47
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.
"Compensating controls are additional security measures that you take to address a vulnerability without remediating the underlying issue."
A compensating control is a control that reduces the risk of an existing or potential control weakness2
In this case, the lack of segregation of duties in the accounting department is a control weakness that increases the risk of fraud or error. The quarterly reviews by a different officer are a compensating control that reduces this risk by providing an independent verification of the transactions recorded by the controller.

NEW QUESTION 51
A security analyst needs to automate the incident response process for malware infections. When the following logs are generated, an alert email should automatically be sent within 30 minutes:

```
Source: Email filtering tool
Event: Malicious message delivered notification
ID: 1905

Source: Antivirus Solution
Event: Virus CS0-726 detected
ID: 2008

Source: Firewall
Event: Outbound connection to known-bad IP blocked
ID: 1987
```

Which of the following is the best way for the analyst to automate alert generation?

A. Deploy a signature-based IDS
B. Install a UEBA-capable antivirus
C. Implement email protection with SPF
D. Create a custom rule on a SIEM

Answer: D

Explanation:
A security information and event management (SIEM) system is a tool that collects and analyzes log data from various sources and provides alerts and reports on security incidents and events. A security analyst can create a custom rule on a SIEM system to automate the incident response process for malware infections. For example, the analyst can create a rule that triggers an alert email when the SIEM system detects logs that match the criteria of malware infection, such as process name, file name, file hash, etc. The alert email can be sent within 30 minutes or any other desired time frame. The other options are not suitable or sufficient for this purpose. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 15; https://www.sans.org/reading-room/whitepapers/analyst/security-information-event-management-siem-impleme

NEW QUESTION 56
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. An accounting supervisor's laptop that is connected to the VPN
D. The laptop of the vice president that is on the corporate LAN

Answer: D

Explanation:
The laptop of the vice president that is on the corporate LAN should be investigated first. According to the CompTIA CySA+ Certification Exam (CS0-002) study guide, when prioritizing security alerts, the analyst should prioritize assets based on the potential impact of a successful attack or compromise. Therefore, the laptop of the vice president, which is connected to the corporate LAN, should be investigated first, as it has the highest potential impact.

NEW QUESTION 58
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

Explanation:
A communications plan is a document that outlines who should be notified and how during an incident response. It can also specify the roles and responsibilities of the incident response team members, the escalation procedures, and the communication channels. Consulting the communications plan is the most appropriate next step in an incident response plan after determining a security incident has occurred. Consulting the malware analysis process, the disaster recovery plan, or the data classification process may be relevant at later stages of the incident response, but not as the next step. Reference: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

NEW QUESTION 60
Which of the following describes the difference between intentional and unintentional insider threats'?

A. Their access levels will be different
B. The risk factor will be the same
C. Their behavior will be different
D. The rate of occurrence will be the same

Answer: C

Explanation:
The difference between intentional and unintentional insider threats is their behavior. Intentional insider threats are malicious actors who deliberately misuse their access to harm the organization or its assets. Unintentional insider threats are careless or negligent users who accidentally compromise the security of the organization or its assets. Their access levels, risk factors, and rates of occurrence may vary depending on various factors, but their behavior is the main distinction. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 12; https://www.cisa.gov/sites/default/files/publications/Insider_Threat_Mitigation_Guide_508.pdf

NEW QUESTION 63
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: C

Explanation:
Domain Keys Identified Mail (DKIM) is an email authentication method that uses a digital signature to let the
receiver of an email know that the message was sent and authorized by the owner of a domain1
DKIM helps prevent phishing emails that spoof or impersonate other domains by verifying the identity and integrity of the sender. DKIM works by adding a DKIM signature header to each outgoing email message, which contains a hash value of selected parts of the message and the domain name of the sender. The sender’s domain also publishes a public key in its DNS records, which can be used by the receiver to decrypt the DKIM signature and compare it with its own hash value of the message. If they match, it means that the message was not altered in transit and that it came from the claimed domain.

NEW QUESTION 66
A security analyst identified one server that was compromised and used as a data making machine, and a few of the hard drive that was created. Which of the following will MOST likely provide information about when and how the machine was compromised and where the malware is located?

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

Answer: A

Explanation:
System timeline reconstruction is a forensic analysis technique that involves creating a chronological record of events that occurred on a system based on various sources of evidence such as log files, registry entries, file timestamps, network traffic, etc. System timeline reconstruction can provide information about when and how the machine was compromised and where the malware is located by showing when suspicious activities or changes took place on the system, such as unauthorized access attempts, file creation or modification, process execution, network connections, etc.

NEW QUESTION 70
A security analyst discovers suspicious host activity while performing monitoring activities. The analyst pulls a packet capture for the activity and sees the following:

Date/time	Destination	Protocol	Host	Info
2020-08-20	92.168.4.52	HTTP	utoftor.com	POST /210/gate.php HTTP/1.1 (Application/octet-stream)

Follow TCP stream:

```
POST /210/gate.php HTTP/1.1
Cache-control: no-cache
Connection: close
Pragma: no-cache
Content-Type: application/octet-stream
User-Agent: Mozilla/4.0
Host: utoftor.com
$s.0.k..4.4.RQA.6….HTTP/1.1 200 OK
Server: nginx/1.6.2
.
```

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.com.

Answer: C

Explanation:
The packet capture shows that the host sent a Client Hello message to utoftor.com on port 443. This message is part of the TLS (Transport Layer Security) handshake protocol, which is used to establish a secure connection between a client and a server1. The Client Hello message contains information such as the supported TLS version, cipher suites, and extensions that the client can use for the secure connection. The server is expected to respond with a Server Hello message that selects the parameters for the secure connection. However, the packet capture does not show any response from the server, which means that the host only attempted to make a secure connection to utoftor.com, but did not succeed. The host did not download (B) or reject (D) any application from utoftor.com.

NEW QUESTION 73
Given the output below:
#nmap 7.70 scan initiated Tues, Feb 8 12:34:56 2022 as: nmap -v -Pn -p 80,8000,443 --script http-* -oA server.out 192.168.220.42
Which of the following is being performed?

A. Cross-site scripting
B. Local file inclusion attack
C. Log4] check
D. Web server enumeration

Answer: D

Explanation:
Web server enumeration is the process of identifying information about a web server, such as its software version, operating system, configuration, services, and vulnerabilities. This can be done using tools like Nmap, which can scan ports and run scripts to gather information. In this question, the Nmap command is using the -p option to scan ports 80, 8000, and 443, which are commonly used for web services. It is also using the --script option to run scripts that start with http-*, which are related to web server enumeration. The output file name server.out also suggests that the purpose of the scan is to enumerate web servers. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 8; https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives

NEW QUESTION 77
Forming a hypothesis, looking for indicators of compromise, and using the findings to proactively improve detection capabilities are examples of the value of:

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

Answer: B

Explanation:
Threat hunting is a proactive process of searching for signs of malicious activity or compromise within a system or network, by using hypotheses, indicators of compromise, and analytical tools. Threat hunting can help improve detection capabilities by identifying unknown threats, uncovering gaps in security controls, and providing insights for remediation and prevention. Vulnerability scanning (A) is a reactive process of scanning systems or networks for known vulnerabilities or weaknesses that can be exploited by attackers. It can help identify and prioritize vulnerabilities, but not proactively hunt for threats. Red teaming © is a simulated attack on a system or network by a group of ethical hackers who act as adversaries and try to breach security controls. It can help test the effectiveness of security defenses and response capabilities, but not proactively hunt for threats. Penetration testing (D) is similar to red teaming, but with a more defined scope and objective. It can help evaluate the security of a system or network by simulating real-world attacks and exploiting vulnerabilities, but not proactively hunt for threats. References: : https://www.techopedia.com/definition/33297/threat-hunting : https://www.techopedia.com/definition/4160/web-application-security-scanner-was : https://www.techopedia.com/definition/32694/red-teaming : https://www.techopedia.com/definition/13493/penetration-testing

NEW QUESTION 80
A network appliance manufacturer is building a new generation of devices and would like to include chipset security improvements. The management team wants the security team to implement a method to prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset. Which of the following would meet this objective?

A. UEFI
B. A hardware security module
C. eFUSE
D. Certificate signed updates

Answer: C

Explanation:
The correct answer is C. eFUSE. An eFUSE is a type of electronic fuse that can be programmed to permanently alter the functionality or configuration of a chipset. An eFUSE can be used to prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset, by locking the firmware to a specific version or preventing unauthorized modifications. An eFUSE can also provide other benefits, such as anti-tampering, anti-counterfeiting, and device authentication1.
* A. UEFI is not correct. UEFI stands for Unified Extensible Firmware Interface, and it is a standard that defines the software interface between an operating system and a platform firmware. UEFI can provide security features, such as secure boot, which verifies the integrity of the boot loader and prevents unauthorized code execution during the boot process. However, UEFI does not prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset2.
* B. A hardware security module is not correct. A hardware security module (HSM) is a physical device that provides secure storage and processing of cryptographic keys and operations. An HSM can protect sensitive data and transactions, such as encryption, decryption, signing, or verification, from unauthorized access or tampering. However, an HSM does not prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset3.
* D. Certificate signed updates are not correct. Certificate signed updates are a method of ensuring the authenticity and integrity of firmware updates by using digital certificates and signatures. Certificate signed updates can prevent malicious or corrupted firmware updates from being installed on the chipset, but they do not prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset. 1: What Is an eFUSE? 2: What Is UEFI? 3: What Is a Hardware Security Module (HSM)?

NEW QUESTION 84
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.
The best way to remediate the vulnerability is to update to the secure hypervisor version. A hypervisor is a software that creates and manages virtual machines on a physical server. A hypervisor can be vulnerable to various attacks, such as privilege escalation, code injection, or denial-of-service. Updating to the secure hypervisor version can help fix any known bugs or flaws in the hypervisor software and prevent attackers from exploiting them. Updating to the secure hypervisor version can also provide additional security features or enhancements that can improve the protection of the virtual machines and their data.

NEW QUESTION 88
Legacy medical equipment, which contains sensitive data, cannot be patched. Which of the following is the best solution to improve the equipment's security posture?

A. Move the legacy systems behind a WAR
B. Implement an air gap for the legacy systems.
C. Place the legacy systems in the perimeter network.
D. Implement a VPN between the legacy systems and the local network.

Answer: B

Explanation:
Implementing an air gap for the legacy systems is the best solution to improve their security posture. An air gap is a physical separation of a system or network from any other system or network that may pose a threat. An air gap can prevent any unauthorized access or data transfer between the isolated system or network and the external environment. Implementing an air gap for the legacy systems can help to protect them from being exploited by attackers who may take advantage of their unpatched vulnerabilities .

NEW QUESTION 90
Which of the following SCAP standards provides standardization tor measuring and describing the seventy of security-related software flaws?

A. OVAL
B. CVSS
C. CVE
D. CCE

Answer: B

Explanation:
CVSS stands for Common Vulnerability Scoring System, and it is a standard for measuring and describing the severity of security-related software flaws. CVSS provides a numerical score and a vector string that represent the characteristics and impact of a vulnerability. CVSS can help prioritize remediation efforts and communicate risk levels to stakeholders.

NEW QUESTION 91
A security analyst is reviewing vulnerability scans from an organization's internet-facing web services. The following is from an output file called ssl-test_webapps.comptia.org:

```
SCAN RESULTS FOR webapps.comptia.org:443 - 52.165.16.154
---------------------------------------------------
* Certificates Information:
Hostname sent for SNI: webapps.comptia.org
Number of certificates detected: 1

Certificate #0 ( _RSAPublicKey )
SHA1 Fingerprint: 44175dea3a5b1a21fb94698072b3427bf4607117
Common Name: *.comptia.org
Public Key Algorithm: _RSAPublicKey
Signature Algorithm: sha256
Key Size: 2048
Exponent: 65537
DNS Subject Alternative Names: ['*.comptia.org']


Certificate #0 - Extensions
OCSP Must-Staple: NOT SUPPORTED - Extension not found
Certificate Transparency: OK - 3 SCTs included
Certificate #0 - OCSP Stapling
NOT SUPPORTED - Server did not send back an OCSP response


* TLS 1.0 Cipher Suites:
Attempted to connect using 80 cipher suites.
The server accepted the following 10 cipher suites:
TLS_RSA_WITH_RC4_128_SHA 128
TLS_RSA_WITH_RC4_128_MD5 128
TLS_RSA_WITH_DES_CBC_SHA 56
TLS_RSA_WITH_AES_256_CBC_SHA 256
TLS_RSA_WITH_AES_128_CBC_SHA 128
TLS_RSA_WITH_3DES_EDE_CBC_SHA 168
TLS_DHE_RSA_WITH_DES_CBC_SHA 56 DH (1024 bits)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA 256 DH (1024 bits)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128 DH (1024 bits)
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA 168 DH (1024 bits)
TLS_DHE_RSA_WITH_AES_256_GCM_SHA256 DH (2048 bits)
The group of cipher suites supported by the server has the following properties:
Forward Secrecy OK - Supported
Legacy RC4 Algorithm INSECURE - Supported
```

Which of the following lines from this output most likely indicates that attackers could quickly use brute force and determine the negotiated secret session key?

A. TLS_RSA_WITH_DES_CBC_SHA 56
B. TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128 DH (1024 bits)
C. TLS_RSA_K1TH_A£S_256_CBC_SHA 256
D. TLS_DHE_RSA_WITH_AES_256_GCM_SHA256 DH (2048 bits)

Answer: A

Explanation:
This line from the output most likely indicates that attackers could quickly use brute force and determine the negotiated secret session key, as it represents a weak cipher suite that uses an outdated encryption algorithm, a small key size, and no forward secrecy. A cipher suite is a combination of cryptographic algorithms and parameters that are used to establish a secure communication channel between two parties. The cipher suite in this line consists of four components: TLS_RSA_WITH_DES_CBC_SHA 56.

- TLS stands for Transport Layer Security, and it is a protocol that provides security and privacy for network communications.
- RSA stands for Rivest-Shamir-Adleman, and it is an algorithm that uses public-key cryptography for key exchange and authentication.
- DES stands for Data Encryption Standard, and it is an algorithm that uses symmetric-key cryptography for data encryption.
- CBC stands for Cipher Block Chaining, and it is a mode of operation that encrypts each block of data by XORing it with the previous ciphertext block.
- SHA stands for Secure Hash Algorithm, and it is an algorithm that produces a fixed-length hash value from any input data.
- 56 stands for the key size in bits, which indicates how strong or secure the encryption is.

The cipher suite in this line is weak because:

- DES is an outdated encryption algorithm that has been broken by brute force attacks, as it has a small key size of 56 bits, which can be easily guessed by modern computers.
- RSA does not provide forward secrecy, which means that if the RSA private key is compromised, all past and future communications encrypted with that key can be decrypted by an attacker.
- SHA is also an outdated hash algorithm that has been replaced by newer versions such as SHA-2 or SHA-3, as it has some vulnerabilities and weaknesses.

NEW QUESTION 96
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: B

Explanation:

SOAR has a wider breadth of capability using orchestration and automation, while SCAP is more limited in scope. SOAR (Security Orchestration, Automation and Response) is a technology that helps coordinate, execute and automate tasks between various people and tools within a single platform. SOAR can help improve the efficiency and effectiveness of security operations by reducing manual effort, enhancing
collaboration, and accelerating incident response1. SCAP (Security Content Automation Protocol) is a standard that enables automated vulnerability management, measurement and policy compliance evaluation of systems deployed in an organization2. SCAP can help assess the security posture and compliance status of systems by using predefined specifications and checklists. However, SCAP does not provide orchestration or automation capabilities beyond vulnerability scanning and reporting.

NEW QUESTION 101
An incident response plan requires systems that contain critical data to be triaged first in the event of a compromise. Which of the following types of data would most likely be classified as critical?

A. Encrypted data
B. data
C. Masked data
D. Marketing data

Answer: B

Explanation:
PII stands for personally identifiable information, and it is any data that can be used to identify, contact, or locate a specific individual, such as name, address, phone number, email, social security number, or biometric data. PII data is considered critical because it can be used by attackers to commit identity theft, fraud, or other crimes. PII data is also subject to various laws and regulations that require organizations to protect it from unauthorized access, use, or disclosure1.

NEW QUESTION 104
A security analyst discovers the accounting department is hosting an accounts receivable form on a public document service. Anyone with the link can access it. Which of the following threats applies to this situation?

A. Potential data loss to external users
B. Loss of public/private key management
C. Cloud-based authentication attack
D. Identification and authentication failures

Answer: A

Explanation:
Potential data loss to external users is a threat that applies to this situation, where the accounting department is hosting an accounts receivable form on a public document service. Anyone with the link can access it. Data loss is an event that results in the destruction, corruption, or unauthorized disclosure of sensitive or confidential data. Data loss can occur due to various reasons, such as human error, hardware failure, malware infection, or cyberattack. In this case, hosting an accounts receivable form on a public document service exposes the data to potential data loss to external users who may access it without authorization or maliciously modify or delete it .

NEW QUESTION 107
During the threat modeling process for a new application that a company is launching, a security analyst needs to define methods and items to take into consideralion Wtiich of the following are part of a known threat modeling method?

A. Threat profile, infrastructure and application vulnerabilities, security strategy and plans
B. Purpose, objective, scope, (earn management, cost, roles and responsibilities
C. Spoofing tampering, repudiation, information disclosure, denial of service elevation of privilege
D. Human impact, adversary's motivation, adversary's resources, adversary's methods

Answer: C

Explanation:
Spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege are part of a known threat modeling method called STRIDE. STRIDE is a mnemonic that stands for six categories of threats that can affect the security of a system or application. STRIDE was developed by Microsoft in 1999 and has been widely adopted as a threat modeling method by many organizations. STRIDE can help identify and prioritize potential threats based on their impact and likelihood1.

NEW QUESTION 109
A security technician is testing a solution that will prevent outside entities from spoofing the company's email domain, which is compatia.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=spfl mx include:_spf.compti
B. org -all" to the DNS record.
C. Add : XT @ "v=spfl mx include:_sp£.comptia.org -all" to the email server.
D. Add TXT @ "v=spfl mx include:_sp£.comptia.org +all" to the domain controller.
E. AddTXT @ "v=apfl mx lnclude:_spf .comptia.org +a 11" to the web server.

Answer: A

Explanation:
Adding TXT @ “v=spfl mx include:_spf.comptia. org -all” to the DNS record can help to prevent outside entities from spoofing the company’s email domain, which is comptia.org. This is an example of a Sender Policy Framework (SPF) record, which is a type of DNS record that specifies which mail servers are authorized to send email on behalf of a domain. SPF records can help to prevent spoofing by allowing the recipient mail servers to check the validity of the sender’s domain against the SPF record. The “-all” at the end of the SPF record indicates that any mail server that is not listed in the SPF record is not authorized to send email for comptia.org .

NEW QUESTION 112
An organization is experiencing security incidents in which a systems administrator is creating unauthorized user accounts A security analyst has created a script to snapshot the system configuration each day. Following iss one of the scripts:

```
cat /etc/passwd > daily_$(date +"%m_%d_%Y")
```

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

```
diff daily_11_03_2019 daily_11_04_2019
```

B)

```
ps -ef | grep admin > daily_process_$(date +%m_%d_%Y")
```

C)

```
more /etc/passwd > daily_$(date  +%m_%d_%Y_%H:%M:%S")
```

D)

```
la -lai /usr/sbin > daily_applications
```

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

Answer: D

Explanation:
Option D would provide the analyst with additional useful information relevant to the above script. Option D is a command that compares two files and shows the differences between them. In this case, the command compares the current snapshot of the system configuration (sysconfig.txt) with the previous snapshot (sysconfig.txt.old). This can help the analyst to identify any changes or anomalies in the system configuration that may indicate unauthorized or malicious activity. Option A is a command that copies a file from one location to another. In this case, the command copies the current snapshot of the system configuration (sysconfig.txt) to a backup location (/backup/sysconfig.txt). This can help the analyst to preserve evidence or restore the system configuration if needed, but it does not provide any additional information relevant to the above script. Option B is a command that prints a file to standard output. In this case, the command prints the current snapshot of the system configuration (sysconfig.txt) to the screen. This can help the analyst to review or analyze the system configuration, but it does not provide any additional information relevant to the above script. Option C is a command that moves a file from one location to another. In this case, the command moves the current snapshot of the system configuration (sysconfig.txt) to another location (/old/sysconfig.txt). This can help the analyst to organize or archive the system configuration files, but it does not provide any additional information relevant to the above script.

NEW QUESTION 117
A security engineer is reviewing security products that identify malicious actions by users as part of a company's insider threat program. Which of the following is the most appropriate product category for this purpose?

A. SCAP
B. SOAR
C. UEBA
D. WAF

Answer: C

Explanation:
UEBA stands for User and Entity Behavior Analytics, which is a category of security products that use machine learning and statistical analysis to identify malicious actions by users or entities on a network. UEBA products can detect anomalous or suspicious behaviors that deviate from normal patterns or baselines, such as data exfiltration, privilege escalation, unauthorized access, insider threats, or compromised accounts. UEBA products can also provide alerts, reports, or recommendations for response actions based on the detected behaviors.

NEW QUESTION 121
A company frequently expenences issues with credential stuffing attacks Which of the following is the BEST control to help prevent these attacks from being successful?

A. SIEM
B. IDS
C. MFA
D. TLS

Answer: C

Explanation:
MFA stands for multi-factor authentication, which is a method of verifying a user’s identity by requiring two or more pieces of evidence, such as something the user knows (e.g., password), something the user has (e.g., token), or something the user is (e.g., fingerprint). MFA is the best control to help prevent credential stuffing attacks from being successful, because even if an attacker obtains a valid username and password from a breached site, they would still need another factor to access the target site. SIEM, IDS, and TLS are other security controls, but they are not as effective as MFA for preventing credential stuffing attacks.
Reference: https://www.cloudflare.com/learning/bots/what-is-credential-stuffing/

NEW QUESTION 126
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: B

Explanation:
A retinal scan is a biometric authentication method that uses the unique pattern of blood vessels in the retina to verify a person's identity. It is considered a strong and reliable authentication method that would enhance the datacenter's security. A physical key, a passphrase, or a fingerprint are other authentication methods, but they are not as secure or reliable as a retinal scan. Reference:
https://www.techopedia.com/definition/2586/retinal-scan

NEW QUESTION 129
Which of following allows Secure Boot to be enabled?

A. eFuse
B. UEFI
C. MSM
D. PAM

Answer: B

Explanation:
UEFI, or Unified Extensible Firmware Interface, is a specification that defines the software interface between an operating system and platform firmware. UEFI replaces the legacy BIOS (Basic Input/Output System) interface that was used to boot and configure computers. UEFI provides several advantages over BIOS, such as faster boot times, better security features, larger disk support, graphical user interface, etc. One of the security features that UEFI supports is Secure Boot, which is a mechanism that ensures that only authorized software can run during the boot process. Secure Boot prevents unauthorized or malicious code from loading or executing before the operating system starts. Secure Boot works by verifying the digital signature of each piece of boot software against a database of trusted keys stored in UEFI firmware. If the signature is valid, the software is allowed to run; otherwise, it is blocked or rejected.

NEW QUESTION 130
A security analyst needs to recommend the best approach to test a new application that simulates abnormal user behavior to find software bugs. Which of the following would best accomplish this task?

A. A static analysis to find libraries with flaws handling user inputs
B. A dynamic analysis using a dictionary to simulate user inputs
C. Reverse engineering to circumvent software protections
D. Fuzzing tools with polymorphic methods

Answer: D

Explanation:
Fuzzing is a technique that involves sending random, malformed, or unexpected inputs to an application to trigger errors, crashes, or vulnerabilities. Fuzzing can be used to test the robustness and security of software, especially when the source code is not available or the input format is complex1. Fuzzing can also simulate abnormal user behavior, such as entering invalid data, clicking on random buttons, or sending malicious requests2.
Fuzzing tools are software programs that automate the process of generating and sending inputs to the application under test. There are different types of fuzzing tools, such as black-box fuzzers, white-box fuzzers, and grey-box fuzzers, depending on the level of information and feedback they have about the application1. Some examples of fuzzing tools are AFL, Peach, and [Sulley].
Polymorphic methods are techniques that allow fuzzing tools to modify or mutate the inputs in different ways, such as changing the length, value, type, or structure of the data. Polymorphic methods can increase the diversity and effectiveness of the inputs and help discover more bugs or vulnerabilities in the application .
Therefore, using fuzzing tools with polymorphic methods would be the best approach to test a new application that simulates abnormal user behavior to find software bugs. This approach would generate a large number of inputs that cover various scenarios and edge cases and expose any flaws or weaknesses in the application's functionality or security.

NEW QUESTION 133
An intrusion detection analyst reported an inbound connection originating from an unknown IP address recorded on the VPN server for multiple internal hosts. During an investigation, a security analyst determines there were no identifiers associated with the hosts. Which of the following should the security analyst enforce to obtain the best information?

A. Update the organization's IP table.
B. Enable user access logging.
C. Shut down all VPN connections.
D. Create rules for the Active Directory.

Answer: B

Explanation:
User access logging (UAL) is a feature on Windows Server operating systems that records the details of
remote access and management activities performed by users on the server. UAL can provide information such as the user name, the source IP address, the destination host name, the protocol used, and the time and duration of the connection1. Enabling user access logging on the VPN server can help the security analyst to obtain the best information to identify and investigate the inbound connection originating from an unknown IP address.

NEW QUESTION 135
A financial organization has offices located globally. Per the organization's policies and procedures, all executives who conduct Business overseas must have their mobile devices checked for malicious software or evidence of tempering upon their return. The information security department oversees the process, and no executive has had a device compromised. The Chief information Security Officer wants to Implement an additional safeguard to protect the organization's data. Which of the following controls would work BEST to protect the privacy of the data if a device is stolen?

A. Implement a mobile device wiping solution for use if a device is lost or stolen.

B. Install a DLP solution to track data now
C. Install an encryption solution on all mobile devices.
D. Train employees to report a lost or stolen laptop to the security department immediately

Answer: A

Explanation:
A mobile device wiping solution is a security feature that allows an organization to remotely erase or delete all data on a mobile device if it is lost or stolen2
A mobile device wiping solution can help protect the privacy of the data on a device and prevent unauthorized access or disclosure of sensitive information. A mobile device wiping solution can be implemented using built-in features of some mobile operating systems, third-party applications, or mobile device management (MDM) software.

NEW QUESTION 136
A company wants to run a leaner team and needs to deploy a threat management system with minimal human Interaction. Which of the following is the server component of the threat management system that can accomplish this goal?

A. STIX
B. OpenlOC
C. CVSS
D. TAXll

Answer: D

Explanation:
TAXII stands for Trusted Automated eXchange of Indicator Information, and it is a server component of a threat management system that can facilitate the exchange of threat intelligence data between different sources and consumers, using a standard protocol and format. TAXII can help deploy a threat management system with minimal human interaction, by automating the collection, processing, and dissemination of threat intelligence data.

NEW QUESTION 141
Given the Nmap request below:

```
Scanner# nmap -p 22,113,139,1433 www.scannable.org - d --packet-trace
Starting Nmap(http://nmap.org)
Nmap scan report for www.scannable.org
SENT(0.0149s) ICMP SCANNER > SCANNABLE
echo request (type=8/code=0) TTL=52 ID=1929
SENT(0.0112s) TCP SCANNER:63541 > SCANNABLE:80 iplen=40 seq=99850910
RCVC(0.0179s) ICMP SCANNABLE > SCANNER echo reply(type-0/code=0 iplen=28 seq=99850910
we got a ping back for SCANNABLE: ID=48822 seq=713 checksum=16000
massping done: num_host:1 num_response:1
Initiating SYN STEALTH Scan against www.scannable.org (SCANNABLE) 3 ports at 00:47
SENT(0.0134s) TCP SCANNER:63517 > SCANNABLE:113 iplen=40 seq=1048634
SENT(0.0148s) TCP SCANNER:63517 > SCANNABLE:139 iplen=40 seq=1048634
SENT(0.0092s) TCP SCANNER:63517 > SCANNABLE:22 iplen=40 seq=1048634
RCVD(0.0151s) TCP SCANNABLE:113 > SCANNER:63517 iplen=40 seq=1048634
RCVD(0.0151s) TCP SCANNABLE:22 > SCANNER:63517 iplen=40 seq=1048634
SENT(0.0097s) TCP SCANNER:63517 > SCANNABLE:139 iplen=40 seq=1048634
The SYN STEALTH Scan took 1.25s to scan 3 total ports
Nmap Report for www.scannable.org (SCANNABLE)

PORT      STATE      SERVICE
22/tcp    open       ssh
113/tcp   closed     auth
139/tcp   filtered   netbios-ssh
1433/tcp  closed     ms-sql
```

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

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

Answer: C

Explanation:
The Nmap command given in the question performs a TCP SYN scan (-sS), a service version detection scan (-sV), an OS detection scan (-O), and a port scan for ports 1-1024 (-p 1-1024) on the host 192.168.1.1. This command will reveal information about the host's operating system, open ports, and running services, which can be used by an attacker to launch a brute-force attack against the host. A brute-force attack is a method of guessing passwords or encryption keys by trying many possible combinations until finding the correct one. An attacker can use the information from the Nmap scan to target specific services or protocols that may have weak or default credentials, such as FTP, SSH, Telnet, or HTTP.

NEW QUESTION 142
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: A

Explanation:
A data governance program is a collection of practices, policies, and procedures that manage, leverage, and protect the data assets of an organization1. It requires changing the workplace culture and adding some software1. To survey sensitive data within the organization, the most accurate method is to perform an enterprise-wide discovery scan that can identify and classify data from various sources and systems2. This way, the analyst can have a comprehensive view of the data landscape and its quality, security, accessibility, and usage. Consulting with an internal data custodian (B) or reviewing enterprise-wide asset inventory © may provide some insights, but not as accurate or complete as a discovery scan. Creating a survey and distributing it to data owners (D) may be time-consuming and unreliable, as data owners may not have the full knowledge or awareness of their data.
References: 1: https://www.analytics8.com/blog/8-steps-to-start-your-data-governance-program/ 2: https://solutionsreview.com/data-management/the-best-data-governance-tools-and-software/

NEW QUESTION 147
Which of the following can detect vulnerable third-parly libraries before code deployment?

A. Impact analysis
B. Dynamic analysis
C. Static analysis
D. Protocol analysis

Answer: C

Explanation:
Static analysis is a method of analyzing the source code or binary code of an application without executing
it. Static analysis can detect vulnerable third-party libraries before code deployment by scanning the code for references to known vulnerable libraries or versions and reporting any issues or risks12.
Impact analysis is a process of assessing the potential effects of a change on a system or service, such as performance, availability, security and compatibility. Impact analysis does not detect vulnerable third-party libraries before code deployment, but rather helps to evaluate and communicate the consequences of a change.
Dynamic analysis is a method of analyzing the behavior or performance of an application by executing it under various conditions or inputs. Dynamic analysis does not detect vulnerable third-party libraries before code deployment, but rather helps to identify any errors or defects that occur at runtime.
Protocol analysis is a method of examining the data exchanged between devices or applications over a network by capturing and interpreting the packets or messages. Protocol analysis does not detect vulnerable third-party libraries before code deployment, but rather helps to monitor and troubleshoot network communication.

NEW QUESTION 149
A security administrator needs to provide access from partners to an Isolated laboratory network inside an organization that meets the following requirements:
• The partners' PCs must not connect directly to the laboratory network.
• The tools the partners need to access while on the laboratory network must be available to all partners
• The partners must be able to run analyses on the laboratory network, which may take hours to complete Which of the following capabilities will MOST likely meet the security objectives of the request?

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

Answer: D

Explanation:
A jump box is a system that is connected to two networks and acts as a gateway or intermediary between them 1. A jump box can help to isolate and secure a network by limiting the direct access to it from other networks.
A jump box can also help to monitor and audit the traffic and activity on the network. A VDI (Virtual Desktop
Infrastructure) is a technology that allows users to access virtual desktops that are hosted on a server2. A VDI can help to provide users with the necessary tools and applications for analysis without installing them on their own PCs. A VDI can also help to reduce the maintenance and management costs of the desktops. A VDI can operate in two modes: persistent and non-persistent. In persistent mode, each user has a dedicated virtual desktop that retains its settings and data across sessions. In non-persistent mode, each user has a temporary virtual desktop that is deleted or reset after each session3. In this scenario, deploying a jump box to allow access to the laboratory network and using VDI in non-persistent mode can meet the security objectives of the request. The jump box can prevent the partners' PCs from connecting directly to the laboratory network and reduce the risk of unauthorized access or compromise. The VDI in non-persistent mode can provide the necessary tools for analysis without storing any data on the partners' PCs or the virtual desktops. The VDI in non-persistent mode can also allow the partners to run long analyses without losing their progress or results. Deploying a firewall (B) may not be sufficient or effective, as a firewall only filters or blocks traffic based on rules and does not provide access or tools for analysis. Using VDI in persistent mode (A) © may not be secure or efficient, as persistent mode stores data on the virtual desktops that may be sensitive or confidential.
References: 1: https://www.techrepublic.com/article/jump-boxes-vs-firewalls/ 2:
https://www.techopedia.com/definition/26139/virtual-desktop-infrastructure-vdi 3: https://www.techopedia.com/definition/31686/resource-exhaustion

NEW QUESTION 151
An organization's Cruel Information Security Officer is concerned the proper control are not in place to identify a malicious insider Which of the following techniques would be BEST to identify employees who attempt to steal data or do harm to the organization?

A. Place a text file named Passwords txt on the local file server and create a SIEM alert when the file is accessed
B. Segment the network so workstations are segregated from servers and implement detailed logging on the jumpbox
C. Perform a review of all users with privileged access and monitor web activity logs from the organization's proxy
D. Analyze logs to determine if a user is consuming large amounts of bandwidth at odd hours ol the day

Answer: D

Explanation:
Analyzing logs is a technique that involves collecting and examining data from various sources, such as network devices, servers, applications, or security tools. Analyzing logs can help identify malicious insiders by detecting anomalous or suspicious activities or behaviors, such as consuming large amounts of bandwidth at odd hours of the day, which could indicate data exfiltration or unauthorized access attempts. Placing a text file named Passwords.txt on the local file server and creating a SIEM alert when the file is accessed, segmenting the network so workstations are segregated from servers and implementing detailed logging on the jumpbox, or performing a review of all users with privileged access and monitoring web activity logs from the organization's proxy are other possible techniques to identify malicious insiders, but they are not as effective or reliable as analyzing logs. Reference: https://www.sans.org/reading-room/whitepapers/logging/detecting-attacks-systems-microsoft-windows-event-lo

NEW QUESTION 154
A security analyst is investigate an no client related to an alert from the threat detection platform on a host (10.0 1.25) in a staging environment that could be running a cryptomining tool because it in sending traffic to an IP address that are related to Bitcoin.
The network rules for the instance are the following:

Rule	Direction	Protocol	SRC	DST	Port	Description
1	inbound	tcp	any	10.0.1.25	80	HTTP
2	inbound	tcp	any	10.0.1.25	443	HTTPS
3	inbound	tcp	10.0.1.0/25	10.0.1.25	22	SSH
4	outbound	udp	10.0.1.25	10.0.1.2	53	DNS
5	outbound	tcp	10.0.1.25	any	any	TCP

Which of the following is the BEST way to isolate and triage the host?

A. Remove rules 1.2. and 3.
B. Remove rules 1.2. 4. and 5.
C. Remove rules 1.2. 3.4. and 5.
D. Remove rules 1.2. and 5.
E. Remove rules 1.4. and 5.
F. Remove rules 4 and 5

Answer: C

Explanation:
The best way to isolate and triage the host is to remove rules 1, 2, 3, 4, and 5. These rules allow inbound and outbound traffic on ports 22 (SSH), 80 (HTTP), and 443 (HTTPS) from any source or destination. By removing these rules, the security analyst can block any network communication to or from the host, preventing any further data exfiltration or malware infection. This will also allow the security analyst to perform a forensic analysis on the host without any interference from external sources.

NEW QUESTION 158
To validate local system-hardening requirements, which of the following types of vulnerability scans would work BEST to verify the scanned device meets security policies?

A. SCAP
B. SAST
C. DAST
D. DACS

Answer: A

Explanation:
SCAP is a protocol designed to assess the security compliance of computers and other devices. It works by scanning systems against security policies, and can help verify that the scanned device meets security requirements. Here is a link to the CompTIA CySA+ Guide's Chapter 5 - Access Controls for more information: https://certification.comptia.org/docs/default-source/exam-objectives/cs0-002.pdf

NEW QUESTION 159
A security analyst is reviewing the following DNS logs as part of security-monitoring activities:
FROM 192.168.1.20 A www.google.com 67.43.45.22
FROM 192.168.1.20 AAAA www.google.com 2006:67:AD:1FAB::102
FROM 192.168.1.43 A www.mail.com 193.56.221.99
FROM 192.168.1.2 A www.company.com 241.23.22.11
FROM 192.168.1.211 A www.uewiryfajfchfaerwfj.co 32.56.32.122
FROM 192.168.1.106 A www.whatsmyip.com 102.45.33.53
FROM 192.168.1.93 ARAA www.nbc.com 2002:10:976::1
FROM 192.168.1.78 A www.comptia.org 122.10.31.87
Which of the following most likely occurred?

A. The attack used an algorithm to generate command and control information dynamically.
B. The attack attempted to contact www.google.com to verify internet connectivity.
C. The attack used encryption to obfuscate the payload and bypass detection by an IDS.
D. The attack caused an internal host to connect to a command and control server.

Answer: A

Explanation:
This is a technique that is commonly used by malware to evade detection and blocking by security tools. The malware generates random domain names that are used to communicate with the command and control server, which can change its IP address frequently. The domain names are usually long and nonsensical, such as www.uewiryfajfchfaerwfj.co in the log. The malware uses a predefined algorithm or a seed value to generate the same domain names as the server, so that they can find each other on the internet12.

NEW QUESTION 162

A security analyst is reviewing the following server statistics:

% CPU	Disk KB in	Disk KB out	Net KB in	Net KB out
99	3122	43	456	34
100	123	56	87	7
99	2	234	3	245
100	78	3	243	43
100	345	867	8243	85
98	22	3	5634	42326
100	435	345	54	42
99	0	4	575	3514

Which of the following Is MOST likely occurring?

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

Answer: C

Explanation:
Resource exhaustion occurs when a system runs out of resources such as memory, CPU, disk space, or network bandwidth due to excessive demand or poor management1. In this case, the server statistics show that the CPU usage is 100%, the memory usage is 99%, and the disk usage is 98%, indicating that the system is suffering from resource exhaustion. This can affect the performance and availability of the system and its applications. A race condition (A) is a condition where the system's behavior depends on the sequence or timing of other uncontrollable events2. Privilege escalation (B) is a situation where an attacker gains unauthorized access to higher privileges or permissions on a system3. VM escape (D) is a technique where an attacker breaks out of a virtual machine and interacts with the host operating system.
References: 1: https://www.techopedia.com/definition/31686/resource-exhaustion 2: https://en.wikipedia.org/wiki/Race_condition 3: https://www.techopedia.com/definition/4111/privilege-escalation : https://www.techopedia.com/definition/32088/vm-escape

NEW QUESTION 166
Which of the following is the best method to review and assess the security of the cloud service models used by a company on multiple CSPs?

A. Unifying and migrating all services in a single CSP
B. Executing an API hardening process on the CSPs' endpoints
C. Integrating the security benchmarks of the CSPs with a CASB
D. Deploying cloud instances using Nikto and OpenVAS

Answer: C

Explanation:
This is the best method to review and assess the security of the cloud service models used by a company on multiple CSPs. CSP stands for cloud service provider, which is a company that offers cloud-based services such as infrastructure, platform, or software. CASB stands for cloud access security broker, which is a software or service that acts as a gateway between the company and the CSPs, and provides visibility, control, compliance, and threat protection for the cloud services.
Integrating the security benchmarks of the CSPs with a CASB means that the company can use a common set of standards and metrics to measure and compare the security posture and performance of different cloud service models, such as IaaS, PaaS, or SaaS. Security benchmarks are predefined criteria or best practices that define the minimum level of security required for a cloud service model. For example, some security benchmarks may include encryption, authentication, logging, auditing, patching, backup, etc. By integrating these benchmarks with a CASB, the company can monitor and enforce them across multiple CSPs, and identify any gaps or risks in their cloud security.

NEW QUESTION 171
The IT department is concerned about the possibility of a guest device infecting machines on the corporate network or taking down the company's singe internet connection. Which of the following should a security analyst recommend to BEST meet the requirements outlined by the IT Department?

A. Require the guest machines to install the corporate-owned EDR solution.
B. Configure NAC to only allow machines on the network that are patched and have active antivirus.
C. Place a firewall In between the corporate network and the guest network
D. Configure the IPS with rules that will detect common malware signatures traveling from the guest network.

Answer: C

Explanation:
A firewall is a device or software that monitors and controls incoming and outgoing network traffic based on predefined rules or policies. A firewall can help prevent unauthorized or malicious traffic from entering or leaving a network, and protect network resources from external threats. Placing a firewall in between the corporate network and the guest network can help prevent a guest device from infecting machines on the corporate network or taking down the company's single internet connection, as it can block or filter any unwanted or harmful traffic from the guest network.

NEW QUESTION 172
A company offers a hardware security appliance to customers that provides remote administration of a device on the customer's network Customers are not authorized to alter the configuration The company deployed a software process to manage unauthorized changes to the appliance log them, and forward them to a central repository for evaluation Which of the following processes is the company using to ensure the appliance is not altered from its ongmal configured state?

A. CI/CD
B. Software assurance
C. Anti-tamper
D. Change management

Answer: C

Explanation:
Anti-tamper is a process that protects a system or device from unauthorized changes or modifications. It can also log and report any attempts to alter the system or device. The company is using anti-tamper to ensure the appliance is not altered from its original configured state. CI/CD, software assurance, and change management are not processes that specifically deal with unauthorized changes. Reference: https://www.acq.osd.mil/se/briefs/16943-DoD-AT-Overview-Brief.pdf

NEW QUESTION 177
A security analyst is designing firewall rules to prevent external IP spoofing Which of the following explains the firewall rule for mitigation?

A. Packets with external source IP addresses do not enter the network from either direction.
B. Packets with internal source IP addresses do not enter the network from the outside.
C. Packets with internal source IP addresses do not exit the network from the inside.
D. Packets with public IP addresses do not pass through the router in either direction.

Answer: B

Explanation:
Packets with internal source IP addresses do not enter the network from the outside. This firewall rule can prevent external IP spoofing, which is an attack technique that involves forging the source IP address of a packet to impersonate another host or network. By blocking packets with internal source IP addresses from entering the network from the outside, the firewall can filter out spoofed packets that claim to originate from the internal network.

NEW QUESTION 178
Members of the sales team are using email to send sensitive client lists with contact information to their personal accounts The company's AUP and code of conduct prohibits this practice. Which of the following configuration changes would improve security and help prevent this from occurring?

A. Configure the DLP transport rules to provide deep content analysis.
B. Put employees' personal email accounts on the mail server on a blocklist.
C. Set up IPS to scan for outbound emails containing names and contact information.
D. Use Group Policy to prevent users from copying and pasting information into emails.
E. Move outbound emails containing names and contact information to a sandbox for further examination.

Answer: A

Explanation:
Data loss prevention (DLP) is a set of policies and tools that aim to prevent unauthorized disclosure of sensitive data. DLP transport rules are rules that apply to email messages that are sent or received by an organization’s mail server. These rules can provide deep content analysis, which means they can scan the content of email messages and attachments for sensitive data patterns, such as client lists or contact information. If a rule detects a violation of the DLP policy, it can take actions such as blocking, quarantining, or notifying the sender or recipient. This would improve security and help prevent sales team members from sending sensitive client lists to their personal accounts. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 14; https://docs.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/data-loss-prevention

NEW QUESTION 179
A company's legal department is concerned that its incident response plan does not cover the countless ways security incidents can occur. The department has 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 have a high chance of reputation harm.
B. Focus on common attack vectors first.
C. Focus on incidents that affect critical systems.
D. Focus on incidents that may require law enforcement support.

Answer: C

Explanation:
An incident response plan should cover the most important and likely scenarios that could compromise the security and operations of an organization. According to various sources of best practice1s23, an incident response plan should start by conducting a risk assessment to identify potential threats and vulnerabilities, and prioritize the critical systems that need to be protected and restored in case of an incident. Focusing on incidents that affect critical systems ensures that the incident response plan covers the most severe and impactful situations that could harm the organization’s mission, reputation, or legal obligations.

NEW QUESTION 181
Which of the following would best protect sensitive data If a device is stolen?

A. Remote wipe of drive
B. Self-encrypting drive
C. Password-protected hard drive
D. Bus encryption

Answer: B

Explanation:
A self-encrypting drive is a type of hard drive that automatically encrypts and decrypts data using a hardware-based mechanism. A self-encrypting drive can best protect sensitive data if a device is stolen, because it prevents unauthorized access to the data without the proper encryption key or password.

NEW QUESTION 183
Which of the following is the primary reason financial institutions may share up-to-date threat intelligence information on a secure feed that is dedicated to their sector?

A. To augment information about common malicious actors and indicators of compromise
B. To prevent malicious actors from knowing they can defend against malicious attacks

C. To keep other industries from accessing information meant for financial institutions
D. To focus on attacks specifically targeted at their customers' mobile applications

Answer: A

Explanation:
This is the primary reason why financial institutions may share up-to-date threat intelligence information on a secure feed that is dedicated to their sector. Threat intelligence is the collection, analysis, and dissemination of information about current or potential threats to an organization's assets, operations, or reputation. By sharing threat intelligence information, financial institutions can benefit from the collective knowledge, experience, and capabilities of their peers and partners, and enhance their situational awareness, threat detection, and incident response. Sharing threat intelligence information can also help financial institutions identify common attack patterns, trends, and techniques, as well as the malicious actors and indicators of compromise (IOCs) associated with them. IOCs are pieces of forensic data that can be used to identify potentially malicious activities or intrusions on a network or system, such as IP addresses, domains, URLs, file hashes, or email addresses

NEW QUESTION 187
Which of the following software assessment methods world peak times?

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

Answer: B

Explanation:
Stress testing is a software assessment method that tests how an application performs under peak times or extreme workloads. Stress testing can help to identify any performance issues, bottlenecks, errors or crashes that may occur when an application faces high demand or concurrent users. Stress testing can also help to determine the maximum capacity and scalability of an application .

NEW QUESTION 188
Several operator workstations are exhibiting unusual behavior, including applications loading slowly, temporary files being overwritten, and reboot notifications to apply antivirus signatures. During an investigation, an analyst finds evidence of Bitcoin mining. Which of the following is the first step the analyst should take to prevent further spread of the mining operation?

A. Reboot each host that is exhibiting the behaviors.
B. Enable the host-based firewalls to prevent further activity.
C. Quarantine all the impacted hosts for forensic analysis.
D. Notify users to turn off all affected devices.

Answer: C

Explanation:
The first step the analyst should take to prevent further spread of the mining operation is to quarantine all the impacted hosts for forensic analysis. Quarantining the hosts can help isolate them from the network, and prevent them from communicating with other devices or servers that may be part of the mining operation. Forensic analysis can help identify the source and scope of the infection, and provide clues for remediation and recovery.

NEW QUESTION 191
Wncn ol the following provides an automated approach 10 checking a system configuration?

A. SCAP
B. CI/CD
C. OVAL
D. Scripting
E. SOAR

Answer: A

Explanation:
SCAP stands for Security Content Automation Protocol, which is a set of standards and specifications that allows automated configuration and vulnerability management of systems. SCAP provides an automated approach to checking a system configuration by using standardized expressions and formats to evaluate the system's compliance with predefined policies or benchmarks. CI/CD, OVAL, scripting, or SOAR are other terms related to automation or security, but they do not provide an automated approach to checking a system configuration. Reference: https://csrc.nist.gov/projects/security-content-automation-protocol

NEW QUESTION 193
An analyst is coordinating with the management team and collecting several terabytes of data to analyze using advanced mathematical techniques in order to find patterns and correlations in events and activities. Which of the following describes what the analyst is doing?

A. Data visualization
B. SOAR
C. Machine learning
D. SCAP

Answer: C

Explanation:
The correct answer is C. Machine learning. Machine learning is a branch of artificial intelligence that uses advanced mathematical techniques, such as statistics, algorithms, and linear algebra, to analyze large amounts of data and find patterns and correlations in events and activities. Machine learning can help to automate

tasks, improve decision making, and enhance security by detecting anomalies, threats, or trends1.
* A. Data visualization is not correct. Data visualization is the process of presenting data in a graphical or pictorial format, such as charts, graphs, maps, or dashboards. Data visualization can help to communicate information, insights, or trends more effectively and intuitively than using text or numbers alone2.
* B. SOAR is not correct. SOAR stands for Security Orchestration, Automation, and Response, and it is a solution that combines various tools and processes to improve the efficiency and effectiveness of security operations. SOAR can help to automate tasks, integrate systems, coordinate actions, and respond to incidents faster and more consistently3.
* D. SCAP is not correct. SCAP stands for Security Content Automation Protocol, and it is a set of standards and specifications that enable the automated assessment, measurement, and reporting of the security posture of systems and networks. SCAP can help to ensure compliance, identify vulnerabilities, and remediate issues.
* 1: What Is Machine Learning? 2: What Is Data Visualization? 3: What Is Security Orchestration, Auto and Response (SOAR)? : [What Is Security Content Automation Protocol (SCAP)?]

NEW QUESTION 196
Which of the following is the most important reason to involve the human resources department in incident response?

A. To better Inform recruiters during hiring so they can include incident response Interview questions
B. To ensure the incident response process captures evidence needed in case of disciplinary actions
C. To validate that the incident response process meets the organization's best practices
D. To prevent Incident responders from Interacting directly with any users

Answer: B

Explanation:
The human resources department should be involved in incident response, to ensure that the incident response process captures evidence needed in case of disciplinary actions against any employees who may have caused or contributed to the incident, either intentionally or unintentionally. The human resources department can also help with enforcing policies and procedures, communicating with employees, and providing legal or ethical guidance.

NEW QUESTION 197
Which of the following are important reasons for performing proactive threat-hunting activities7 (Select two).

A. To ensure all alerts are fully investigated
B. To test incident response capabilities
C. To uncover unknown threats
D. To allow alerting rules to be more specific
E. To create a new security baseline
F. To improve user awareness about security threats

Answer: CE

Explanation:
Proactive threat-hunting is the process of actively searching for unknown threats in the network, rather than waiting for alerts or indicators of compromise. Some of the important reasons for performing proactive
threat-hunting activities are:
- To uncover unknown threats that may have evaded detection by existing security tools or controls, and to mitigate them before they cause damage or data loss.
- To create a new security baseline that reflects the current state of the network, and to identify any anomalies or deviations from the normal behavior or activity.

NEW QUESTION 202
An analyst Is reviewing a web developer's workstation for potential compromise. While examining the workstation's hosts file, the analyst observes the following:

```
192.168.3.249    localhost
127.0.0.1        sitedev.local
::1              localhost ip6-localhost ip6-
                 loopback
198.51.100.5     comptia.co
```

Which of the following hosts file entries should the analyst use for further investigation?

A. ::1
B. 127.0.0.1
C. 192.168.3.249
D. 198.51.100.5

Answer: D

Explanation:
The hosts file is a text file that maps hostnames to IP addresses, and it can be used to override DNS resolution. The hosts file entries that should be used for further investigation are the ones that point to external or suspicious IP addresses, such as 198.51.100.5, which is a reserved IP address for documentation purposes. The other entries are either loopback addresses (::1 and 127.0.0.1) or internal network addresses (192.168.3.249), which are less likely to be malicious.

NEW QUESTION 207
A security analyst is performing a Diamond Model analysis of an incident the company had last quarter. A potential benefit of this activity is that it can identify:

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

Answer: A

Explanation:
A Diamond Model analysis of an incident is a framework that identifies the four essential features of an attack: adversary, capability, infrastructure, and victim1
By analyzing these features and their relationships, a security
analyst can gain insights into the attack's objectives, methods, sources, and targets. A potential benefit of this activity is that it can identify detection and prevention capabilities to improve, such as gaps in security
controls, indicators of compromise, or mitigation strategies2
References: 1
What is the Diamond Model of Intrusion Analysis2? How to use the MITRE ATT&CK®
framework and diamond model of intrusion analysis together

NEW QUESTION 209
A security analyst is evaluating the following support ticket:
Issue: Marketing campaigns are being filtered by the customer's email servers.
Description: Our marketing partner cannot send emails using our email address. The following log messages were collected from multiple customers:
• The SPF result is PermError.
• The SPF result is SoftFail or Fail.
• The 550 SPF check failed.
Which of the following should the analyst do next?

A. Ask the marketing partner's ISP to disable the DKIM setting.
B. Request approval to disable DMARC on the company's ISP.
C. Ask the customers to disable SPF validation.
D. Request a configuration change on the company's public DNS.

Answer: D

Explanation:
The analyst should request a configuration change on the company's public DNS as the next step, as this can help resolve the issue of marketing campaigns being filtered by the customer's email servers. The issue is caused by SPF validation failures, which indicate that the marketing partner's email address is not authorized to send emails on behalf of the company's domain. SPF stands for Sender Policy Framework, and it is a mechanism that allows domain owners to specify which IP addresses or hosts are allowed to send emails using their domain name. SPF validation is done by checking the SPF record of the sender's domain in the public DNS, and comparing it with the IP address or host name of the sender's email server. To fix this issue, the analyst should request a configuration change on the company's public DNS to add or update the SPF record to include the marketing partner's email address or IP address as a valid sender.

NEW QUESTION 211
A security analyst is attempting to resolve an incident in which highly confidential company pricing information was sent to clients. It appears this information was unintentionally sent by an employee who attached it to public marketing material. Which of the following configuration changes would work BEST to limit the risk of this incident being repeated?

A. Add client addresses to the blocklist.
B. Update the DLP rules and metadata.
C. Sanitize the marketing material.
D. Update the insider threat procedures.

Answer: B

Explanation:
Data Loss Prevention (DLP) is a security technology designed to detect, prevent, and respond to the unauthorized disclosure of confidential data. By updating the DLP rules and metadata, it is possible to better define what types of confidential information can be shared and limit access to any sensitive documents.
DLP rules and metadata can help to identify, classify and label sensitive data based on its content and context. DLP rules and metadata can also help to enforce actions or policies on sensitive data, such as blocking, encrypting or alerting .

NEW QUESTION 214
During routine monitoring a security analyst identified the following enterpnse network traffic: Packet capture output:

No.	Source	Destination	Protocol	Info
105	66.187.224.210	192.168.12.21	DNS	Standard query response A 209.132.177.50
106	192.168.12.21	209.132.177.50	TCP	48890 > http [SYN] Seq=0 len=0 MSS=1460 TSV=1535
107	209.132.177.50	192.168.12.21	TCP	http > 48890 [SYN, ACK] Seq=0 Ack=1 Win=5792 len=0
108	192.168.12.21	209.132.177.50	TCP	48890 > http [ACK] Seq=1 Ack=1 len=0
109	192.168.12.21	209.132.177.50	HTTP	GET / HTTP/1.1

Which of the following BEST describes what the security analyst observed?

A. 66.187.224.210 set up a DNS hijack with 192.168.12.21.
B. 192.168.12.21 made a TCP connection to 66 187 224 210
C. 192.168.12.21 made a TCP connection to 209 132 177 50
D. 209.132.177.50 set up a TCP reset attack to 192 168 12 21

Answer: C

Explanation:

The security analyst observed that 192.168.12.21 made a TCP connection to 209.132.177.50. This can be inferred from the packet capture output, which shows the following sequence of packets:

- Packet 1: A SYN packet from 192.168.12.21 to 209.132.177.50 on port 80 (HTTP). This is the first step of the TCP three-way handshake, where the source initiates a connection request to the destination.
- Packet 2: A SYN-ACK packet from 209.132.177.50 to 192.168.12.21 on port 80 (HTTP). This is the second step of the TCP three-way handshake, where the destination acknowledges and accepts the connection request from the source.
- Packet 3: An ACK packet from 192.168.12.21 to 209.132.177.50 on port 80 (HTTP). This is the third and final step of the TCP three-way handshake, where the source confirms and completes the connection establishment with the destination.

These packets indicate that a TCP connection was successfully established between 192.168.12.21 and 209.132.177.50 on port 80.

NEW QUESTION 216
During a routine security review, anomalous traffic from 9.9.9.9 was observed accessing a web server in the corporate perimeter network. The server is mission critical and must remain accessible around the world to serve web content. The Chief Information Security Officer has directed that improper traffic must be restricted. The following output is from the web server:

```
netstat -an

Active Connections
Proto          Local address      Foreign address    State
TCP            0.0.0.0:135        0.0.0.0:0          LISTENING
TCP            0.0.0.0:445        0.0.0.0:0          LISTENING
TCP            0.0.0.0:80         0.0.0.0:0          LISTENING
TCP            0.0.0.0:443        0.0.0.0:0          LISTENING
TCP            10.0.1.5:445       9.9.9.9:44251      ESTABLISHED
TCP            10.0.1.5.443       9.9.9.9:44252      ESTABLISHED
TCP            10.0.1.5:135       10.0.1.20:53243    ESTABLISHED
```

Which of the following is the best method to accomplish this task?

A. Adjusting the IDS to block anomalous activity
B. Implementing port security
C. Adding 9.9.9.9 to the blocklist
D. Adjusting the firewall

Answer: D

Explanation:
Based on the output of the “netstat -an” command, it seems that the web server is listening on port 80 for HTTP traffic and port 443 for HTTPS traffic. The anomalous traffic from 9.9.9.9 is accessing the web server on port 443, which means it is using a secure connection.
The best method to accomplish the task of restricting improper traffic from 9.9.9.9 is D. Adjusting the firewall. A firewall is a device or software that controls the flow of network traffic based on predefined rules. By adjusting the firewall rules, you can block or allow specific IP addresses, ports, protocols, or domains from accessing your web server.

NEW QUESTION 221
During a company’s most recent incident, a vulnerability in custom software was exploited on an externally facing server by an APT. The lessons-learned report noted the following:
• The development team used a new software language that was not supported by the security team's automated assessment tools.
• During the deployment, the security assessment team was unfamiliar with the new language and struggled to evaluate the software during advanced testing. Therefore, the vulnerability was not detected.
• The current IPS did not have effective signatures and policies in place to detect and prevent runtime attacks on the new application.
To allow this new technology to be deployed securely going forward, which of the following will BEST address these findings? (Choose two.)

A. Train the security assessment team to evaluate the new language and verify that best practices for secure coding have been followed
B. Work with the automated assessment-tool vendor to add support for the new language so these vulnerabilities are discovered automatically
C. Contact the human resources department to hire new security team members who are already familiar with the new language
D. Run the software on isolated systems so when they are compromised, the attacker cannot pivot to adjacent systems
E. Instruct only the development team to document the remediation steps for this vulnerability
F. Outsource development and hosting of the applications in the new language to a third-party vendor so the risk is transferred to that provider

Answer: AB

Explanation:
The solution will address the findings that the development team used a new software language that was not supported by the security team's automated assessment tools and the security assessment team was unfamiliar with the new language and struggled to evaluate the software during advanced testing. The training of the security assessment team and working with the automated assessment-tool vendor to add support for the new language will ensure that future deployments of the new technology are secure and the vulnerabilities are detected and prevented.

NEW QUESTION 222
Which of the following is the software development process by which function, usability, and scenarios are tested against a known set of base requirements?

A. Security regression testing
B. Code review
C. User acceptance testing

D. Stress testing

Answer: C

Explanation:
"User acceptance testing (UAT) is the last phase of the software testing process. During UAT, actual software users test the software to make sure it can handle required tasks in real-world scenarios, according to specifications." https://www.plutora.com/blog/uat-user-acceptance-testing
User acceptance testing is the software development process by which function, usability, and scenarios are tested against a known set of base requirements. User acceptance testing (UAT) is the final stage of software development before production. It is used to get feedback from users who test the software and its user interface (UI). UAT is usually done manually, with users creating real-world situations and testing how the software reacts and performs. UAT is used to determine if end-users accept software before it's made public. Client or business requirements determine whether it fulfills the expectations originally set in its development2.

NEW QUESTION 226
Due to continued support of legacy applications, an organization's enterprise password complexity rules are inadequate for its required security posture. Which of the following is the BEST compensating control to help reduce authentication compromises?

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

Answer: B

Explanation:
Multifactor authentication is a method of verifying a user's identity by requiring two or more pieces of evidence, such as something the user knows (e.g., password), something the user has (e.g., token), or something the user is (e.g., fingerprint). Multifactor authentication is the best compensating control to help reduce authentication compromises when the organization's enterprise password complexity rules are inadequate for its required security posture. Smart cards, biometrics, or increased password-rotation frequency are other possible controls, but they are not as effective or comprehensive as multifactor authentication.
Reference:
https://www.csoonline.com/article/3239144/what-is-multifactor-authentication-mfa-how-it-works-and-why-you

NEW QUESTION 230
Data sovereignty - Wikipedi2a What Is Data Sovereignty? Everything You Need to Know - What is data sovereignty?
Which of the following is the BEST way to gather patch information on a specific server?

A. Event Viewer
B. Custom script
C. SCAP software
D. CI/CD

Answer: B

Explanation:
A custom script is a piece of code that can be written to perform a specific task or automate a process. A custom script can be used to gather patch information on a specific server by querying the server's operating system, registry, or patch management software and retrieving the relevant data. A custom script can be more flexible and efficient than other methods, such as Event Viewer, SCAP software, or CI/CD, which may not provide the exact information needed or may require additional steps or tools.

NEW QUESTION 234
Which of the following, BEST explains the function of TPM?

A. To provide hardware-based security features using unique keys
B. To ensure platform confidentiality by storing security measurements
C. To improve management of the OS installation.
D. To implement encryption algorithms for hard drives

Answer: A

Explanation:
TPM (Trusted Platform Module) is a hardware chip that provides security features using unique keys2. TPM can store cryptographic keys that are used for encryption, authentication, digital signatures, and other security functions. TPM can also generate random keys that are unique to each device and never leave the chip. TPM can protect these keys from unauthorized access or tampering by using hardware isolation and encryption3. TPM can also measure and verify the integrity of the operating system and firmware on a device by using a process called attestation. TPM does not ensure platform confidentiality by storing security measurements (B), as security measurements are used for attestation, not confidentiality. TPM does not improve management of OS installation ©, as OS installation is not directly related to TPM functionality. TPM does not implement encryption algorithms for hard drives (D), as encryption algorithms are implemented by software such as BitLocker, which can use TPM keys for encryption.
References: 2:
https://support.microsoft.com/en-us/topic/what-is-tpm-705f241d-025d-4470-80c5-4feeb24fa1ee 3: https://www.techopedia.com/definition/24771/technical-controls : https://www.techopedia.com/definition/25888/security-development-lifecycle-sdl

NEW QUESTION 235
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

Explanation:
Data enrichment is the result that the security team hopes to accomplish by adding these sources to the SIEM. Data enrichment is a process that enhances, refines, or otherwise improves raw data by adding context, meaning, or value to it. Data enrichment can help security analysts gain more insights from the events processed by the SIEM, such as identifying the root cause, severity, or impact of an incident3. Data enrichment can also help security analysts correlate events from different sources and reduce false positives or negatives.

NEW QUESTION 239
A company wants to ensure confidential data from its storage media files is sanitized so the drives cannot oe reused. Which of the following is the BEST approach?

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

Answer: B

Explanation:
https://legalshred.com/degaussing-vs-hard-drive-shredding/
The best and most secure method of rendering hard drive information completely unusable is to completely destroy it through hard drive shredding
Shredding is a method of physically destroying storage media files by cutting them into small pieces using a machine called a shredder. Shredding can ensure that confidential data from storage media files is sanitized so the drives cannot be reused, as it makes it impossible to recover any data from the shredded pieces.

NEW QUESTION 240
After examine a header and footer file, a security analyst begins reconstructing files by scanning the raw data bytes of a hard disk and rebuilding them. Which of the following techniques is the analyst using?

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

Answer: B

Explanation:
Three common types of file carving methods are as follows: Header- and footer-based carving, which focuses on headers like those found in JPEG files. For example, JPEGs can be found by looking for \xFF\xD8 in the header and \xFF\xD9 in the footer. Content-based carving techniques look for information about the content of a file such as character counts and text recognition. File structure-based carving techniques that use information about the structure of files.
File carving is a technique for recovering files from raw data bytes by scanning and rebuilding them based on their file headers and footers. File headers and footers are sequences of bytes that indicate the beginning and end of a file format, such as JPEG, PDF, ZIP, etc. File carving can be used to reconstruct files that are deleted, corrupted, fragmented, or encrypted by bypassing the file system structure and looking for recognizable patterns in the data3
The analyst used file carving to reconstruct files from a hard disk by scanning the raw
data bytes and rebuilding them based on their file headers and footers.

NEW QUESTION 241
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: C

Explanation:
Ransomware is a type of malware that encrypts the files or disks of a victim’s device and demands a ransom for the decryption key. Ransomware can cause significant damage, disruption, and data loss for individuals and organizations. To prevent this type of incident in the future, the best strategy is to combine user education and data protection. A ransomware awareness program can help users recognize and avoid potential ransomware attacks, such as phishing emails, malicious attachments, or compromised websites. A secure and verifiable backup system can help users recover their data in case of a ransomware infection, without paying the ransom or relying on the attackers. A backup system should be regularly tested and updated, and stored offline or in a separate location from the original data.

NEW QUESTION 244
A company has a cluster of web servers that is critical to the business. A systems administrator installed a utility to troubleshoot an issue, and the utility caused the entire cluster to 90 offline. Which of the following solutions would work BEST prevent to this from happening again?

A. Change management
B. Application whitelisting
C. Asset management
D. Privilege management

Answer: A

Explanation:

Change Management
o The process through which changes to the configuration of information systems are monitored and controlled, as part of the organization's overall configuration management efforts
o Each individual component should have a separate document or database record that describes its initial state and subsequent changes
Configuration information Patches installed
Backup records Incident reports/issues
o Change management ensures all changes are planned and controlled to minimize risk of a service disruption
Change management is a process that ensures changes to systems or processes are introduced in a controlled and coordinated manner. Change management helps to minimize the impact of changes on the business operations and avoid unintended consequences or errors3
Change management can help prevent the issue of utility installation affecting the web server cluster by ensuring that the utility is properly planned, tested, approved, documented, communicated, and monitored.

NEW QUESTION 248
A security analyst is investigating an active threat of the system memory. While narrowing down the source of the threat, the analyst is inspecting all processes to isolate suspicious activity Which of the following techniques is the analyst using?

A. Live forensics
B. Logical acquisition
C. Timeline analysis
D. Static acquisition

Answer: A

Explanation:
Live forensics is a technique that involves investigating an active threat on a system without shutting it down or altering its state, by using tools such as memory dumpers, process explorers, registry editors, or network analyzers. Live forensics can help preserve volatile data that may be lost if the system is powered off or rebooted, such as system memory, network connections, running processes, etc. Live forensics can also help identify and stop malicious activities in real time.

NEW QUESTION 250
The help desk is having difficulty keeping up with all onboarding and offboarding requests. Managers often submit, requests for new users at the last minute. causing the help desk to scramble to create accounts across many different Interconnected systems. Which of the following solutions would work BEST to assist the help desk with the onboarding and offboarding process while protecting the company's assets?

A. MFA
B. CASB
C. SSO
D. RBAC

Answer: D

Explanation:
RBAC (Role-Based Access Control) is a solution that would work best to assist the help desk with the onboarding and offboarding process while protecting the company’s assets. RBAC is a method of granting access to resources based on the roles of users within an organization. RBAC simplifies the management of user permissions by assigning predefined roles to users based on their job functions, rather than granting individual permissions to each user. RBAC can help automate the onboarding and offboarding process by enabling the help desk to quickly create or delete user accounts and assign or revoke access rights based on the roles of the users1. RBAC can also help protect the company’s assets by enforcing the principle of least privilege, which means that users only have access to the resources they need to perform their duties and nothing more2.

NEW QUESTION 252
.....

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

CS0-002 Practice Exam Features:

* CS0-002 Questions and Answers Updated Frequently

* CS0-002 Practice Questions Verified by Expert Senior Certified Staff

* CS0-002 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CS0-002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year