CompTIA

Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

NEW QUESTION 1
In SIEM software, a security analysis selected some changes to hash signatures from monitored files during the night followed by SMB brute-force attacks against the file servers Based on this behavior, which of the following actions should be taken FIRST to prevent a more serious compromise?

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

Answer: C

Explanation:
The first action that should be taken to prevent a more serious compromise is to check the hash signatures, comparing them with malware databases to verify if the files are infected. This will help to determine if the changes to hash signatures were caused by malicious software or legitimate updates. If the files are infected, they should be quarantined and removed from the network. Checking the hash signatures will also help to identify the type and source of the malware, which can inform further actions such as blocking malicious domains or IPs, updating antivirus signatures, or notifying users3.

NEW QUESTION 2
An IT security analyst has received an email alert regarding a vulnerability within the new fleet of vehicles the company recently purchased. Which of the following attack vectors is the vulnerability MOST likely targeting?

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

Answer: B

Explanation:
The Controller Area Network - CAN bus is a message-based protocol designed to allow the Electronic Control Units (ECUs) found in today's automobiles, as well as other devices, to communicate with each other in a reliable, priority-driven fashion. Messages or "frames" are received by all devices in the network, which does not require a host computer.
CAN bus stands for Controller Area Network bus, which is a communication protocol that allows different devices and components in a vehicle to communicate and exchange data. The vulnerability within the new fleet of vehicles is most likely targeting the CAN bus, because it could allow an attacker to manipulate or disrupt the operation of the vehicle. SCADA, Modbus, and IoT are other terms related to communication protocols or systems, but they are not specific to vehicles.
Reference: https://www.csoonline.com/article/3218104/what-is-a-can-bus-and-how-can-it-be-hacked.html

NEW QUESTION 3
Which of the following is a vulnerability associated with the Modbus protocol?

A. Weak encryption
B. Denial of service
C. Unchecked user input
D. Lack of authentication

Answer: D

Explanation:
Modbus is a communication protocol that is widely used in industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems. However, Modbus was not designed to provide security and it is vulnerable to various cyberattacks. One of the main vulnerabilities of Modbus is the lack of authentication, which means that any device on the network can send or receive commands without verifying its identity or authority. This can lead to unauthorized access, data manipulation, or denial of service attacks on the ICS or SCADA system.
Some examples of attacks that exploit the lack of authentication in Modbus are:

- Detection attack: An attacker can scan the network and discover the devices and their addresses, functions, and registers by sending Modbus requests and observing the responses. This can reveal sensitive information about the system configuration and operation1.
- Command injection attack: An attacker can send malicious commands to the devices and modify their settings, values, or outputs. For example, an attacker can change the speed of a motor, open or close a valve, or turn off a switch23.
- Response injection attack: An attacker can intercept and alter the responses from the devices and deceive the master or other devices about the true state of the system. For example, an attacker can fake a normal response when there is an error or an alarm23.
- Denial of service attack: An attacker can flood the network with Modbus requests or commands and overload the devices or the communication channel. This can prevent legitimate requests or commands from being processed and disrupt the normal operation of the system14.

To mitigate these attacks, some security measures that can be applied to Modbus are:

- Encryption: Encrypting the Modbus messages can prevent eavesdropping and tampering by unauthorized parties. However, encryption can also introduce additional overhead and latency to the communication56.
- Authentication: Adding authentication mechanisms to Modbus can ensure that only authorized devices can send or receive commands. Authentication can be based on passwords, certificates, tokens, or other methods56.
- Firewall: Installing a firewall between the Modbus network and other networks can filter out unwanted traffic and block unauthorized access. A firewall can also enforce rules and policies for Modbus communication24.
- Intrusion detection system: Deploying an intrusion detection system (IDS) on the Modbus network can monitor the traffic and detect anomalous or malicious activities. An IDS can also alert the operators or trigger countermeasures when an attack is detected24.

NEW QUESTION 4
A Chief Information Officer wants to implement a BYOD strategy for all company laptops and mobile phones. The Chief Information Security Officer is concerned with ensuring all devices are patched and running some sort of protection against malicious software. Which of the following existing technical controls should a security analyst recommend to best meet all the requirements?

A. EDR
B. Port security
C. NAC
D. Segmentation

Answer: A

Explanation:
EDR stands for endpoint detection and response, which is a type of security solution that monitors and protects all devices that are connected to a network, such as laptops and mobile phones. EDR can help to ensure that all devices are patched and running some sort of protection against malicious software by providing continuous visibility, threat detection, incident response, and remediation capabilities. EDR can also help to enforce security policies and compliance requirements across all devices .

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.

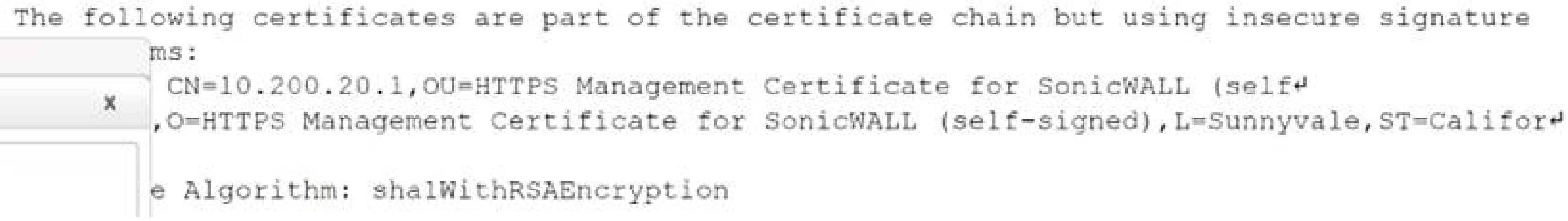
NEW QUESTION 6
Which of the following BEST identifies the appropriate use of threat intelligence as a function of detection and response?

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

Answer: B

Explanation:
Threat intelligence can be used to identify likely attack scenarios within an organization based on the organization's specific vulnerabilities, assets, and threat landscape. Threat intelligence can help security teams anticipate and prepare for potential attacks, as well as detect and respond to ongoing attacks more effectively1. Threat intelligence can also provide insights into the threat actors, their motivations, and their tactics, techniques, and procedures (TTPs)2.

NEW QUESTION 7
While reviewing a vulnerability assessment, an analyst notices the following issue is identified in the report: this finding, which of the following would be most appropriate for the analyst to recommend to the network engineer?



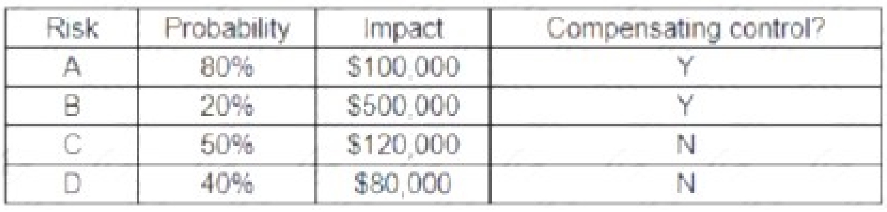
```
The following certificates are part of the certificate chain but using insecure signature
ms:
 CN=10.200.20.1,OU=HTTPS Management Certificate for SonicWALL (self↵
,O=HTTPS Management Certificate for SonicWALL (self-signed),L=Sunnyvale,ST=Califor↵

e Algorithm: shalWithRSAEncryption
```

A. Reconfigure the device to support only connections leveraging TLSv1.2.
B. Obtain a new self-signed certificate and select AES as the hashing algorithm.
C. Replace the existing certificate with a certificate that uses only MD5 for signing.
D. Use only signed certificates with cryptographically secure certificate sources.

Answer: A

Explanation:
The vulnerability assessment report shows that the device is using SSLv3, which is an outdated and insecure protocol for secure communication over a network. SSLv3 has several known vulnerabilities, such as POODLE, that allow attackers to decrypt or modify the encrypted data. To remediate this issue, the analyst should recommend reconfiguring the device to support only connections leveraging TLSv1.2, which is a newer and more secure protocol that provides stronger encryption, authentication, and integrity protection for the data transmitted over the network.

NEW QUESTION 8
An organization has the following risk mitigation policies
• Risks without compensating controls will be mitigated first it the nsk value is greater than $50,000
• Other nsk mitigation will be pnontized based on risk value. The following risks have been identified:



Risk	Probability	Impact	Compensating control?
A	80%	$100,000	Y
B	20%	$500,000	Y
C	50%	$120,000	N
D	40%	$80,000	N

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

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

Answer: C

Explanation:
The order of priority for risk mitigation from highest to lowest is C, B, A, D. This order is based on applying the risk mitigation policies of the organization. According to the first policy, risks without compensating controls will be mitigated first if the risk value is greater than $50,000. Risk C has no compensating controls and a risk value of $75,000, so it is the highest priority. Risk B also has no compensating controls, but a risk value of $40,000, so it is the second priority. According to the second policy, other risk mitigation will be prioritized based on risk value. Risk A has a risk value of $60,000 and a compensating control of encryption, so it is the third priority. Risk D has a risk value of $50,000 and a compensating control of backup power supply, so it is the lowest priority.

NEW QUESTION 9
An analyst is working on a method to allow secure access to a highly sensi-tive server. The solution must allow named individuals remote access to data contained on the box and must limit access to a single IP address. Which of the following solutions would best meet these requirements?

A. Jump box
B. Software-defined networking
C. VLAN
D. ACL

Answer: A

Explanation:
A jump box is a secure computer that can be used to access a remote server or network. It acts as an intermediary between the user and the target system, and can limit access to specific IP addresses. A jump box can also provide logging and auditing of the user's actions on the remote system. A jump box is a common solution for accessing highly sensitive servers or networks1.

NEW QUESTION 10
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 10
Which of the following is MOST important when developing a threat hunting program?

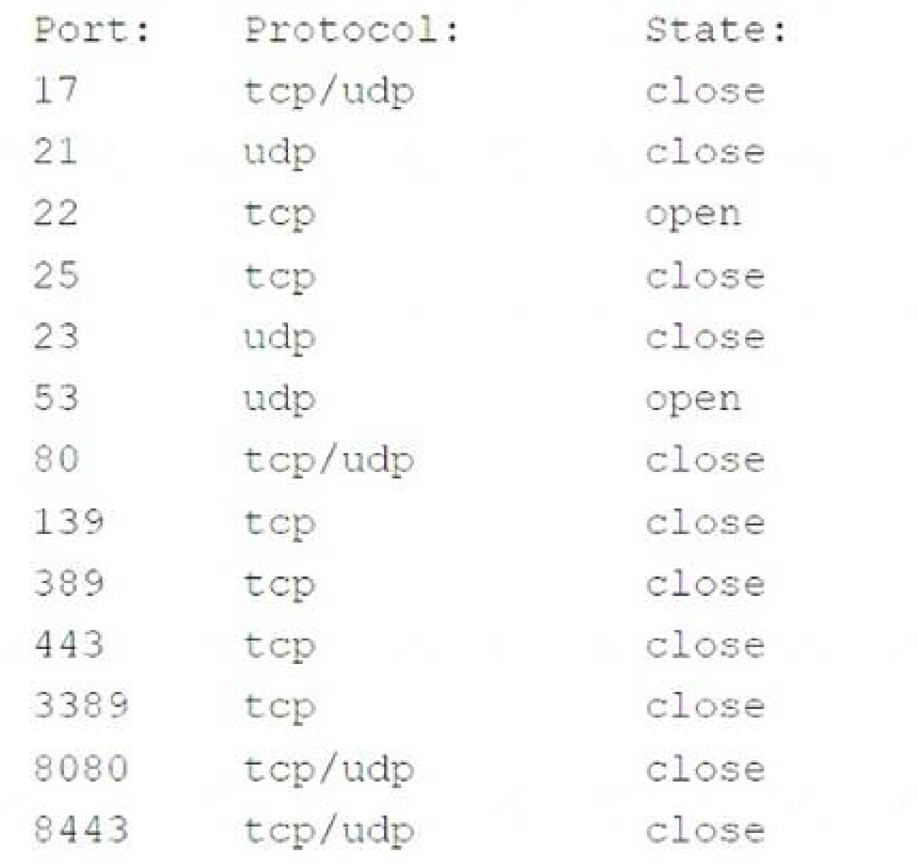
A. Understanding penetration testing techniques
B. Understanding how to build correlation rules within a SIEM
C. Understanding security software technologies
D. Understanding assets and categories of assets

Answer: D

Explanation:
Understanding assets and categories of assets is most important when developing a threat hunting program. Assets are anything that have value to an organization, such as data, systems, networks, applications, devices, people, processes, or reputation. Categories of assets are groups of assets that share common characteristics or attributes, such as type, function, location, owner, or criticality. Understanding assets and categories of assets can help to identify and prioritize the potential targets and impact of threats in an organization. Understanding assets and categories of assets can also help to determine and apply appropriate security controls and measures for each asset or category. Understanding assets and categories of assets can also help to collect and analyze

relevant data and indicators for each asset or category during threat hunting activities. Understanding penetration testing techniques (A) is not most important when developing a threat hunting program. Penetration testing techniques are methods or tools that are used to simulate attacks on a system or network to evaluate its security posture and identify vulnerabilities or weaknesses. Penetration testing techniques can help to validate and improve the security of an organization, but they are not directly related to threat hunting activities. Penetration testing techniques are reactive rather than proactive approaches to security. Understanding how to build correlation rules within a SIEM (B) is also not most important when developing a threat hunting program. Correlation rules are logic statements that define relationships or patterns between different events or data points in a system or network. A SIEM (Security Information and Event Management) is a software solution that collects, analyzes, and correlates data from various sources in an organization to provide security monitoring and alerting capabilities1. Correlation rules can help to detect and respond to known threats in an organization, but they are not sufficient for threat hunting activities. Correlation rules are based on predefined criteria rather than hypotheses or assumptions about unknown threats. Understanding security software technologies © is also not most important when developing a threat hunting program. Security software technologies are applications or programs that provide security functions or features for an organization, such as antivirus software, firewalls, encryption software, VPNs (Virtual Private Networks), etc2. Security software technologies can help to protect an organization from various threats, but they are not essential for threat hunting activities. Security software technologies are based on signatures or heuristics rather than indicators of compromise or behavioral analysis.
References: 1: https://www.techopedia.com/definition/24771/technical-controls 2: https://www.techopedia.com/definition/25888/security-development-lifecycle-sdl

NEW QUESTION 13
A security analyst scans the company's external IP range and receives the following results from one of the hosts:



```
Port:     Protocol:      State:
17        tcp/udp        close
21        udp            close
22        tcp            open
25        tcp            close
23        udp            close
53        udp            open
80        tcp/udp        close
139       tcp            close
389       tcp            close
443       tcp            close
3389      tcp            close
8080      tcp/udp        close
8443      tcp/udp        close
```

Which of the following best represents the security concern?

A. A remote communications port is exposed.
B. The FTP port should be using TCP only.
C. Microsoft RDP is accepting connections on TCP.
D. The company's DNS server is exposed to everyone.

Answer: C

Explanation:
The correct answer is C. Microsoft RDP is accepting connections on TCP. Microsoft RDP stands for Microsoft Remote Desktop Protocol, and it is a protocol that allows users to remotely access and control a Windows computer or server. RDP uses TCP port 3389 by default, and this port is open on the host according to the results. This indicates that the host is allowing RDP connections from anyone on the internet, which poses a security concern. An attacker could exploit vulnerabilities in RDP or use brute force attacks to gain unauthorized access to the host and compromise its data or resources1.
* A. A remote communications port is exposed is not correct. A remote communications port is a generic term for any port that allows remote access or communication with a host. There are many types of remote communications ports, such as SSH, Telnet, FTP, or RDP, and each one has its own security implications. The results do not specify which remote communications port is exposed, so this answer is too vague and inaccurate.
* B. The FTP port should be using TCP only is not correct. FTP stands for File Transfer Protocol, and it is a protocol that allows users to transfer files between hosts. FTP uses TCP ports 20 and 21 by default, and these ports are closed on the host according to the results. However, FTP can also use UDP ports 20 and 21 for data transfer in some cases, such as when using passive mode or extended passive mode2. Therefore, it is not true that FTP should be using TCP only, and this answer does not represent a security concern.
* D. The company’s DNS server is exposed to everyone is not correct. DNS stands for Domain Name System, and it is a system that translates domain names into IP addresses. DNS uses UDP port 53 by default, and this port is open on the host according to the results. This indicates that the host is providing DNS services to anyone on the internet, which may or may not be a security concern depending on the configuration and purpose of the host. For example, if the host is a public DNS server that is intended to serve DNS queries from anyone, then this answer does not represent a security concern. However, if the host is a private DNS server that is meant to serve DNS queries only from authorized users or devices, then this answer could represent a security concern.
* 1: What Is Remote Desktop Protocol (RDP)? 2: FTP - File Transfer Protocol : [What Is Domain Name S (DNS)?]

NEW QUESTION 18
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 21
An organization wants to implement controls for protecting private information at rest. Which of the following would meet the organization's need?

A. Non-disclosure agreements
B. Retention policies
C. Data minimization
D. Encryption

Answer: D

Explanation:
The correct answer is D. Encryption. Encryption is a technical control that transforms data into an unreadable format using a secret key or algorithm. Encryption can protect data at rest by preventing unauthorized access, modification, or exfiltration of the data. Encryption can also protect data in transit and in use, depending on the type and level of encryption applied1.

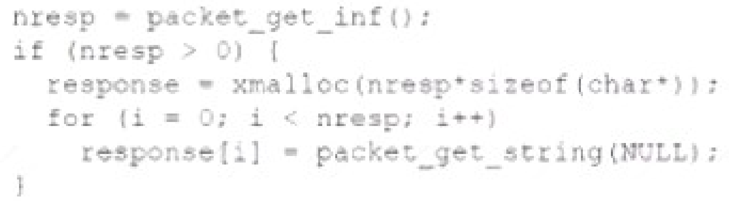
NEW QUESTION 22
A team of network security analysts is examining network traffic to determine if sensitive data was exfiltrated. Upon further investigation, the analysts believe confidential data was compromised. Which of the following capabilities would BEST defend against this type of sensitive data exfiltration?

A. Deploy an edge firewall.
B. Implement DLP
C. Deploy EDR.
D. Encrypt the hard drives

Answer: B

Explanation:
DLP, or Data Loss Prevention, is a cybersecurity solution that detects and prevents data breaches. It blocks the extraction of sensitive data and prevents the unauthorized or inappropriate sharing, transfer, or use of data. It also helps organizations comply with data protection regulations and policies1
DLP can help defend against sensitive data exfiltration by monitoring and controlling data movement across networks, devices, applications, and cloud services. DLP can also alert or block users from sending or uploading sensitive data to untrusted destinations or recipients.

NEW QUESTION 24
A security analyst found an old version of OpenSSH running on a DMZ server and determined the following piece of code could have led to a command execution through an integer overflow;



```
nresp = packet_get_inf();
if (nresp > 0) {
  response = xmalloc(nresp*sizeof(char*));
  for (i = 0; i < nresp; i++)
    response[i] = packet_get_string(NULL);
}
```

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

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

Answer: C

Explanation:
The security analyst should implement a control that uses built-in functions from libraries to check and handle long numbers properly. This will help prevent integer overflow vulnerabilities, which occur when a value is moved into a variable type too small to hold it. For example, if an integer variable can only store values up to 255, and a value of 256 is assigned to it, the variable will overflow and wrap around to 0. This can cause unexpected program behavior or lead to buffer overflow vulnerabilities if the overflowed value is used as an index or size for memory allocation1. Built-in functions from libraries can help avoid integer overflow by performing checks on the input values and the resulting values, and throwing exceptions or errors if they exceed the limits of the variable type2.

NEW QUESTION 29
A security analyst is concerned the number of security incidents being reported has suddenly gone down. Daily business interactions have not changed, and no following should the analyst review FIRST?

A. The DNS configuration
B. Privileged accounts
C. The IDS rule set
D. The firewall ACL

Answer: C

Explanation:
The security analyst should review the IDS rule set first. The IDS (Intrusion Detection System) is a tool that monitors network traffic and alerts on any suspicious or

malicious activity. The IDS rule set is a set of conditions or patterns that define what constitutes normal or abnormal behavior on the network. The IDS rule set can affect the number of security incidents being reported, as it determines what triggers an alert or not3. The security analyst should review the IDS rule set to check if it is up to date, accurate, and comprehensive. If the IDS rule set is outdated, inaccurate, or incomplete, it may miss some incidents or generate false positives or negatives.

NEW QUESTION 34
A new variant of malware is spreading on the company network using TCP 443 to contact its
command-and-control server The domain name used for callback continues to change, and the analyst is unable to predict future domain name variance Which of the following actions should the analyst take to stop malicious communications with the LEAST disruption to service?

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

Answer: A

Explanation:
A sinkhole is a technique that redirects malicious network traffic to a controlled destination, such as a fake server or a black hole. A sinkhole can be used to stop malicious communications with a command-and-control server by preventing the malware from reaching its intended destination. A high entropy level means that the sinkhole can generate random domain names that match the changing domain name used by the malware for callback. Blocking TCP/443 at the edge router, disabling TCP/53 at the perimeter firewall, or configuring the DNS forwarders to use recursion are other possible actions that could stop malicious communications, but they could also disrupt legitimate services that use those protocols or settings. Reference: https://www.cisco.com/c/en/us/about/security-center/dns-sinkholing.html

NEW QUESTION 36
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 40
Which of the following attack techniques has the GREATEST likelihood of quick success against Modbus assets?

A. Remote code execution
B. Buffer overflow
C. Unauthenticated commands
D. Certificate spoofing

Answer: C

Explanation:
Modbus is a communication protocol that is widely used in industrial control systems (ICS). Modbus does not have any built-in security features, such as authentication or encryption, which makes it vulnerable to various attacks. One of the most common and effective attack techniques against Modbus assets is to send unauthenticated commands to manipulate or disrupt the operation of the devices. Remote code execution, buffer overflow, and certificate spoofing are other attack techniques, but they have less likelihood of quick success against Modbus assets. Reference:
https://www.sciencedirect.com/science/article/pii/S2405959517300045

NEW QUESTION 44
Which of the following data exfiltration discoveries would most likely require communicating a breach to regulatory agencies?

A. CRM data
B. PHI files
C. SIEM logs
D. UEBA metrics

Answer: B

Explanation:
PHI stands for protected health information, which is any information that relates to the health or health care of an individual and can be used to identify that person. PHI is regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which sets national standards for the privacy and security of health information. HIPAA requires covered entities, such as health care providers, health plans, and health care clearinghouses, to notify individuals and regulatory agencies of any breach of unsecured PHI. A breach is defined as the unauthorized acquisition, access, use, or disclosure of PHI that compromises the

privacy or security of the information

NEW QUESTION 49
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 51
An analyst receives artifacts from a recent Intrusion and is able to pull a domain, IP address, email address, and software version. When of the following points of the Diamond Model of Intrusion Analysis does this intelligence represent?

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

Answer: A

Explanation:
The Diamond Model of Intrusion Analysis is a framework for analyzing and understanding malicious activity on a system or network. It defines the basic atomic element of any intrusion activity as the event, which
consists of four core features: adversary, infrastructure, capability, and victim. These features are connected by edges that represent their underlying relationships and arranged in the shape of a diamond1
The infrastructure feature refers to the physical or logical communication structures that are used by the adversary to deliver a capability or interact with a victim. Examples of infrastructure elements are IP addresses, domain names, email addresses, servers, routers, etc. The domain, IP address, email address, and software version that the analyst extracted from the artifacts are all examples of infrastructure elements that can be used to identify or track the adversary’s activity.

NEW QUESTION 53
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 55
A security analyst discovers the company's website is vulnerable to cross-site scripting. Which of the following solutions will best remedy the vulnerability?

A. Prepared statements
B. Server-side input validation
C. Client-side input encoding
D. Disabled JavaScript filtering

Answer: B

Explanation:
Server-side input validation is a solution that can prevent cross-site scripting (XSS) vulnerabilities by checking and filtering any user input that is sent to the server before rendering it on a web page. Server-side input validation can help to ensure that the user input conforms to the expected format, length and type, and does not contain any malicious characters or syntax that may alter the logic or behavior of the web page. Server-side input validation can also reject or sanitize any input that does not meet the validation criteria .

NEW QUESTION 60
As part of the senior leadership team's ongoing nsk management activities the Chief Information Security Officer has tasked a security analyst with coordinating the right training and testing methodology to respond to new business initiatives or significant changes to existing ones The management team wants to examine a new business process that would use existing infrastructure to process and store sensitive data Which of the following would be appropnate for the security analyst

to coordinate?

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

Answer: C

Explanation:
Threat modeling is a process that helps identify and analyze the potential threats and vulnerabilities of a system or process. It can help evaluate the security risks and mitigation strategies of a new business process that would use existing infrastructure to process and store sensitive data. A black-box penetration testing engagement, a tabletop exercise, or a business impact analysis are other methods that can be used to assess the security or resilience of a system or process, but they are not as appropriate as threat modeling for coordinating the right training and testing methodology to respond to new business initiatives or significant changes to existing ones. Reference: https://owasp.org/www-community/Application_Threat_Modeling

NEW QUESTION 62
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 65
A company is setting up a small, remote office to support five to ten employees. The company's home office is in a different city, where the company uses a cloud service provider for its business applications and a local server to host its data. To provide shared access from the remote office to the local server and the business applications, which of the following would be the easiest and most secure solution?

A. Use a VPC to host the company's data and keep the current solution for the business applications.
B. Use a new server for the remote office to host the data and keep the current solution for the business applications.
C. Use a VDI for the home office and keep the current solution for the business applications.
D. Use a VPN to access the company's data in the home office and keep the current solution for the business applications.

Answer: D

Explanation:
The correct answer is D. Use a VPN to access the company’s data in the home office and keep the current solution for the business applications. A virtual private network (VPN) is a technology that creates a secure and encrypted connection over a public network, such as the internet. A VPN can allow users to access resources on a remote network, such as a server, as if they were on the same local network. A VPN can provide shared access from the remote office to the company’s data in the home office, while maintaining security and privacy1.

NEW QUESTION 70
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 71
Which of the following describes the mam difference between supervised and unsupervised machine-learning algorithms that are used in cybersecurity applications?

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

Answer: B

Explanation:
Supervised and unsupervised machine-learning algorithms are two types of machine-learning methods that are used in cybersecurity applications. Machine learning is a branch of artificial intelligence that enables systems to learn from data and improve their performance without explicit programming.
Supervised machine-learning algorithms are trained on labeled data, which means that each data point has a known outcome or class. Supervised algorithms learn to map input data to output data by finding patterns or rules from the training data. Supervised algorithms require security analyst feedback to provide labels for the data and evaluate the accuracy of the algorithm's predictions. Examples of supervised machine-learning algorithms are classification and regression.
Unsupervised machine-learning algorithms are trained on unlabeled data, which means that each data point has no known outcome or class. Unsupervised algorithms learn to discover hidden structures or patterns from the data without any guidance or feedback. Unsupervised algorithms do not require security analyst feedback, as they do not rely on predefined labels or outcomes. Examples of unsupervised machine-learning algorithms are clustering and anomaly detection.

NEW QUESTION 75
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 79
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 84
Which of the following solutions is the BEST method to prevent unauthorized use of an API?

A. HTTPS
B. Geofencing
C. Rate liming
D. Authentication

Answer: D

Explanation:
Authentication is a method of verifying a user's identity by requiring some piece 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). Authentication is the best method to prevent unauthorized use of an API, because it ensures that only legitimate users can access or use the API functions or data. HTTPS, geofencing, or rate limiting are other methods that can enhance the security or performance of an API, but they do not prevent unauthorized use of an API. Reference: https://www.redhat.com/en/topics/api/what-is-api-security

NEW QUESTION 85
A threat feed disclosed a list of files to be used as an loC for a zero-day vulnerability. A cybersecurity analyst decided to include a custom lookup for these files on the endpoint's log-in script as a mechanism to:

A. automate malware signature creation.
B. close the threat intelligence cycle loop.
C. generate a STIX object for the TAXII server
D. improve existing detection capabilities.

Answer: D

Explanation:
The analyst decided to include a custom lookup for these files on the endpoint's log-in script as a mechanism to improve existing detection capabilities, by

checking if any of these files are present on the endpoints during log-in. This can help identify any compromised endpoints that may have been infected by the zero-day vulnerability, and alert the analyst for further investigation or response.

NEW QUESTION 86
A cybersecurity analyst is supporting an Incident response effort via threat Intelligence Which of the following is the analyst most likely executing?

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

Answer: D

Explanation:
Indicator enrichment and research pivoting are steps in the threat intelligence process that involve gathering additional information and context about the indicators of compromise (IoCs) that are related to an incident, and using them to identify other potential sources of threat data or evidence. For example, an analyst can enrich an IoC such as an IP address by looking up its geolocation, reputation, or associated domains, and then pivot to other sources of threat intelligence that may have more information about the IP address or its activities.

NEW QUESTION 90
Company A is m the process of merging with Company B As part of the merger, connectivity between the ERP systems must be established so portent financial information can be shared between the two entitles. Which of the following will establish a more automated approach to secure data transfers between the two entities?

A. Set up an FTP server that both companies can access and export the required financial data to a folder.
B. Set up a VPN between Company A and Company
C. granting access only lo the ERPs within theconnection
D. Set up a PKI between Company A and Company B and Intermediate shared certificates between the two entities
E. Create static NATs on each entity's firewalls that map lo the ERP systems and use native ERP authentication to allow access.

Answer: C

Explanation:
The security analyst should set up a PKI (Public Key Infrastructure) between Company A and Company B and exchange shared certificates between the two entities. This will allow them to establish a more automated approach to secure data transfers between their ERP systems. A PKI is a system that provides encryption and authentication services using public key cryptography. A PKI consists of certificates, certificate authorities (CAs), and other components that enable users to securely exchange data over untrusted networks. By exchanging shared certificates between Company A and Company B, they can verify each other’s identity and encrypt their data using public and private keys.

NEW QUESTION 93
An organization discovers motherboards within the environment that appear to have been physically altered during the manufacturing process. Which of the following is the BEST course of action to mitigate the risk of this reoccurring?

A. Perform an assessment of the firmware to determine any malicious modifications.
B. Conduct a trade study to determine if the additional risk constitutes further action.
C. Coordinate a supply chain assessment to ensure hardware authenticity.
D. Work with IT to replace the devices with the known-altered motherboards.

Answer: C

Explanation:
A supply chain assessment is a process that evaluates the security and integrity of the suppliers and vendors that provide hardware or software to an organization. It can help identify and mitigate the risk of tampered or counterfeit products that could compromise the organization’s security or performance. Coordinating a supply chain assessment to ensure hardware authenticity is the best course of action to mitigate the risk of motherboards that have been physically altered during the manufacturing process. Performing an assessment of the firmware, conducting a trade study, or working with IT to replace the devices are other possible actions, but they are not as effective or proactive as coordinating a supply chain assessment. Reference:
https://www.nist.gov/system/files/documents/2017/04/28/sp800-161.pdf

NEW QUESTION 97
Which of the following is a difference between SOAR and SCAP?

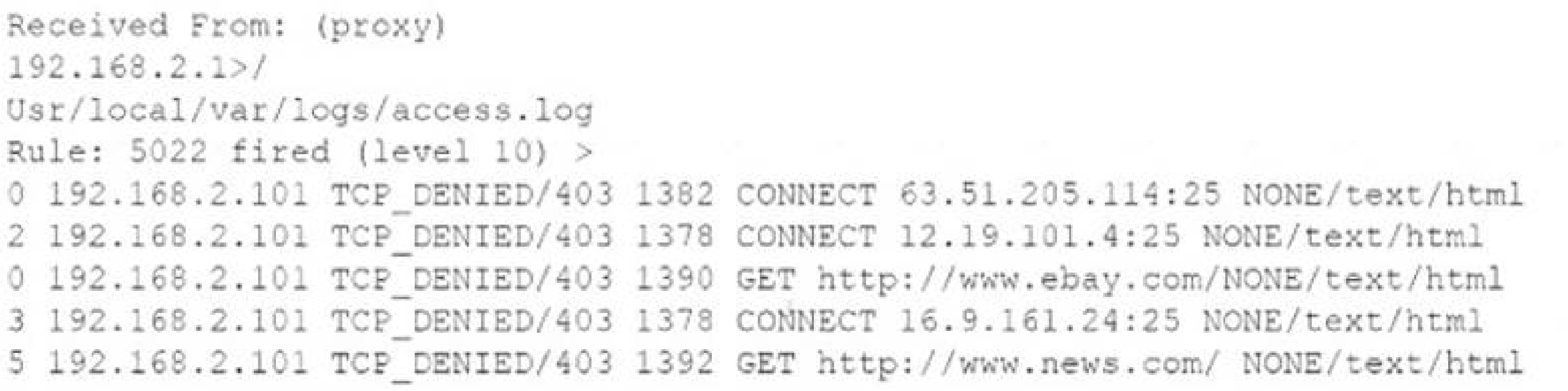
A. SOAR can be executed taster and with fewer false positives than SCAP because of advanced heunstics
B. SOAR has a wider breadth of capability using orchestration and automation, while SCAP is more limited in scope
C. SOAR is less expensive because process and vulnerability remediation is more automated 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 98

A security analyst notices the following proxy log entries:



```
Received From: (proxy)
192.168.2.1>/
Usr/local/var/logs/access.log
Rule: 5022 fired (level 10) >
0 192.168.2.101 TCP_DENIED/403 1382 CONNECT 63.51.205.114:25 NONE/text/html
2 192.168.2.101 TCP_DENIED/403 1378 CONNECT 12.19.101.4:25 NONE/text/html
0 192.168.2.101 TCP_DENIED/403 1390 GET http://www.ebay.com/NONE/text/html
3 192.168.2.101 TCP_DENIED/403 1378 CONNECT 16.9.161.24:25 NONE/text/html
5 192.168.2.101 TCP_DENIED/403 1392 GET http://www.news.com/ NONE/text/html
```

Which of the following is the user attempting to do based on the log entries?

A. Use a DoS attack on external hosts.
B. Exfiltrate data.
C. Scan the network.
D. Relay email.

Answer: C

Explanation:
Scanning the network is what the user is attempting to do based on the log entries. The log entries show that the user is sending ping requests to various IP addresses on different ports using a proxy server. Ping requests are a common network diagnostic tool that can be used to test network connectivity and latency by sending packets of data and measuring their response time. However, ping requests can also be used by attackers to scan the network and discover active hosts, open ports, or potential vulnerabilities .

NEW QUESTION 99
A customer notifies a security analyst that a web application is vulnerable to information disclosure The analyst needs to indicate the seventy of the vulnerability based on its CVSS score, which the analyst needs to calculate When analyzing the vulnerability the analyst realizes that tor the attack to be successful, the Tomcat configuration file must be modified Which of the following values should the security analyst choose when evaluating the CVSS score?

A. Network
B. Physical
C. Adjacent
D. Local

Answer: C

Explanation:
The Common Vulnerability Scoring System (CVSS) is a standard for measuring the severity of vulnerabilities in software systems. One of the factors that affects the CVSS score is the attack vector, which describes how the vulnerability can be exploited. The possible values for the attack vector are network, adjacent network, local, or physical. In this case, the analyst should choose local as the value for the attack vector, because the Tomcat configuration file must be modified for the attack to be successful, which implies that the attacker needs local access to the system. Network, adjacent network, or physical are not appropriate values for the attack vector in this scenario. Reference:
https://www.first.org/cvss/v3.1/specification-document#Vector-String

NEW QUESTION 104
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 .

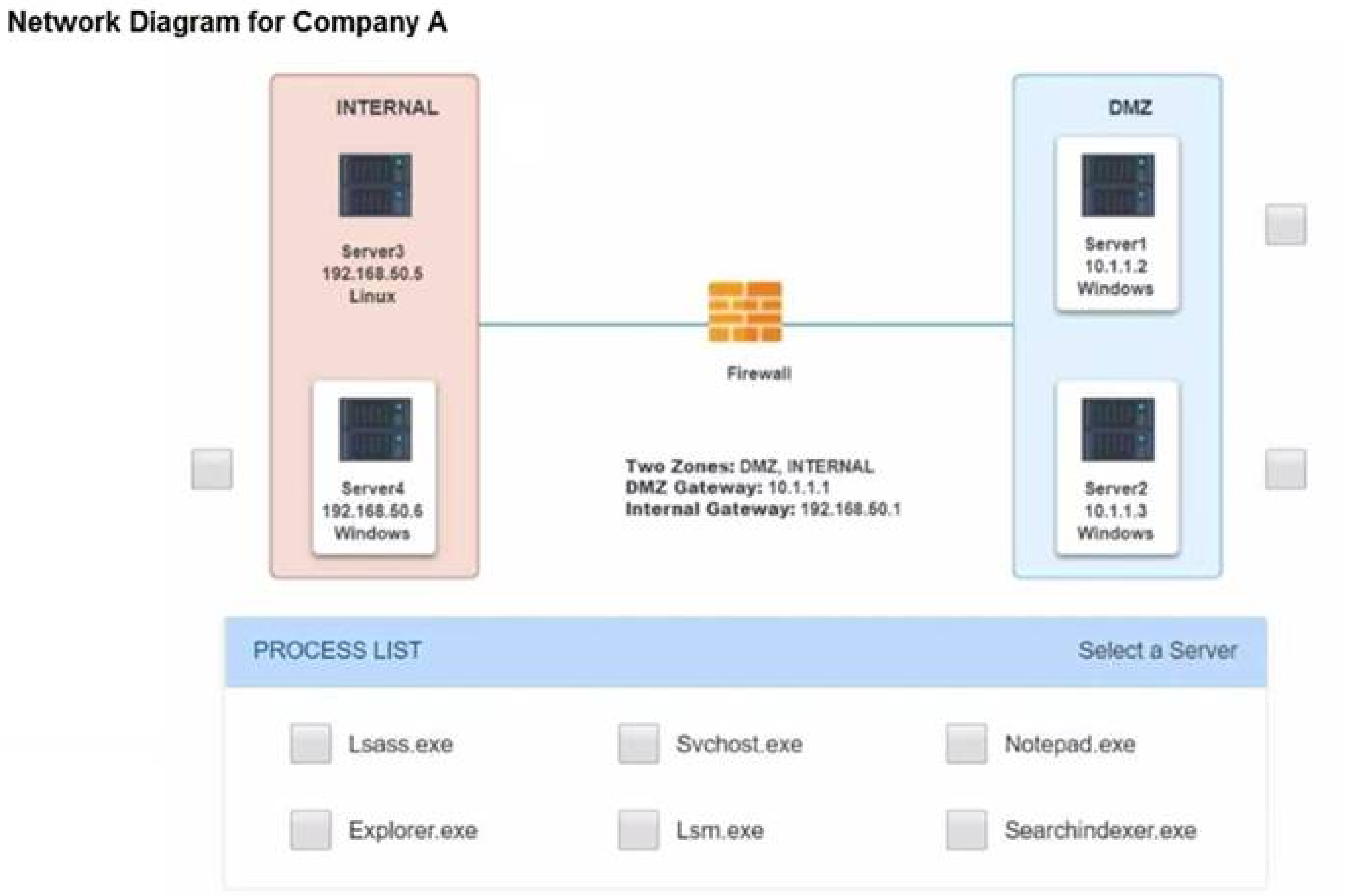
NEW QUESTION 105
A vulnerability scanner has identified an out-of-support database software version running on a server. The software update will take six to nine months to complete. The management team has agreed to a one-year extended support contract with the software vendor. Which of the following BEST describes the risk treatment in this scenario?

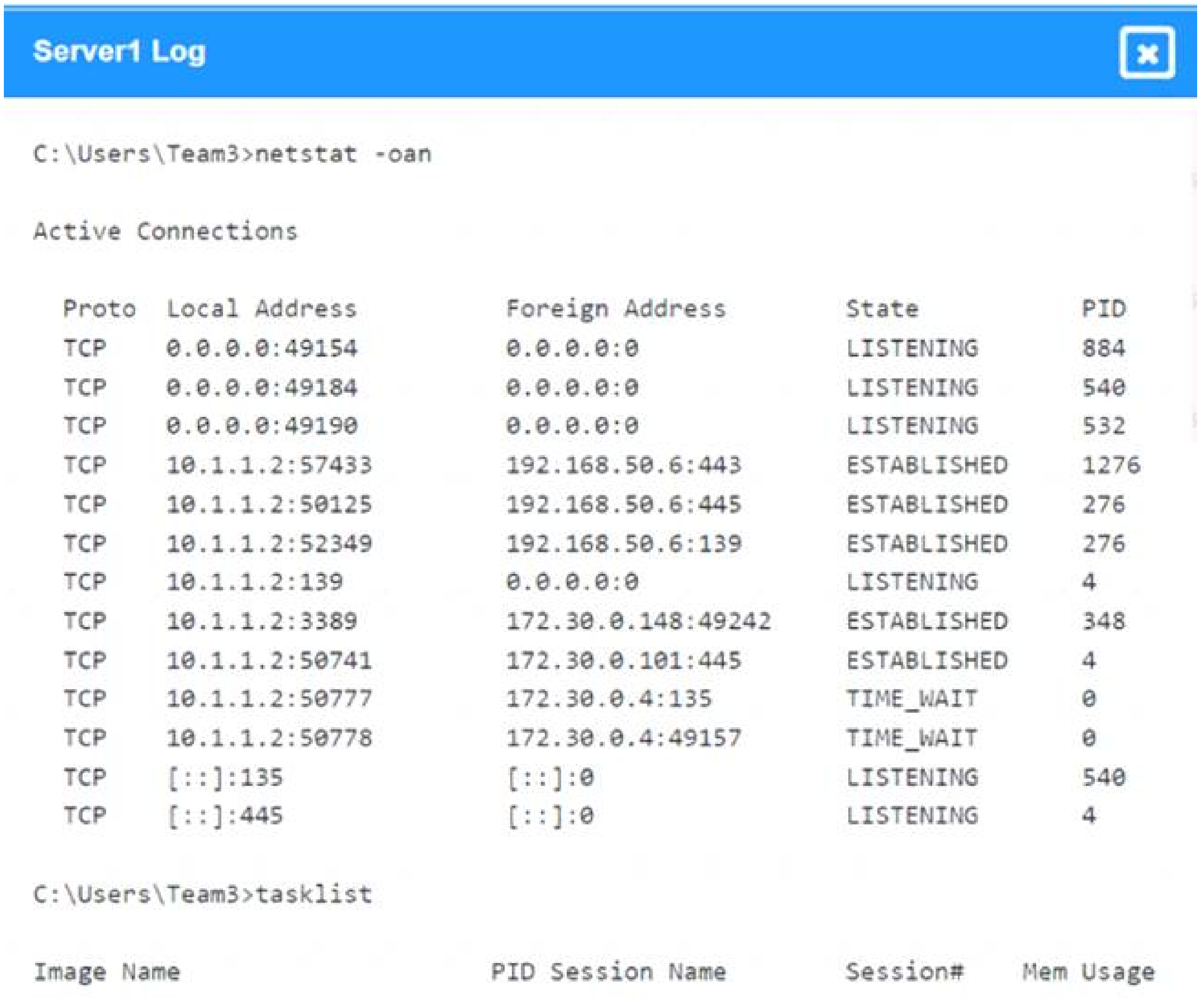
A. The extended support mitigates any risk associated with the software.
B. The extended support contract changes this vulnerability finding to a false positive.
C. The company is transferring the risk for the vulnerability to the software vendor.
D. The company is accepting the inherent risk of the vulnerability.

Answer: C

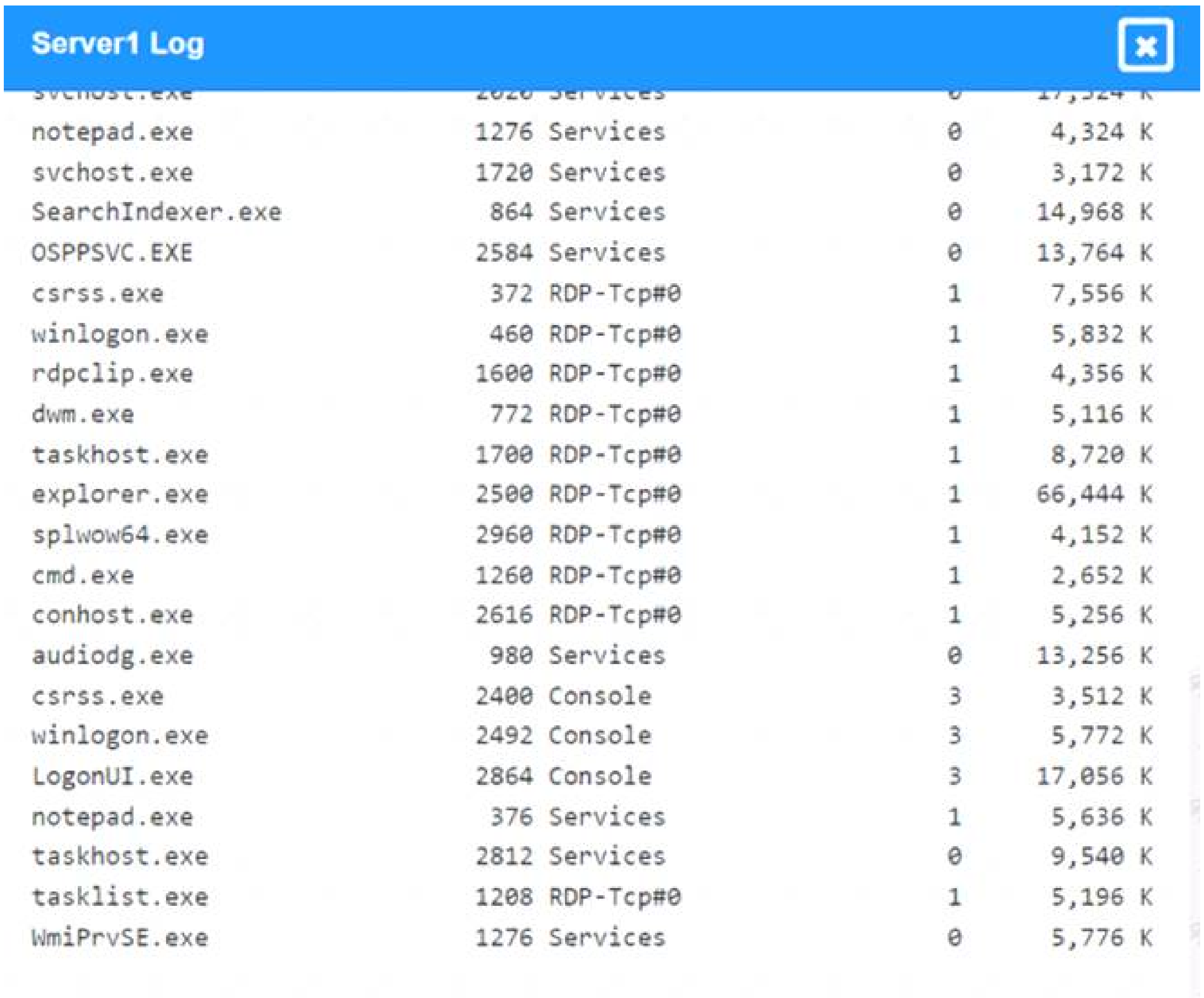
Explanation:
The company is transferring the risk for the vulnerability to the software vendor. Risk transfer is a risk treatment strategy that involves shifting the potential loss or impact of a risk to a third party, such as an insurance company or a vendor. Risk transfer does not eliminate the risk, but it reduces the organization's exposure or liability for the risk1. In this scenario, the company is transferring the risk for the vulnerability in the out-of-support database software to the software vendor by signing an extended support contract. The extended support contract means that the software vendor will continue to provide security patches and updates for the software until the company can complete the software update. This reduces the likelihood and impact of a potential exploit of the vulnerability.

NEW QUESTION 109
Malware is suspected on a server in the environment.
The analyst is provided with the output of commands from servers in the environment and needs to review all output files in order to determine which process running on one Of the servers may be malware.
INSTRUCTIONS
Servers 1 , 2, and 4 are clickable. Select the Server and the process that host the malware.





```
C:\Users\Team3>netstat -oan

Active Connections

  Proto  Local Address          Foreign Address        State          PID
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING      884
  TCP    0.0.0.0:49184          0.0.0.0:0              LISTENING      540
  TCP    0.0.0.0:49190          0.0.0.0:0              LISTENING      532
  TCP    10.1.1.2:57433         192.168.50.6:443       ESTABLISHED    1276
  TCP    10.1.1.2:50125         192.168.50.6:445       ESTABLISHED    276
  TCP    10.1.1.2:52349         192.168.50.6:139       ESTABLISHED    276
  TCP    10.1.1.2:139           0.0.0.0:0              LISTENING      4
  TCP    10.1.1.2:3389          172.30.0.148:49242     ESTABLISHED    348
  TCP    10.1.1.2:50741         172.30.0.101:445       ESTABLISHED    4
  TCP    10.1.1.2:50777         172.30.0.4:135         TIME_WAIT      0
  TCP    10.1.1.2:50778         172.30.0.4:49157       TIME_WAIT      0
  TCP    [::]:135               [::]:0                 LISTENING      540
  TCP    [::]:445               [::]:0                 LISTENING      4

C:\Users\Team3>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
```



```
svchost.exe                    2020 Services                    0      17,324 K
notepad.exe                    1276 Services                    0       4,324 K
svchost.exe                    1720 Services                    0       3,172 K
SearchIndexer.exe               864 Services                    0      14,968 K
OSPPSVC.EXE                    2584 Services                    0      13,764 K
csrss.exe                       372 RDP-Tcp#0                   1       7,556 K
winlogon.exe                    460 RDP-Tcp#0                   1       5,832 K
rdpclip.exe                    1600 RDP-Tcp#0                   1       4,356 K
dwm.exe                         772 RDP-Tcp#0                   1       5,116 K
taskhost.exe                   1700 RDP-Tcp#0                   1       8,720 K
explorer.exe                   2500 RDP-Tcp#0                   1      66,444 K
splwow64.exe                   2960 RDP-Tcp#0                   1       4,152 K
cmd.exe                        1260 RDP-Tcp#0                   1       2,652 K
conhost.exe                    2616 RDP-Tcp#0                   1       5,256 K
audiodg.exe                     980 Services                    0      13,256 K
csrss.exe                      2400 Console                     3       3,512 K
winlogon.exe                   2492 Console                     3       5,772 K
LogonUI.exe                    2864 Console                     3      17,056 K
notepad.exe                     376 Services                    1       5,636 K
taskhost.exe                   2812 Services                    0       9,540 K
tasklist.exe                   1208 RDP-Tcp#0                   1       5,196 K
WmiPrvSE.exe                   1276 Services                    0       5,776 K
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Server1 and svchost.exe

NEW QUESTION 114
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 118
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 121

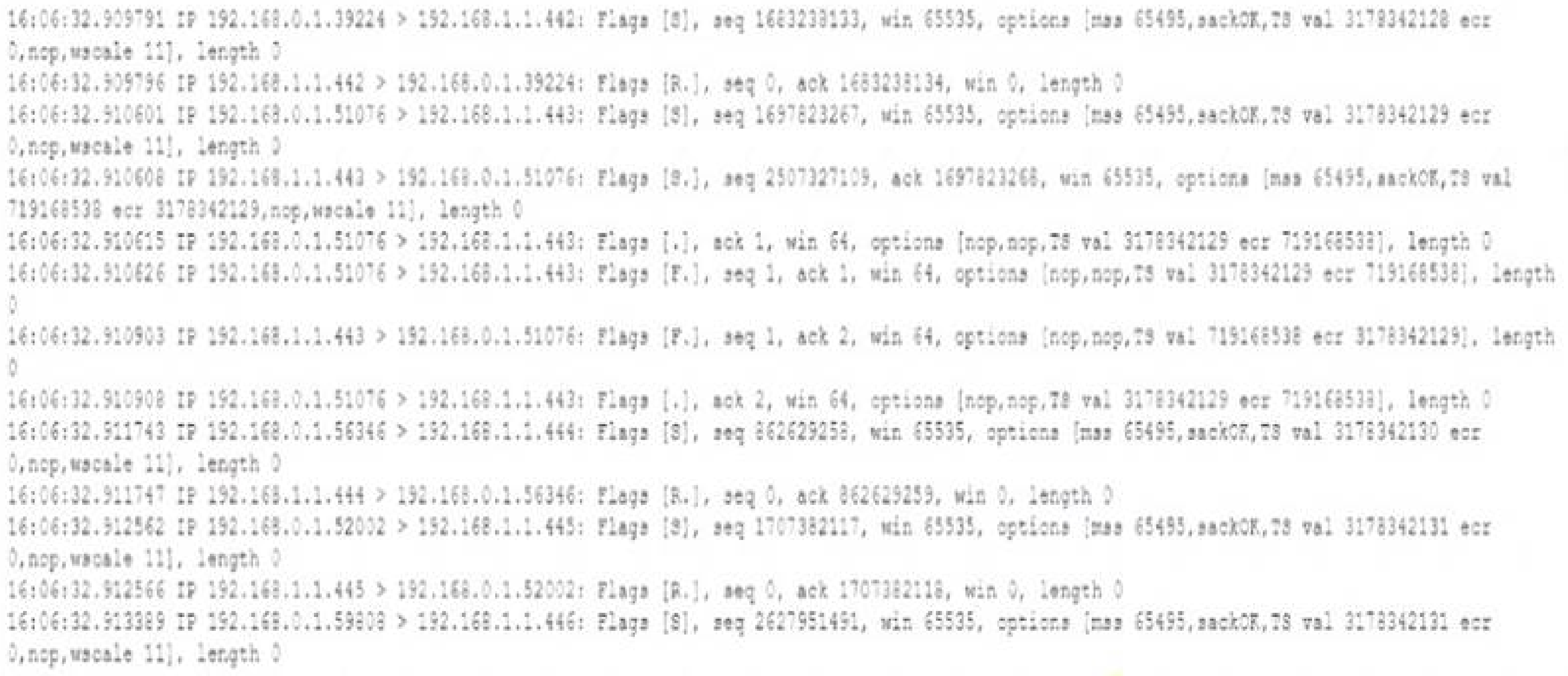
A financial organization has offices located globally. Per the organization's policies and procedures, all executives who conduct Business overseas must have their mobile devices checked for malicious software or evidence of tempering upon their return. The information security department oversees the 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 124
A security analyst is reviewing the output of tcpdump to analyze the type of activity on a packet capture:



```
16:06:32.909791 IP 192.168.0.1.39224 > 192.168.1.1.442: Flags [S], seq 1683238133, win 65535, options [mss 65495,sackOK,TS val 3178342128 ecr
0,nop,wscale 11], length 0
16:06:32.909796 IP 192.168.1.1.442 > 192.168.0.1.39224: Flags [R.], seq 0, ack 1683238134, win 0, length 0
16:06:32.910601 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [S], seq 1697823267, win 65535, options [mss 65495,sackOK,TS val 3178342129 ecr
0,nop,wscale 11], length 0
16:06:32.910608 IP 192.168.1.1.443 > 192.168.0.1.51076: Flags [S.], seq 2507327109, ack 1697823268, win 65535, options [mss 65495,sackOK,TS val
719168538 ecr 3178342129,nop,wscale 11], length 0
16:06:32.910615 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [.], ack 1, win 64, options [nop,nop,TS val 3178342129 ecr 719168538], length 0
16:06:32.910626 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [F.], seq 1, ack 1, win 64, options [nop,nop,TS val 3178342129 ecr 719168538], length
0
16:06:32.910903 IP 192.168.1.1.443 > 192.168.0.1.51076: Flags [F.], seq 1, ack 2, win 64, options [nop,nop,TS val 719168538 ecr 3178342129], length
0
16:06:32.910908 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [.], ack 2, win 64, options [nop,nop,TS val 3178342129 ecr 719168538], length 0
16:06:32.911743 IP 192.168.0.1.56346 > 192.168.1.1.444: Flags [S], seq 862629258, win 65535, options [mss 65495,sackOK,TS val 3178342130 ecr
0,nop,wscale 11], length 0
16:06:32.911747 IP 192.168.1.1.444 > 192.168.0.1.56346: Flags [R.], seq 0, ack 862629259, win 0, length 0
16:06:32.912562 IP 192.168.0.1.52002 > 192.168.1.1.445: Flags [S], seq 1707382117, win 65535, options [mss 65495,sackOK,TS val 3178342131 ecr
0,nop,wscale 11], length 0
16:06:32.912566 IP 192.168.1.1.445 > 192.168.0.1.52002: Flags [R.], seq 0, ack 1707382118, win 0, length 0
16:06:32.913389 IP 192.168.0.1.59808 > 192.168.1.1.446: Flags [S], seq 2627951491, win 65535, options [mss 65495,sackOK,TS val 3178342131 ecr
0,nop,wscale 11], length 0
```

Which of the following generated the above output?

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

Answer: B

Explanation:
A port scan generated the output. A port scan is a type of attack that probes a host or a network for open ports or services. A port scan can help an attacker discover potential vulnerabilities or entry points for further exploitation. The output shows that tcpdump captured packets with different flags, such as SYN, ACK, RST, and FIN, which indicate different stages of the TCP three-way handshake or connection termination. The output also shows that the source IP address 192.168.1.100 sent packets to different destination ports on the target IP address 192.168.1.101, such as 22, 23, 25, 80, and 443. These are common ports that an attacker would scan to find out what services are running on the target.

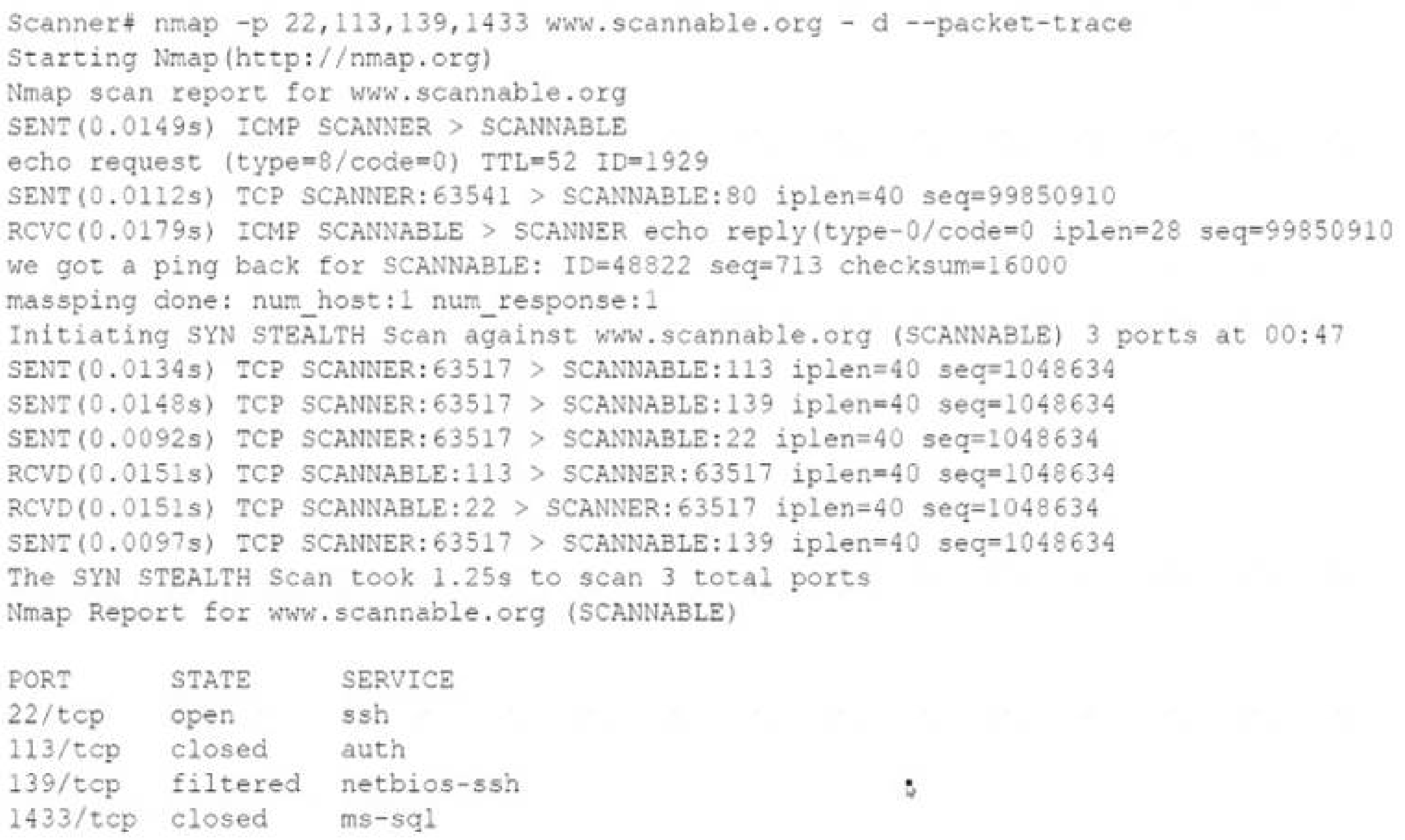
NEW QUESTION 127
A company wants to run a leaner team and needs to deploy a threat management system with minimal human Interaction. Which of the following is the server component of the threat management system that can accomplish this goal?

A. STIX
B. OpenIOC
C. CVSS
D. TAXII

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 131
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 135
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 140
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 143
A manufacturing company uses a third-party service provider lor Tier 1 security support One of the requirements is that the provider must only source talent from its own country due to geopolitical and national security interests Which of the following can the manufacturing company implement to ensure the third-party service provider meets this requirement?

A. Implement a secure supply chain program with governance
B. Implement blacklisting for IP addresses from outside the country
C. Implement strong authentication controls for all contractors
D. Implement user behavior analytics for key staff members

Answer: A

Explanation:
Implementing a secure supply chain program with governance would be the best way to ensure the third-party service provider meets the requirement of only sourcing talent from its own country. A secure supply chain program is a set of policies, procedures, and controls that aim to protect the integrity and security of the products and services delivered by third-party vendors. A secure supply chain program can help mitigate the risks of geopolitical and national security interests by verifying the origin, identity, and trustworthiness of the vendors and their employees1. Governance is a key component of a secure supply chain program, as it provides oversight, accountability, and enforcement of the policies and procedures.

NEW QUESTION 147
A Chief Information Security Officer (CISO) is concerned about new privacy regulations that apply to the company. The CISO has tasked a security analyst with finding the proper control functions to verify that a user's data is not altered without the user's consent. Which of the following would be an appropriate course of action?

A. Automate the use of a hashing algorithm after verified users make changes to their data.
B. Use encryption first and then hash the data at regular, defined times.
C. Use a DLP product to monitor the data sets for unauthorized edits and changes.
D. Replicate the data sets at regular intervals and continuously compare the copies for unauthorized changes.

Answer: A

Explanation:
Automating the use of a hashing algorithm after verified users make changes to their data is an appropriate course of action to verify that a user’s data is not altered without the user’s consent. Hashing is a technique that produces a unique and fixed-length value for a given input, such as a file or a message. Hashing can help to verify the data integrity by comparing the hash values of the original and modified data. If the hash values match, then the data has not been altered without the user’s consent. If the hash values differ, then the data may have been tampered with or corrupted .

NEW QUESTION 150
In web application scanning, static analysis refers to scanning:

A. the system for vulnerabilities before installing the application.
B. the compiled code of the application to detect possible issues.
C. an application that is installed and active on a system.
D. an application that is installed on a system that is assigned a static IP.

Answer: B

Explanation:
This type of analysis is performed before the application is installed and active on a system, and it involves
examining the code without actually executing it in order to identify potential vulnerabilities or security risks.
As per CYSA+ 002 Study Guide: Static analysis is conducted by reviewing the code for an application. Static analysis does not run the program; instead, it focuses on understanding how the program is written and what the code is intended to do.
Static analysis refers to scanning the source code or the compiled code of an application without executing it, to identify potential vulnerabilities, errors, or bugs. Static analysis can help improve the quality and security of the code before it is deployed or run4

NEW QUESTION 152
A developer is working on a program to convert user-generated input in a web form before it is displayed by the browser. This technique is referred to as:

A. output encoding.
B. data protection.
C. query parameterization.
D. input validation.

Answer: A

Explanation:
Output encoding is a technique that converts user-generated input in a web form before it is displayed by the browser. Output encoding is a form of data sanitization that prevents cross-site scripting (XSS) attacks, which occur when malicious scripts are injected into web pages and executed by unsuspecting users4. Output encoding works by replacing special characters in user input, such as <, >, ", ', &, etc., with their
HTML-encoded equivalents, such as <, >, ", ', &, etc. This prevents the browser from interpreting the user input as HTML or JavaScript code and executing it.

NEW QUESTION 154
A forensics investigator is analyzing a compromised workstation. The investigator has cloned the hard drive and needs to verify that a bit-level image copy of a hard drive is an exact clone of the original hard drive that was collected as evidence. Which of the following should the investigator do?

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

Answer: D

Explanation:
A hash is a mathematical function that produces a unique value for a given input. A hash can be used to verify that a bit-level image copy of a hard drive is an exact clone of the original hard drive by comparing the hash values of both drives. If the hash values match, then the drives are identical. If the hash values differ, then there is some discrepancy between the drives. Inserting the hard drive on a test computer and booting the computer, recording the serial numbers of both hard drives, or comparing the file-directory listing of both hard drives are not reliable methods to verify that a bit-level image copy of a hard drive is an exact clone of the original hard drive. Reference: https://www.forensicswiki.org/wiki/Hashing

NEW QUESTION 158
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 159
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 164
A company's Chief Information Officer wants to use a CASB solution to ensure policies are being met during cloud access. Due to the nature of the company's business and risk appetite, the management team elected to not store financial information in the cloud. A security analyst needs to recommend a solution to mitigate the threat of financial data leakage into the cloud. Which of the following should the analyst recommend?

A. Utilize the CASB to enforce DLP data-at-rest protection for financial information that is stored on premises.
B. Do not utilize the CASB solution for this purpose, but add DLP on premises for data in motion.
C. Utilize the CASB to enforce DLP data-in-motion protection for financial information moving to the cloud.
D. Do not utilize the CASB solution for this purpose, but add DLP on premises for data at rest.

Answer: C

Explanation:
"CASB solutions generally offer their own DLP policy engine, allowing you to configure DLP policies in a CASB and apply them to cloud services."
https://www.mcafee.com/blogs/enterprise/cloud-security/how-a-casb-integrates-with-an-on-premises-dlp-solutio
CASB stands for Cloud Access Security Broker, which is a solution that monitors and controls the access and usage of cloud services by an organization’s users. DLP stands for Data Loss Prevention, which is a solution that prevents unauthorized disclosure or leakage of sensitive data. Utilizing the CASB to enforce DLP data-in-motion protection for financial information moving to the cloud is the best recommendation for a security analyst to mitigate the threat of financial data

leakage into the cloud, because it would prevent users from uploading or transferring financial information to cloud services that are not authorized or secure. Utilizing the CASB to enforce DLP data-at-rest protection for financial information that is stored on premises, not utilizing the CASB solution for this purpose but adding DLP on premises for data in motion or data at rest are other possible recommendations, but they are not as effective or relevant as utilizing the CASB to enforce DLP data-in-motion protection for financial information moving to the cloud. Reference: https://www.csoonline.com/article/3200344/what-is-a-casb-and-why-do-you-need-one.html

NEW QUESTION 168
An organization supports a large number of remote users. Which of the following is the best option to protect the data on the remote users' laptops?

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

Answer: D

Explanation:
Using whole disk encryption is the best option to protect the data on the remote users' laptops. Whole disk encryption is a technique that encrypts all data on a hard disk drive, including the operating system, applications and files. Whole disk encryption can prevent unauthorized access to the data if the laptop is lost, stolen or compromised. Whole disk encryption can also protect the data from physical attacks, such as removing the hard disk and connecting it to another device .

NEW QUESTION 171
A security analyst wants to capture large amounts of network data that will be analyzed at a later time. The packet capture does not need to be in a format that is readable by humans, since it will be put into a binary file called "packetCapture." The capture must be as efficient as possible, and the analyst wants to minimize the likelihood that packets will be missed. Which of the following commands will best accomplish the analyst's objectives?

A. tcpdump -w packetCapture
B. tcpdump -a packetCapture
C. tcpdump -n packetCapture
D. nmap -v > packetCapture
E. nmap -oA > packetCapture

Answer: A

Explanation:
The tcpdump command is a network packet analyzer tool that can capture and display network traffic. The -w option specifies a file name to write the captured packets to, in a binary format that can be read by tcpdump or other tools later. This option is useful for capturing large amounts of network data that will be analyzed at a later time, as the question requires. The packet capture does not need to be in a format that is readable by humans, since it will be put into a binary file called “packetCapture”. The capture must be as efficient as possible, and the -w option minimizes the processing and output overhead of tcpdump, reducing the likelihood that packets will be missed.

NEW QUESTION 174
Which of the following is the best reason why organizations need operational security controls?

A. To supplement areas that other controls cannot address
B. To limit physical access to areas that contain sensitive data
C. To assess compliance automatically against a secure baseline
D. To prevent disclosure by potential insider threats

Answer: A

Explanation:
Operational security controls are security measures that are implemented and executed by people rather than by systems. Operational security controls are needed to supplement areas that other controls, such as technical or physical controls, cannot address. For example, operational security controls can include policies, procedures, training, awareness, audits, reviews, testing, etc. These controls can help ensure that employees follow best practices, comply with regulations, detect and report incidents, and respond to emergencies. The other options are not specific to operational security controls or are too narrow in scope. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 14; https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/operational-security-controls

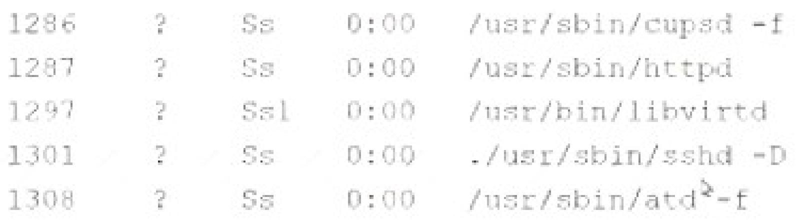
NEW QUESTION 179
The security team decides to meet informally to discuss and test the response plan for potential security breaches and emergency situations. Which of the following types of training will the security team perform?

A. Tabletop exercise
B. Red-team attack
C. System assessment implementation
D. Blue-team training
E. White-team engagement

Answer: A

Explanation:
A tabletop exercise is a type of training used to assess an organization's preparedness in responding to emergencies and security breaches. It involves discussing various scenarios and simulating how the organization would react in each situation.
https://www.comptia.org/content/tabletop-exercises.

NEW QUESTION 181
A security analyst is investigating a compromised Linux server. The analyst issues the ps command and receives the following output:



```
1286    ?    Ss     0:00    /usr/sbin/cupsd -f
1287    ?    Ss     0:00    /usr/sbin/httpd
1297    ?    Ssl    0:00    /usr/bin/libvirtd
1301    ?    Ss     0:00    ./usr/sbin/sshd -D
1308    ?    Ss     0:00    /usr/sbin/atd -f
```

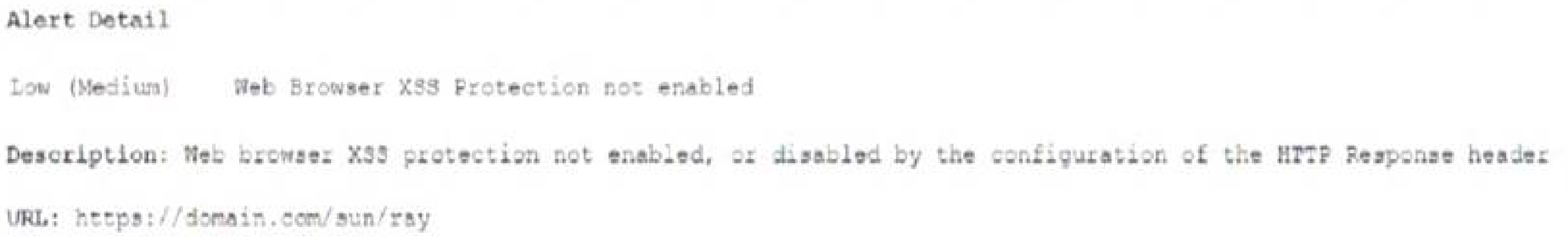
Which of the following commands should the administrator run next to further analyze the compromised system?

A. gbd /proc/1301
B. rpm -V openssh-server
C. /bin/Is -1 /proc/1301/exe
D. kill -9 1301

Answer: C

Explanation:
/bin/ls -1 /proc/1301/exe is the command that will show the absolute path to the executed binary file associated with the process ID 1301, which is ./usr/sbin/sshd. This information can help the security analyst determine if the binary is an official version and has not been modified, which could be an indicator of a compromise. /proc/1301/exe is a special symbolic link that points to the executable file that was used to start the process 1301 .

NEW QUESTION 183
A security analyst sees the following OWASP ZAP output from a scan that was performed against a modern version of Windows while testing for client-side vulnerabilities:



```
Alert Detail

Low (Medium)     Web Browser XSS Protection not enabled

Description: Web browser XSS protection not enabled, or disabled by the configuration of the HTTP Response header

URL: https://domain.com/sun/ray
```

Which of the following is the MOST likely solution to the listed vulnerability?

A. Enable the browser's XSS filter.
B. Enable Windows XSS protection
C. Enable the browser's protected pages mode
D. Enable server-side XSS protection

Answer: A

Explanation:
Enabling the browser’s XSS filter would be the most likely solution to the listed vulnerability. The vulnerability is a reflected cross-site scripting (XSS) attack, which occurs when a malicious script is injected into a web page that reflects user input back to the browser without proper validation or encoding. The malicious script can then execute in the browser and perform various actions, such as stealing cookies, redirecting to malicious sites, or displaying fake content2. Enabling the browser’s XSS filter can help prevent reflected XSS attacks by detecting and blocking malicious scripts before they execute in the browser3.

NEW QUESTION 184
A company's blocklist has outgrown the current technologies in place. The ACLs are at maximum, and the IPS signatures only allow a certain amount of space for domains to be added, creating the need for multiple signatures. Which of the following configuration changes to the existing controls would be the MOST appropriate to improve performance?

A. Implement a host-file-based solution that will use a list of all domains to deny for all machines on the network.
B. Create an IDS for the current blocklist to determine which domains are showing activity and may need to be removed
C. Review the current blocklist and prioritize it based on the level of threat severit
D. Add the domains with the highest severity to the blocklist.
E. Review the current blocklist to determine which domains can be removed from the list and then update the ACLs

Answer: D

Explanation:
This is the most effective way to improve performance, as it allows you to reduce the amount of domains in the blocklist and reduce the size of the ACLs. By reviewing the blocklist and removing domains that are no longer active or no longer pose a threat, the blocklist can be reduced and the ACLs updated accordingly. This will reduce the amount of traffic and processing power required to manage the blocklist, and can help improve overall performance.

NEW QUESTION 187
While monitoring the information security notification mailbox, a security analyst notices several emails were repotted as spam. Which of the following should the analyst do FIRST?

A. Block the sender In the email gateway.
B. Delete the email from the company's email servers.
C. Ask the sender to stop sending messages.
D. Review the message in a secure environment.

Answer: D

Explanation:
The security analyst should review the message in a secure environment first. This will help determine if the message is indeed spam or if it contains any malicious content, such as malware attachments or phishing links. Reviewing the message in a secure environment means using a sandbox or an isolated system that can

prevent any potential harm to the analyst’s system or network. If the message is confirmed to be spam or malicious, then the analyst can take further actions, such as blocking the sender, deleting the email, or notifying the users 3.

NEW QUESTION 191
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 .

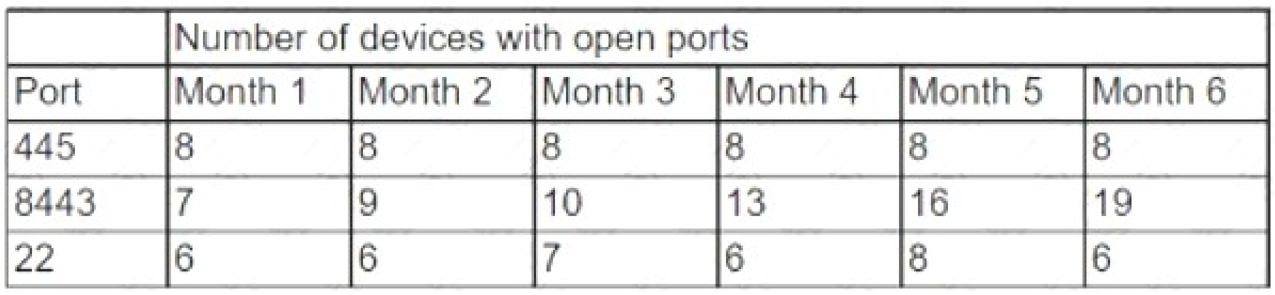
NEW QUESTION 193
Which of the following types of controls defines placing an ACL on a file folder?

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

Answer: A

Explanation:
"Technical controls enforce confidentiality, integrity, and availability in the digital space. Examples of technical security controls include firewall rules, access control lists, intrusion prevention systems, and encryption."
A technical control is a type of control that uses technology or software to protect data and systems from unauthorized access or misuse3. A technical control can include encryption, authentication, firewalls, antivirus software, and other mechanisms that rely on hardware or software. Placing an ACL (access control list) on a file folder is an example of a technical control. An ACL is a list of permissions that specifies who can access or modify a file or folder4. An ACL can help to enforce confidentiality, integrity, and availability of data by restricting access to authorized users only.

NEW QUESTION 195
A security analyst is reviewing port scan data that was collected over the course of several months. The following data represents the trends:



	Number of devices with open ports					
Port	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6
445	8	8	8	8	8	8
8443	7	9	10	13	16	19
22	6	6	7	6	8	6

Which of the following is the BEST action for the security analyst to take after analyzing the trends?

A. Review the system configurations to determine if port 445 needs to be open.
B. Assume there are new instances of Apache in the environment.
C. Investigate why the number of open SSH ports varied during the six months.
D. Raise a concern to a supervisor regarding possible malicious use Of port 8443.

Answer: C

Explanation:
According to the CompTIA CySA+ Certification Exam Study guide, the best action for the security analyst to take after analyzing the trends is to investigate why the number of open SSH ports varied during the six months. This could indicate that malicious actors are attempting to gain access to the system, and it would be important to find out the root cause of this activity in order to prevent further intrusions. Additionally, raising a concern to a supervisor regarding possible malicious use of port 8443 would also be a prudent step, as this port is often used by attackers. As stated in the study guide, "Monitoring network ports and traffic can provide insight into suspicious activity and may be necessary to identify malicious activities". Additionally, "Ports can be used to gain unauthorized access to a system, so it is important to monitor the ports and to take steps to ensure that only necessary ports are open".

NEW QUESTION 197
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 202
Which of the following is the best method to ensure secure boot UEFI features are enabled to prevent boot malware?

A. Enable secure boot in the hardware and reload the operating system.
B. Reconfigure the system's MBR and enable NTFS.
C. Set I-JEFI to legacy mode and enable security features.
D. Convert the legacy partition table to UEFI and repair the operating system.

Answer: A

Explanation:
The correct answer is A. Enable secure boot in the hardware and reload the operating system. Secure boot is a feature of UEFI that ensures that only trusted and authorized code can execute during the boot process. Secure boot can prevent boot malware, such as rootkits or bootkits, from compromising the system before the operating system loads1. To enable secure boot, the hardware must support UEFI and have a firmware that implements the secure boot protocol. The operating system must also support UEFI and have a digital
signature that matches the keys stored in the firmware. If the operating system was installed in legacy mode or does not have a valid signature, it may not boot with secure boot enabled. Therefore, it may be necessary to reload the operating system after enabling secure boot in the hardware2.
* B. Reconfigure the system's MBR and enable NTFS is not correct. MBR stands for Master Boot Record, and it is a legacy partitioning scheme that stores information about the partitions and the boot loader on a disk. NTFS stands for New Technology File System, and it is a file system that supports features such as encryption, compression, and access control. Reconfiguring the system's MBR and enabling NTFS would not enable secure boot UEFI features, as they are not related to UEFI or secure boot. Moreover, MBR is incompatible with UEFI, as UEFI requires a different partitioning scheme called GPT (GUID Partition Table)3.
* C. Set UEFI to legacy mode and enable security features is not correct. Legacy mode is a compatibility mode that allows UEFI systems to boot using legacy BIOS methods. Legacy mode disables some of the features and benefits of UEFI, such as secure boot, faster boot time, or larger disk support. Setting UEFI to legacy mode would not enable secure boot UEFI features, but rather disable them.
* D. Convert the legacy partition table to UEFI and repair the operating system is not correct. Converting the legacy partition table to UEFI means changing the partitioning scheme from MBR to GPT, which is required for UEFI systems to boot. However, this alone would not enable secure boot UEFI features, as it also depends on the firmware settings and the operating system support. Repairing the operating system may or may not fix any issues caused by converting the partition table, but it would not necessarily enable secure boot either.
1: What Is Secure Boot? 2: How to Enable Secure Boot 3: MBR vs GPT: Which One Is Better for You [UEFI vs Legacy BIOS – The Ultimate Comparison Guide]

NEW QUESTION 207
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 208
A small organization has proprietary software that is used internally. The system has not been wen maintained and cannot be updated with the rest or the environment. Which of the following is the BEST solution?

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

Answer: A

Explanation:
A virtualized system is a system that runs on a software layer called a hypervisor that emulates the hardware resources of a physical machine. A virtualized system can have its own operating system, applications, and data that are isolated from other virtualized systems or the host machine3
A virtualized system can be a
solution for a small organization that has proprietary software that is used internally but cannot be updated with the rest of the environment. By virtualizing the system and decommissioning the physical machine, the organization can achieve several benefits, such as:
- Reducing hardware costs and maintenance
- Improving performance and scalability
- Enhancing security and compliance
- Simplifying backup and recovery
- Enabling portability and compatibility

NEW QUESTION 212

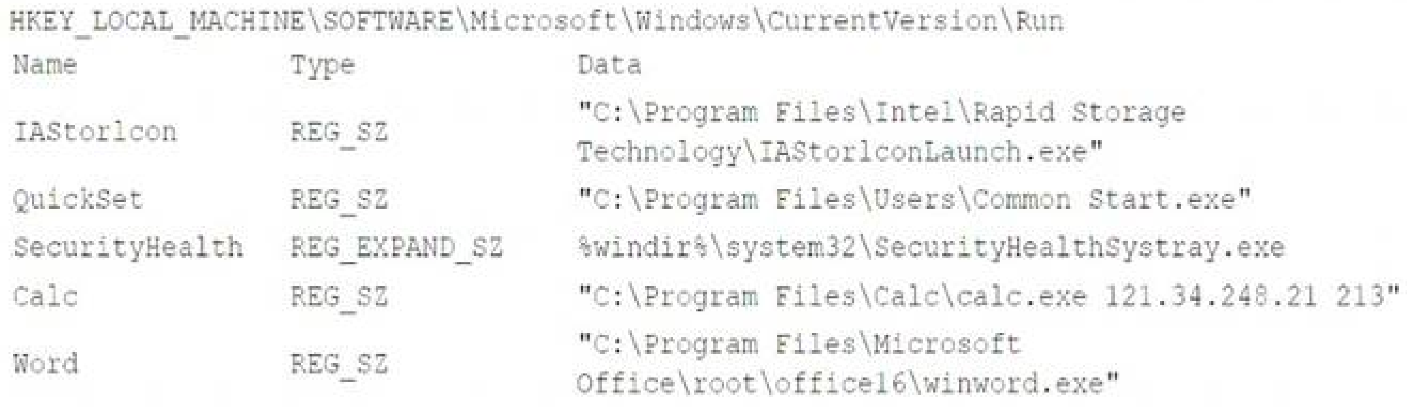
A company has a cluster of web servers that is critical to the business. A systems administrator installed a utility to troubleshoot an issue, and the utility caused the entire cluster to 90 offline. Which of the following solutions would work BEST prevent to this from happening again?

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 216
An analyst is reviewing registry keys for signs of possible compromise. The analyst observes the following entries:



HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
IAStorlcon	REG_SZ	"C:\Program Files\Intel\Rapid Storage Technology\IAStorlconLaunch.exe"
QuickSet	REG_SZ	"C:\Program Files\Users\Common Start.exe"
SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe
Calc	REG_SZ	"C:\Program Files\Calc\calc.exe 121.34.248.21 213"
Word	REG_SZ	"C:\Program Files\Microsoft Office\root\office16\winword.exe"

Which of the following entries should the analyst investigate first?

A. IAStorIcon
B. Quickset
C. SecurityHealth
D. calc
E. Word

Answer: D

Explanation:
The calc entry is a suspicious registry entry that should be investigated first by the analyst. The calc entry is located in the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run registry key, which is a common location for malware to persist and execute on system startup. The calc entry has a data value of “C:\Windows\System32\calc.exe”, which is the path to the legitimate Windows Calculator program. However, this program does not need to run on system startup, and it could be a disguise for a malicious executable that has replaced or renamed the original calculator program. The calc entry could also be a sign of a fileless malware attack, where the attacker uses the legitimate calculator program to execute malicious commands or scripts in memory1.

NEW QUESTION 217
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 220
Which of the following APT adversary archetypes represent non-nation-state threat actors? (Select TWO)

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

F. Spider

Answer: AD

Explanation:
Kitten and Jackal are two APT (Advanced Persistent Threat) adversary archetypes that represent non-nation-state threat actors. APT adversary archetypes are categories of threat actors that share common characteristics, such as motivation, objectives, capabilities, or tactics. APT adversary archetypes can help security analysts understand and prioritize the threats they face2. Kitten is a term used to describe Iranian-based threat actors that are typically not backed by the Iranian government. They are motivated by ideological or religious beliefs and target political or regional adversaries3. Jackal is a term used to describe cybercriminal groups that operate as mercenaries or proxies for other threat actors. They are motivated by financial gain and target various sectors and regions.

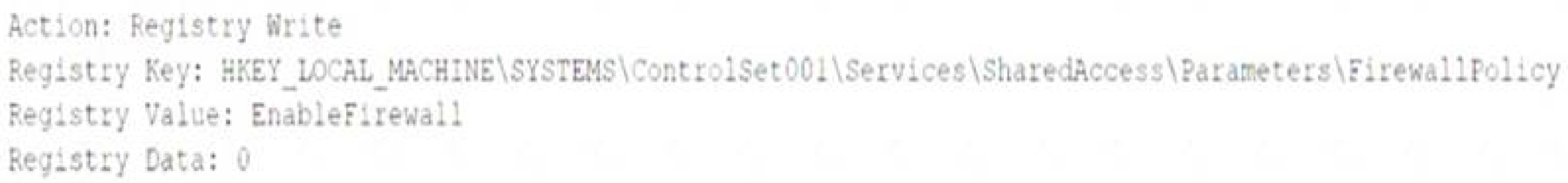
NEW QUESTION 222
Which of the following BEST describes HSM?

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

Answer: B

Explanation:
HSM (Hardware Security Module) is a computing device that manages digital keys, performs encryption/decryption functions, and maintains other cryptographic functions2. HSM is a dedicated crypto processor that is specifically designed for the protection of the crypto key lifecycle. HSM can store cryptographic keys that are used for encryption, authentication, digital signatures, and other security functions. HSM can also generate random keys that are unique to each device and never leave the chip. HSM can protect these keys from unauthorized access or tampering by using hardware isolation and encryption3. HSM can also measure and verify the integrity of the operating system and firmware on a device by using a process called attestation. HSM does not manage cryptography (A), as cryptography is the science or art of creating and using secret codes. HSM does not manage physical keys ©, as physical keys are tangible objects that are used to lock or unlock something. HSM does not manage algorithms (D), as algorithms are sets of rules or instructions that are used to solve problems or perform tasks.
References: 2: https://www.techopedia.com/definition/24771/technical-controls 3: https://www.techopedia.com/definition/25888/security-development-lifecycle-sdl

NEW QUESTION 223
An analyst received an alert regarding an application spawning a suspicious command shell process Upon further investigation, the analyst observes the following registry change occurring immediately after the suspicious event:



```
Action: Registry Write
Registry Key: HKEY_LOCAL_MACHINE\SYSTEMS\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy
Registry Value: EnableFirewall
Registry Data: 0
```

Which of the following was the suspicious event able to accomplish?

A. Impair defenses.
B. Establish persistence.
C. Bypass file access controls.
D. Implement beaconing.

Answer: B

Explanation:
The suspicious event was able to accomplish establishing persistence by creating a registry change that runs a command shell process every time a user logs on. The registry change modifies the Userinit value under the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon key, which specifies what programs should run when a user logs on to Windows. By appending “cmd.exe,” to the existing value, the event ensures that a command shell process will be launched every time a user logs on, which can allow the attacker to maintain access to the system or execute malicious commands. The other options are not related to the registry change. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 10; https://docs.microsoft.com/en-us/windows/win32/sysinfo/userinit-entry

NEW QUESTION 228
After a series of Group Policy Object updates, multiple services stopped functioning. The systems administrator believes the issue resulted from a Group Policy Object update but cannot validate which update caused the Issue. Which of the following security solutions would resolve this issue?

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

Answer: C

Explanation:
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 errors1
Change management can help resolve the issue of
Group Policy Object updates affecting multiple services by ensuring that the updates are properly planned, tested, approved, documented, communicated, and monitored.

NEW QUESTION 233
While going through successful malware cleanup logs, an analyst notices an old worm that has been replicating itself across the company's network Reinfection of

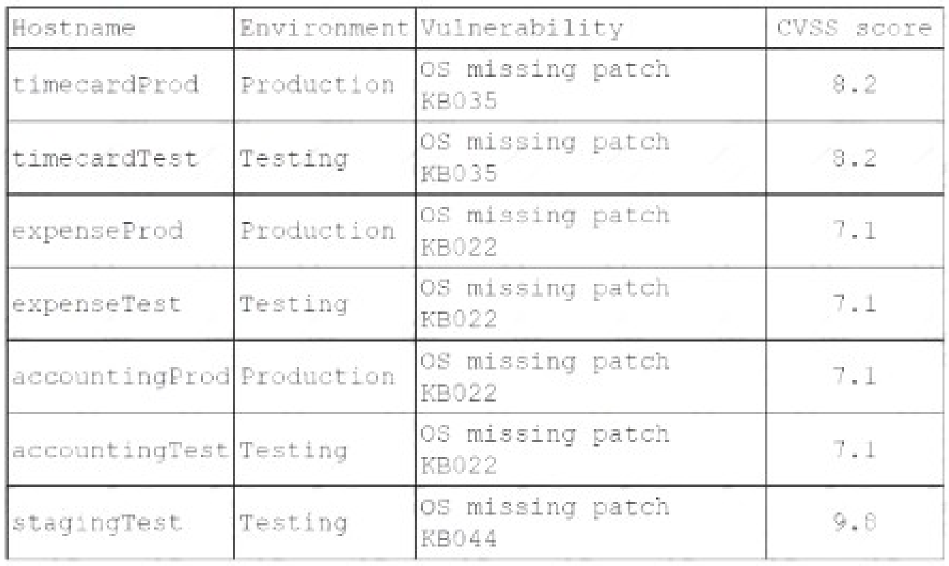
the malware can be prevented with a patch; however, most of the affected systems cannot be patched because the patch would make the system unstable. Which of the following should the analyst recommend to best prevent propagation of the malware throughout the network?

A. Segmenting the network to include all legacy systems
B. Placing vulnerable devices behind a firewall
C. Scanning the entire network for malware weekly
D. Patching systems when possible and monitoring the rest of them

Answer: A

Explanation:
Segmenting the network to include all legacy systems is a strategy that can prevent the propagation of the malware throughout the network, by isolating the systems that cannot be patched from the rest of the network. Segmenting the network can also reduce the exposure and impact of the malware, by limiting its access to other resources or systems.

NEW QUESTION 237
An organization has the following vulnerability remediation policies:
• For production environment servers:
• Vulnerabilities with a CVSS score of 9.0 or greater must be remediated within 48 hours.
• Vulnerabilities with a CVSS score of 5.0 to 8.9 must be remediated within 96 hours.
• Vulnerabilities in lower environments may be left unremediated for up to two weeks.
* All vulnerability remediations must be validated in a testing environment before they are applied in the production environment.
The organization has two environments: production and testing. The accountingProd server is the only server that contains highly sensitive information.
A recent vulnerability scan provided the following report:



Hostname	Environment	Vulnerability	CVSS score
timecardProd	Production	OS missing patch KB035	8.2
timecardTest	Testing	OS missing patch KB035	8.2
expenseProd	Production	OS missing patch KB022	7.1
expenseTest	Testing	OS missing patch KB022	7.1
accountingProd	Production	OS missing patch KB022	7.1
accountingTest	Testing	OS missing patch KB022	7.1
stagingTest	Testing	OS missing patch KB044	9.8

Which of the following identifies the server that should be patched first? (Choose Two)

A. timecardProd
B. timecardTesl
C. expense Prod
D. expenseTest
E. accountingProd
F. accountingTest
G. stagingTest

Answer: CE

Explanation:
These servers should be patched first because they have vulnerabilities with CVSS scores of 9.0 and 8.9 respectively, which fall under the policy of remediating within 48 hours and 96 hours for production environment servers. The other servers either have lower CVSS scores, are in lower environments, or do not contain highly sensitive information.

NEW QUESTION 241
A Chief Information Secunty Officer has asked for a list of hosts that have critical and high-seventy findings as referenced in the CVE database. Which of the following tools would produce the assessment output needed to satisfy this request?

A. Nessus
B. Nikto
C. Fuzzer
D. Wireshark
E. Prowler

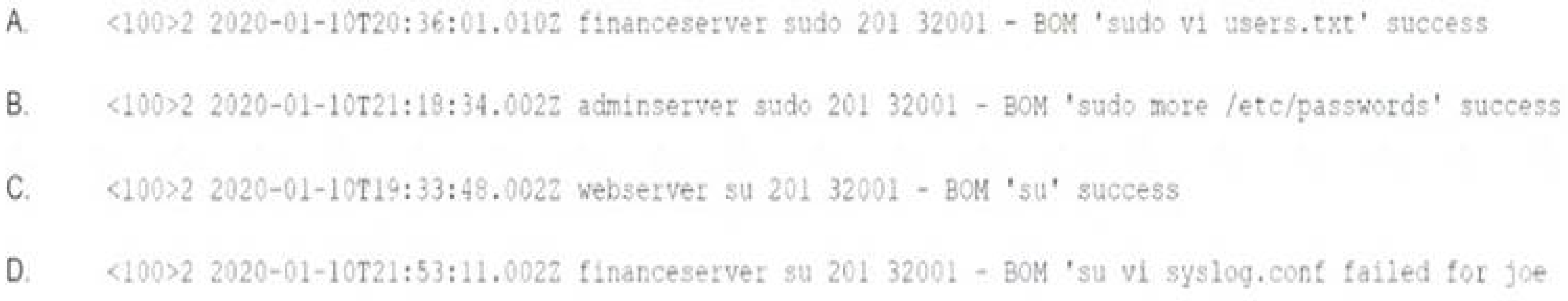
Answer: A

Explanation:
Nessus is a tool that would produce the assessment output needed to satisfy the request. Nessus is a vulnerability scanner that can scan a network or a system for known vulnerabilities and generate reports based on the findings. Nessus can also compare the vulnerabilities it finds with the Common Vulnerabilities and Exposures (CVE) database, which is a standardized list of publicly known security vulnerabilities and exposures2. Nessus can help identify hosts that have critical and high-severity findings as referenced in the CVE database.

NEW QUESTION 244
An organization prohibits users from logging in to the administrator account. If a user requires elevated permissions. the user's account should be part of an administrator group, and the user should escalate permission only as needed and on a temporary basis. The organization has the following reporting priorities when reviewing system activity:

- Successful administrator login reporting priority - high
- Failed administrator login reporting priority - medium
- Failed temporary elevated permissions - low
- Successful temporary elevated permissions - non-reportable

A security analyst is reviewing server syslogs and sees the following: Which of the following events is the HIGHEST reporting priority?



```
A.    <100>2 2020-01-10T20:36:01.010Z financeserver sudo 201 32001 - BOM 'sudo vi users.txt' success

B.    <100>2 2020-01-10T21:18:34.002Z adminserver sudo 201 32001 - BOM 'sudo more /etc/passwords' success

C.    <100>2 2020-01-10T19:33:48.002Z webserver su 201 32001 - BOM 'su' success

D.    <100>2 2020-01-10T21:53:11.002Z financeserver su 201 32001 - BOM 'su vi syslog.conf failed for joe
```

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

Answer: A

Explanation:
Option A shows a successful administrator login from an IP address that is not part of the organization's network. This is a high reporting priority event, because it violates the organization's policy that prohibits users from logging in to the administrator account and it could indicate a compromise of the administrator credentials or a malicious insider. Option B shows a failed administrator login from an IP address that is part of the organization's network. This is a medium reporting priority event, because it could indicate an unauthorized attempt to access the administrator account. Option C shows a failed temporary elevated permission request from a user account that is part of the organization's network. This is a low reporting priority event, because it could indicate a user error or a legitimate need for elevated permission that was denied. Option D shows a successful temporary elevated permission request from a user account that is part of the organization's network. This is a non-reportable event, because it complies with the organization's policy that allows users to escalate permission only as needed and on a temporary basis. Reference: https://www.sans.org/reading-room/whitepapers/logging/detecting-attacks-systems-microsoft-windows-event-lo

NEW QUESTION 248
During a review of recent network traffic, an analyst realizes the team has seen this same traffic multiple times in the past three weeks, and it resulted in confirmed malware activity The analyst also notes there is no other alert in place for this traffic After resolving the security incident, which of the following would be the BEST action for the analyst to take to increase the chance of detecting this traffic in the future?

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

Answer: C

Explanation:
Communicate the security incident to the threat team for further review and analysis. This would allow the threat team to investigate the source and nature of the malicious traffic and create appropriate alerts or signatures to detect it in the future. Sharing details with human resources, noting the incident, or reporting it to a manager would not increase the chance of detection.

NEW QUESTION 253
A developer downloaded and attempted to install a file transfer application in which the installation package is bundled with acKvare. The next-generation antivirus software prevented the file from executing, but it did not remove the file from the device. Over the next few days, more developers tried to download and execute the offending file. Which of the following changes should be made to the security tools to BEST remedy the issue?

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

Answer: D

Explanation:
Blocking the download of the file via the web proxy is the best change to make to the security tools to remedy the issue. A web proxy is a server that acts as an intermediary between a client and a web server, filtering or modifying requests and responses according to predefined rules1. Blocking the download of the file via the web proxy can prevent developers from accessing and executing the offending file that is bundled with adware. This can reduce the risk of infection or compromise of the developer workstations and improve their performance and security. Blacklisting the hash in the next-generation antivirus system (A) is not the best change to make to the security tools to remedy the issue. Blacklisting is a technique that involves blocking or denying access to known malicious or unwanted entities based on their identifiers, such as hashes, IP addresses, domains, etc2. Blacklisting the hash in the next-generation antivirus system can prevent developers from executing the offending file that is bundled with adware, but it does not prevent them from downloading it. This can still consume network bandwidth and disk space and expose developers to potential threats. Manually deleting the file from each of the workstations (B) is not the best change to make to the security tools to remedy the issue. Manually deleting the file from each of the workstations can remove the offending file that is bundled with adware, but it does not prevent developers from downloading it again. This can be a time-consuming and inefficient process that requires human intervention and coordination. Removing administrative rights from all developer workstations © is not the best change to make to the security tools to remedy the issue. Removing administrative rights from all developer workstations can limit developers' ability to install or execute unauthorized or malicious applications, such as adware, but it does not prevent them from downloading them. This can also affect developers' productivity and functionality by restricting their access to legitimate applications or settings.
References: 1: https://www.techopedia.com/definition/24771/technical-controls 2: https://www.techopedia.com/definition/25888/security-development-lifecycle-sdl

NEW QUESTION 256

……

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

100% Actual & Verified — Instant Download, Please Click
Order The CS0-002 Practice Test Here