CompTIA

Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

NEW QUESTION 1
An organization wants to collect IoCs from multiple geographic regions so it can sell the information to its customers. Which of the following should the organization deploy to accomplish this task?

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

Answer: A

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

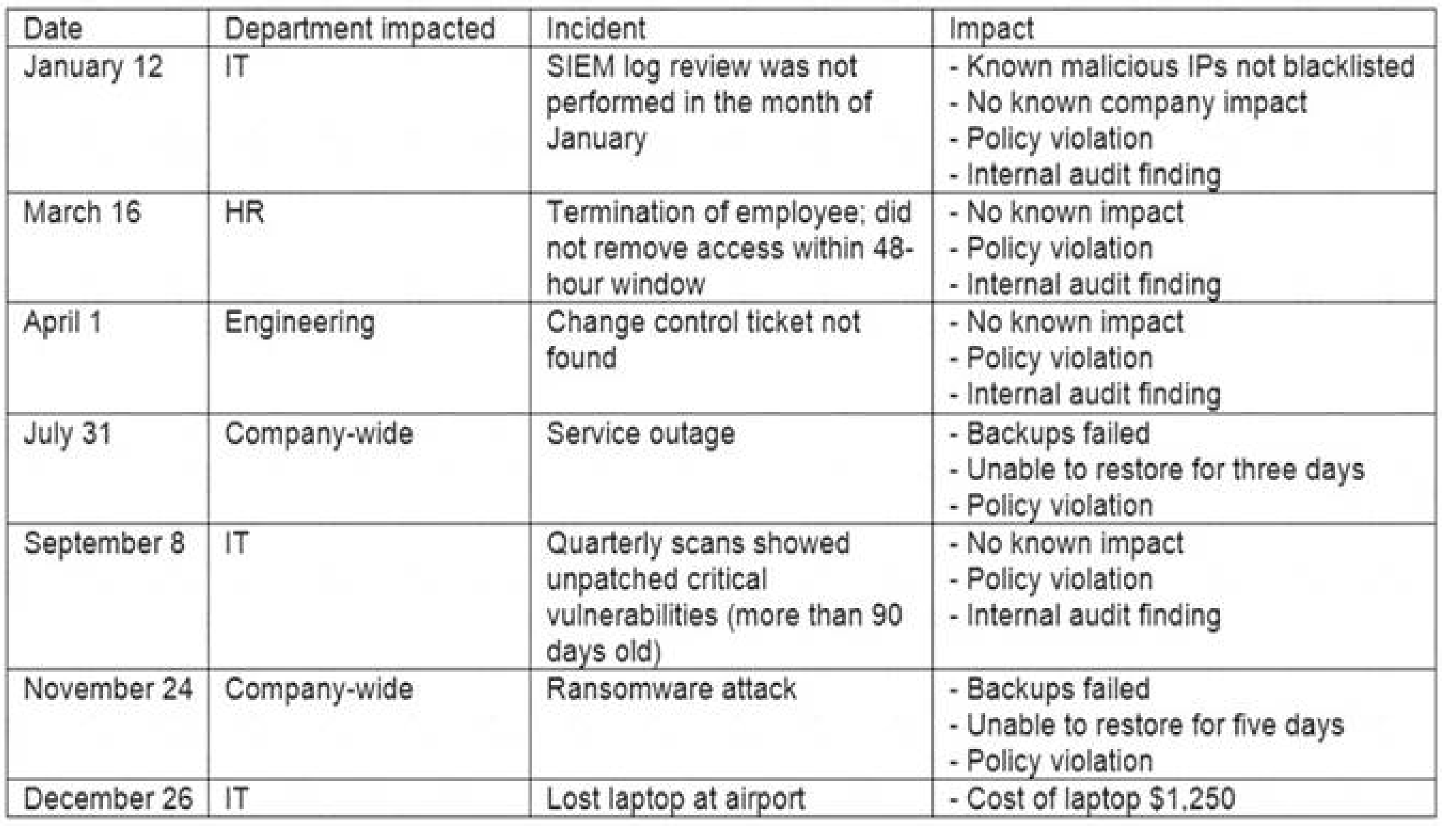
NEW QUESTION 2
As part of an Intelligence feed, a security analyst receives a report from a third-party trusted source. Within the report are several detrains and reputational information that suggest the company's employees may be targeted for a phishing campaign. Which of the following configuration changes would be the MOST appropriate for Mergence gathering?

A. Update the whitelist.
B. Develop a malware signature.
C. Sinkhole the domains
D. Update the Blacklist

Answer: D

Explanation:
A blacklist is a list of domains, IP addresses, email addresses, or other identifiers that are known or suspected to be malicious or harmful. A blacklist can be used to block or filter unwanted or dangerous traffic from reaching a network or system2
Updating the blacklist can help prevent phishing campaigns by adding the
domains or email addresses of the phishing sources to the list and preventing them from sending emails to the company's employees.

NEW QUESTION 3
The steering committee for information security management annually reviews the security incident register for the organization to look for trends and systematic issues. The steering committee wants to rank the risks based on past incidents to improve the security program for next year. Below is the incident register for the organization:



Date	Department impacted	Incident	Impact
January 12	IT	SIEM log review was not performed in the month of January	- Known malicious IPs not blacklisted - No known company impact - Policy violation - Internal audit finding
March 16	HR	Termination of employee; did not remove access within 48-hour window	- No known impact - Policy violation - Internal audit finding
April 1	Engineering	Change control ticket not found	- No known impact - Policy violation - Internal audit finding
July 31	Company-wide	Service outage	- Backups failed - Unable to restore for three days - Policy violation
September 8	IT	Quarterly scans showed unpatched critical vulnerabilities (more than 90 days old)	- No known impact - Policy violation - Internal audit finding
November 24	Company-wide	Ransomware attack	- Backups failed - Unable to restore for five days - Policy violation
December 26	IT	Lost laptop at airport	- Cost of laptop $1,250

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

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

Answer: C

Explanation:
Investing in a failover and redundant system, as necessary, is the best solution to improve the availability of the organization's systems based on past incidents. A failover system is a backup system that automatically takes over the operation of a primary system in case of a failure or outage. A redundant system is a duplicate system that runs simultaneously with the primary system and provides backup functionality if needed. Investing in a failover and redundant system can help to ensure that the organization's systems are always available and can handle the workload without interruption or degradation .

NEW QUESTION 4

A security analyst needs to provide the development team with secure connectivity from the corporate network to a three-tier cloud environment. The developers require access to servers in all three tiers in order to perform various configuration tasks. Which of the following technologies should the analyst implement to provide secure transport?

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

Answer: D

Explanation:
A VPN is a secure network connection that allows users to access their private corporate networks over the internet, while keeping the connection encrypted and secure. This makes it an ideal solution for providing the development team with secure connectivity from the corporate network to a three-tier cloud environment.
https://www.comptia.org/content/virtual-private-networks

NEW QUESTION 5
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 6
Which of the following is the most effective approach to minimize the occurrence of vulnerabilities introduced by unintentional misconfigurations in the cloud?

A. Requiring security training certification before granting access to staff
B. Migrating all resources to a private cloud deployment
C. Restricting changes to the deployment of validated IaC templates
D. Reducing IaaS deployments by fostering serverless architectures

Answer: C

Explanation:
IaC stands for infrastructure as code, which is a practice of using code or configuration files to automate the provisioning and management of cloud resources. IaC templates can help ensure consistency, repeatability, and scalability of cloud deployments, as well as reduce human errors and misconfigurations. However, IaC templates need to be validated and tested before deployment, and any changes to the templates should be controlled and monitored. This can help minimize the occurrence of vulnerabilities introduced by unintentional misconfigurations in the cloud

NEW QUESTION 7
A company is aiming to test a new incident response plan. The management team has made it clear that the initial test should have no impact on the environment. The company has limited
resources to support testing. Which of the following exercises would be the best approach?

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

Answer: A

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

NEW QUESTION 8
A company's threat team has been reviewing recent security incidents and looking for a common theme. The team discovered the incidents were caused by incorrect configurations on the impacted systems. The issues were reported to support teams, but no action was taken. Which of the following is the next step the company should take to ensure any future issues are remediated?

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

Answer: A

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

NEW QUESTION 9
An online gaming company was impacted by a ransomware attack. An employee opened an attachment that was received via an SMS attack on a company-issue firewall. Which following actions would help during the forensic analysis of the mobile device? (Select TWO).

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

Answer: CE

Explanation:
Documenting the respective chain of custody and performing a memory dump of the mobile device for analysis would help during the forensic analysis of the mobile device. The chain of custody is a record of who handled the evidence, when, where, how, and why. The chain of custody helps to preserve the integrity and admissibility of the evidence by preventing tampering, alteration, or loss1. A memory dump is a process of capturing and storing the contents of the device’s memory (RAM) for analysis. A memory dump can help to recover volatile data that may be lost when the device is powered off or rebooted, such as running processes, network connections, encryption keys, or malware traces2.

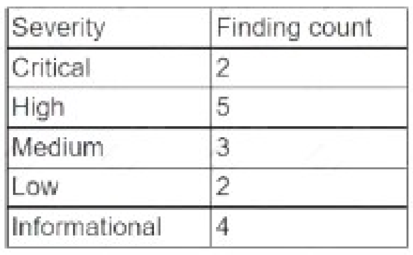
NEW QUESTION 10
A company notices unknown devices connecting to the internal network and would like to implement a solution to block all non-corporate managed machines. Which of the following solutions would be best to accomplish this goal?

A. WPA2 for W1F1 networks
B. NAC with 802.1X implementation
C. Extensible Authentication Protocol
D. RADIUS with challenge/response

Answer: B

Explanation:
This solution is the best to accomplish the goal of blocking all non-corporate managed machines from connecting to the internal network. NAC stands for network access control, which is a method of enforcing policies and rules on network devices based on their identity, role, location, and other attributes. 802.1X is a standard for port-based network access control, which authenticates devices before granting them access to a network port or wireless access point.

NEW QUESTION 10
During the onboarding process for a new vendor, a security analyst obtains a copy of the vendor's latest penetration test summary:



Severity	Finding count
Critical	2
High	5
Medium	3
Low	2
Informational	4

Performed by: Vendor Red Team Last performed: 14 days ago
Which of the following recommendations should the analyst make first?

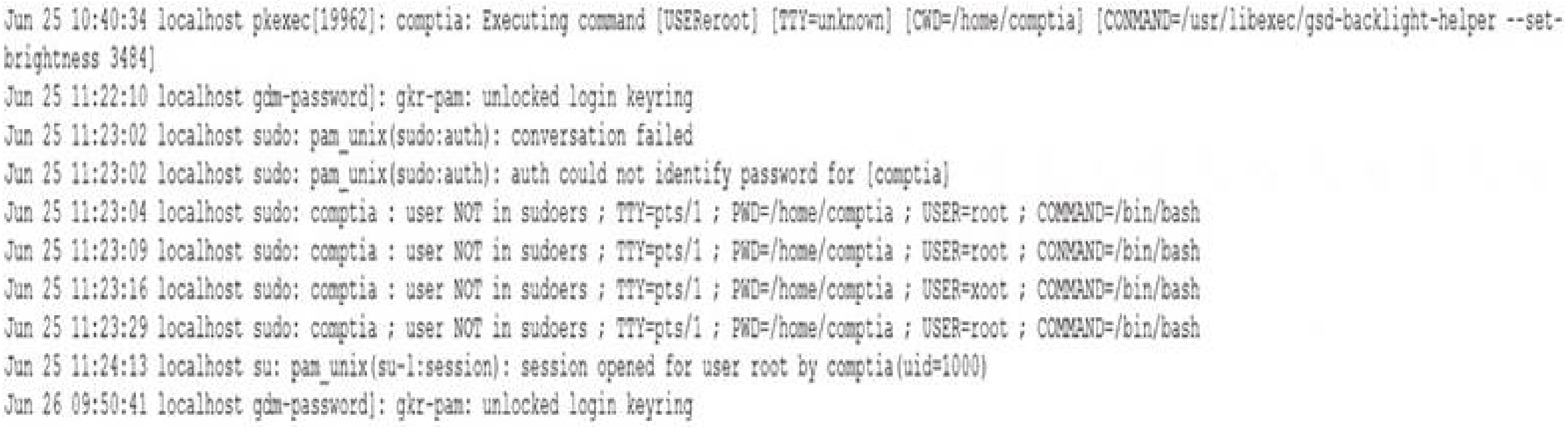
A. Perform a more recent penetration test.
B. Continue vendor onboarding.

C. Disclose details regarding the findings.
D. Have a neutral third party perform a penetration test.

Answer: C

Explanation:
The analyst should disclose details regarding the findings of the vendor's latest penetration test summary as the first recommendation, as this can help assess the vendor's security posture and identify any potential risks or issues that may affect the organization. The analyst should review the findings and ask for more information about the scope, methodology, and remediation actions of the penetration test, as well as any evidence or artifacts that support the findings.

NEW QUESTION 15
When investigating a report of a system compromise, a security analyst views the following /var/log/secure log file:



```
Jun 25 10:40:34 localhost pkexec[19962]: comptia: Executing command [USEReroot] [TTY=unknown] [CWD=/home/comptia] [CONMAND=/usr/libexec/gsd-backlight-helper --set-
brightness 3484]
Jun 25 11:22:10 localhost gdm-password]: gkr-pam: unlocked login keyring
Jun 25 11:23:02 localhost sudo: pam_unix(sudo:auth): conversation failed
Jun 25 11:23:02 localhost sudo: pam_unix(sudo:auth): auth could not identify password for [comptia]
Jun 25 11:23:04 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; COMMAND=/bin/bash
Jun 25 11:23:09 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; CONMAND=/bin/bash
Jun 25 11:23:16 localhost sudo: comptia : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=xoot ; COMMAND=/bin/bash
Jun 25 11:23:29 localhost sudo: comptia ; user NOT in sudoers ; TTY=pts/1 ; PWD=/home/comptia ; USER=root ; COMMAND=/bin/bash
Jun 25 11:24:13 localhost su: pam_unix(su-l:session): session opened for user root by comptia(uid=1000)
Jun 26 09:50:41 localhost gdm-password]: gkr-pam: unlocked login keyring
```

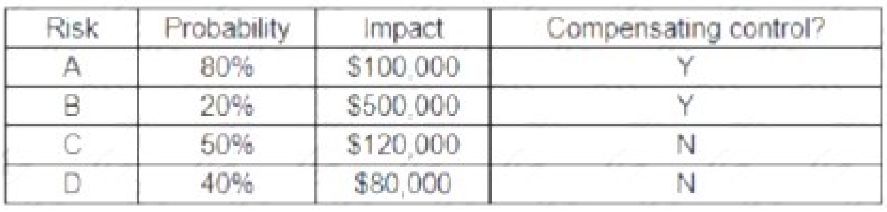
Which of the following can the analyst conclude from viewing the log file?

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

Answer: B

Explanation:
The /var/log/secure log file is a file that records security-related events on a Linux system, such as authentication attempts or sudo commands. The log file shows that the comptia user executed the sudo su command, which allows the user to switch to the root account and gain superuser privileges. The log file does not show that the comptia user knows the sudo password, knows the root password, or added himself or herself to the /etc/sudoers file. Reference:
https://www.cyberciti.biz/faq/linux-log-files-location-and-how-do-i-view-logs-files/

NEW QUESTION 20
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

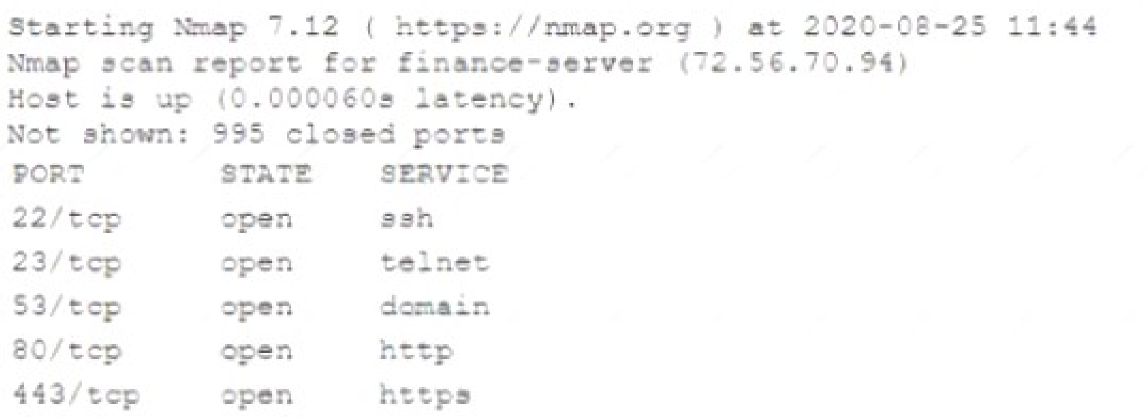
Which of the following is the ordei of priority for risk mitigation from highest to lowest?

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 21
A cybersecunty analyst needs to harden a server that is currently being used as a web server The server needs to be accessible when entenng www company com into the browser Additionally web pages require frequent updates which are performed by a remote contractor Given the following output:



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

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

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

Answer: DF

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

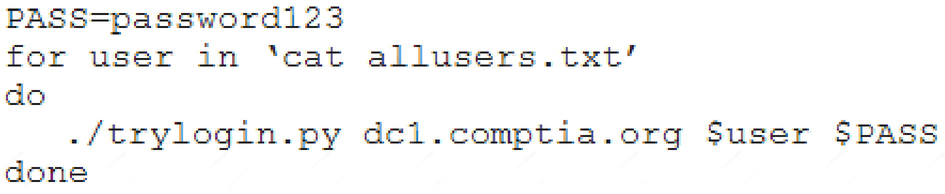
NEW QUESTION 22
An analyst is working on a method to allow secure access to a highly sensi-tive server. The solution must allow named individuals remote access to data contained on the box and must limit access to a single IP address. Which of the following solutions would best meet these requirements?

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 23
When investigating a compromised system, a security analyst finds the following script in the /tmp directory:



```
PASS=password123
for user in 'cat allusers.txt'
do
   ./trylogin.py dc1.comptia.org $user $PASS
done
```

Which of the following attacks is this script attempting, and how can it be mitigated?

A. This is a password-hijacking attack, and it can be mitigated by using strong encryption protocols.
B. This is a password-spraying attack, and it can be mitigated by using multifactor authentication.
C. This is a password-dictionary attack, and it can be mitigated by forcing password changes every 30 days.
D. This is a credential-stuffing attack, and it can be mitigated by using multistep authentication.

Answer: B

Explanation:
https://owasp.org/www-community/attacks/Password_Spraying_Attack
A credential stuffing attack would be using the full credentials and most likely being used across many common platforms. A credential stuffing attack depends on the reuse of passwords. With so many people reusing their passwords for multiple accounts, just one set of credentials is enough to expose most or all of their accounts.

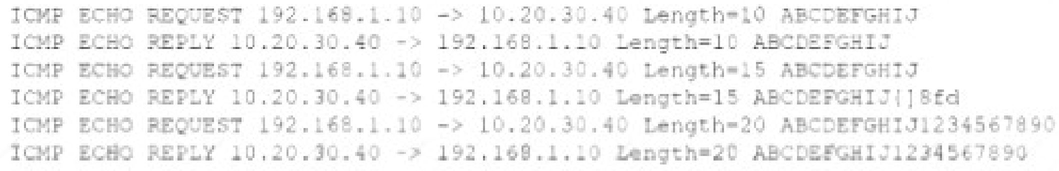
NEW QUESTION 25
A security analyst was transferred to an organization's threat-hunting team to track specific activity throughout the enterprise environment The analyst must observe and assess the number ot times this activity occurs and aggregate the results. Which of the following is the BEST threat-hunting method for the analyst to use?

A. Stack counting
B. Searching
C. Clustering
D. Grouping

Answer: A

Explanation:
Stack counting is the best threat-hunting method for the analyst to use to observe and assess the number of times a specific activity occurs and aggregate the results. Stack counting is a technique that involves collecting data from multiple sources, such as logs, events, or alerts, and grouping them by a common attribute, such as an IP address, a user name, or a process name. Stack counting can help identify patterns, trends, outliers, or anomalies in the data that may indicate malicious activity or compromise.

NEW QUESTION 27
An analyst is reviewing the following output as part of an incident:



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

Which of the Wowing is MOST likely happening?

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

Answer: A

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

NEW QUESTION 30
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

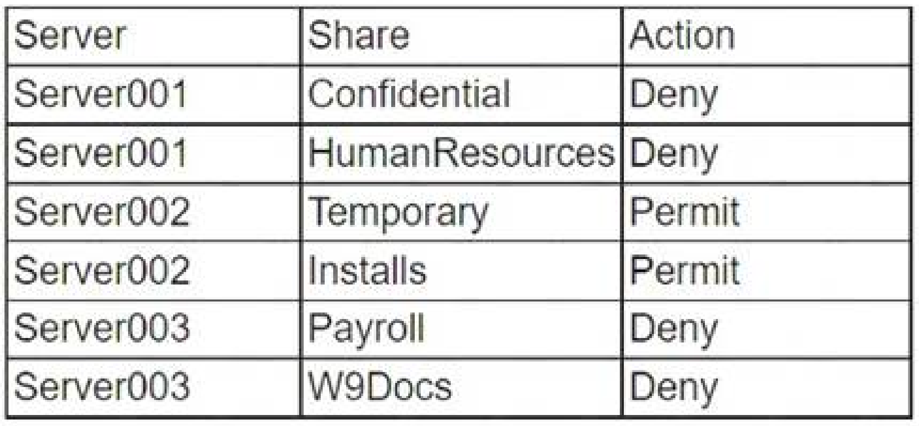
Answer: C

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 32
While reviewing abnormal user activity, a security analyst notices a user has the following fileshare activities:



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

Which of the following should the analyst do first?

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

Answer: A

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

NEW QUESTION 37
A financial institution's business unit plans to deploy a new technology in a manner that violates existing information security standards. Which of the following actions should the Chief Information Security Officer (CISO) take to manage any type of violation?

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

Answer: B

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

NEW QUESTION 38
Which of the following best explains why it is important for companies to implement both privacy and security policies?

A. Private data is insecure by design, so different programs ensure both policies are addressed.
B. Security policies will automatically ensure the data complies with privacy regulations.
C. Privacy policies will satisfy all regulations to secure consumer and sensitive company data.
D. Both policies have some overlap, but the differences can have regulatory consequences.

Answer: D

Explanation:
The correct answer is D. Both policies have some overlap, but the differences can have regulatory consequences. Privacy and security policies are both important for companies to protect their data and comply with various laws and regulations. However, privacy and security policies are not the same, and they have different goals and requirements.
Privacy policies are nontechnical controls that define how a company collects, uses, shares, and protects personal information from its customers, employees, or partners. Privacy policies are based on the principles of data minimization, consent, transparency, and accountability. Privacy policies aim to respect the rights and preferences of data subjects and comply with different privacy regulations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA)1.
Security policies are technical or nontechnical controls that define how a company protects its data and systems from unauthorized access, modification, or destruction. Security policies are based on the principles of confidentiality, integrity, and availability. Security policies aim to prevent or mitigate the impact of cyberattacks and comply with different security standards, such as the Payment Card Industry Data Security Standard (PCI DSS) or the ISO/IEC 27000 series2.
Privacy and security policies have some overlap, as they both involve data protection and compliance. However, they also have some differences, as they address different aspects and risks of data processing. For example, a company may have a strong security policy that encrypts its data, but it may still violate a privacy policy if it collects or shares more data than necessary or without consent. Conversely, a company may have a clear privacy policy that informs its customers about its data practices, but it may still suffer a security breach if it does not implement adequate security measures3.

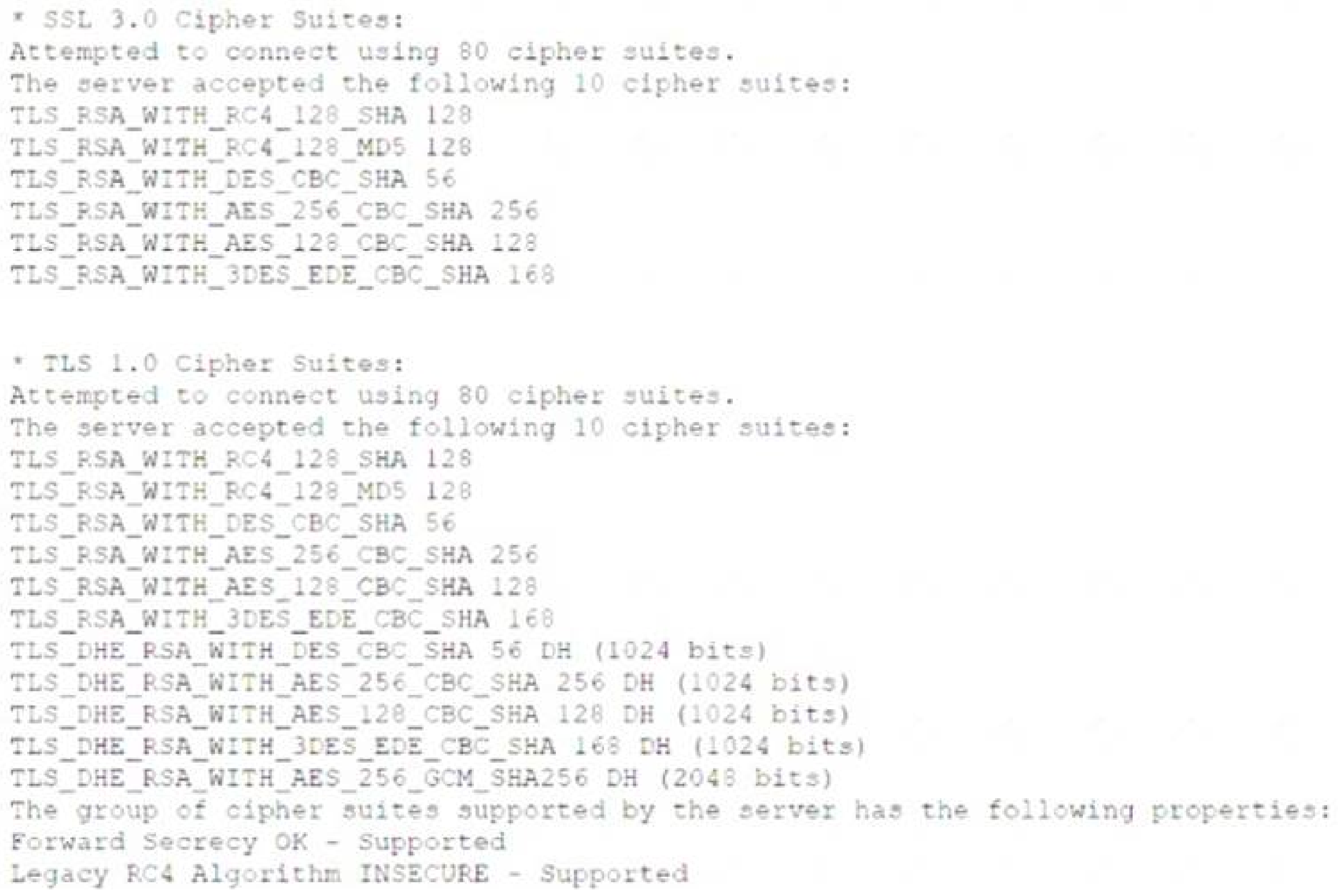
NEW QUESTION 40
After examining a header and footer file, a security analyst begins reconstructing files by scanning the raw data bytes of a hard disk and rebuilding them. Which of the following techniques is the analyst using?

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

Answer: B

Explanation:
File carving is a technique that involves scanning the raw data bytes of a hard disk and rebuilding files by using information found in file headers and footers. File carving can help recover files that have been deleted or corrupted or that are not recognized by the file system. File carving does not rely on metadata or directory structures to locate files, but rather on file signatures or patterns that indicate the start and end of files. File carving can be performed manually or automatically using tools or software that support various file formats. Header analysis (A) is a technique that involves examining file headers to determine file types or formats. Header analysis can help identify files that have been renamed or disguised or that have unknown extensions. Header analysis does not involve reconstructing files by scanning raw data bytes. Metadata analysis © is a technique that involves examining metadata to extract information about files or file systems. Metadata analysis can help determine file attributes such as name, size, date, location, owner, etc. Metadata analysis does not involve reconstructing files by scanning raw data bytes

NEW QUESTION 43
Which of the following lines from this output most likely indicates that attackers could quickly use brute force and determine the negotiated secret session key?



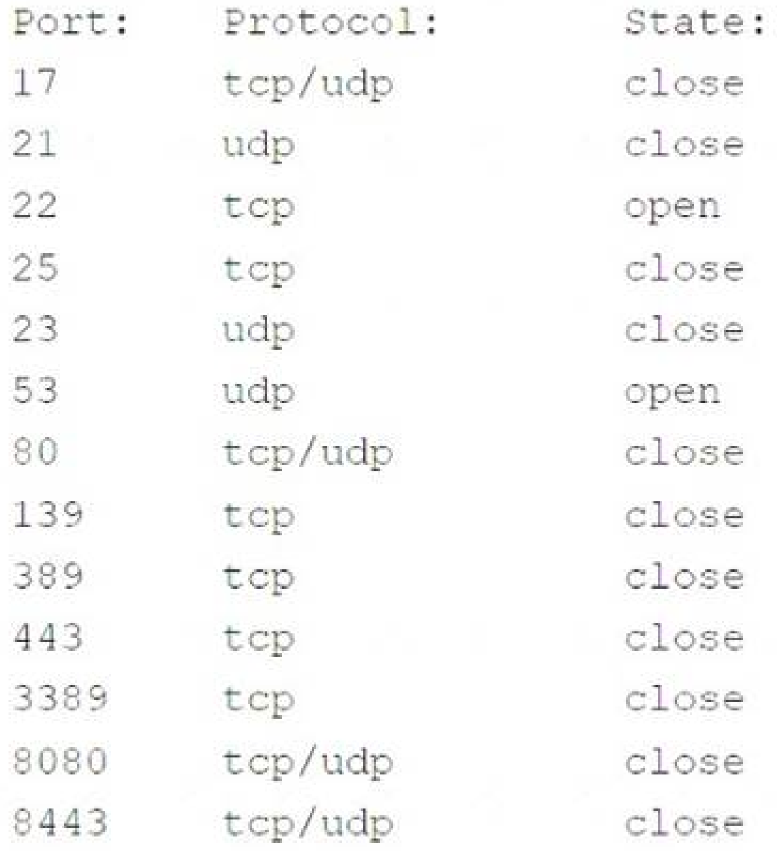
```
* SSL 3.0 Cipher Suites:
Attempted to connect using 80 cipher suites.
The server accepted the following 10 cipher suites:
TLS_RSA_WITH_RC4_128_SHA 128
TLS_RSA_WITH_RC4_128_MD5 128
TLS_RSA_WITH_DES_CBC_SHA 56
TLS_RSA_WITH_AES_256_CBC_SHA 256
TLS_RSA_WITH_AES_128_CBC_SHA 128
TLS_RSA_WITH_3DES_EDE_CBC_SHA 168

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

A. TLS_RSA_WITH_DES_CBC_SHA 56
B. TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128 DH (1024 bits)
C. TLS_RSA_WITH_AES_256_CBC_SHA 256
D. TLS_DHE_RSA_WITH_AES_256_GCM_SHA256 DH (2048 bits)

Answer: B

Explanation:
The line from this output that most likely indicates that attackers could quickly use brute force and determine the negotiated secret session key is TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128 DH (1024 bits). This line indicates that the cipher suite uses Diffie-Hellman ephemeral (DHE) key exchange with RSA authentication, AES 128-bit encryption with cipher block chaining (CBC) mode, and SHA-1 hashing. The DHE key exchange uses a 1024-bit Diffie-Hellman group, which is considered too weak for modern security standards and can be broken by attackers using sufficient computing power. The other lines indicate stronger cipher suites that use longer key lengths or more secure algorithms. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 9;
https://learn.microsoft.com/en-us/windows/win32/secauthn/cipher-suites-in-schannel

NEW QUESTION 44
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 45
A consultant evaluating multiple threat intelligence leads to assess potential risks for a client. Which of the following is the BEST approach for the consultant to consider when modeling the client's attack surface?

A. Ask for external scans from industry peers, look at the open ports, and compare Information with the client.
B. Discuss potential tools the client can purchase lo reduce the livelihood of an attack.
C. Look at attacks against similar industry peers and assess the probability of the same attacks happening.
D. Meet with the senior management team to determine if funding is available for recommended solutions.

Answer: C

Explanation:
A good approach for modeling the client's attack surface is to look at attacks against similar industry peers and assess the probability of the same attacks happening. This can help the consultant to identify the most relevant and likely threats for the client based on their industry sector, size, location, and other factors. This can also help the consultant to prioritize the most critical risks and recommend appropriate mitigation strategies. Asking for external scans from industry peers (A) may not be feasible or reliable, as industry peers may not share their scan results or have different security configurations and vulnerabilities than the client. Discussing potential tools the client can purchase (B) may not be effective, as tools alone cannot reduce the likelihood of an attack without proper implementation and management. Meeting with senior management team (D) may not be helpful, as funding is not directly related to modeling the attack surface and may depend on other factors such as budget constraints and risk appetite.

NEW QUESTION 49
An analyst is responding to an incident within a cloud infrastructure Based on the logs and traffic analysis, the analyst thinks a container has been compromised Which of the following should Ihe analyst do FIRST?

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

Answer: D

Explanation:
The analyst should isolate the container from production using a predefined policy template first. Isolating the container is a containment measure that can help prevent the spread of the compromise to other containers or systems in the cloud infrastructure. Containment is an important step in the incident response process, as it can limit the impact and damage of an incident. Using a predefined policy template can help automate and standardize the isolation process, ensuring that it is done quickly and consistently1.

NEW QUESTION 52
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 53
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 54
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 58
A security team has begun updating the risk management plan incident response plan and system security plan to ensure compliance with secunty review guidelines Which of the (olowing can be executed by internal managers to simulate and validate the proposed changes'?

A. Internal management review
B. Control assessment
C. Tabletop exercise
D. Peer review

Answer: C

Explanation:
A tabletop exercise is a simulation of a security incident or scenario that involves the participation of key stakeholders and decision-makers. It can be used to test and validate the effectiveness of the organization's plans, policies, and procedures, such as the risk management plan, incident response plan, and system security plan. A tabletop exercise can also help identify gaps or weaknesses in the plans and improve the communication and coordination among the participants. An internal management review, a control assessment, a peer review, or a scripting are other possible methods to evaluate and validate a new product's security capabilities, but they are not as comprehensive or interactive as a tabletop exercise. Reference: https://www.csoonline.com/article/3444488/what-is-a-tabletop-exercise-how-to-run-a-security-scenario-in-6-ste

NEW QUESTION 61
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 63
A systems administrator believes a user's workstation has been compromised. The workstation's performance has been lagging significantly for the past several hours. The administrator runs the task list
/ v command and receives the following output:

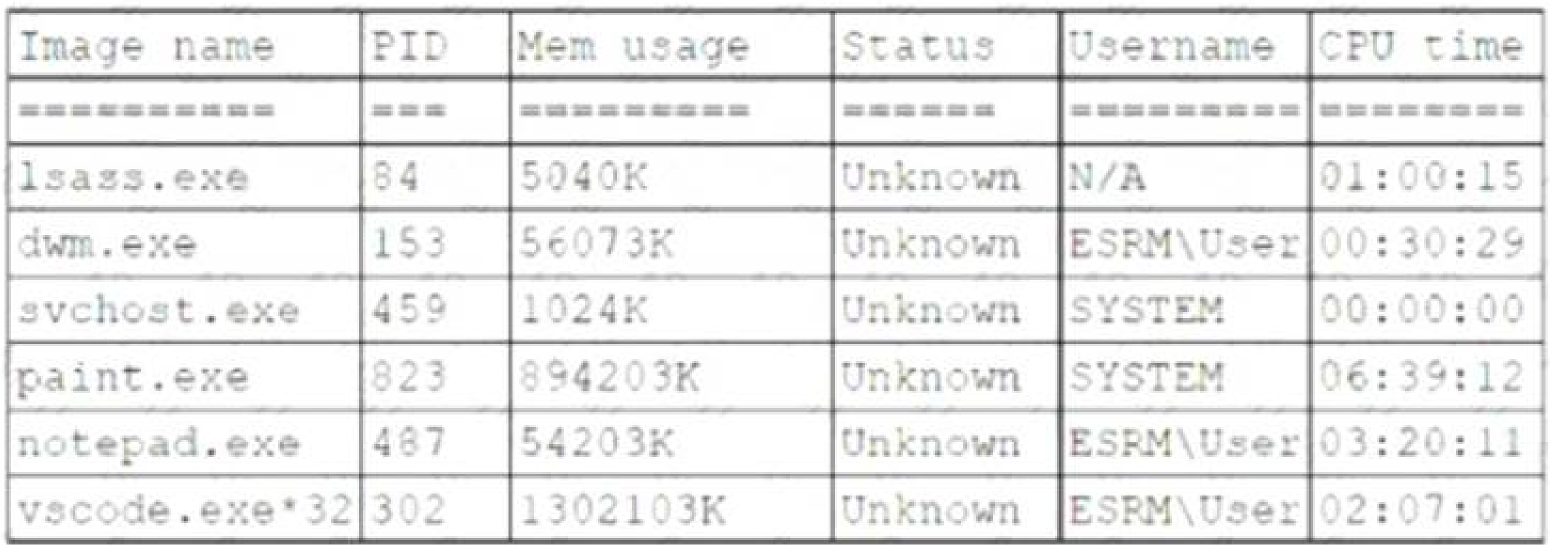


Image name	PID	Mem usage	Status	Username	CPU time
==========	===	=========	======	=========	========
lsass.exe	84	5040K	Unknown	N/A	01:00:15
dwm.exe	153	56073K	Unknown	ESRM\User	00:30:29
svchost.exe	459	1024K	Unknown	SYSTEM	00:00:00
paint.exe	823	894203K	Unknown	SYSTEM	06:39:12
notepad.exe	487	54203K	Unknown	ESRM\User	03:20:11
vscode.exe*32	302	1302103K	Unknown	ESRM\User	02:07:01

Which of the following should a security analyst recognize as an indicator of compromise?

A. dwm.exe being executed under the user context
B. The high usage of vscod
C. exe * 32
D. The abnormal behavior of paint.exe
E. svchost.exe being executed as SYSTEM

Answer: B

Explanation:
The tasklist command is used to display a list of all running processes on a system. In this output, the security analyst should recognize the high memory usage (1302103K) of vscode.exe * 32, which is an indication that this process is consuming a large amount of system resources. This could be a sign that the system has been compromised, as malware often uses system resources to perform malicious activities.

NEW QUESTION 66
A security analyst needs to recommend a solution that will allow users at a company to access cloud-based SaaS services but also prevent them from uploading and exflltrating data. Which of the following solutions should the security analyst recommend?

A. CASB
B. MFA
C. VPN
D. VPS
E. DLP

Answer: A

Explanation:
A cloud access security broker (CASB) is a solution that acts as a gatekeeper between users and cloud-based SaaS services. A CASB can enforce security policies, such as data loss prevention (DLP), encryption, authentication, or access control, to protect sensitive data from unauthorized access, upload, or exfiltration. A CASB can also provide visibility and monitoring of cloud usage and activity1.

NEW QUESTION 68
An analyst receives an alert from the continuous-monitoring solution about unauthorized changes to the firmware versions on several field devices. The asset owners confirm that no firmware version updates were performed by authorized technicians, and customers have not reported any performance issues or outages. Which Of the following actions would be BEST for the analyst to recommend to the asset owners to secure the devices from further exploitation?

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

Answer: C

Explanation:
If were referring to other devices, yes - Implement BIOS passwords before they are compromised. But the ones that were already compromised, they need to be removed from the system to avoid further exploitation. Plus, if you put a password on there, the attacker may now have your password.
Remove the assets from the production network for analysis. If the analyst receives an alert about unauthorized changes to the firmware versions on several field devices, the best action to recommend to the asset owners is to remove the assets from the production network for analysis. This would prevent further exploitation of the devices by isolating them from potential attackers and allow the analyst to investigate the source and nature of the unauthorized changes. Changing the passwords on the devices, implementing BIOS passwords, or reporting the findings to the threat intel community are other possible actions, but they are not as effective or urgent as removing the assets from the production network for analysis. Reference: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

NEW QUESTION 69
An organizational policy requires one person to input accounts payable and another to do accounts receivable. A separate control requires one person to write a check and another person to sign all checks greater than $5,000 and to get an additional signature for checks greater than $10,000. Which of the following controls has the organization implemented?

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

Answer: A

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

NEW QUESTION 72
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 73
An organization implemented an extensive firewall access-control blocklist to prevent internal network ranges from communicating with a list of IP addresses of known command-and-control domains A security analyst wants to reduce the load on the firewall. Which of the following can the analyst implement to achieve similar protection and reduce the load on the firewall?

A. A DLP system
B. DNS sinkholing
C. IP address allow list
D. An inline IDS

Answer: B

Explanation:
DNS sinkholing is a mechanism that can prevent internal network ranges from communicating with a list of IP addresses of known command-and-control domains by returning a false or controlled IP address for those domains. This can reduce the load on the firewall by intercepting the DNS requests before they reach the firewall and diverting them to a sinkhole server. The other options are not relevant or effective for this purpose. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 9; https://www.enisa.europa.eu/topics/incident-response/glossary/dns-sinkhole

NEW QUESTION 78
An employee contacts the SOC to report a high-severity bug that was identified in a new, internally developed web application, which went live in production last week. The SOC staff did not receive contact details or escalation procedures to follow. Which of the following stages of the SDLC
process was overlooked?

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

Answer: B

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

NEW QUESTION 79
A security analyst is correlating, ranking, and enriching raw data into a report that will be interpreted by humans or machines to draw conclusions and create actionable recommendations Which of the following steps in the intelligence cycle is the security analyst performing?

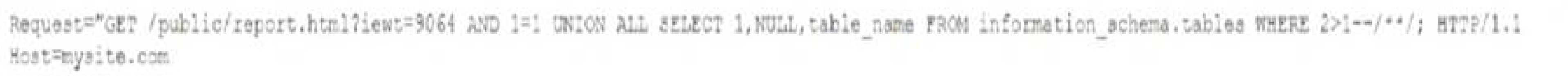
A. Analysis and production
B. Processing and exploitation
C. Dissemination and evaluation
D. Data collection
E. Planning and direction

Answer: B

Explanation:
Processing and exploitation is the step in the intelligence cycle that involves converting raw data into a format that can be used for analysis and producing

intelligence products that can be disseminated to consumers. The security analyst is performing this step by correlating, ranking, and enriching raw data into a report. Analysis and production, dissemination and evaluation, data collection, and planning and direction are other steps in the intelligence cycle, but they do not match the description of the security analyst's task. Reference:
https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-cycle.htm

NEW QUESTION 80
A security analyst is reviewing WAF alerts and sees the following request:



```
Request="GET /public/report.html?iewt=9064 AND 1=1 UNION ALL SELECT 1,NULL,table_name FROM information_schema.tables WHERE 2>1--/**/; HTTP/1.1
Host=mysite.com
```

Which of the following BEST describes the attack?

A. SQL injection
B. LDAP injection
C. Command injection
D. Denial of service

Answer: A

Explanation:
The attack is a SQL injection attack. SQL injection is a type of attack that exploits a security vulnerability in an application's software that allows user input to be executed as SQL commands by the underlying database3. SQL injection can enable an attacker to perform various malicious actions on the database, such as reading, modifying, deleting or creating data; executing commands; or bypassing authentication. The request shows that the attacker has entered a malicious SQL statement in the username parameter that attempts to drop (delete) all tables in the database.

NEW QUESTION 83
Which of me following are reasons why consumer IoT devices should be avoided in an enterprise environment? (Select TWO)

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

Answer: BD

Explanation:
Consumer IoT devices are devices that connect to the internet and provide various functions or services for personal or home use, such as smart speakers, cameras, thermostats, etc. Consumer IoT devices should be avoided in an enterprise environment because they may pose security risks or challenges for the organization's network and data. Some of the reasons why consumer IoT devices should be avoided are:

> The devices may have weak or known passwords: Many consumer IoT devices come with default or hardcoded passwords that are easy to guess or find online. Some devices may not allow users to change their passwords or enforce strong password policies. This can make them vulnerable to brute-force attacks or unauthorized access by attackers.

> The devices may utilize unsecure network protocols: Many consumer IoT devices use unsecure network protocols to communicate with other devices or servers, such as HTTP, FTP, Telnet, etc. These protocols do not encrypt or authenticate the data they transmit or receive, which can expose them to interception, modification, or spoofing by attackers.

NEW QUESTION 84
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 88
During an Incident, it Is determined that a customer database containing email addresses, first names, and last names was exfiltrated. Which ot the following should the security analyst do NEXT?

A. Consult with the legal department for regulatory impact.
B. Encrypt the database with available tools.
C. Email the customers to inform them of the breach.
D. Follow the incident communications process.

Answer: D

Explanation:
An incident communications process is a set of procedures that defines how to communicate with internal and external stakeholders during and after an incident, such as customers, employees, management, regulators and media. An incident communications process can help to provide accurate, timely and consistent information about the incident, its impact and the actions taken to resolve it. An incident communications process can also help to maintain trust and reputation, comply with legal obligations and prevent misinformation or confusion3.

NEW QUESTION 89
Forming a hypothesis, looking for indicators of compromise, and using the findings to proactively improve detection capabilities are examples of the value of:

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

Answer: B

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

NEW QUESTION 94
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 97
A threat hurting team received a new loC from an ISAC that follows a threat actor's profile and activities. Which of the following should be updated NEXT?

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

Answer: D

Explanation:
The IDS signature should be updated next after receiving a new IoC (Indicator of Compromise) from an ISAC (Information Sharing and Analysis Center) that follows a threat actor's profile and activities. An IoC is a piece of evidence or artifact that suggests a system or network has been compromised or attacked by a threat actor4. An IoC can be an IP address, domain name, URL, file hash, email address, registry key, etc. An ISAC is a nonprofit organization that collects, analyzes, and shares threat intelligence and best practices among its members within a specific sector or industry5. An ISAC can help to improve the security awareness and preparedness of its members by providing timely and relevant information about emerging threats and incidents.

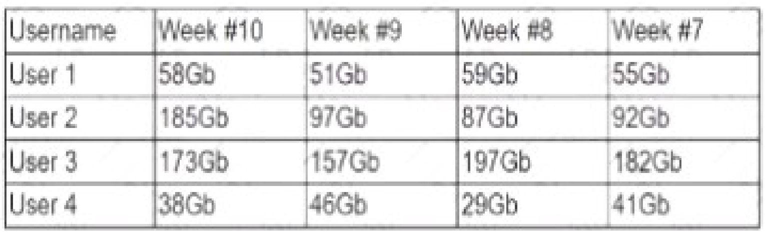
NEW QUESTION 102
A manufacturing company uses a third-party service provider for Tier 1 security support. One of the requirements is that the provider must only source talent from its own country due to geopolitical and national security interests. Which of the following can the manufacturing company implement to ensure the third-party service provider meets this requirement?

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

Answer: A

Explanation:
A secure supply chain program is a set of processes and practices that aim to protect the supply chain from various risks, such as cyberattacks, data breaches, fraud, theft, sabotage, or natural disasters1. A secure supply chain program can help to ensure the integrity, availability, and confidentiality of the products, services, data, and systems involved in the supply chain. A secure supply chain program with governance means that there are clear roles, responsibilities, policies, procedures, and controls for managing the security of the supply chain. This can help to monitor and enforce the compliance of the third-party service provider with the requirement to source talent from its own country. A secure supply chain program with governance can also help to identify and mitigate any potential threats or vulnerabilities in the supply chain. Implementing blacklisting for IP addresses from outside the country (B) may not be sufficient or effective, as IP addresses can be spoofed or bypassed by attackers. Implementing strong authentication controls for all contractors © may not be relevant or adequate, as authentication controls do not prevent the sourcing of talent from other countries. Implementing user behavior analytics for key staff members (D) may not be applicable or useful, as user behavior analytics do not verify the origin or location of the talent.

NEW QUESTION 105
A security analyst is reviewing the following Internet usage trend report:



Username	Week #10	Week #9	Week #8	Week #7
User 1	58Gb	51Gb	59Gb	55Gb
User 2	185Gb	97Gb	87Gb	92Gb
User 3	173Gb	157Gb	197Gb	182Gb
User 4	38Gb	46Gb	29Gb	41Gb

Which of the following usernames should the security analyst investigate further?

A. User1
B. User 2
C. User 3
D. User 4

Answer: D

Explanation:
The Internet usage trend report shows that User 4 has an unusually high amount of data downloaded compared to other users. User 4 downloaded 2.5 GB of data in one day, while the average data downloaded by other users was around 0.2 GB. This could indicate that User 4 is engaged in some suspicious or malicious activity, such as downloading unauthorized or illegal content, exfiltrating sensitive data, or installing malware. Therefore, the security analyst should investigate User 4 further to determine the nature and source of the data downloaded.

NEW QUESTION 107
Ensuring that all areas of security have the proper controls is a primary reason why organizations use:

A. frameworks.
B. directors and officers.
C. incident response plans.
D. engineering rigor.

Answer: A

Explanation:
Ensuring that all areas of security have the proper controls is a primary reason why organizations use frameworks. Frameworks provide an organized structure for organizations to evaluate their security posture and implement the necessary security measures for their operations. Frameworks such as NIST, COBIT, and ISO 27001 provide guidance on how to develop, implement and monitor security policies, controls, and procedures for an organization. Additionally, frameworks provide a benchmark for organizations to measure their security posture against and create a roadmap for continued improvement.

NEW QUESTION 110
A security analyst discovers the accounting department is hosting an accounts receivable form on a public document service. Anyone with the link can access it.
Which of the following threats applies to this situation?

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

Answer: A

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

NEW QUESTION 111
A security analyst needs to provide the development learn with secure connectivity from the corporate network to a three-tier cloud environment. The developers require access to servers in all three tiers in order to perform various configuration tasks. Which of the following technologies should the analyst implement to provide secure transport?

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

Answer: D

Explanation:
What is the difference between VPN and VPC?
Just as a virtual private network (VPN) provides secure data transfer over the public Internet, a VPC provides secure data transfer between a private enterprise and a public cloud provider.
VPN (Virtual Private Network) is a technology that provides secure connectivity from the corporate network to a cloud environment. VPN creates an encrypted tunnel between the two networks, allowing developers to access servers in all three tiers of the cloud environment without exposing their traffic to interception or tampering. VPN can also provide authentication and authorization mechanisms to verify the identity and permissions of the developers.

NEW QUESTION 115
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 119
Which of the following is a reason for correctly identifying APTs that might be targeting an organization?

A. APTs' passion for social justice will make them ongoing and motivated attackers.
B. APTs utilize methods and technologies differently than other threats
C. APTs are primarily focused on financial gam and are widely available over the internet.
D. APTs lack sophisticated methods, but their dedication makes them persistent.

Answer: B

Explanation:
APTs utilize methods and technologies differently than other threats. APTs stand for Advanced Persistent Threats, and they are sophisticated and stealthy attacks that target specific organizations or networks over a long period of time, often with political or financial motives. APTs utilize methods and technologies differently than other threats, such as using custom-made malware, exploiting zero-day vulnerabilities, leveraging social engineering techniques, or employing multiple vectors of attack. APTs can also evade detection by existing security tools or controls, by using encryption, obfuscation, proxy servers, or other techniques to hide their activities or communications.

NEW QUESTION 122
A security analyst responds to a series of events surrounding sporadic bandwidth consumption from an endpoint device. The security analyst then identifies the following additional details:
- Bursts of network utilization occur approximately every seven days.
- The content being transferred appears to be encrypted or obfuscated.
- A separate but persistent outbound TCP connection from the host to infrastructure in a third-party cloud is in place.
- The HDD utilization on the device grows by 10GB to 12GB over the course of every seven days.
- Single file sizes are 10GB.

Which of the following describes the most likely cause of the issue?

A. Memory consumption
B. Non-standard port usage
C. Data exfiltration
D. System update
E. Botnet participant

Answer: C

Explanation:
data exfiltration is the unauthorized transfer of data from an organization’s network to an external destination, usually for malicious purposes such as espionage, sabotage, or theft. The details given in the question suggest that data exfiltration is occurring from an endpoint device. The bursts of network utilization every seven days indicate periodic data transfers. The content being transferred appears to be encrypted or obfuscated to avoid detection or analysis. The persistent outbound TCP connection from the host to infrastructure in a third-party cloud indicates a possible command and control channel for an attacker. The HDD utilization on the device grows by 10GB to 12GB over the course of every seven days, and single file sizes are 10GB, indicating that large amounts of data are being collected and compressed before being exfiltrated.

NEW QUESTION 127
A code review reveals a web application is using lime-based cookies for session management. This is a security concern because lime-based cookies are easy to:

A. parameterize.
B. decode.
C. guess.

D. decrypt.

Answer: B

Explanation:
Lime-based cookies are a type of cookies that use lime encoding to store data in a web browser. Lime
encoding is a simple substitution cipher that replaces each character in a string with another character based on a fixed key. Lime-based cookies are easy to decode because the key is publicly available and the encoding algorithm is simple. Anyone who intercepts or accesses the lime-based cookies can easily decode them and read the data stored in them. This is a security concern because lime-based cookies are often used for session management, which means they store information about the user's identity and preferences on a web application. If an attacker can decode the lime-based cookies, they can impersonate the user or access their sensitive information.

NEW QUESTION 130
During the threat modeling process for a new application that a company is launching, a security analyst needs to define methods and items to take into consideralion Wtiich of the following are part of a known threat modeling method?

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

Answer: C

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

NEW QUESTION 133
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 134
A company's Chief Information Security Officer [CISO) is concerned about the integrity of some highly confidential files. Any changes to these files must be tied back to a specific authorized user's activity session. Which of the following is the best technique to address the CISO's concerns?

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

Answer: B

Explanation:
Regularly use SHA-256 to hash the directory containing the sensitive information. Monitor the files for unauthorized changes. This option is the best technique to ensure the integrity of the files and tie any changes to a specific user session. Hashing is a process that generates a unique value for a given input, and any modification to the input will result in a different hash value. By using SHA-256, which is a secure hashing algorithm, the analyst can compare the hash values of the files before and after each user session and detect any unauthorized changes.

NEW QUESTION 137
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 141
A user receives a potentially malicious attachment that contains spelling errors and a PDF document. A security analyst reviews the email and decides to download the attachment to a Linux sandbox for review. Which of the following commands would most likely indicate if the email is malicious?

A. sha256sum ~/Desktop/fi1e.pdf
B. /bin/;s -1 ~/Desktop/fi1e.pdf
C. strings ~/Desktop/fi1e.pdf | grep -i “<script”
D. cat < ~/Desktop/file.pdf | grep —i .exe

Answer: C

Explanation:
This command would most likely indicate if the email attachment is malicious, as it would display any JavaScript code embedded in the PDF file. JavaScript code can be used by attackers to execute malicious commands or scripts on the victim’s system when the PDF file is opened1. The strings command extracts the printable characters from a binary file, such as a PDF file, and the grep -i “<script” option searches for the presence of JavaScript code in a case-insensitive manner2.

NEW QUESTION 145
A security analyst needs to determine the best method for securing access to a top-secret datacenter Along with an access card and PIN code, which of the following additional authentication methods would be BEST to enhance the datacenter's security?

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

Answer: B

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

NEW QUESTION 148
A Chief Executive Officer (CEO) is concerned the company will be exposed to data sovereignty issues as a result of some new privacy regulations to help mitigate this risk. The Chief Information Security Officer (CISO) wants to implement an appropriate technical control. Which of the following would meet the requirement?

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

Answer: D

Explanation:
Data Sovereignty means that data is subject to the laws and regulations of the geographic location where that data is collected and processed. Data sovereignty is a country-specific requirement that data must remain within the borders of the jurisdiction where it originated. At its core, data sovereignty is about protecting sensitive, private data and ensuring it remains under the control of its owner. You're only worried about that if you're in multiple locations. .
https://www.virtru.com/blog/gdpr-data-sovereignty-matters-globally
Geographic access requirements are an appropriate technical control to implement to mitigate data sovereignty issues. Data sovereignty issues arise when data is subject to different laws and regulations depending on where it is stored or processed. For example, some countries may have stricter data protection or privacy laws than others, or may impose restrictions on cross-border data transfers. Geographic access requirements can help ensure that data is only accessed from locations that comply with the applicable laws and regulations, and prevent unauthorized access from locations that do not.

NEW QUESTION 152
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 153
An employee observes degraded system performance on a Windows workstation. While attempting to access documents, the employee notices the file icons appear abnormal and the file extensions have been changed. The employee instantly shuts down the machine and alerts a supervisor.
Which of the following forensic evidence will be lost as a result of these actions?

A. All user actions prior to shutting down the machine
B. All information stored in the machine's local database
C. All cached items that are queued to be written to the registry
D. Volatile artifacts in the system's memory

Answer: D

Explanation:
Volatile artifacts are data that is stored in a computer’s volatile memory while it is running, such as open network connections, running processes, encryption keys, and internet history. Volatile artifacts can provide
valuable evidence for forensic investigations, especially for detecting and analyzing malware or malicious activities that do not leave traces on the hard drive. However, volatile artifacts are wiped off the system’s memory once the power is turned off, so they cannot be recovered later

NEW QUESTION 158
A security analyst who works in the SOC receives a new requirement to monitor for indicators of compromise. Which of the following is the first action the analyst should take in this situation?

A. Develop a dashboard to track the indicators of compromise.
B. Develop a query to search for the indicators of compromise.
C. Develop a new signature to alert on the indicators of compromise.
D. Develop a new signature to block the indicators of compromise.

Answer: B

Explanation:
Developing a query to search for the indicators of compromise is the first action the analyst should take in this situation. Indicators of compromise (IOCs) are pieces of information that suggest a system or network has been compromised by an attacker. IOCs can include IP addresses, domain names, file hashes, URLs, or other artifacts that are associated with malicious activity. Developing a query to search for IOCs can help to identify any potential incidents or threats in the environment and initiate further investigation or response .

NEW QUESTION 161
A company wants to run a leaner team and needs to deploy a threat management system with minimal human Interaction. Which of the following is the server component of the threat management system that can accomplish this goal?

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

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 164
A security analyst discovers suspicious activity going to a high-value corporate asset. After reviewing the traffic, the security analyst identifies that malware was successfully installed on a machine. Which of the following should be completed first?

A. Create an IDS signature of the malware file.
B. Create an IPS signature of the malware file.
C. Remove the malware from the host.
D. Contact the systems administrator.

Answer: C

Explanation:
According to the CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives1, one of the skills required for the exam is to “apply incident response procedures and analyze potential indicators of
compromise (IOCs)”. The document also states that “the first step in incident response is to contain the incident and prevent further damage” (page 14).
Based on this information, the best answer to your question is C. Remove the malware from the host. This would prevent the malware from spreading to other machines or exfiltrating data from the infected host.

NEW QUESTION 169
An online gaming company was impacted by a ransomware attack. An employee opened an attachment that was received via an SMS attack on a company-issued mobile device while connected to the network. Which of the following actions would help during the forensic analysis of the mobile device? (Select TWO).

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

Answer: CE

Explanation:
Documenting the chain of custody is an important step in the forensic analysis of any device, as it helps to ensure that all evidence is collected and preserved correctly. A memory dump is also essential, as it can provide information about the state of the device when the attack occurred and can be used for further analysis.
Documenting the respective chain of custody can help to preserve the integrity and admissibility of the evidence collected from the mobile device during the forensic analysis. Chain of custody is a record of who handled, accessed or modified the evidence, when, where, how and why . Performing a memory dump of the mobile device for analysis can help to extract volatile data from the mobile device that may contain valuable information about the ransomware attack, such as processes, network connections or encryption keys. Memory dump is a process of copying the contents of the memory (RAM) to a file or storage device .
References: https://www.techopedia.com/definition/23371/chain-of-custody https://www.techopedia.com/definition/10339/memory-dump

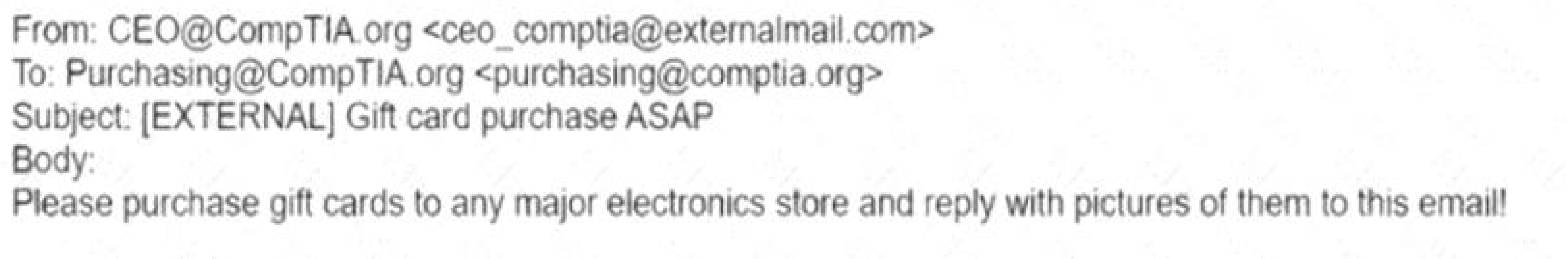
NEW QUESTION 172
Which of the following can detect vulnerable third-parly libraries before code deployment?

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

Answer: C

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

NEW QUESTION 174
An email analysis system notifies a security analyst that the following message was quarantined and requires further review.



From: CEO@CompTIA.org <ceo_comptia@externalmail.com>
To: Purchasing@CompTIA.org <purchasing@comptia.org>
Subject: [EXTERNAL] Gift card purchase ASAP
Body:
Please purchase gift cards to any major electronics store and reply with pictures of them to this email!

Which of the following actions should the security analyst take?

A. Release the email for delivery due to its importance.
B. Immediately contact a purchasing agent to expedite.
C. Delete the email and block the sender.
D. Purchase the gift cards and submit an expense report.

Answer: C

Explanation:
The email message that was quarantined and requires further review is an example of a phishing attempt that tries to trick the recipient into buying gift cards for a fake urgent request from a senior executive. The security analyst should delete the email and block the sender to prevent further attempts from reaching other users in the organization. Releasing the email for delivery, contacting a purchasing agent to expedite, or purchasing the gift cards and submitting an expense report are actions that would fall for the phishing attempt and result in financial loss or reputation damage for the organization. Reference: https://www.csoonline.com/article/3444488/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent

NEW QUESTION 178
A security analyst is scanning the network to determine if a critical security patch was applied to all systems in an enterprise. The Organization has a very low tolerance for risk when it comes to resource availability. Which of the following is the BEST approach for configuring and scheduling the scan?

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

Answer: D

Explanation:
A vulnerability scan is a process of identifying and assessing known vulnerabilities in a system or network
using automated tools or software1

A vulnerability scan can help improve the security posture of a vulnerability management program by detecting and prioritizing potential weaknesses that could be exploited by attackers. To increase the security posture of a vulnerability scan, the following actions can be taken:

- Expand the ports being scanned to include all ports: This means scanning all possible ports on a system or network, not just the well-known or commonly used ones. This can help discover more vulnerabilities that may be hidden or overlooked on less frequently used ports.
- Increase the scan interval to a number the business will accept without causing service interruption: This means scanning more frequently or regularly, but not so often that it causes performance issues or downtime for the system or network. This can help keep up with new vulnerabilities that may emerge over time and reduce the window of opportunity for attackers.
- Enable authentication and perform credentialed scans: This means using login credentials or SSH keys on an asset to get deeper access to its data, processes, configurations, and vulnerabilities2

This can help discover more vulnerabilities that cannot be seen from the network, such as insecure versions of software or poor security permissions.

NEW QUESTION 181
An organization has the following policy statements:
• All emails entering or leaving the organization will be subject to inspection for malware, policy violations, and unauthorized coolant.
•AM network activity will be logged and monitored.
• Confidential data will be tagged and tracked
• Confidential data must never be transmitted in an unencrypted form.
• Confidential data must never be stored on an unencrypted mobile device. Which of the following is the organization enforcing?

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

Answer: B

Explanation:
Data privacy policy is the organization's policy that defines how it collects, uses, stores, and shares personal data of its customers, employees, or other stakeholders. Data privacy policy also covers how the organization complies with relevant data protection laws and regulations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). The policy statements listed in the question are examples of data privacy policy provisions that aim to protect the confidentiality, integrity, and availability of personal data.

NEW QUESTION 184
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 186
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 189
Industry partners from critical infrastructure organizations were victims of attacks on their SCADA devices. The attacker was able to gain access to the SCADA by logging in to an account with weak credentials. Which of the following identity and access management solutions would help to mitigate this risk?

A. Multifactor authentication
B. Manual access reviews
C. Endpoint detection and response
D. Role-based access control

Answer: D

Explanation:
RBAC helps organizations manage access to critical infrastructure networks by assigning access based on roles. This allows organizations to control who can access specific resources and helps eliminate weak credentials that attackers could exploit. Manual reviews and endpoint detection and response can also help to mitigate risk, but role based access control is the best solution for this scenario.

NEW QUESTION 190
To validate local system-hardening requirements, which of the following types of vulnerability scans would work BEST to verify the scanned device meets security policies?

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

Answer: A

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

NEW QUESTION 193
A company's application development has been outsourced to a third-party development team. Based on the SLA. The development team must follow industry best practices for secure coding. Which of the following is the BEST way to verify this agreement?

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

Answer: B

Explanation:
Detailed
Security regression testing is a type of testing that verifies that the security features and functionality of an application are not compromised or broken by any changes or updates in the code2. Security regression testing can help to ensure that the application follows industry best practices for secure coding and does not introduce any new vulnerabilities or weaknesses. Security regression testing can be performed manually or automatically using tools or scripts that check for common security flaws and compliance with security standards. Security regression testing can also help to validate the error-handling capabilities of an application by testing how it responds to different types of inputs and scenarios. Input validation (A) is a technique that checks whether the inputs to an application are valid and expected before processing them3. Input validation can help to prevent some types of security attacks, such as injection attacks or buffer overflows, but it is not a way to verify that an application follows industry best practices for secure
coding. Input validation is part of secure coding, not a way to test it. Application fuzzing © is a technique that tests an application by sending random or malformed inputs to it and observing its behavior4. Application fuzzing can help to discover some types of security vulnerabilities, such as memory leaks or crashes, but it is not a comprehensive way to verify that an application follows industry best practices for secure coding. Application fuzzing may not cover all possible inputs and scenarios and may not check for compliance with security standards. User acceptance testing (D) is a technique that tests an application by involving end users or customers in evaluating its functionality and usability. User acceptance testing can help to ensure that an application meets the user requirements and expectations, but it is not a reliable way to verify that an application follows industry best practices for secure coding. User acceptance testing may not focus on security aspects and may not detect subtle or hidden security flaws. Stress testing (E) is a technique that tests an application by subjecting it to high levels of load or demand. Stress testing can help to evaluate the performance and reliability of an application under extreme conditions, but it is not a relevant way to verify that an application follows industry best practices for secure coding. Stress testing does not check for security issues and may not reflect normal usage patterns.
References: 2: https://www.techopedia.com/definition/31686/resource-exhaustion 3: https://www.techopedia.com/definition/13493/penetration-testing 4: https://www.techopedia.com/definition/25888/security-development-lifecycle-sdl : https://www.techopedia.com/definition/24771/technical-controls : https://www.techopedia.com/definition/32088/vm-escape

NEW QUESTION 197
A security analyst is trying to track physical locations of threat actors via SIEM log information. However, correlating IP addresses with geolocation is taking a long time, so the analyst asks a security engineer to add geolocation to the SIEM tool. This is an example of using:

A. security orchestration, automation, and response.
B. continuous integration.
C. data enrichment.
D. threat feeds.

Answer: C

Explanation:
Data enrichment is a process that adds event and non-event contextual information to security event data in order to transform raw data into meaningful insights123. Geolocation is one example of contextual information that can be used to enrich security event data, such as IP addresses, and provide more information about the physical locations of threat actors. Data enrichment can help security analysts perform threat detection, threat hunting, and incident response more effectively and efficiently.

NEW QUESTION 198
A company offers a hardware security appliance to customers that provides remote administration of a device on the customer's network Customers are not authorized to alter the configuration The company deployed a software process to manage unauthorized changes to the appliance log them, and forward them to a central repository for evaluation Which of the following processes is the company using to ensure the appliance is not altered from its ongmal configured state?

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

Answer: C

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

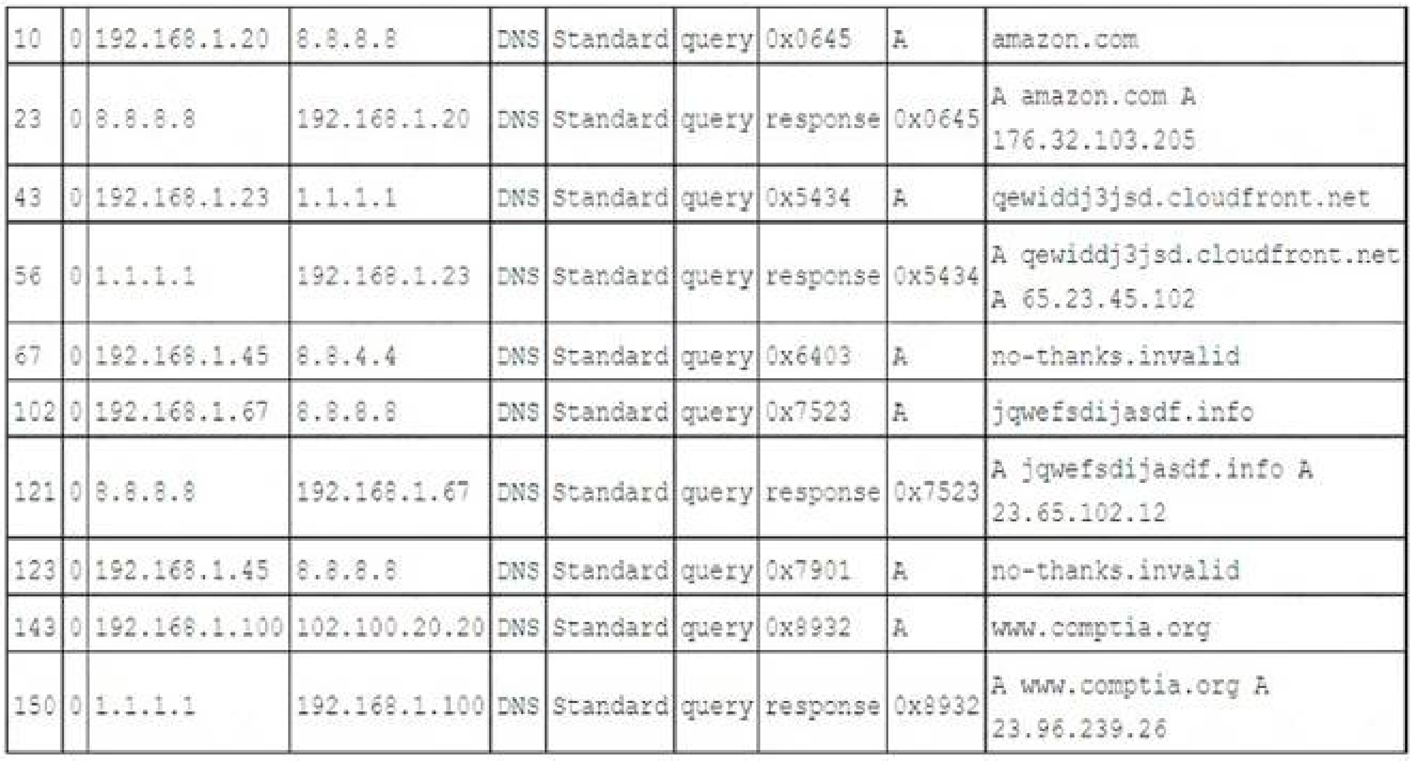
NEW QUESTION 201
A forensics investigator is analyzing a compromised workstation. The investigator has cloned the hard drive and needs to verify that a bit-level image copy of a hard drive is an exact clone of the original hard drive that was collected as evidence. Which of the following should the investigator 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 205
A cybersecurity analyst inspects DNS logs on a regular basis to identify possible IOCs that are not triggered by known signatures. The analyst reviews the following log snippet:



10	0	192.168.1.20	8.8.8.8	DNS	Standard	query	0x0645	A	amazon.com
23	0	8.8.8.8	192.168.1.20	DNS	Standard	query	response	0x0645	A amazon.com A 176.32.103.205
43	0	192.168.1.23	1.1.1.1	DNS	Standard	query	0x5434	A	qewiddj3jsd.cloudfront.net
56	0	1.1.1.1	192.168.1.23	DNS	Standard	query	response	0x5434	A qewiddj3jsd.cloudfront.net A 65.23.45.102
67	0	192.168.1.45	8.8.4.4	DNS	Standard	query	0x6403	A	no-thanks.invalid
102	0	192.168.1.67	8.8.8.8	DNS	Standard	query	0x7523	A	jqwefsdijasdf.info
121	0	8.8.8.8	192.168.1.67	DNS	Standard	query	response	0x7523	A jqwefsdijasdf.info A 23.65.102.12
123	0	192.168.1.45	8.8.8.8	DNS	Standard	query	0x7901	A	no-thanks.invalid
143	0	192.168.1.100	102.100.20.20	DNS	Standard	query	0x8932	A	www.comptia.org
150	0	1.1.1.1	192.168.1.100	DNS	Standard	query	response	0x8932	A www.comptia.org A 23.96.239.26

Which of the following should the analyst do next based on the information reviewed?

A. The analyst should disable DNS recursion.
B. The analyst should block requests to no—thank
C. invalid.
D. The analyst should disconnect host 192.168.1.67.
E. The analyst should sinkhole 102.100.20.20.
F. The analyst should disallow queries to the 8.8.8.8 resolver.

Answer: B

Explanation:
The correct answer is B. The analyst should block requests to no-thanks.invalid. The log snippet shows a DNS query from host 192.168.1.67 to the public resolver 8.8.8.8 for the domain name no-thanks.invalid, which is resolved to the IP address 102.100.20.20. This is a possible indicator of compromise (IOC), as no-thanks.invalid is a known malicious domain that is used by attackers to exfiltrate data or execute
commands on compromised hosts1. The analyst should block requests to this domain to prevent further communication with the attacker's server and investigate the host 192.168.1.67 for signs of infection.
* A. The analyst should disable DNS recursion is not correct. DNS recursion is a process where a DNS server queries other DNS servers on behalf of a client until it finds the authoritative answer for a domain name2.
Disabling DNS recursion would prevent the DNS server from resolving any domain names that are not in its cache or zone files, which would affect the normal functionality of the network and the internet access of the clients.
* C. The analyst should disconnect host 192.168.1.67 is not correct. Disconnecting host 192.168.1.67 would stop the communication with the malicious domain, but it would also disrupt the legitimate activities of the host and its user. Moreover, disconnecting the host would not remove the malware or root cause of the compromise, and it would not prevent the host from reconnecting to the malicious domain once it is online again.
* D. The analyst should sinkhole 102.100.20.20 is not correct. Sinkholing is a technique that redirects malicious or unwanted traffic to a controlled destination, such as a fake or isolated server3. Sinkholing 102.100.20.20 would prevent the communication with the malicious domain, but it would also require access and control over the public resolver 8.8.8.8, which is not owned or managed by the analyst or the company.
* E. The analyst should disallow queries to the 8.8.8.8 resolver is not correct. Disallowing queries to the 8.8.8.8 resolver would prevent the communication with the malicious domain, but it would also affect the resolution of other legitimate domain names that are not in the local DNS server's cache or zone files.
* 1: DNS Tunneling: how DNS can be (ab)used by malicious actors 2: What Is DNS Recursion? 3: What Sinkhole Attack?

NEW QUESTION 208
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 211
Several operator workstations are exhibiting unusual behavior, including applications loading slowly, temporary files being overwritten, and reboot notifications to apply antivirus signatures. During an investigation, an analyst finds evidence of Bitcoin mining. Which of the following is the first step the analyst should take to prevent further spread of the mining operation?

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

Answer: C

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

NEW QUESTION 213
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 217
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.

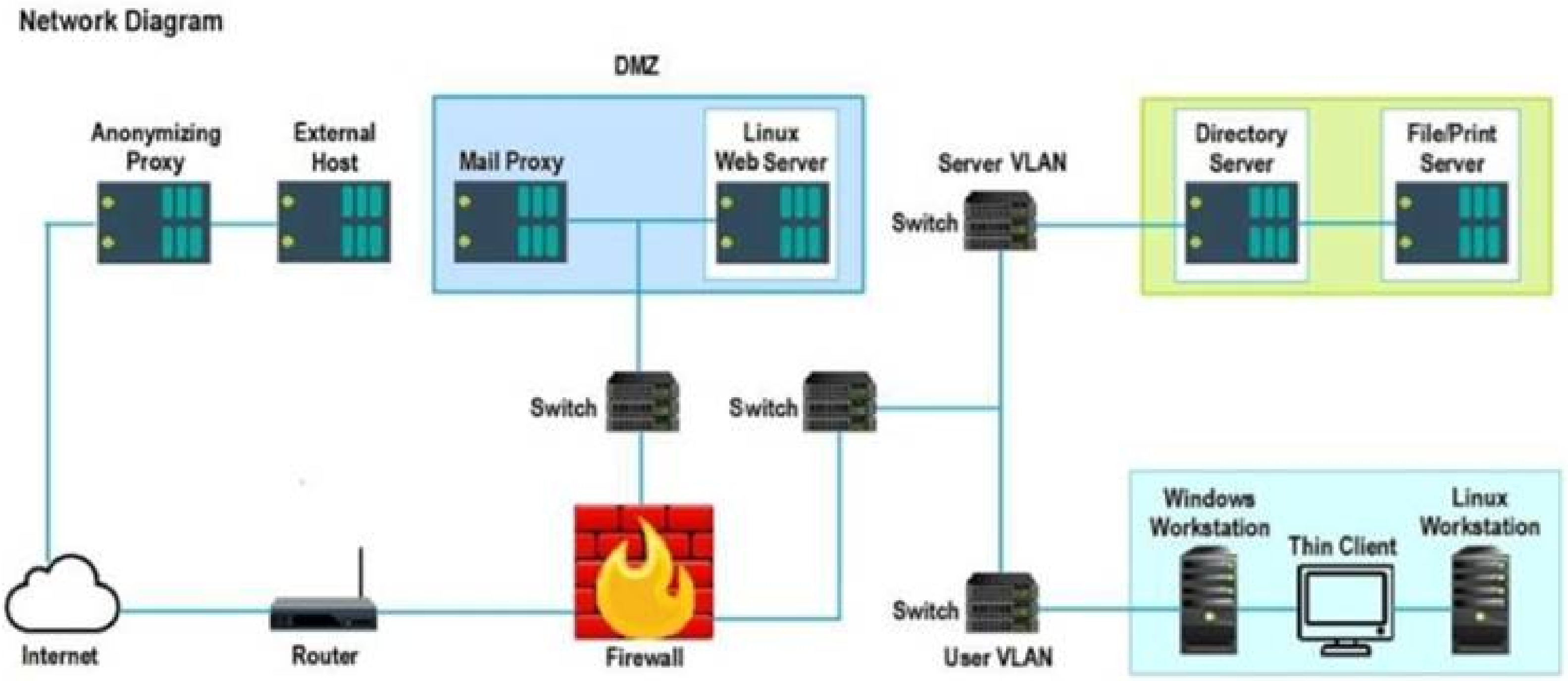
NEW QUESTION 218
A security analyst has received a report that servers are no longer able to connect to the network. After many hours of troubleshooting, the analyst determines a Group Policy Object is responsible for the network connectivity Issues. Which of the following solutions should the security analyst recommend to prevent an interruption of service in the future?

A. Cl/CD pipeline
B. Impact analysis and reporting
C. Appropriate network segmentation
D. Change management process

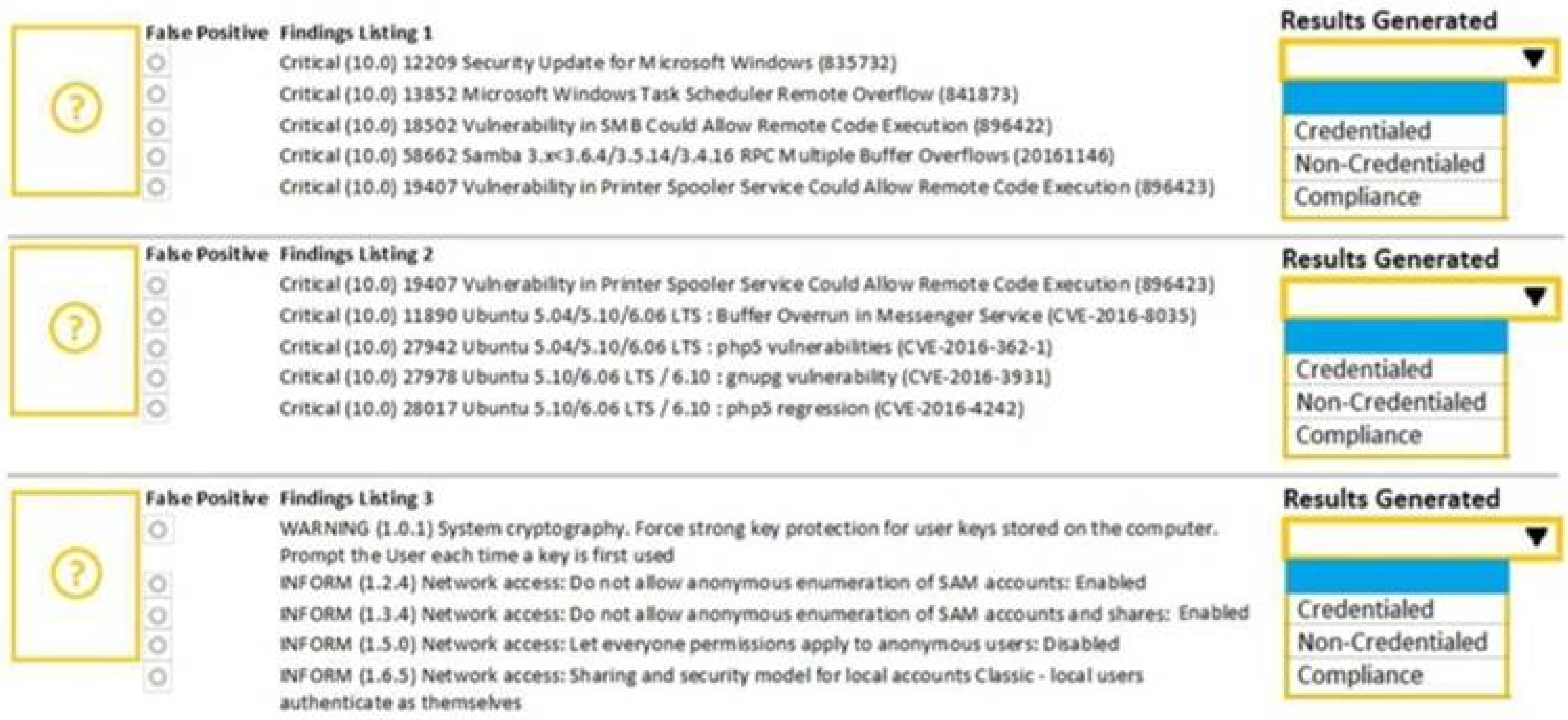
Answer: D

Explanation:
A change management process is a set of procedures that ensures that any changes to a system or service are planned, tested, approved, implemented and documented in a controlled and consistent manner. A change management process can prevent an interruption of service caused by a Group Policy Object (GPO) by ensuring that the GPO is properly configured, tested and authorized before applying it to the servers. A change management process can also provide a way to roll back or undo the changes if they cause any problems.
A CI/CD pipeline is a method of delivering software applications that involves continuous integration (CI) and continuous delivery (CD). CI is the process of merging code changes from multiple developers into a shared repository and testing them automatically. CD is the process of deploying the code changes to different environments (such as testing, staging and production) and releasing them to customers. A CI/CD pipeline does not prevent an interruption of service caused by a GPO, but rather helps to deliver software applications faster and more reliably.
An impact analysis and reporting is a process of assessing the potential effects of a change on a system or service, such as performance, availability, security and compatibility. An impact analysis and reporting can help to identify and mitigate any risks or issues associated with a change. However, an impact analysis and reporting does not prevent an interruption of service caused by a GPO, but rather helps to evaluate and communicate the consequences of a change.
Appropriate network segmentation is a practice of dividing a network into smaller subnetworks or segments based on different criteria, such as function, location or security level. Appropriate network segmentation can improve the performance, security and manageability of a network by reducing congestion, isolating threats and controlling access. However, appropriate network segmentation does not prevent an interruption of service caused by a GPO, but rather helps to protect and optimize a network.

NEW QUESTION 223
A security analyst performs various types of vulnerability scans. Review the vulnerability scan results to determine the type of scan that was executed and if a false positive occurred for each device.
Instructions:
Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan.
For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.
Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results. The Linux Web Server, File-Print Server and Directory Server are draggable.
If at any time you would like to bring back the initial state of the simulation, please select the Reset All button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



Hot Area:



False Positive | Findings Listing 1

- ○ Critical (10.0) 12209 Security Update for Microsoft Windows (835732)
- ○ Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873)
- ○ Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422)
- ○ Critical (10.0) 58662 Samba 3.x<3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146)
- ○ Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)

Results Generated ▼
Credentialed
Non-Credentialed
Compliance

False Positive | Findings Listing 2

- ○ Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)
- ○ Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035)
- ○ Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS : php5 vulnerabilities (CVE-2016-362-1)
- ○ Critical (10.0) 27978 Ubuntu 5.10/6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931)
- ○ Critical (10.0) 28017 Ubuntu 5.10/6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)

Results Generated ▼
Credentialed
Non-Credentialed
Compliance

False Positive | Findings Listing 3

- ○ WARNING (1.0.1) System cryptography. Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used
- ○ INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled
- ○ INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled
- ○ INFORM (1.5.0) Network access: Let everyone permissions apply to anonymous users: Disabled
- ○ INFORM (1.6.5) Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves

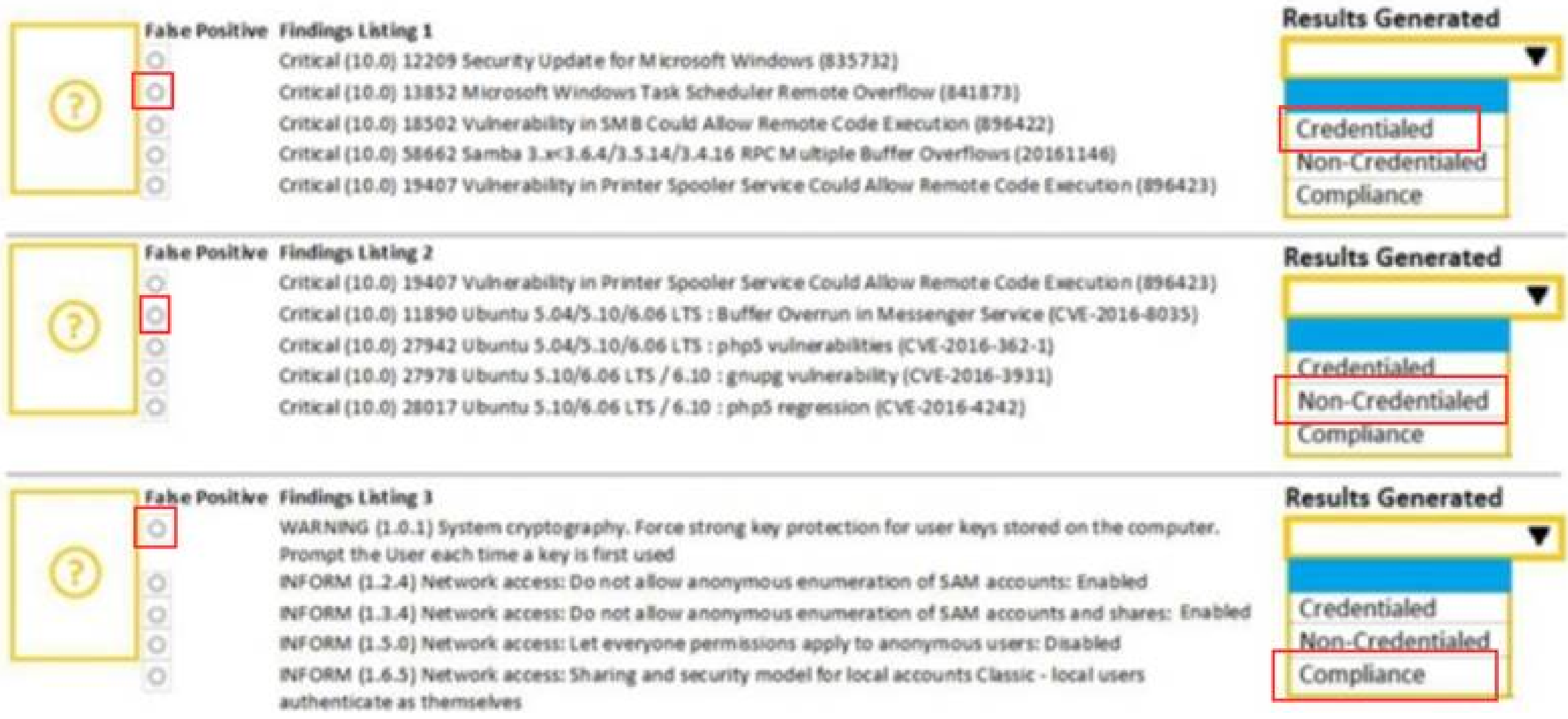
Results Generated ▼
Credentialed
Non-Credentialed
Compliance

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Hot Area:



False Positive | Findings Listing 1

- ○ Critical (10.0) 12209 Security Update for Microsoft Windows (835732)
- [✓ ○] Critical (10.0) 13852 Microsoft Windows Task Scheduler Remote Overflow (841873)
- ○ Critical (10.0) 18502 Vulnerability in SMB Could Allow Remote Code Execution (896422)
- ○ Critical (10.0) 58662 Samba 3.x<3.6.4/3.5.14/3.4.16 RPC Multiple Buffer Overflows (20161146)
- ○ Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)

Results Generated ▼
[✓ Credentialed]
Non-Credentialed
Compliance

False Positive | Findings Listing 2

- ○ Critical (10.0) 19407 Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423)
- [✓ ○] Critical (10.0) 11890 Ubuntu 5.04/5.10/6.06 LTS : Buffer Overrun in Messenger Service (CVE-2016-8035)
- ○ Critical (10.0) 27942 Ubuntu 5.04/5.10/6.06 LTS : php5 vulnerabilities (CVE-2016-362-1)
- ○ Critical (10.0) 27978 Ubuntu 5.10/6.06 LTS / 6.10 : gnupg vulnerability (CVE-2016-3931)
- ○ Critical (10.0) 28017 Ubuntu 5.10/6.06 LTS / 6.10 : php5 regression (CVE-2016-4242)

Results Generated ▼
Credentialed
[✓ Non-Credentialed]
Compliance

False Positive | Findings Listing 3

- [✓ ○] WARNING (1.0.1) System cryptography. Force strong key protection for user keys stored on the computer. Prompt the User each time a key is first used
- ○ INFORM (1.2.4) Network access: Do not allow anonymous enumeration of SAM accounts: Enabled
- ○ INFORM (1.3.4) Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled
- ○ INFORM (1.5.0) Network access: Let everyone permissions apply to anonymous users: Disabled
- ○ INFORM (1.6.5) Network access: Sharing and security model for local accounts Classic - local users authenticate as themselves

Results Generated ▼
Credentialed
Non-Credentialed
[✓ Compliance]

NEW QUESTION 228
Wncn ol the following provides an automated approach 10 checking a system configuration?

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

Answer: A

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

NEW QUESTION 230
An analyst is coordinating with the management team and collecting several terabytes of data to analyze using advanced mathematical techniques in order to find patterns and correlations in events and activities. Which of the following describes what the analyst is doing?

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

Answer: C

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

NEW QUESTION 235
......

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