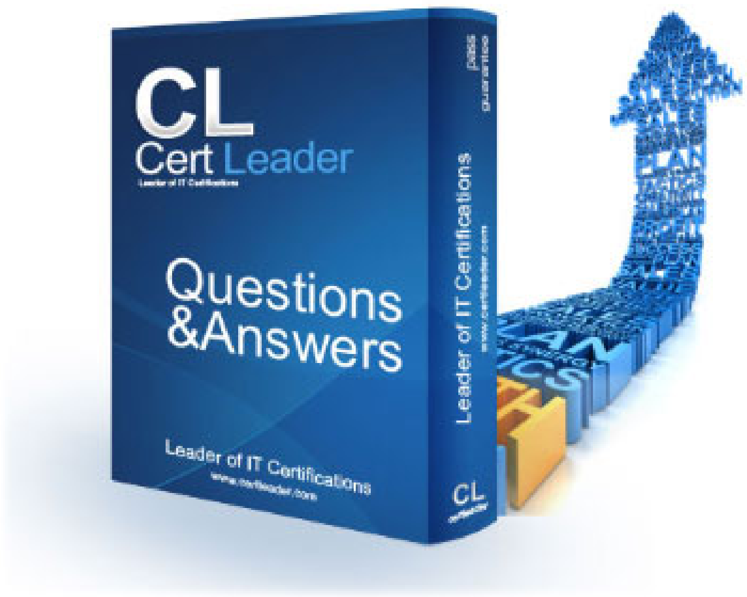
CS0-002 Dumps

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

https://www.certleader.com/CS0-002-dumps.html



NEW QUESTION 1
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 2
An application has been updated to fix a vulnerability. Which of the following would ensure that previously patched vulnerabilities have not been reintroduced?

A. Stress testing
B. Regression testing
C. Code review
D. Peer review

Answer: B

Explanation:
Regression testing is a type of software testing that ensures that a recent program or code change has not adversely affected existing features123 Regression testing is useful for checking if previously patched vulnerabilities have not been reintroduced by the new update.
Stress testing is a type of software testing that evaluates the performance and reliability of a system under extreme conditions, such as high load, limited resources, or concurrent users. Stress testing is not directly related to checking for vulnerabilities.
Code review is a process of examining the source code of a software program to find and fix errors, improve quality, and ensure compliance with standards and best practices. Code review can help prevent vulnerabilities from being introduced in the first place, but it does not verify that existing features are working as expected after a code change.
Peer review is a process of evaluating the work of another person or group of people, such as a research paper, a report, or a design. Peer review can provide feedback and suggestions for improvement, but it does not test the functionality or security of a software product.

NEW QUESTION 3
Due to a rise m cyberattackers seeking PHI, a healthcare company that collects highly sensitive data from millions of customers is deploying a solution that will ensure the customers' data is protected by the organization internally and externally Which of the following countermeasures can BEST prevent the loss of customers' sensitive data?

A. Implement privileged access management
B. Implement a risk management process
C. Implement multifactor authentication
D. Add more security resources to the environment

Answer: A

Explanation:
Implementing privileged access management (PAM) would be the best countermeasure to prevent the loss of customers’ sensitive data due to a rise in cyberattackers seeking PHI (Protected Health Information). PAM is a solution that helps to control and monitor the access and use of privileged accounts, such as administrator or root accounts, that have elevated permissions or access to sensitive data. PAM can help prevent unauthorized or accidental use of privileged accounts by enforcing strict access policies, such as requiring approval, authentication, or auditing for each access request. PAM can also help rotate or expire the passwords of privileged accounts to reduce the risk of compromise2. PAM can help protect PHI from cyberattackers who may try to exploit privileged accounts to access or exfiltrate sensitive data.

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.

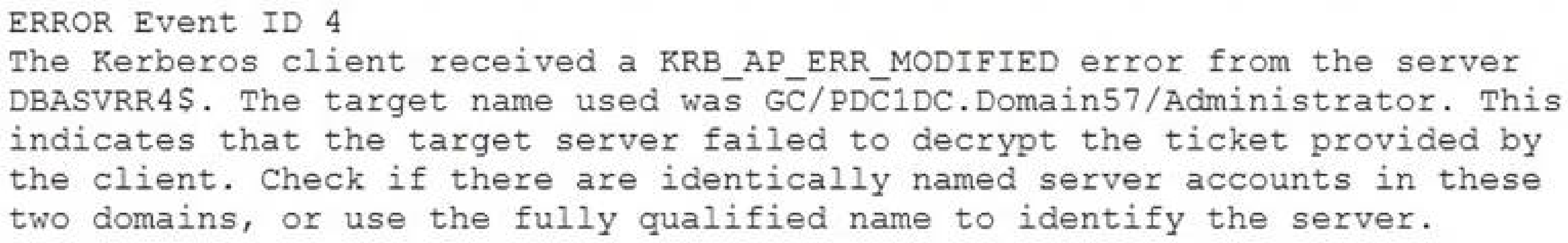
NEW QUESTION 6
A security technician configured a NIDS to monitor network traffic. Which of the following is a condition in which harmless traffic is classified as a potential network attack?

A. True positive
B. True negative
C. False positive
D. False negative

Answer: C

Explanation:
A false positive is a condition in which harmless traffic is classified as a potential network attack by a NIDS. A NIDS is a network intrusion detection system that monitors network traffic for any signs of malicious or anomalous activity. A false positive can result in unnecessary alerts or actions by the NIDS, such as blocking legitimate traffic or generating false alarms. False positives can be caused by various factors, such as misconfigured rules, outdated signatures, noisy network traffic or benign anomalies3 .

NEW QUESTION 7
A security analyst reviews SIEM logs and discovers the following error event:



```
ERROR Event ID 4
The Kerberos client received a KRB_AP_ERR_MODIFIED error from the server
DBASVRR4$. The target name used was GC/PDC1DC.Domain57/Administrator. This
indicates that the target server failed to decrypt the ticket provided by
the client. Check if there are identically named server accounts in these
two domains, or use the fully qualified name to identify the server.
```

Which of the following environments does the analyst need to examine to continue troubleshooting the event?

A. Proxy server
B. SQL server
C. Windows domain controller
D. WAF appliance
E. DNS server

Answer: C

Explanation:
A Windows domain controller is a server that manages authentication and authorization for users and computers in a Windows domain. A Windows domain controller uses Active Directory Domain Services (AD DS) to store information about users, groups, computers, policies, and other objects in a domain. A Windows domain controller can generate event logs that record various activities and events related to security, system, application, etc. The event log shown in the question indicates that it was generated by a Windows domain controller with an IP address of 10.0.0.1 and a hostname of DC01.

NEW QUESTION 8

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 laC templates
D. Reducing laaS 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 9
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 10
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 10
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 12
Which of the following is an advantage of continuous monitoring as a way to help protect an enterprise?

A. Continuous monitoring leverages open-source tools, thereby reducing cost to the organization.
B. Continuous monitoring responds to active Intrusions without requiring human assistance.

C. Continuous monitoring blocks malicious activity by connecting to real-lime threat feeds.
D. Continuous monitoring uses automation to identify threats and alerts in real time

Answer: D

Explanation:
Continuous monitoring uses automation to identify threats and alerts in real time. This is an advantage of continuous monitoring as a way to help protect an enterprise because it enables faster detection and response to security incidents, reduces the risk of human error, and improves the overall security posture and compliance of the organization.

NEW QUESTION 15
A security officer needs to find the most cost-effective solution to the current data privacy and protection gap found in the last security assessment Which of the following is the BEST recommendation?

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

Answer: B

Explanation:
Creating a data minimization plan would be the most cost-effective solution to the current data privacy and protection gap found in the last security assessment. Data minimization is a principle that states that organizations should collect, store, process, and retain only the minimum amount of personal data that is necessary for their legitimate purposes. Data minimization can help reduce the risk of data breaches, data leaks, or data misuse by limiting the exposure and access to sensitive data. Data minimization can also help comply with data protection regulations, such as the General Data Protection Regulation (GDPR), that require organizations to justify their data collection and processing activities. Data minimization can be achieved by implementing various measures, such as deleting or anonymizing unnecessary data, applying retention policies, or using encryption or pseudonymization techniques.

NEW QUESTION 20
A security operations manager wants some recommendations for improving security monitoring. The security team currently uses past events to create an IOC list for monitoring.
Which of the following is the best suggestion for improving monitoring capabilities?

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

Answer: C

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

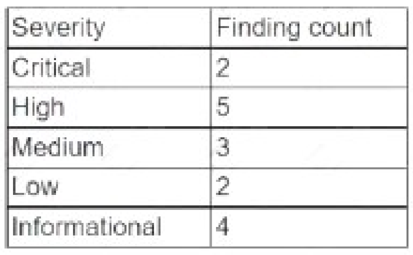
NEW QUESTION 25
An analyst reviews the most recent vulnerability management report and notices a firewall with 99.98% required uptime is reporting different firmware versions on scans than were reported in previous scans. The vendor released new firewall firmware a few months ago. Which of the following will the analyst most likely do next given the requirements?

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

Answer: B

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

NEW QUESTION 27
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?

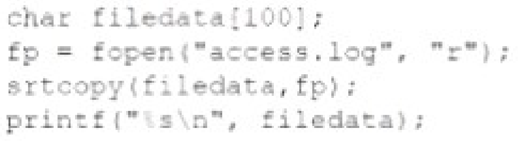
A. Perform a more recent penetration test.
B. Continue vendor onboarding.

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 31
An internally developed file-monitoring system identified the following except as causing a program to crash often:



```
char filedata[100];
fp = fopen("access.log", "r");
srtcopy(filedata,fp);
printf("%s\n", filedata);
```

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

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

Answer: B

Explanation:
The security analyst should recommend replacing the strcpy function with a safer alternative. The strcpy function is a C library function that copies a string from one buffer to another. However, this function does not check the size of the destination buffer, which can lead to buffer overflow vulnerabilities if the source string is longer than the destination buffer. Buffer overflow vulnerabilities can allow attackers to execute arbitrary code or crash the program. A safer alternative to strcpy is strncpy, which limits the number of characters copied to the size of the destination buffer.

NEW QUESTION 34
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 36
An organization is concerned about the security posture of vendors with access to its facilities and systems. The organization wants to implement a vendor review process to ensure \hi> policies implemented by vendors are in line with its own. Which of the following will provide the highest assurance of compliance?

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

Answer: C

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

NEW QUESTION 40
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.

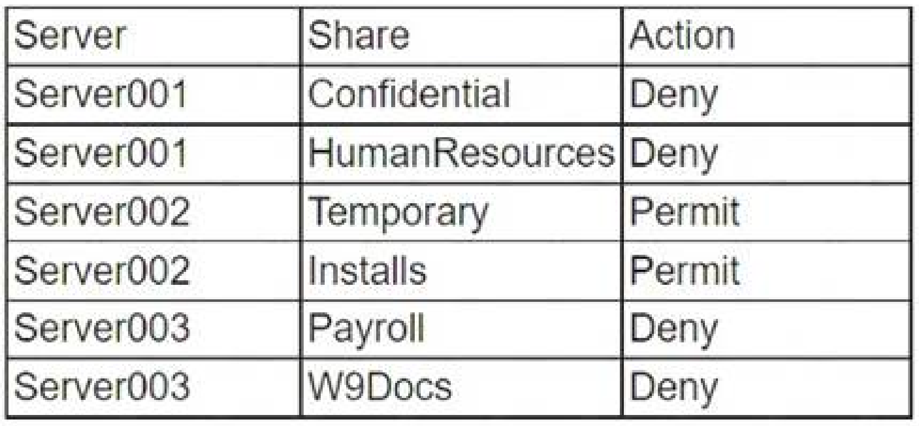
NEW QUESTION 42
A company's Chief Information Security Officer (CISO) published an Internet usage policy that prohibits employees from accessing unauthorized websites. The IT department whitelisted websites used for business needs. The CISO wants the security analyst to recommend a solution that would improve security and support employee morale. Which of the following security recommendations would allow employees to browse
non-business-related websites?

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

Answer: A

Explanation:
A virtual machine alternative is a solution that allows employees to access non-business-related websites on a separate virtual machine that is isolated from the company's network and data. This way, the employees can browse the internet without compromising the security or performance of the company's systems3

NEW QUESTION 43
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 47
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 49
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

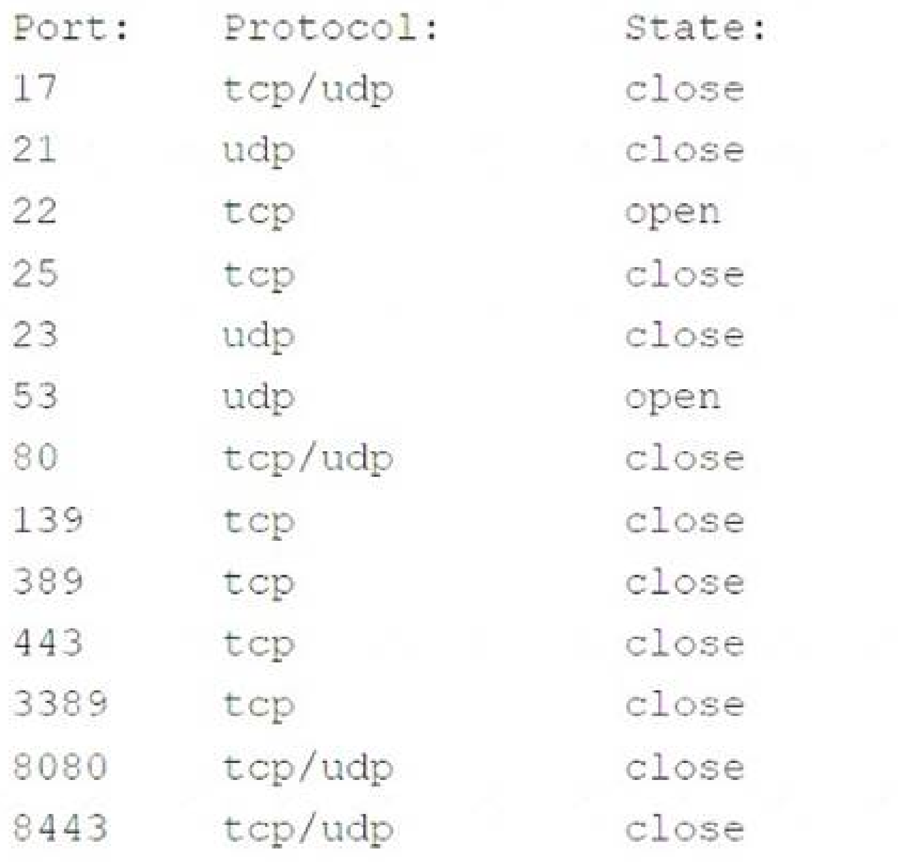
NEW QUESTION 52
An application developer needs help establishing a digital certificate for a new application. Which of the following illustrates a certificate management best practice?

A. Ensure the certificate Is applied to the certificate revocation list.
B. Ensure the certificate key algorithm is SHA-1 compliant.
C. Ensure the certificate is requested from a trusted CA.
D. Ensure the developer has self-signed the certificate.
E. Ensure the certificate key is less than 1028 bits long.

Answer: C

Explanation:
The best practice for establishing a digital certificate for a new application is to ensure the certificate is requested from a trusted CA. A CA stands for Certificate Authority, and it is an entity that issues and verifies digital certificates, which are electronic documents that contain a public key and a digital signature that prove the identity and authenticity of an application, a website, or a person. Requesting a certificate from a trusted CA can help ensure that the certificate is valid, secure, and recognized by other parties.

NEW QUESTION 55
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)?]

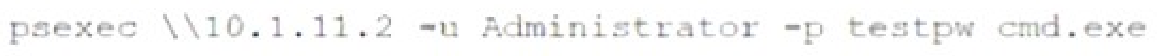
NEW QUESTION 56
A security analyst is concerned about sensitive data living on company file servers following a zero-day attack that nearly resulted in a breach of millions of customer records. The after action report indicates a lack of controls around the file servers that contain sensitive data. Which of the following DLP considerations would best help the analyst to classify and address the sensitive data on the file servers?

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

Answer: C

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

NEW QUESTION 60
While reviewing system logs, a network administrator discovers the following entry:



```
psexec \\10.1.11.2 -u Administrator -p testpw cmd.exe
```

Which of the following occurred?

A. An attempt was made to access a remote workstation.
B. The PsExec services failed to execute.
C. A remote shell failed to open.
D. A user was trying to download a password file from a remote system.

Answer: D

Explanation:
The output shows an entry from a system log that indicates a user was trying to download a password file from a remote system using PsExec. PsExec is a command-line tool that allows users to execute processes on remote systems. The entry shows that the user “administrator” tried to run PsExec with the following parameters: \192.168.1.100 -u administrator -p P@ssw0rd -c cmd.exe /c type c:\windows\system32\config\SAM > \192.168.1.101\c$\temp\sam.txt This means that the user tried to connect to the remote system with IP address 192.168.1.100 using the username “administrator” and password “P@ssw0rd”, copy cmd.exe to the remote system, and execute it with the command “type c:\windows\system32\config\SAM > \192.168.1.101\c$\temp\sam.txt”. This command attempts to read the SAM file, which contains hashed passwords of local users, and write it to a file on another system with IP address 192.168.1.101. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 8; https://docs.microsoft.com/en-us/sysinternals/downloads/psexec

NEW QUESTION 64
Which of the following attack techniques has the GREATEST likelihood of quick success against Modbus assets?

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

Answer: C

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

NEW QUESTION 67
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 72
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 76
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 77
A security analyst discovers the company's website is vulnerable to cross-site scripting. Which of the following solutions will best remedy the vulnerability?

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

Answer: B

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

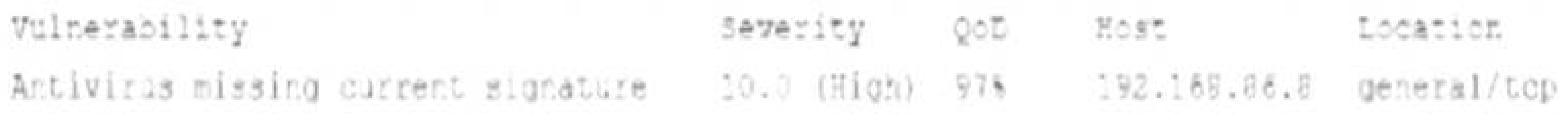
NEW QUESTION 79
An employee contacts the SOC to report a high-severity bug that was identified in a new, internally developed web application, which went live in production last week. The SOC staff did not receive contact details or escalation procedures to follow. Which of the following stages of the 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 84
A security is reviewing a vulnerability scan report and notes the following finding:



Vulnerability	Severity	QoD	Host	Location
Antivirus missing current signature	10.0 (High)	97%	192.168.86.8	general/tcp

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

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

Answer: D

Explanation:
The vulnerability scan report shows that the workstation has a high-risk vulnerability (CVE-2019-0708) that affects Remote Desktop Services on Windows systems. This vulnerability allows remote code execution without authentication or user interaction, and can be exploited by sending specially crafted requests to the target system1
As part of the detection and analysis procedures, the analyst should confirm the workstation's
signatures against the most current signatures. This can help verify if the workstation has been patched or updated to address the vulnerability, or if it is still vulnerable and needs remediation. The analyst can use tools such as Windows Update or Microsoft Baseline Security Analyzer to check the workstation's patch level and compare it with the latest available signatures.

NEW QUESTION 88
During an incident response procedure, a security analyst extracted a binary file from the disk of a compromised server. Which of the following is the best approach for analyzing the file without executing it?

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

Answer: C

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

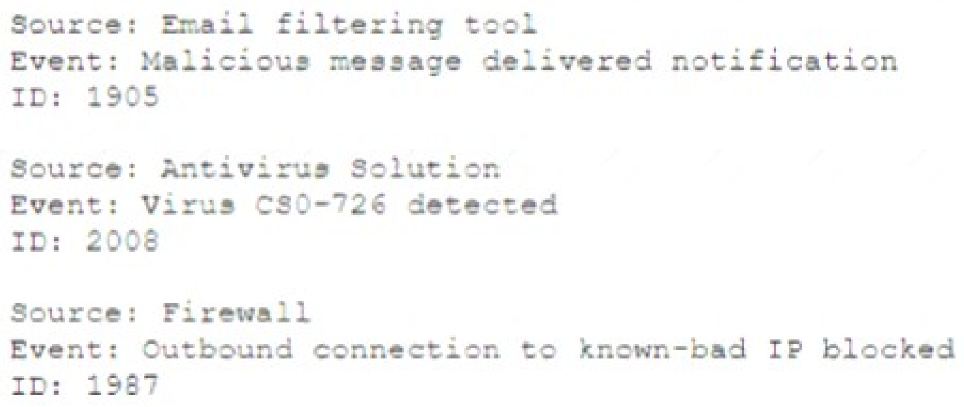
NEW QUESTION 91
A security analyst works for a biotechnology lab that is planning to release details about a new cancer treatment. The analyst has been instructed to tune the SIEM softvare and IPS in preparation for the
announcement. For which of the following concerns will the analyst most likely be monitoring?

A. Intellectual property loss
B. PII loss
C. Financial information loss
D. PHI loss

Answer: A

Explanation:
SIEM software is a tool that provides a single centralized platform for the collection, monitoring, and management of security-related events and log data from across the enterprise1. SIEM software can help security analysts detect, investigate, and respond to threats, as well as comply with regulations and standards.
IPS stands for Intrusion Prevention System. It is a device or software that monitors network traffic and blocks or modifies malicious packets before they reach their destination2. IPS can help security analysts prevent attacks, protect sensitive data, and reduce network downtime.
A security analyst working for a biotechnology lab that is planning to release details about a new cancer treatment would most likely be monitoring for A. Intellectual property loss. Intellectual property (IP) refers t the creations of the mind, such as inventions, designs, artistic works, or trade secrets3. IP loss occurs when someone steals, leaks, or misuses the IP of an organization without authorization.
The biotechnology lab's new cancer treatment is an example of IP that has high value and potential impact on the market and society. Therefore, the security analyst would want to protect it from competitors, hackers, or other malicious actors who might try to access it illegally or sabotage it. The security analyst would use SIEM software and IPS to monitor for any signs of unauthorized access, data exfiltration, or tampering with the lab's network or systems.

NEW QUESTION 94
A security analyst needs to automate the incident response process for malware infections. When the following logs are generated, an alert email should automatically be sent within 30 minutes:



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

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

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

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

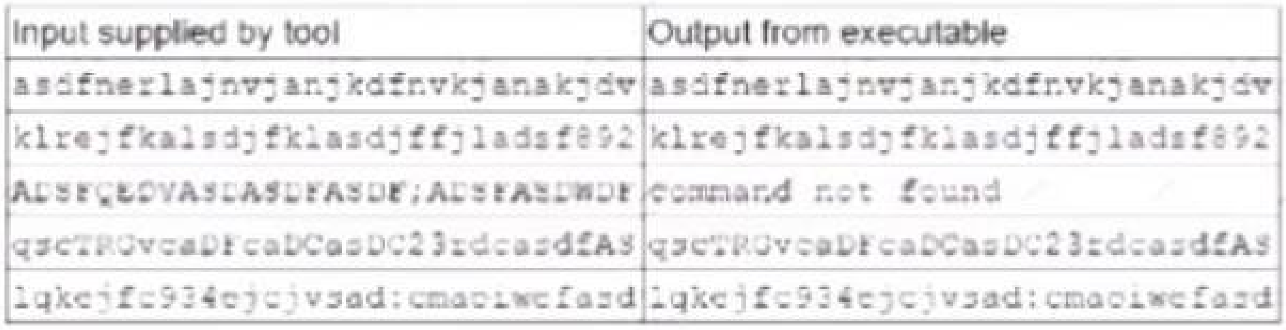
A. Deploy a signature-based IDS

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

Answer: D

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

NEW QUESTION 96
A security analyst is running a tool against an executable of an unknown source. The Input supplied by the tool to the executable program and the output from the executable are shown below:



Input supplied by tool	Output from executable
asdfnerlajnvjanjkdfnvkjanakjdv	asdfnerlajnvjanjkdfnvkjanakjdv
klrejfkalsdjfklasdjffjladsf892	klrejfkalsdjfklasdjffjladsf892
ADSFQEDVASDASDFASDF;ADSFASDWDF	command not found
qscTRGvcaDFcaDCasDC23rdcasdfAS	qscTRGvcaDFcaDCasDC23rdcasdfAS
1qkcjfc934cjcjvsad:cmaciwcfasd	1qkcjfc934cjcjvsad:cmaciwcfasd

Which of the following should the analyst report after viewing this Information?

A. A dynamic library that is needed by the executable a missing
B. Input can be crafted to trigger an Infection attack in the executable
C. The toot caused a buffer overflow in the executable's memory
D. The executable attempted to execute a malicious command

Answer: C

Explanation:
A buffer overflow is a type of attack that exploits a vulnerability in an application or program that does not properly check the size or boundaries of an input. A buffer overflow occurs when an attacker supplies more data than the buffer can hold, causing the excess data to overwrite adjacent memory locations. This can result in unpredictable behavior, such as crashes, errors, data corruption, or execution of malicious code2
The tool that the analyst ran against the executable supplied an input that was too long for the buffer allocated by the executable. This caused a buffer overflow in the executable's memory, as indicated by the error message "Segmentation fault (core dumped)".

NEW QUESTION 98
A company is setting up a small, remote office to support five to ten employees. The company's home office is in a different city, where the company uses a cloud service provider for its business applications and a local server to host its data. To provide shared access from the remote office to the local server and the business applications, which of the following would be the easiest and most secure solution?

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

Answer: D

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

NEW QUESTION 101
An organization needs to secure sensitive data on its critical networks by implementing controls to mitigate APTs. The current policy does not provide any guidance or processes that support the mitigation of APTs. Which of the following technologies should the organization implement lo secure sensitive data? (Select two).

A. WAF
B. VPN
C. VPC
D. IPS
E. SIEM
F. SSO

Answer: DE

Explanation:
IPS and SIEM are technologies that can help secure sensitive data on critical networks by implementing controls to mitigate APTs. IPS stands for Intrusion Prevention System, and it is a device or software that monitors network traffic and blocks or prevents malicious packets or activities based on predefined rules or signatures. IPS can help detect and stop APTs that may try to exploit vulnerabilities or bypass security controls on critical networks. SIEM stands for Security Information and Event Management, and it is a system that collects, correlates, analyzes, and reports security data from various sources, such as logs, alerts,

events, etc. SIEM can help identify and respond to APTs that may exhibit anomalous or suspicious behavior patterns on critical networks.

NEW QUESTION 104
Which of the following describes the mam difference between supervised and unsupervised machine-learning algorithms that are used in cybersecurity applications?

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

Answer: B

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

NEW QUESTION 109
An analyst determines a security incident has occurred Which of the following is the most appropnate NEXT step in an incident response plan?

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

Answer: D

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

NEW QUESTION 111
A development team recently released a new version of a public-facing website for testing prior to production. The development team is soliciting the help of various teams to validate the functionality of the website due to its high visibility. Which of the following activities best describes the process the development team is initiating?

A. Static analysis
B. Stress testing
C. Code review
D. User acceptance testing

Answer: D

Explanation:
User acceptance testing is a process of verifying that a software application meets the requirements and expectations of the end users before it is released to production. User acceptance testing can help to validate the functionality, usability, performance and compatibility of the software application with real-world scenarios and feedback . User acceptance testing can involve various teams, such as developers, testers, customers and stakeholders.

NEW QUESTION 113
An organization recently discovered that spreadsheet files containing sensitive financial data were improperly stored on a web server. The management team wants to find out if any of these files were downloaded by pubic users accessing the server. The results should be written to a text file and should induce the date. time, and IP address associated with any spreadsheet downloads. The web server's log file Is named webserver log, and the report We name should be accessreport.txt. Following is a sample of the web servefs.log file:
2017-0-12 21:01:12 GET /index.htlm - @4..102.33.7 - return=200 1622
Which of the following commands should be run if an analyst only wants to include entries in which spreadsheet was successfully downloaded?

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

Answer: C

Explanation:
The grep command is a tool that searches for a pattern of characters in a file or input and prints the matching lines1
The egrep command is a variant of grep that supports extended regular expressions, which allow more complex and flexible pattern matching2
The more command is a filter that displays the contents of a file or input one screen at a time3

The pipe symbol (|) is used to redirect the output of one command to the input of another command. The redirection symbol (>) is used to redirect the output of a command to a file.
The command given in option C performs the following steps:

- It uses the more command to display the contents of the webserver.log file.
- It pipes the output of the more command to the grep command, which searches for lines that contain '*.xls', which is a pattern that matches any file name ending with .xls (a spreadsheet file extension).
- It pipes the output of the grep command to the egrep command, which searches for lines that contain 'return=200', which is a pattern that matches any HTTP status code of 200 (which indicates a successful request).
- It redirects the output of the egrep command to a file named accessreport.txt, which contains the date, time, and IP address associated with any spreadsheet downloads.

NEW QUESTION 115
Which of the following solutions is the BEST method to prevent unauthorized use of an API?

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

Answer: D

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

NEW QUESTION 116
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 117
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 120
An organization discovers motherboards within the environment that appear to have been physically altered during the manufacturing process. Which of the following is the BEST course of action to mitigate the risk of this reoccurring?

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

Answer: C

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

NEW QUESTION 122
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 124
Which of the following is a difference between SOAR and SCAP?

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

Answer: B

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

NEW QUESTION 128
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 132
Ensuring that all areas of security have the proper controls is a primary reason why organizations use:

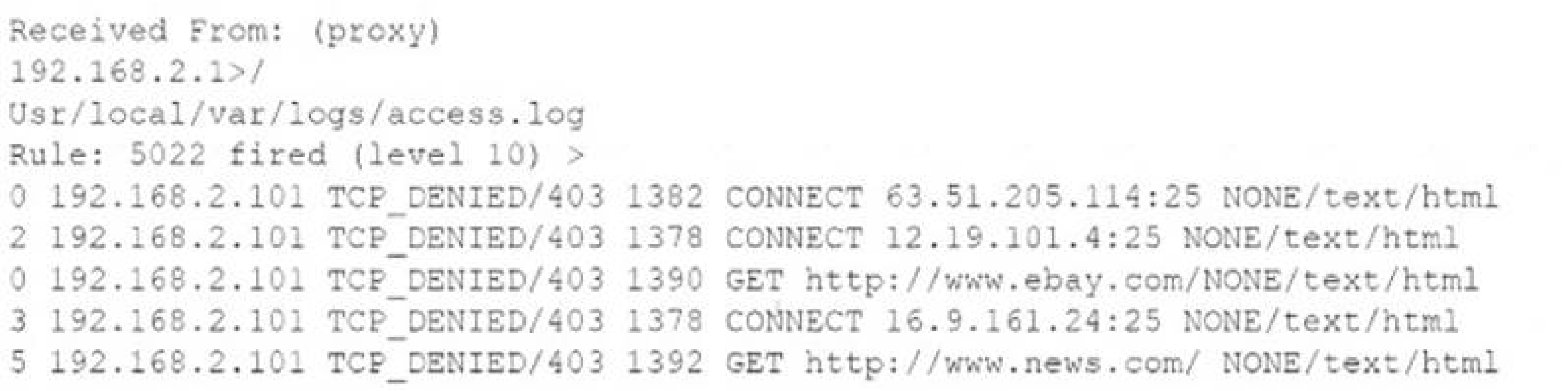
A. frameworks.
B. directors and officers.
C. incident response plans.
D. engineering rigor.

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 136
A security analyst notices the following proxy log entries:



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

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

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

Answer: C

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

NEW QUESTION 139
A Chief Information Security Officer has requested a security measure be put in place to redirect certain traffic on the network. Which of the following would best resolve this issue?

A. Sinkholing
B. Blocklisting
C. Geoblocking
D. Sandboxing

Answer: A

Explanation:
Sinkholing is a technique for manipulating data flow in a network; you redirect traffic from its intended destination to a server of your choosing. It can be used maliciously, to steer legitimate traffic away from its intended recipient, but security professionals more commonly use sinkholing as a tool for research and reacting to attacks1.
For example, sinkholing can be used to redirect traffic from a botnet or a malware-infected host to a server under the control of the defender, where the traffic can be analyzed, blocked, or neutralized. This can help identify and isolate compromised devices, prevent command-and-control communication, and disrupt malicious activities2.
The other options are not the best solutions for the following reasons:

- Blocklisting is a technique for preventing access to or communication with certain IP addresses, domains, or applications that are known or suspected to be malicious. Blocklisting can be implemented using firewalls, routers, proxies, or software tools. Blocklisting can protect a network from unwanted or harmful traffic, but it does not redirect the traffic to a different destination.
- Geoblocking is a technique for restricting access to or communication with certain IP addresses, domains, or applications based on their geographic location. Geoblocking can be implemented using firewalls, routers, proxies, or software tools. Geoblocking can protect a network from unauthorized or undesirable traffic from specific regions or countries, but it does not redirect the traffic to a different destination.
- Sandboxing is a technique for isolating and executing potentially malicious code or applications in a separate and secure environment. Sandboxing can be implemented using virtual machines, containers, or software tools. Sandboxing can protect a network from malware infection or damage, but it does not redirect the network traffic to a different destination.

NEW QUESTION 141
The majority of a company's employees have stated they are unable to perform their job duties due to outdated workstations, so the company has decided to institute BYOD. Which of the following would a security analyst MOST likely recommend for securing the proposed solution?

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

Answer: B

Explanation:
VDI means virtual desktop interface. Using VDI, you can maintain a standard image and remove the threat of an infected machine plugging into your network.
A firewalled environment for client devices and a secure VDI (Virtual Desktop Infrastructure) for BYOD users would be the most likely recommendation for securing the proposed solution. A firewalled environment can help isolate and protect the client devices from unauthorized network access or attacks. A secure VDI can provide a virtualized desktop environment for BYOD users that can be centrally managed and controlled by the organization. A VDI can also prevent data leakage

or malware infection from BYOD devices, as the data and applications are stored on the server side rather than on the device itself5.

NEW QUESTION 144
According to a static analysis report for a web application, a dynamic code evaluation script injection vulnerability was found. Which of the following actions is the BEST option to fix the vulnerability in the source code?

A. Delete the vulnerable section of the code immediately.
B. Create a custom rule on the web application firewall.
C. Validate user input before execution and interpretation.
D. Use parameterized queries.

Answer: C

Explanation:
Validating user input before execution and interpretation can help to prevent dynamic code evaluation script injection vulnerabilities by checking and filtering any malicious input from the user that may contain code or commands. Dynamic code evaluation script injection is a type of vulnerability that occurs when an application accepts user input and executes or interprets it as part of its own code without proper validation or sanitization. This can allow an attacker to inject arbitrary code or commands into the application and execute them with the same privileges as the application . Validating user input before execution and interpretation can help to ensure that the input conforms to the expected format, length and type, and does not contain any malicious characters or syntax that may alter the logic or behavior of the application .

NEW QUESTION 145
An organization is required to be able to consume multiple threat feeds simultaneously and to provide actionable intelligence to various teams. The organization would also like to be able to leverage the intelligence to enrich security event data. Which of the following functions would most likely help the security analyst meet the organization's requirements?

A. Vulnerability management
B. Risk management
C. Detection and monitoring
D. Incident response

Answer: C

Explanation:
The correct answer is C. Detection and monitoring. Detection and monitoring is a function that involves collecting, analyzing, and correlating data from various sources, such as threat feeds, logs, alerts, or events, to identify and respond to potential or ongoing threats. Detection and monitoring can help the organization to consume multiple threat feeds simultaneously and to provide actionable intelligence to various teams, such as security operations center (SOC) analysts, incident responders, or threat hunters. Detection and monitoring can also help the organization to leverage the intelligence to enrich security event data, such as adding context, severity, or priority to the events1.
* A. Vulnerability management is not correct. Vulnerability management is a function that involves identifying, assessing, and mitigating the weaknesses or flaws in systems, applications, or networks that could be exploited by attackers. Vulnerability management can help the organization to reduce its attack surface and prevent potential breaches, but it does not directly involve consuming multiple threat feeds simultaneously or providing actionable intelligence to various teams.
* B. Risk management is not correct. Risk management is a function that involves identifying, analyzing, and evaluating the risks that could affect the organization's assets, operations, or objectives. Risk management can help the organization to prioritize and implement appropriate controls or mitigation strategies to reduce the likelihood or impact of the risks, but it does not directly involve consuming multiple threat feeds simultaneously or providing actionable intelligence to various teams.
* D. Incident response is not correct. Incident response is a function that involves preparing for, detecting, containing, analyzing, and recovering from security incidents that compromise the confidentiality, integrity, or availability of the organization's assets or operations. Incident response can help the organization to minimize the damage and restore normal operations as quickly as possible, but it does not directly involve consuming multiple threat feeds simultaneously or providing actionable intelligence to various teams.
1: Cybersecurity Analyst+ - CompTIA

NEW QUESTION 149
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 153

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

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

Answer: B

Explanation:
SaaS stands for Software as a Service, which is a cloud model that allows users to access software applications over the internet without installing or maintaining them on their own devices. SaaS will allow all data to be kept on the third-party network, because the software applications and the data they generate or process are stored on the cloud provider's servers. VDI, CASB, and FaaS are other terms related to cloud computing or security, but they do not match the description of keeping all data on the third-party network. Reference: https://www.ibm.com/cloud/learn/software-as-a-service

NEW QUESTION 157
A vulnerability scanner has identified an out-of-support database software version running on a server. The software update will take six to nine months to complete. The management team has agreed to a one-year extended support contract with the software vendor. Which of the following BEST describes the risk treatment in this scenario?

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

Answer: C

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

NEW QUESTION 159
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 160
A company frequently expenences issues with credential stuffing attacks Which of the following is the BEST control to help prevent these attacks from being successful?

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

Answer: C

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

NEW QUESTION 164
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 165
An organization is concerned about the proper handling of data and wants to implement measures to help safeguard customer data and the organization's proprietary information from exposure. Which of the following is the first step to improve awareness of overall privacy and protection?

A. Perform user acceptance testing.
B. Implement corporate policies.
C. Conduct biannual training.
D. Review data classification processes.

Answer: D

Explanation:
Data classification is the process of categorizing data based on its level of sensitivity, value, and risk. Data classification can help determine the appropriate level of protection and access control for each type of data.
Data classification processes should be reviewed regularly to ensure that they are aligned with the organization’s goals, policies, and standards. Data classification processes should also reflect the changing nature and value of data, as well as the evolving threats and regulations in the data environment.
Reviewing data classification processes can help improve awareness of overall privacy and protection by:

- Educating data owners and users about their roles and responsibilities in handling data.
- Establishing clear and consistent criteria for labeling and handling data.
- Identifying and prioritizing the most critical and sensitive data assets.
- Applying the appropriate security measures and controls for each data category.
- Reducing the risk of data loss, theft, or misuse.

NEW QUESTION 170
A security analyst needs to recommend the best approach to test a new application that simulates abnormal user behavior to find software bugs. Which of the following would best accomplish this task?

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

Answer: D

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

NEW QUESTION 171
A security analyst notices the following entry while reviewing the server togs OR 1=1' ADD USER attacker' PW 1337password' ---Which of the following events occurred?

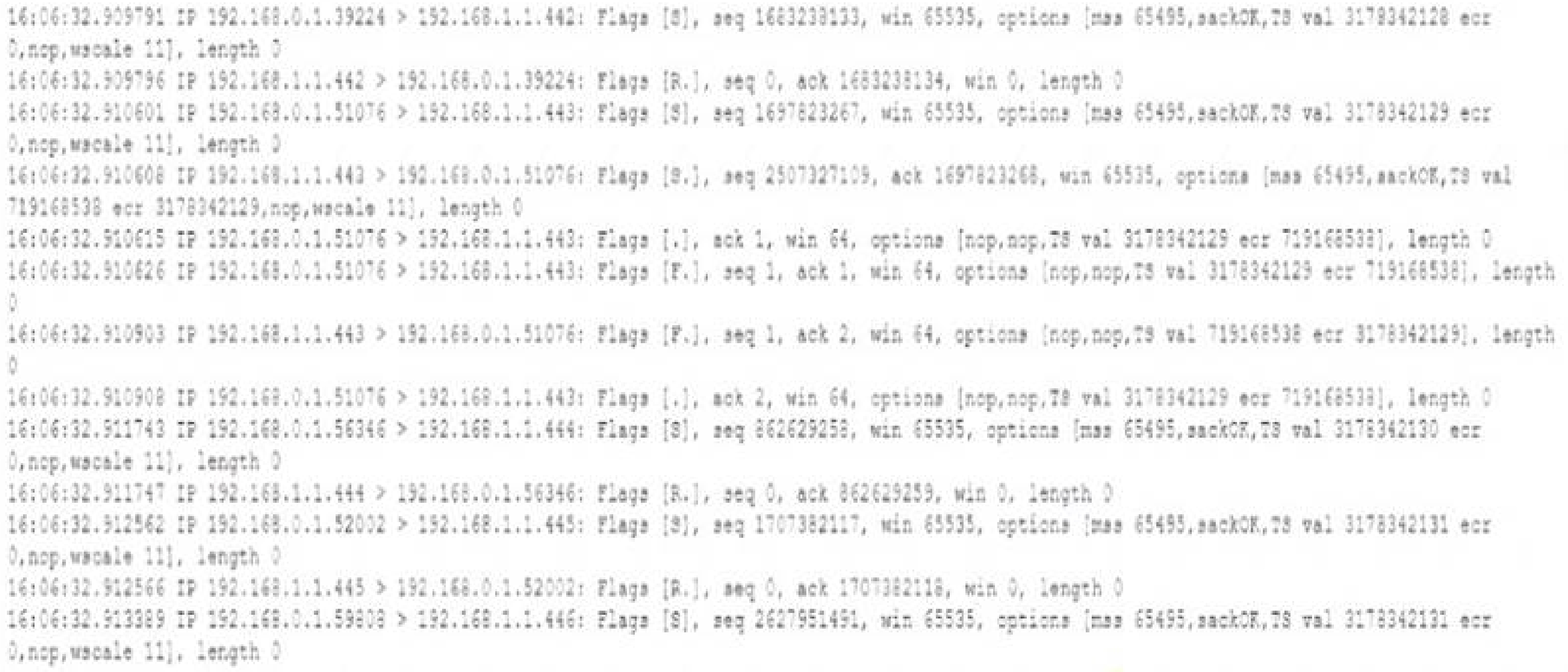
A. CSRF
B. XSS
C. SQLi
D. RCE

Answer: C

Explanation:
SQLi stands for SQL injection, which is a type of attack that injects malicious SQL statements into a web application’s input fields or parameters. The attacker can use SQLi to execute unauthorized commands on the database server, such as adding a new user or retrieving sensitive data. The entry in the server logs shows an example of a SQLi attack that tries to add a new user named attacker with the password 1337password. CSRF, XSS, and RCE are other types of attacks, but they do not match the description of the entry in the server logs. Reference: https://owasp.org/www-community/attacks/SQL_Injection

NEW QUESTION 173

A security analyst is reviewing the output of tcpdump to analyze the type of activity on a packet capture:



```
16:06:32.909791 IP 192.168.0.1.39224 > 192.168.1.1.442: Flags [S], seq 1683238133, win 65535, options [mss 65495,sackOK,TS val 3178342128 ecr
0,nop,wscale 11], length 0
16:06:32.909796 IP 192.168.1.1.442 > 192.168.0.1.39224: Flags [R.], seq 0, ack 1683238134, win 0, length 0
16:06:32.910601 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [S], seq 1697823267, win 65535, options [mss 65495,sackOK,TS val 3178342129 ecr
0,nop,wscale 11], length 0
16:06:32.910608 IP 192.168.1.1.443 > 192.168.0.1.51076: Flags [S.], seq 2507327109, ack 1697823268, win 65535, options [mss 65495,sackOK,TS val
719168538 ecr 3178342129,nop,wscale 11], length 0
16:06:32.910615 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [.], ack 1, win 64, options [nop,nop,TS val 3178342129 ecr 719168538], length 0
16:06:32.910626 IP 192.168.0.1.51076 > 192.168.1.1.443: Flags [F.], seq 1, ack 1, win 64, options [nop,nop,TS val 3178342129 ecr 719168538], length
0

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

Which of the following generated the above output?

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

Answer: B

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

NEW QUESTION 177
A current, validated DLP solution Is now in place because of a previous data breach However, a new data breach has taken place The following symptoms were observed shorty after a recent sales meeting:
* Sensitive corporate documents appeared on the dark web.
* Unusually large packets of data were being sent out.
Which of the following is most likely occurring?

A. Documents are not tagged properly to restrict sharing.
B. An insider threat is exfiltration data.
C. The DLP solution is not configured for unsecured web traffic
D. File audits are not enabled on CASB.

Answer: B

Explanation:
This is most likely occurring based on the symptoms observed after a recent sales meeting. An insider threat is a person who has legitimate access to an organization’s network or data and uses it for malicious purposes, such as stealing, leaking, or sabotaging information. The symptoms suggest that someone from the sales team or someone who attended the meeting has copied sensitive corporate documents and uploaded them to the dark web using large data packets.

NEW QUESTION 180
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 184
An analyst needs to understand how an attacker compromised a server. Which of the following procedures will best deliver the information that is necessary to reconstruct the steps taken by the attacker?

A. Scan the affected system with an anti-malware tool and check for vulnerabilities with a vulnerability scanner.
B. Extract the server's system timeline, verifying hashes and network connections during a certain time frame.
C. Clone the entire system and deploy it in a network segment built for tests and investigations while monitoring the system during a certain time frame.
D. Clone the server's hard disk and extract all the binary files, comparing hash signatures with malware databases.

Answer: B

Explanation:
The correct answer is B. Extract the server's system timeline, verifying hashes and network connections during a certain time frame. A system timeline is a chronological record of the events and activities that occurred on a system, such as file creation, modification, or deletion, process execution, registry changes, or network connections. A system timeline can help an analyst to understand how an attacker compromised a server by showing the sequence of actions and artifacts left by the attacker. An analyst can also verify the hashes of the files and processes involved in the compromise and compare them with known malware signatures or databases. Additionally, an analyst can check the network connections made by the server during the compromise and identify the source and destination IP addresses, ports, and protocols used by the attacker1.

NEW QUESTION 187
An analyst reviews a legacy Windows XP system and concludes an attacker executed code that modified the contents of the system's memory. Which of the following attack techniques did the attacker use?

A. Rootkit
B. Backdoor
C. Privilege escalation
D. Buffer overflow

Answer: D

Explanation:
A buffer overflow is an attack technique that exploits a vulnerability in a program's memory management, by sending more data than the buffer can hold. This can cause the program to overwrite adjacent memory locations, and execute arbitrary code injected by the attacker.

NEW QUESTION 190
A development team has asked users to conduct testing to ensure an application meets the needs of the business. Which of the fallowing types of testing docs This describe?

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

Answer: A

Explanation:
Acceptance testing is a type of testing that involves verifying that an application meets the needs and expectations of the business and the end users. Acceptance testing is usually performed by users or customers who evaluate the application's functionality, usability, performance, reliability, and compatibility. Acceptance testing helps to ensure that the application delivers the required value and quality before it goes into production.

NEW QUESTION 192
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

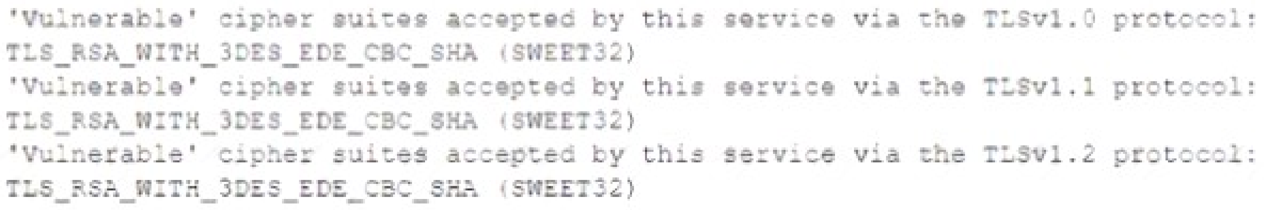
NEW QUESTION 195
A manufacturing company uses a third-party service provider lor Tier 1 security support One of the requirements is that the provider must only source talent from its own country due to geopolitical and national security interests Which of the following can the manufacturing company implement to ensure the third-party service provider meets this requirement?

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

Answer: A

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

NEW QUESTION 197
During a review of the vulnerability scan results on a server, an information security analyst notices the following:



```
'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
```

The MOST appropriate action for the analyst to recommend to developers is to change the web server so:

A. It only accepts TLSvl 2
B. It only accepts cipher suites using AES and SHA
C. It no longer accepts the vulnerable cipher suites
D. SSL/TLS is offloaded to a WAF and load balancer

Answer: C

Explanation:
A cipher suite is a set of algorithms that defines how the encryption, authentication, and integrity of data are performed during a secure communication session. Some cipher suites are considered vulnerable or weak because they use outdated or insecure algorithms that can be easily broken or compromised by attackers. The vulnerability scan results show that the web server accepts several vulnerable cipher suites, such as RC4, MD5, or DES. The best action for the analyst to recommend to developers is to change the web server so it no longer accepts the vulnerable cipher suites and only accepts the secure ones. Changing the web server so it only accepts TLSv1.2, only accepts cipher suites using AES and SHA, or offloading SSL/TLS to a WAF and load balancer are other possible actions, but they are not as specific or effective as changing the web server so it no longer accepts the vulnerable cipher suites. Reference:
https://www.acunetix.com/blog/articles/tls-ssl-cipher-hardening/

NEW QUESTION 201
An organization is performing a risk assessment to prioritize resources for mitigation and remediation based on impact. Which of the following metrics, in addition to the CVSS for each CVE, would best enable the organization to prioritize its efforts?

A. OS type
B. OS or application versions
C. Patch availability
D. System architecture
E. Mission criticality

Answer: C

Explanation:
A risk assessment is a process of identifying, analyzing, and evaluating the potential threats and vulnerabilities that may affect an organization’s assets, operations, or objectives. A risk assessment matrix is a tool that can help prioritize the risks based on their likelihood and impact1.
The CVSS (Common Vulnerability Scoring System) is a standard framework for rating the severity of vulnerabilities in software systems. The CVSS provides a numerical score from 0 to 10, as well as a qualitative rating from Low to Critical, based on the characteristics and consequences of the vulnerability2.
However, the CVSS score alone may not be sufficient to determine the priority of mitigation and remediation actions for each vulnerability. Other factors that may influence the decision include:

- Patch availability: This metric indicates whether there is a fix or update available for the vulnerability from the vendor or developer. Patch availability can affect the urgency and feasibility of remediation, as well as the risk exposure and potential damage of exploitation. For example, a vulnerability with a high CVSS score but with a readily available patch may be less critical than a vulnerability with a lower CVSS score but with no patch available3.
- Mission criticality: This metric reflects the importance and value of the asset or system affected by the vulnerability to the organization’s mission, goals, or functions. Mission criticality can affect the impact and priority of remediation, as well as the risk tolerance and acceptance level of the organization. For example, a vulnerability with a high CVSS score but affecting a non-essential system may be less critical than a vulnerability with a lower CVSS score but affecting a core system4.
- OS type: This metric indicates the operating system (OS) of the asset or system affected by the vulnerability. OS type can affect the likelihood and complexity of exploitation, as well as the availability and compatibility of patches or mitigations. For example, a vulnerability with a high CVSS score but affecting an uncommon or unsupported OS may be less critical than a vulnerability with a lower CVSS score but affecting a widely used or supported OS3.
- OS or application versions: This metric indicates the specific version of the OS or application affected by the vulnerability. OS or application versions can affect the applicability and relevance of the vulnerability, as well as the availability and compatibility of patches or mitigations. For example, a vulnerability with a high CVSS score but affecting an outdated or obsolete version may be less critical than a vulnerability with a lower CVSS score but affecting a current or popular version3.
- System architecture: This metric indicates the design and configuration of the asset or system affected by the vulnerability. System architecture can affect the exposure and accessibility of the vulnerability, as well as the effectiveness and efficiency of patches or mitigations. For example, a vulnerability with a high CVSS score but affecting an isolated or segmented system may be less critical than a vulnerability with a lower CVSS score but affecting an interconnected or integrated system3.

Therefore, to best enable the organization to prioritize its efforts based on impact, patch availability is one of the most important metrics to consider in addition to the CVSS score for each CVE (Common Vulnerabilities and Exposures). Patch availability can directly influence the risk level and remediation strategy for each vulnerability.

NEW QUESTION 202

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 205
A security analyst is reviewing the following DNS logs as part of security-monitoring activities:

```
FROM 192.168.1.20 A www.google.com 67.43.45.22
FROM 192.168.1.20 AAAA www.google.com 2006:67:AD:1FAB::102
FROM 192.168.1.43 A www.mail.com 193.56.221.99
FROM 192.168.1.2 A www.company.com 241.23.22.11
FROM 192.168.1.211 A www.uewiryfajfchfaerwfj.co 32.56.32.122
FROM 192.168.1.106 A www.whatsmyip.com 102.45.33.53
FROM 192.168.1.93 ARAA www.nbc.com 2002:10:976::1
FROM 192.168.1.78 A www.comptia.org 122.10.31.87
```

Which of the following most likely occurred?

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

Answer: A

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

NEW QUESTION 210
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 215
industry partners from critical infrastructure organizations were victims of attacks on their SCADA devices. The attacks used privilege escalation to gain access to SCADA administration 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:
Role-based access control (RBAC) is a method of restricting access to resources based on the roles of users within an organization. RBAC assigns permissions and privileges to roles, rather than individual users, and grants access based on the principle of least privilege3
RBAC can help mitigate the risk of privilege escalation attacks on SCADA devices by ensuring that only authorized users have access to SCADA administration and management functions, and that they have the minimum level of access required to perform their tasks.

NEW QUESTION 219
A security analyst performed a targeted system vulnerability scan to obtain critical information. After the output result, the analyst used the OVAL XML language to review and calculate the discovered risk. Which of the following types of scans did the security analyst perform?

A. Active

B. Network map
C. Passive
D. External

Answer: A

Explanation:
An active scan is a type of system vulnerability scan that involves sending probes or packets to the target system, and analyzing the responses or behaviors of the system. An active scan can help obtain critical information about the system, such as open ports, running services, operating system, software versions, etc. An active scan can also use OVAL XML language to review and calculate the discovered risk. OVAL stands for Open Vulnerability and Assessment Language, and it is a standard for describing and exchanging information about system vulnerabilities and configurations.

NEW QUESTION 222
In web application scanning, static analysis refers to scanning:

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

Answer: B

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

NEW QUESTION 223
A cyber-security analyst is implementing a new network configuration on an existing network access layer to prevent possible physical attacks. Which of the following BEST describes a solution that would apply and cause fewer issues during the deployment phase?

A. Implement port security with one MAC address per network port of the switch.
B. Deploy network address protection with DHCP and dynamic VLANs.
C. Configure 802.1X and EAPOL across the network
D. Implement software-defined networking and security groups for isolation

Answer: A

Explanation:
The security analyst should implement port security with one MAC address per network port of the switch. This will help prevent possible physical attacks on the network access layer, such as MAC flooding or MAC spoofing. Port security is a feature that allows a switch to limit the number of MAC addresses that can be learned on a specific port. By setting the limit to one MAC address per port, the switch will only allow traffic from the device that is connected to that port, and drop any traffic from other devices that try to use that
port. This will prevent attackers from connecting unauthorized devices to the network or impersonating
legitimate devices by changing their MAC addresses3.

NEW QUESTION 226
A developer is working on a program to convert user-generated input in a web form before it is displayed by the browser. This technique is referred to as:

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

Answer: A

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

NEW QUESTION 230
During an incident investigation, a security analyst discovers the web server is generating an unusually high volume of logs The analyst observes the following response codes:
• 20% of the logs are 403
• 20% of the logs are 404
• 50% of the logs are 200
• 10% of the logs are other codes
The server generates 2MB of logs on a daily basis, and the current day log is over 200MB. Which of the following commands should the analyst use to identify the source of the activity?

A. cat access_log Igrep " 403 "
B. cat access_log Igrep " 200 "
C. cat access_log Igrep " 100 "
D. cat access_log Igrep " 4 04 "

E. cat access_log Igrep " 204 "

Answer: B

Explanation:
Requests sent from the same IP address using different user agents are likely to be malicious or suspicious, as they indicate that an attacker is trying to evade detection or bypass security controls by changing their browser or device identification. These requests may indicate that an attacker is using automated tools or scripts to scan or attack the web server.
Requests identified by a threat intelligence service with a bad reputation are also likely to be malicious or suspicious, but they are not the source of the activity, as they originate from different IP addresses. These requests may indicate that an attacker is trying to exploit a vulnerability or perform reconnaissance on the web server.
Requests blocked by the web server per the input sanitization are not likely to be the source of the activity, as they indicate that the web server has successfully prevented an attack by validating and filtering any malicious input from the requests. These requests may indicate that an attacker is trying to inject malicious code or commands into the web server.
Failed log-in attempts against the web application are not likely to be the source of the activity, as they indicate that the web application has successfully prevented unauthorized access by verifying and rejecting any invalid credentials from the requests. These requests may indicate that an attacker is trying to guess or brute-force passwords or usernames for the web application.
Requests sent by NICs with outdated firmware are not likely to be the source of the activity, as they indicate that some devices on the network have not been updated with the latest security patches or features for their network interface cards (NICs). These requests may indicate that some devices are vulnerable to network attacks or have performance issues.
Existence of HTTP/501 status codes generated to the same IP address are not likely to be the source of the activity, as they indicate that the web server has encountered an error or does not support a request method from the client. These requests may indicate that an attacker is trying to use an invalid or unsupported method to access the web server.

NEW QUESTION 232
A security analyst identified some potentially malicious processes after capturing the contents of memory from a machine during incident response. Which of the following procedures is the NEXT step for further in investigation?

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

Answer: D

Explanation:
Reverse engineering is a process of analyzing a system or a component to understand how it works and how it was made. Reverse engineering can be used to examine malicious processes captured from memory and determine their functionality, origin, and purpose. Reverse engineering can help identify the type of malware, its infection vector, its capabilities, its communication methods, and its indicators of compromise2

NEW QUESTION 237
A security analyst is designing firewall rules to prevent external IP spoofing Which of the following explains the firewall rule for mitigation?

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

Answer: B

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

NEW QUESTION 238
Members of the sales team are using email to send sensitive client lists with contact information to their personal accounts The company's AUP and code of conduct prohibits this practice. Which of the following configuration changes would improve security and help prevent this from occurring?

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

Answer: A

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

NEW QUESTION 243
Which of the following would best protect sensitive data If a device is stolen?

A. Remote wipe of drive

B. Self-encrypting drive
C. Password-protected hard drive
D. Bus encryption

Answer: B

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

NEW QUESTION 246
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 250
......