CompTIA

Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
The management team has asked a senior security engineer to explore DLP security solutions for the company's growing use of cloud-based storage. Which of the following is an appropriate solution to control the sensitive data that is being stored in the cloud?

A. NAC
B. IPS
C. CASB
D. WAF

Answer: C

Explanation:
A cloud access security broker (CASB) is a security solution that monitors and controls the use of cloud-based services and applications. A CASB can provide data loss prevention (DLP) capabilities for sensitive data that is being stored in the cloud, such as encryption, masking, tokenization, or redaction. A CASB can also enforce policies and compliance requirements for cloud usage, such as authentication, authorization, auditing, and reporting. The other options are not appropriate solutions for controlling sensitive data in the cloud. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 14; https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security

NEW QUESTION 2
The steering committee for information security management annually reviews the security incident register for the organization to look for trends and systematic issues. The steering committee wants to rank the risks based on past incidents to improve the security program for next year. Below is the incident register for the organization:

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

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

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

Answer: C

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

NEW QUESTION 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
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 6
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 7
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 8
A company notices unknown devices connecting to the internal network and would like to implement a solution to block all non-corporate managed machines.
Which of the following solutions would be best to accomplish this goal?

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

Answer: B

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

NEW QUESTION 9
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 10
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

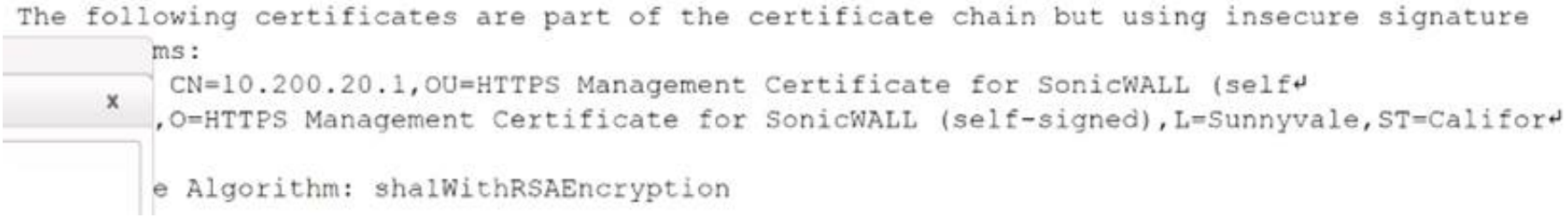
NEW QUESTION 10
An analyst reviews the most recent vulnerability management report and notices a firewall with 99.98% required uptime is reporting different firmware versions on scans than were reported in previous scans. The vendor released new firewall firmware a few months ago. Which of the following 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 15
While reviewing a vulnerability assessment, an analyst notices the following issue is identified in the report: this finding, which of the following would be most appropriate for the analyst to recommend to the network engineer?



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

Answer: A

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

NEW QUESTION 16
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 17
An organization has the following risk mitigation policies
• Risks without compensating controls will be mitigated first it the nsk value is greater than $50,000
• Other nsk mitigation will be pnontized based on risk value. The following risks have been identified:

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

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

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

Answer: C

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

NEW QUESTION 19
While implementing a PKI for a company, a security analyst plans to utilize a dedicated server as the
certAcate authority that is only used to sign intermediate certificates. Which of the following are the MOST secure states for the certificate authority server when it is not in use? (Select TWO)

A. On a private VLAN
B. Full disk encrypted
C. Powered off
D. Backed up hourly
E. VPN accessible only
F. Air gapped

Answer: CF

Explanation:
The most secure states for the certificate authority server when it is not in use are powered off and air gapped. Powering off the server will prevent any unauthorized access or tampering with the server while it is idle. Air gapping the server will isolate it from any network connections, making it inaccessible to remote attackers or malware. These measures will help to protect the integrity and confidentiality of the certificate authority server and its keys.

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

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

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

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

Answer: B

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

NEW QUESTION 27
Some hard disks need to be taken as evidence for further analysis during an incident response. Which of the following procedures must be completed FIRST for this type of evidence acquisition?

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

Answer: B

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

NEW QUESTION 31
A SIEM analyst receives an alert containing the following URL:

http://companywebsite.com/displayPicture?filename=../../../etc/passwd

Which of the following BEST describes the attack?

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

Answer: D

Explanation:
A directory traversal attack is a type of web application attack that exploits insufficient input validation or filtering to access files or directories that are outside of the web root folder. A directory traversal attack can allow an attacker to read, modify, or execute files on the target server that are not intended to be accessible via web requests. The URL in the alert contains an example of a directory traversal attack, as indicated by the use of "…/" sequences in the query string. These sequences are used to navigate up one level in the directory hierarchy, potentially reaching sensitive files or folders on the server. In this case, the attacker is trying to access /etc/passwd file, which contains user account information on Linux systems.

NEW QUESTION 34
Which of the following should a database administrator for an analytics firm implement to best protect PII from an insider threat?

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

Answer: C

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

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

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

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

NEW QUESTION 36
A company needs to expand Its development group due to an influx of new feature requirements (rom Its customers. To do so quickly, the company is using Junior-level developers to fill in as needed. The company has found a number of vulnerabilities that have a direct correlation to the code contributed by the junior-level developers. Which of the following controls would best help to reduce the number of software vulnerabilities Introduced by this situation?

A. Requiring senior-level developers to review code written by junior-level developers
B. Hiring senior-level developers only
C. Allowing only senior-level developers to write code for new features
D. Using authorized source code repositories only

Answer: A

Explanation:
This control would best help to reduce the number of software vulnerabilities introduced by this situation because it ensures that code quality and security standards are met before deploying to production.
Senior-level developers can provide feedback, guidance, and corrections to junior-level developers and catch any errors or flaws in their code.

NEW QUESTION 40
A security analyst is monitoring a company's network traffic and finds ping requests going to accounting and human resources servers from a SQL server. Upon investigation, the analyst discovers a technician responded to potential network connectivity issues. Which of the following is the best way for the security analyst to respond?

A. Report this activity as a false positive, as the activity is legitimate.
B. Isolate the system and begin a forensic investigation to determine what was compromised.
C. Recommend network segmentation to the management team as a way to secure the various environments.
D. Implement host-based firewalls on all systems to prevent ping sweeps in the future.

Answer: A

Explanation:
Reporting this activity as a false positive, as the activity is legitimate, is the best way for the security analyst to respond. A false positive is a condition in which harmless traffic is classified as a potential network attack by a security monitoring tool. Ping requests are a common network diagnostic tool that can be used to test network connectivity issues. The technician who responded to potential network connectivity issues was performing a legitimate task and did not pose any threat to the accounting and human resources servers .

NEW QUESTION 43
Which of the following is MOST important when developing a threat hunting program?

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

Answer: D

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

NEW QUESTION 44
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
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 52
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
An analyst is responding to an incident within a cloud infrastructure Based on the logs and traffic analysis, the analyst thinks a container has been compromised
Which of the following should Ihe analyst do FIRST?

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

Answer: D

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

NEW QUESTION 60
An organization wants to implement controls for protecting private information at rest. Which of the following would meet the organization's need?

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

Answer: D

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

NEW QUESTION 63
A security analyst found an old version of OpenSSH running on a DMZ server and determined the following piece of code could have led to a command execution through an integer overflow;

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

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

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

Answer: C

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

NEW QUESTION 68
A new variant of malware is spreading on the company network using TCP 443 to contact its
command-and-control server The domain name used for callback continues to change, and the analyst is unable to predict future domain name variance Which of the following actions should the analyst take to stop malicious communications with the LEAST disruption to service?

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

Answer: A

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

NEW QUESTION 73
A computer hardware manufacturer developing a new SoC that will be used by mobile devices. The SoC should not allow users or the process to downgrade from a newer firmware to an older one. Which of the following can the hardware manufacturer implement to prevent firmware downgrades?

A. Encryption
B. eFuse
C. Secure Enclave
D. Trusted execution

Answer: B

Explanation:
An eFuse, or electronic fuse, is a microscopic fuse put into a computer chip that can be blown by applying a high voltage or current. Once blown, an eFuse cannot be reset or repaired, and its state can be read by software or hardware2
An eFuse can be used by a hardware manufacturer to prevent firmware downgrades on a
system-on-chip (SoC) that will be used by mobile devices. An eFuse can store information such as the firmware version, security level, or device configuration on the chip. When a newer firmware is installed, an eFuse can be blown to indicate the update and prevent reverting to an older firmware. This can help protect the device from security vulnerabilities, compatibility issues, or unauthorized modifications.

NEW QUESTION 78
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 83
A systems administrator believes a user's workstation has been compromised. The workstation's performance has been lagging significantly for the past several hours. The administrator runs the task list
/ v command and receives the following output:

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

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

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

Answer: B

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

NEW QUESTION 85
Which of the following factors would determine the regulations placed on data under data sovereignty laws?

A. What the company intends to do with the data it owns
B. The company's data security policy
C. The type of data the company stores
D. The data laws of the country in which the company is located

Answer: D

Explanation:
The data laws of the country in which the company is located would determine the regulations placed on data under data sovereignty laws. Data sovereignty laws are laws that govern how data is collected, stored, processed, and transferred within a country’s jurisdiction. Data sovereignty laws can vary from country to country, depending on their legal system, political system, culture, and values. Data sovereignty laws can affect how companies handle their data, especially when they operate across borders or use cloud services. For example, some countries may have strict data protection or privacy laws that require companies to obtain consent from data subjects before collecting or processing their data. Some countries may also have data localization or data residency laws that require companies to store their data within the country’s borders or limit cross-border data transfers.

NEW QUESTION 86
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 exfllltrating 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 88
A security analyst is reviewing the following server statistics:

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

Which of the following is MOST likely occurring?

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

Answer: C

Explanation:
Resource exhaustion is most likely occurring on the server. Resource exhaustion is a condition where a system runs out of resources, such as CPU, memory, disk space, or network bandwidth, due to excessive demand or consumption by one or more processes. Resource exhaustion can cause performance degradation, system instability, or denial-of-service. The server statistics show that the CPU usage is 100%, the memory usage is 99%, and the disk usage is 98%. These indicate that the server is under heavy load and has little or no resources available to handle incoming requests or perform other tasks.

NEW QUESTION 93
An organization wants to consolidate a number of security technologies throughout the organization and standardize a workflow for identifying security issues prioritizing the severity and automating a response Which of the following would best meet the organization's needs'?

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

Answer: C

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

NEW QUESTION 98
An organization implemented an extensive firewall access-control blocklist to prevent internal network ranges from communicating with a list of IP addresses of known command-and-control domains A security analyst wants to reduce the load on the firewall. Which of the following can the analyst implement to achieve similar protection and reduce the load on the firewall?

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

Answer: B

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

NEW QUESTION 100
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 102
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 107
An incident response team detected malicious software that could have gained access to credit card data. The incident response team was able to mitigate significant damage and implement corrective actions. By having incident response mechanisms in place. Which of the following should be notified for lessons learned?

A. The human resources department
B. Customers
C. Company leadership
D. The legal team

Answer: C

Explanation:
Lessons learned is a critical stage of incident response that involves evaluating the effectiveness of the response, identifying gaps and areas for improvement, and updating the incident response plan accordingly1.
Company leadership should be involved in this process to ensure they are aware of the incident, its impact, and the actions taken to prevent or mitigate future incidents. Additionally, company leadership can provide support and guidance for implementing the recommendations from the lessons learned session2.

NEW QUESTION 111
The following output is from a tcpdump al the edge of the corporate network:

```
12:47:22.179345 PPPoE  [ses 0x8122] IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto IPv6 (41), length 92) 10.5.1.1 > 198.134.5.201: IP6 (hlim 63, next-heade:
TCP (6) payload length: 32) 2001:67c:2158:a019::ace.53104 > 2001:0:5ef5:79fd:380c:1d57:a601:24fa.13788: Flags [S], cksum 0x58cf (correct), seq 1155375165, win 8192,
options [mss 1412,nop,wscale 2,nop,nop,sackOK], length 0

12:47:22.251065 PPPoE  [ses 0x8122] IP (tos 0x0, ttl 59, id 0, offset 0, flags [DF], proto IPv6 (41), length 92) 198.134.5.201 > 10.5.1.1: IP6 (hlim 127, next-
heade: TCP (6) payload length: 32) 2001:0:5ef5:79fd:380c:1d57:a601:24fa.13788 > 2001:67c:2158:a019::ace.53104: Flags [S.], cksum 0xd361 (correct), seq 2642471061,
ack 1155375166, win 8192, options [mss 1220,nop,wscale 6,nop,nop,sackOK], length 0
```

Which of the following best describes the potential security concern?

A. Payload lengths may be used to overflow buffers enabling code execution.
B. Encapsulated traffic may evade security monitoring and defenses
C. This traffic exhibits a reconnaissance technique to create network footprints.
D. The content of the traffic payload may permit VLAN hopping.

Answer: B

Explanation:
Encapsulated traffic may evade security monitoring and defenses by hiding or obfuscating the actual content or source of the traffic. Encapsulation is a technique that wraps data packets with additional headers or protocols to enable communication across different network types or layers. Encapsulation can be used for legitimate purposes, such as tunneling, VPNs, or NAT, but it can also be used by attackers to bypass security controls or detection mechanisms that are not able to inspect or analyze the encapsulated traffic .

NEW QUESTION 114
An information security analyst discovered a virtual machine server was compromised by an attacker. Which of the following should be the first steps to confirm and respond to the incident? (Select two).

A. Pause the virtual machine.
B. Shut down the virtual machine.
C. Take a snapshot of the virtual machine.
D. Remove the NIC from the virtual machine.
E. Review host hypervisor log of the virtual machine.
F. Execute a migration of the virtual machine.

Answer: AC

Explanation:
These steps are the best to confirm and respond to the incident because they preserve the state of the compromised server for further analysis and evidence collection. Pausing the virtual machine prevents any further changes or damage by the attacker, while taking a snapshot creates a copy of the virtual machine's memory and disk contents.

NEW QUESTION 119

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 120
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 122
A security analyst observes a large amount of scanning activity coming from an IP address outside the organization's environment. Which of the following should the analyst do to block this activity?

A. Create an IPS rule to block the subnet.
B. Sinkhole the IP address.
C. Create a firewall rule to block the IP address.
D. Close all unnecessary open ports.

Answer: C

Explanation:
A firewall is a device or software that controls the incoming and outgoing network traffic based on predefined rules. Creating a firewall rule to block the IP address that is scanning the organization's environment is an effective way to stop this activity and prevent potential attacks. Creating an IPS rule to block the subnet, sinkholing the IP address, or closing all unnecessary open ports are other possible actions, but they are not as specific or efficient as creating a firewall rule to block the IP address. Reference: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/firewall.html

NEW QUESTION 127
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 * xls > accessreport.txt
B. more webserver.log > grep "xls > egrep -E 'success' > accessreport.txt
C. more webserver.log | grep ' -E "return=200 | accessreport.txt
D. more webserver.log | grep -A *.xls < 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 129
Which of me following are reasons why consumer IoT devices should be avoided in an enterprise environment? (Select TWO)

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

Answer: BD

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

- The devices may have weak or known passwords: Many consumer IoT devices come with default or hardcoded passwords that are easy to guess or find online. Some devices may not allow users to change their passwords or enforce strong password policies. This can make them vulnerable to brute-force attacks or unauthorized access by attackers.
- The devices may utilize unsecure network protocols: Many consumer IoT devices use unsecure network protocols to communicate with other devices or servers, such as HTTP, FTP, Telnet, etc. These protocols do not encrypt or authenticate the data they transmit or receive, which can expose them to interception, modification, or spoofing by attackers.

NEW QUESTION 130
A security analyst discovers suspicious host activity while performing monitoring activities. The analyst pulls a packet capture for the activity and sees the following:

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

Follow TCP stream:

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

Which of the following describes what has occurred?

A. The host attempted to download an application from utoftor.com.
B. The host downloaded an application from utoftor.com.
C. The host attempted to make a secure connection to utoftor.com.
D. The host rejected the connection from utoftor.com.

Answer: C

Explanation:

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

NEW QUESTION 133
A network appliance manufacturer is building a new generation of devices and would like to include chipset security improvements. The management team wants the security team to implement a method to prevent security weaknesses that could be reintroduced by downgrading the firmware version on the chipset. Which of the following would meet this objective?

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

Answer: C

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

NEW QUESTION 138
A cybersecurity analyst is supporting an Incident response effort via threat Intelligence Which of the following is the analyst most likely executing?

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

Answer: D

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

NEW QUESTION 142
Legacy medical equipment, which contains sensitive data, cannot be patched. Which of the following is the best solution to improve the equipment's security posture?

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

Answer: B

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

NEW QUESTION 146
An organization completed an internal assessment of its policies and procedures. The audit team identified a deficiency in the policies and procedures for PH. Which of the following should be the first step to secure the organization's Pll?

A. Complete Pll training within the organization.
B. Contact all Pll data owners within the organization.
C. Identify what type of Pll is on the network.
D. Formalize current Pll documentation.

Answer: C

Explanation:
PII stands for Personally Identifiable Information, and it is any data that can be used to identify, locate, or contact an individual. Examples of PII include names, addresses, phone numbers, email addresses, social security numbers, bank account numbers, etc. The first step to secure the organization's PII is to identify what type of PII is on the network, where it is stored, who has access to it, and how it is transmitted. This can help determine the scope and impact of the deficiency in the policies and procedures for PII.

NEW QUESTION 151
A threat hurting team received a new IoC 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 156
An analyst is performing a BIA and needs to consider measures and metrics. Which of the following would help the analyst achieve this objective? (Select two).

A. Time to reimage the server
B. Minimum data backup volume
C. Disaster recovery plan for non-critical services
D. Maximum downtime before impact is unacceptable
E. Time required to inform stakeholders about outage
F. Total time accepted for business process outage

Answer: DF

Explanation:
The objective of a BIA is to determine the potential impacts of various disruptions on the business processes and functions, and to establish the recovery priorities and objectives for each process and function. To achieve this objective, the analyst needs to consider various measures and metrics that can quantify the impacts and the recovery requirements. Some of the common measures and metrics that are used in a BIA are:

- Maximum downtime before impact is unacceptable: This metric defines the maximum amount of time that a business process or function can be disrupted without causing significant or irreversible damage to the organization's reputation, operations, finances, or legal obligations. This metric is also known as the maximum tolerable downtime (MTD) or maximum tolerable period of disruption (MTPD). It helps to determine the recovery time objective (RTO), which is the target time for restoring the process or function to an acceptable level of service after a disruption1.
- Total time accepted for business process outage: This metric defines the total amount of time that a business process or function can be out of service within a given period, such as a day, a week, or a month. This metric is also known as the recovery point objective (RPO), which is the maximum amount of data loss or corruption that can be tolerated after a disruption1. It helps to determine the backup frequency and retention policy for the data and systems that support the process or function.
- Time required to inform stakeholders about outage: This metric defines the time frame for communicating with the internal and external stakeholders who are affected by or involved in the disruption and recovery of a business process or function. This metric helps to establish the crisis communication plan and protocol, which specifies who, what, when, where, why, and how to communicate during and after a disruption2. It also helps to manage the expectations and perceptions of the stakeholders and to maintain their trust and confidence in the organization.
- Time to reimage the server: This metric defines the time needed to restore a server to its original or desired state after a disruption. This metric helps to estimate the resources and efforts required for recovering the server and its applications. It also helps to evaluate the feasibility and effectiveness of different recovery strategies, such as restoring from backup, rebuilding from scratch, or replacing with a spare3.
- Minimum data backup volume: This metric defines the minimum amount of data that needs to be backed up regularly to ensure the continuity and integrity of a business process or function. This metric helps to optimize the backup process and reduce the storage costs and bandwidth consumption. It also helps to identify the critical data elements and sources that are essential for the process or function4.

NEW QUESTION 157
A security analyst is reviewing the following Internet usage trend report:

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

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

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

Answer: D

Explanation:
The Internet usage trend report shows that User 4 has an unusually high amount of data downloaded compared to other users. User 4 downloaded 2.5 GB of data

in one day, while the average data downloaded by other users was around 0.2 GB. This could indicate that User 4 is engaged in some suspicious or malicious activity, such as downloading unauthorized or illegal content, exfiltrating sensitive data, or installing malware. Therefore, the security analyst should investigate User 4 further to determine the nature and source of the data downloaded.

NEW QUESTION 159
During an audit several customer order forms were found to contain inconsistencies between the actual price of an item and the amount charged to the customer Further investigation narrowed the cause of the issue to manipulation of the public-facing web form used by customers to order products Which of the following would be the BEST way to locate this issue?

A. Reduce the session timeout threshold
B. Deploy MFA for access to the web server
C. Implement input validation
D. Run a static code scan

Answer: C

Explanation:
In this scenario, the issue is related to manipulation of the public-facing web form, indicating that attackers might be altering the prices before submitting the form. One of the best ways to prevent such attacks is to implement input validation, which can help ensure that the data submitted to the web form is correct, complete, and in the expected format. Input validation can also help prevent SQL injection and other types of web-based attacks.

NEW QUESTION 161
An organization announces that all employees will need to work remotely for an extended period of time. All employees will be provided with a laptop and supported hardware to facilitate this requirement. The organization asks the information security division to reduce the risk during this time. Which of the following is a technical control that will reduce the risk of data loss if a laptop is lost or stolen?

A. Requiring the use of the corporate VPN
B. Requiring the screen to be locked after five minutes of inactivity
C. Requiring the laptop to be locked in a cabinet when not in use
D. Requiring full disk encryption

Answer: D

Explanation:
Full disk encryption (FDE) is a technical control that encrypts all the data on a disk drive, including the operating system and applications. FDE prevents unauthorized access to the data if the disk drive is lost or stolen, as it requires a password or key to decrypt the data. FDE can be implemented using software or hardware solutions and can protect data at rest on laptops and other devices. The other options are not technical controls or do not reduce the risk of data loss if a laptop is lost or stolen. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 10; https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview

NEW QUESTION 163
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 164
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 169
A customer notifies a security analyst that a web application is vulnerable to information disclosure The analyst needs to indicate the seventy of the vulnerability based on its CVSS score, which the analyst needs to calculate When analyzing the vulnerability the analyst realizes that tor the attack to be successful, the Tomcat configuration file must be modified Which of the following values should the security analyst choose when evaluating the CVSS score?

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

Answer: C

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

NEW QUESTION 172
The majority of a company's employees have stated they are unable to perform their job duties due to outdated workstations, so the company has decided to institute BYOD. Which of the following would a security analyst MOST likely recommend for securing the proposed solution?

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

Answer: B

Explanation:
VDI means virtual desktop interface. Using VDI, you can maintain a standard image and remove the threat of an infected machine plugging into your network.
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 176
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 177

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 181
A code review reveals a web application is using lime-based cookies for session management. This is a security concern because lime-based cookies are easy to:

A. parameterize.
B. decode.
C. guess.
D. decrypt.

Answer: B

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

NEW QUESTION 186
An organization wants to move non-essential services into a cloud computing environment. The management team has a cost focus and would like to achieve a recovery time objective of 12 hours. Which of the following cloud recovery strategies would work best to attain the desired outcome?

A. Duplicate all services in another instance and load balance between the instances.
B. Establish a hot site with active replication to another region within the same cloud provider.
C. Set up a warm disaster recovery site with the same cloud provider in a different region.
D. Configure the systems with a cold site at another cloud provider that can be used for failover.

Answer: C

Explanation:
Setting up a warm disaster recovery site with the same cloud provider in a different region can help to achieve a recovery time objective (RTO) of 12 hours while keeping the costs low. A warm disaster recovery site is a partially configured site that has some of the essential hardware and software components ready to be activated in case of a disaster. A warm site can provide faster recovery than a cold site, which has no preconfigured components, but lower costs than a hot site, which has fully configured and replicated components. Using the same cloud provider can help to simplify the migration and synchronization processes, while using a different region can help to avoid regional outages or disasters .

NEW QUESTION 190
A company's Chief Information Security Officer [CISO) is concerned about the integrity of some highly confidential files. Any changes to these files must be tied back to a specific authorized user's activity session. Which of the following is the best technique to address the ClSO's concerns?

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

Answer: B

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

NEW QUESTION 195
An organization is experiencing security incidents in which a systems administrator is creating unauthorized user accounts A security analyst has created a script to snapshot the system configuration each day. Following iss one of the scripts:

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

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

```
diff daily_11_03_2019 daily_11_04_2019
```

B)

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

C)

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

D)

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

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

Answer: D

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

NEW QUESTION 200
An incident response team is responding to a breach of multiple systems that contain Pll and PHI Disclosure of the incident to external entities should be based on:

A. the responder's discretion.
B. the public relations policy.
C. the communication plan.
D. the senior management team's guidance.

Answer: C

Explanation:
The communication plan is an important part of incident response, as it outlines how and when information about the incident should be shared with external entities.
A communication plan is a set of procedures and protocols that define how an organization should communicate with external entities during times of emergency or security incident. The plan typically outlines how and when information about the incident should be shared, and ensures that any relevant stakeholders are informed of the incident in a timely manner. It also serves as a guide for determining what information to share with outside parties. Here is a link to an article from CompTIA's website about the importance of a communication plan for incident response for your reference:
https://www.comptia.org/content/incident-response-communication-plan

NEW QUESTION 201
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 203
A technician working at company.com received the following email:

From: joe@gmail.com
To: technician@company.com
Subject: FW: Need help with my computer

Dear tech support,

Please contact me at +1-555-867-5309 as my computer was not fixed by the previous technician. My employee ID is 030234 and the computer serial # is A238482

---- Forward Message ----
From: joe@company.com
To: joe@gmail.com
Subject: FW: Need help with my computer

Dear joe, rebooting you computer should solve the issue.

After looking at the above communication, which of the following should the technician recommend to the security team to prevent exposure of sensitive information and reduce the risk of corporate data being stored on non-corporate assets?

A. Forwarding of corporate email should be disallowed by the company.
B. A VPN should be used to allow technicians to troubleshoot computer issues securely.
C. An email banner should be implemented to identify emails coming from external sources.
D. A rule should be placed on the DLP to flag employee IDs and serial numbers.

Answer: C

Explanation:
An email banner is a message that is added to the top or bottom of an email to provide some information or
warning to the recipient. An email banner should be implemented to identify emails coming from external sources to prevent exposure of sensitive information and reduce the risk of corporate data being stored on
non-corporate assets. An email banner can help employees recognize phishing or spoofing attempts and avoid clicking on malicious links or attachments. It can also remind employees not to share confidential information with external parties or forward corporate emails to personal accounts. The other options are not relevant or effective for this purpose. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 13;
https://www.csoonline.com/article/3235970/what-is-spoofing-definition-and-how-to-prevent-it.html

NEW QUESTION 207
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 208
An employee observes degraded system performance on a Windows workstation. While attempting to access documents, the employee notices the file icons appear abnormal and the file extensions have been changed. The employee instantly shuts down the machine and alerts a supervisor.
Which of the following forensic evidence will be lost as a result of these actions?

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

Answer: D

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

NEW QUESTION 211
A security analyst who works in the SOC receives a new requirement to monitor for indicators of compromise. Which of the following is the first action the analyst

should take in this situation?

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

Answer: B

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

NEW QUESTION 215
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 1663238133, 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 1663238134, 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 [R.], 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 218
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 221
An organization is focused on restructuring its data governance programs and an analyst has been Tasked with surveying sensitive data within the organization.
Which of the following is the MOST accurate method for the security analyst to complete this assignment?

A. Perform an enterprise-wide discovery scan.
B. Consult with an internal data custodian.

C. Review enterprise-wide asset Inventory.
D. Create a survey and distribute it to data owners.

Answer: A

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

NEW QUESTION 225
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 228
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 231
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:
A data minimization plan is a strategy that aims to reduce the amount and type of data that an organization collects, stores, and processes. It can help improve data privacy and protection by limiting the exposure and impact of a data breach or loss. Creating a data minimization plan is the best recommendation for a security officer who needs to find the most cost-effective solution to the current data privacy and protection gap. Requiring users to sign NDAs, adding access control requirements, or implementing a data loss prevention solution are other possible solutions, but they are not as cost-effective as creating a data minimization plan. Reference:
https://www.csoonline.com/article/3603898/data-minimization-what-is-it-and-how-to-implement-it.html

NEW QUESTION 234
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 235
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 240
A security analyst is investigate an no client related to an alert from the threat detection platform on a host (10.0 1.25) in a staging environment that could be running a cryptomining tool because it in sending traffic to an IP address that are related to Bitcoin.
The network rules for the instance are the following:

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

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

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

Answer: C

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

NEW QUESTION 242
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 245
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 249
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 254
A security analyst is investigating a reported phishing attempt that was received by many users throughout the company The text of one of the emails is shown below:

```
Return-Path: <security@off1ce365.com>
Received: from [122.167.40.119]
Message-ID: <FE3638ACA.2020509@off1ce365.com>
Date: 23 May 2020 11:40:36 -0400
From: security@off1ce365.com
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: Paul Vieira <pvieira@company.com>
Subject: Account Lockout
Content-Type: HTML;
```

Office 365 User.
It looks like you account has been locked out Please click this link and follow the pfompts to restore access Regards. Security Team
Due to the size of the company and the high storage requirements, the company does not log DNS requests or perform packet captures of network traffic, but rt does log network flow data Which of the following commands will the analyst most likely execute NEXT?

A. telnet office365.com 25

B. tracert 122.167.40.119
C. curl http:// accountfix-office365.com/logi
D. php
E. nslookup accountfix-office365.com

Answer: D

Explanation:
nslookup is a command-line tool that can query the Domain Name System (DNS) and display information about domain names and IP addresses. The security analyst can use nslookup to find out the IP address of the malicious domain accountfix-office365.com that was used in the phishing attempt. This could help the analyst to block or trace the source of the attack. telnet, tracert, and curl are other command-line tools, but they are not as useful as nslookup for investigating a phishing attempt based on a domain name. Reference: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/nslookup

NEW QUESTION 257
A security analyst is reviewing the following server statistics:

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

Which of the following Is MOST likely occurring?

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

Answer: C

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

NEW QUESTION 260
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 262
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 265
Which of the following is the best method to review and assess the security of the cloud service models used by a company on multiple CSPs?

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

Answer: C

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

NEW QUESTION 268
.....

Relate Links

100% Pass Your CS0-002 Exam with Exambible Prep Materials

https://www.exambible.com/CS0-002-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/