CompTIA

Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

NEW QUESTION 1
As part of an Intelligence feed, a security analyst receives a report from a third-party trusted source. Within the report are several detrains and reputational information that suggest the company's employees may be targeted for a phishing campaign. Which of the following configuration changes would be the MOST appropriate for Mergence gathering?

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

Answer: D

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

NEW QUESTION 2
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 Chief Information Officer wants to implement a BYOD strategy for all company laptops and mobile phones. The Chief Information Security Officer is concerned with ensuring all devices are patched and running some sort of protection against malicious software. Which of the following existing technical controls should a security analyst recommend to best meet all the requirements?

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

Answer: A

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

NEW QUESTION 5
A 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 6
A manufacturing company has joined the information sharing and analysis center for its sector. As a benefit, the company will receive structured loC data contributed by other members. Which of the following best describes the utility of this data?

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

Answer: B

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

NEW QUESTION 7
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 8
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 9
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 10
During the onboarding process for a new vendor, a security analyst obtains a copy of the vendor's latest penetration test summary:

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

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

A. Perform a more recent penetration test.
B. Continue vendor onboarding.
C. Disclose details regarding the findings.
D. Have a neutral third party perform a penetration test.

Answer: C

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

NEW QUESTION 10
When investigating a report of a system compromise, a security analyst views the following /var/log/secure log file:

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

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

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

Answer: B

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

NEW QUESTION 14
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 16
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 17
A cybersecunty analyst needs to harden a server that is currently being used as a web server The server needs to be accessible when entenng www company com into the browser Additionally web pages require frequent updates which are performed by a remote contractor Given the following output:

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

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

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

Answer: DF

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

NEW QUESTION 21
An IT security analyst has received an email alert regarding vulnerability within the new fleet of vehicles the company recently purchased. Which of the following attack vectors is the vulnerability MOST likely targeting?

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

Answer: B

Explanation:
CAN bus (Controller Area Network) is a vehicle bus standard designed to allow microcontrollers and devices to communicate with each other's applications without a host computer1. CAN bus is a message-based protocol, designed originally for multiplex electrical wiring within automobiles to save on copper, but it can also be used in many other contexts. CAN bus enables each device to send and receive data on a shared network, reducing the need for complex wiring and increasing reliability and performance. CAN bus is one of the five protocols used in the on-board diagnostics (OBD)-II vehicle diagnostics standard. A vulnerability within the new fleet of vehicles that the company recently purchased is most likely targeting CAN bus, as it is a common and critical communication system in modern vehicles. An attacker could exploit a vulnerability in CAN bus to compromise or manipulate various vehicle functions or systems, such as braking, steering, engine control, airbags, etc. SCADA (A) stands for Supervisory Control And Data Acquisition, which is a system that monitors and controls industrial processes or infrastructure2. SCADA is not a vehicle bus standard and is not likely to be targeted by a vulnerability within a fleet of vehicles. Modbus © is a serial communications protocol that connects industrial electronic devices3. Modbus is not a vehicle bus standard and is not likely to be targeted by a vulnerability within a fleet of vehicles. IoT (D) stands for Internet of Things, which is a network of physical objects that are embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems over the internet. IoT is not a vehicle bus standard and is not likely to be targeted by a vulnerability within a fleet of vehicles.
References: 1: https://www.techopedia.com/definition/24771/technical-controls 2: https://www.techopedia.com/definition/25888/security-development-lifecycle-sdl 3: https://www.techopedia.com/definition/31686/resource-exhaustion : https://www.techopedia.com/definition/13493/penetration-testing

NEW QUESTION 22
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 26
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 27
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 29
Which of the following best explains why it is important for companies to implement both privacy and security policies?

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

Answer: D

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

NEW QUESTION 33
After examining a header and footer file, a security analyst begins reconstructing files by scanning the raw data bytes of a hard disk and rebuilding them. Which of the following techniques is the analyst using?

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

Answer: B

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

NEW QUESTION 34
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 36
A routine vulnerability scan detected a known vulnerability in a critical enterprise web application. Which of the following would be the BEST next step?

A. Submit a change request to have the system patched
B. Evaluate the risk and criticality to determine it further action is necessary
C. Notify a manager of the breach and initiate emergency procedures.

D. Remove the application from production and Inform the users.

Answer: B

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

NEW QUESTION 41
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 43
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 47
While reviewing system logs, a network administrator discovers the following entry:

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

Which of the following occurred?

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

Answer: D

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

NEW QUESTION 50
A new government regulation requires that organizations only retain the minimum amount of data on a person to perform the organization's necessary activities. Which of the following techniques would help an organization comply with this new regulation?

A. Storing the highest-risk data in a separate and secured environment
B. Limiting access to data on a need-to-know basis
C. Deidentlfying a data subject throughout the organization's applications
D. Having a privacy expert peer review source code before deployment

Answer: C

Explanation:
Deidentifying a data subject means removing or obscuring any data that can be used to identify, locate, or contact an individual, such as names, addresses, phone numbers, email addresses, social security numbers, etc. Deidentifying a data subject throughout the organization’s applications can help comply with the new regulation that requires only retaining the minimum amount of data on a person to perform the organization’s necessary activities.

NEW QUESTION 55
Which of the following BEST describes what an organizations incident response plan should cover regarding how the organization handles public or private disclosures of an incident?

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

Answer: B

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

NEW QUESTION 59
Which of the following data exfiltration discoveries would most likely require communicating a breach to regulatory agencies?

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

Answer: B

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

NEW QUESTION 61
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 66
The following output is from a tcpdump al the edge of the corporate network:

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 69
During a routine review of service restarts a security analyst observes the following in a server log:

```
2020-04-12 05:30:34 ircd.exe MD5:1FD92EA11890CD4B7A85133FF780EB09 PID:1170
2020-04-16 05:00:59 ircd.exe MD5:1FD92EA11890CD4B7A85133FF780EB09 PID:1422
2020-04-17 05:16:13 ircd.exe MD5:1FD92EA11890CD4B7A85133FF780EB09 PID:1523
2020-04-18 05:29:41 ircd.exe MD5:90EB29AE33DFA9AA00B16788934801EF PID:1672
2020-04-22 04:59:50 ircd.exe MD5:90EB29AE33DFA9AA00B16788934801EF PID:1788
2020-04-23 05:21:29 ircd.exe MD5:90EB29AE33DFA9AA00B16788934801EF PID:1827
2020-04-24 05:18:38 ircd.exe MD5:90EB29AE33DFA9AA00B16788934801EF PID:1501
```

Which of the following is the GREATEST security concern?

A. The daemon's binary was AChanged
B. Four consecutive days of monitoring are skipped in the tog
C. The process identifiers for the running service change
D. The PIDs are continuously changing

Answer: A

Explanation:
A daemon is a program that runs in the background on a system and performs certain tasks or services without user intervention. A daemon’s binary is the executable file that contains the code and instructions for the daemon to run. The server log shows that the daemon’s binary was changed on Aug 1 2020 at 00:00:01 by an unknown user with UID 0 (root). This is the greatest security concern, because it could indicate that an attacker has gained root access to the system and modified the daemon’s binary with malicious code that could compromise the system’s security or functionality. Four consecutive days of monitoring being skipped in the log, the process identifiers for the running service changing, or the PIDs continuously changing are not security concerns, but rather normal events that could occur due to system maintenance, updates, restarts, or scheduling. Reference: https://www.linux.com/training-tutorials/what-are-linux-daemons/

NEW QUESTION 73
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 78
A security analyst is running a tool against an executable of an unknown source. The Input supplied by the tool to the executable program and the output from the executable are shown below:

Input supplied by tool	Output from executable
asdfnerlajnvjanjkdfnvkjanakjdv	asdfnerlajnvjanjkdfnvkjanakjdv
klrejfkalsdjfklasdjffjladsf892	klrejfkalsdjfklasdjffjladsf892
ADSFQEOVASLASDFASDF;ADSFASDWDF	command not found
qscTRGvcaDFcaDCasDC23zdcasdfAS	qscTRGvcaDFcaDCasDC23zdcasdfAS
lqkcjfc934cjcjvsad:cmaciwcfasd	lqkcjfc934cjcjvsad:cmaciwcfasd

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

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

Answer: C

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

NEW QUESTION 82
A security analyst is correlating, ranking, and enriching raw data into a report that will be interpreted by humans or machines to draw conclusions and create actionable recommendations Which of the following steps in the intelligence cycle is the security analyst performing?

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

Answer: B

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

NEW QUESTION 85
A security manager has asked an analyst to provide feedback on the results of a penetration test. After reviewing the results, the manager requests information regarding the possible exploitation of vulnerabilities. Which of the following information data points would be MOST useful for the analyst to provide to the security manager, who would then communicate the risk factors to the senior management team? (Select TWO).

A. Probability
B. Adversary capability
C. Attack vector
D. Impact
E. Classification
F. Indicators of compromise

Answer: BD

Explanation:
According to the CompTIA CySA+ (CS0-002) best practices, the most useful information data points to provide to the security manager for communicating the risk factors to senior management are the impact and adversary capability. The impact refers to the potential consequences of a successful attack or exploitation of a vulnerability, such as data loss or system compromise. The adversary capability refers to the ability of an attacker to exploit a vulnerability, including their technical expertise and resources. Together, these data points help to provide a complete picture of the risk associated with a vulnerability, and allow senior management to make informed decisions regarding risk mitigation and remediation. The other data points, such as probability, attack vector, classification, and indicators of compromise, can also be valuable, but the impact and adversary capability are considered the most critical for prioritizing risk mitigation efforts.

NEW QUESTION 90
Which of the following describes the difference between intentional and unintentional insider threats'?

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

Answer: C

Explanation:
The difference between intentional and unintentional insider threats is their behavior. Intentional insider threats are malicious actors who deliberately misuse their access to harm the organization or its assets. Unintentional insider threats are careless or negligent users who accidentally compromise the security of the

organization or its assets. Their access levels, risk factors, and rates of occurrence may vary depending on various factors, but their behavior is the main distinction. References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 12; https://www.cisa.gov/sites/default/files/publications/Insider_Threat_Mitigation_Guide_508.pdf

NEW QUESTION 95
A development team recently released a new version of a public-facing website for testing prior to production. The development team is soliciting the help of various teams to validate the functionality of the website due to its high visibility. Which of the following activities best describes the process the development team is initiating?

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

Answer: D

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

NEW QUESTION 97
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 100
A security analyst identified one server that was compromised and used as a data making machine, and a few of the hard drive that was created. Which of the following will MOST likely provide information about when and how the machine was compromised and where the malware is located?

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

Answer: A

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

NEW QUESTION 104
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 109
Which of the following solutions is the BEST method to prevent unauthorized use of an API?

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

Answer: D

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

NEW QUESTION 112
During an Incident, it Is determined that a customer database containing email addresses, first names, and last names was exfiltrated. Which ot the following should the security analyst do NEXT?

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

Answer: D

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

NEW QUESTION 116
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 118
An organization's internal department frequently uses a cloud provider to store large amounts of sensitive data. A threat actor has deployed a virtual machine to at the use of the cloud hosted hypervisor, the threat actor has escalated the access rights. Which of the following actions would be BEST to remediate the vulnerability?

A. Sandbox the virtual machine.
B. Implement an MFA solution.
C. Update lo the secure hypervisor version.
D. Implement dedicated hardware for each customer.

Answer: C

Explanation:
MFA can be used to reduce the likelihood that the attacker gains access to the VM, however, the scenario specifically states that the attacker was able to escalate rights and the question asks what can be done to remediate the vulnerability. the vulnerability in this case would be the ability to escalate rights.
The best way to remediate the vulnerability is to update to the secure hypervisor version. A hypervisor is a software that creates and manages virtual machines on a physical server. A hypervisor can be vulnerable to various attacks, such as privilege escalation, code injection, or denial-of-service. Updating to the secure hypervisor version can help fix any known bugs or flaws in the hypervisor software and prevent attackers from exploiting them. Updating to the secure hypervisor version can also provide additional security features or enhancements that can improve the protection of the virtual machines and their data.

NEW QUESTION 119
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 121
Company A is m the process of merging with Company B As part of the merger, connectivity between the ERP systems must be established so portent financial information can be shared between the two entitles. Which of the following will establish a more automated approach to secure data transfers between the two entities?

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

Answer: C

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

NEW QUESTION 125
An organization discovers motherboards within the environment that appear to have been physically altered during the manufacturing process. Which of the following is the BEST course of action to mitigate the risk of this reoccurring?

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

Answer: C

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

NEW QUESTION 127
A threat hurting team received a new loC from an ISAC that follows a threat actor's profile and activities. Which of the following should be updated NEXT?

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

Answer: D

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

NEW QUESTION 131
A security analyst is reviewing vulnerability scans from an organization's internet-facing web services. The following is from an output file called ssl-test_webapps.comptia.org:

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

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


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


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

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

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

Answer: A

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

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

The cipher suite in this line is weak because:
-

DES is an outdated encryption algorithm that has been broken by brute force attacks, as it has a small key size of 56 bits, which can be easily guessed by modern computers.

- RSA does not provide forward secrecy, which means that if the RSA private key is compromised, all past and future communications encrypted with that key can be decrypted by an attacker.
- SHA is also an outdated hash algorithm that has been replaced by newer versions such as SHA-2 or SHA-3, as it has some vulnerabilities and weaknesses.

NEW QUESTION 132
A manufacturing company uses a third-party service provider for Tier 1 security support. One of the requirements is that the provider must only source talent from its own country due to geopolitical and national security interests. Which of the following can the manufacturing company implement to ensure the third-party service provider meets this requirement?

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

Answer: A

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

NEW QUESTION 137
Ensuring that all areas of security have the proper controls is a primary reason why organizations use:

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

Answer: A

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

NEW QUESTION 140
A security analyst discovers the accounting department is hosting an accounts receivable form on a public document service. Anyone with the link can access it. Which of the following threats applies to this situation?

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

Answer: A

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

NEW QUESTION 142
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 147
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 150
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 151
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 155
Which of the following is a reason for correctly identifying APTs that might be targeting an organization?

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

Answer: B

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

NEW QUESTION 159
A security technician is testing a solution that will prevent outside entities from spoofing the company's email domain, which is compatia.org. The testing is successful, and the security technician is prepared to fully implement the solution. Which of the following actions should the technician take to accomplish this task?

A. Add TXT @ "v=spfl mx include:_spf.compti
B. org -all" to the DNS record.
C. Add : XT @ "v=spfl mx include:_sp£.comptia.org -all" to the email server.
D. Add TXT @ "v=spfl mx include:_sp£.comptia.org +all" to the domain controller.
E. AddTXT @ "v=apfl mx lnclude:_spf .comptia.org +a 11" to the web server.

Answer: A

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

NEW QUESTION 161
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 162
A security analyst needs to determine the best method for securing access to a top-secret datacenter Along with an access card and PIN code, which of the following additional authentication methods would be BEST to enhance the datacenter's security?

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

Answer: B

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

NEW QUESTION 163
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 167
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 170
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 174
A security analyst is supporting an embedded software team. Which of the following is the best recommendation to ensure proper error handling at runtime?

A. Perform static code analysis.
B. Require application fuzzing.
C. Enforce input validation.
D. Perform a code review.

Answer: D

Explanation:
Performing a code review is the best recommendation to ensure proper error handling at runtime for an embedded software team. A code review is a process of examining and evaluating source code by one or more developers other than the original author. A code review can help to identify and fix any errors, bugs, vulnerabilities, or inefficiencies in the code before it is deployed or executed. A code review can also help to ensure that the code follows the best practices, standards, and guidelines for error handling at runtime .

NEW QUESTION 177
An email analysis system notifies a security analyst that the following message was quarantined and requires further review.

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

Which of the following actions should the security analyst take?

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

Answer: C

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

NEW QUESTION 179
A security analyst is scanning the network to determine if a critical security patch was applied to all systems in an enterprise. The Organization has a very low tolerance for risk when it comes to resource availability. Which of the following is the BEST approach for configuring and scheduling the scan?

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

Answer: D

Explanation:
A vulnerability scan is a process of identifying and assessing known vulnerabilities in a system or network
using automated tools or software1
A vulnerability scan can help improve the security posture of a vulnerability management program by detecting and prioritizing potential weaknesses that could be exploited by attackers. To increase the security posture of a vulnerability scan, the following actions can be taken:

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

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

NEW QUESTION 184
An analyst is responding 10 an incident involving an attack on a company-owned mobile device that was being used by an employee to collect data from clients in the held. Maiware was loaded on the device via the installation of a third-party software package The analyst has baselined the device Which of the following should the analyst do to BEST mitigate future attacks?

A. Implement MDM
B. Update the maiware catalog
C. Patch the mobile device's OS
D. Block third-party applications

Answer: D

Explanation:
Blocking third-party applications would be the best way to mitigate future attacks on company-owned mobile devices that are used by employees to collect data from clients in the field. Third-party applications are applications that are not developed or authorized by the device manufacturer or operating system provider1. Third-party applications can pose a security risk for mobile devices, as they may contain malware, spyware, or other malicious code that can compromise the device or its data2. Blocking third-party applications can help prevent employees from installing unauthorized or untrusted applications on company-owned mobile devices and reduce the attack surface.

NEW QUESTION 185
A forensic examiner is investigating possible malware compromise on an active endpoint device. Which of the following steps should the examiner perform first?

A. Verify the hash value of the image with the value of the copy.
B. Use a write blocker to create an image of the hard drive.
C. Create a memory dump from RAM.
D. Download and apply the latest AV signature.
E. Reimage the hard drive and apply the latest updates.

Answer: C

Explanation:
A memory dump is a snapshot of the contents of the random access memory (RAM) of a system at a given
point in time. A memory dump can provide valuable information for a forensic examiner who is investigating possible malware compromise on an active endpoint device, such as running processes, open files, network connections, encryption keys, or malware artifacts. Creating a memory dump from RAM should be the first step that the examiner performs, as it preserves the volatile data that could be lost or altered if the system is powered off or rebooted1.

NEW QUESTION 189
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 190
Industry partners from critical infrastructure organizations were victims of attacks on their SCADA devices. The attacker was able to gain access to the SCADA by logging in to an account with weak credentials. Which of the following identity and access management solutions would help to mitigate this risk?

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

Answer: D

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

NEW QUESTION 193
The Chief Information Security Officer (CISO) of a large financial institution is seeking a solution that will block a predetermined set of data points from being transferred or downloaded by employees. The CISO also wants to track the data assets by name, type, content, or data profile.
Which of the following BEST describes what the CIS wants to purchase?

A. Asset tagging
B. SIEM
C. File integrity monitor
D. DLP

Answer: D

Explanation:
DLP (Data Loss Prevention) is what the CISO wants to purchase. DLP is a solution that prevents unauthorized or accidental disclosure of sensitive data by monitoring, detecting, and blocking data transfers or downloads that violate predefined policies or rules3. DLP can also track and classify data assets based on various criteria, such as name, type, content, or data profile4. DLP can help protect data from insider threats, external attackers, or human errors.

NEW QUESTION 194
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 197
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 202
The IT department is concerned about the possibility of a guest device infecting machines on the corporate network or taking down the company's singe internet connection. Which of the following should a security analyst recommend to BEST meet the requirements outlined by the IT Department?

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

Answer: C

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

NEW QUESTION 206
A security analyst needs to provide a copy of a hard drive for forensic analysis. Which of the following would allow the analyst to perform the task?
A)

```
dcfldd if=/dev/one of=/mnt/usb/evidence.bin hash=md5,sha1 hashlog=/mnt/usb/evidence.bin.hashlog
```

B)

```
dd if=/dev/sda of=/mnt/usb/evidence.bin bs=4096; sha512sum /mnt/usb/evidence.bin > /mnt/usb/evidence.bin.hash
```

C)

```
tar -zcf /mnt/usb/evidence.tar.gz / -except /mnt :sha256sum /mnt/usb/evidence.tar.gz > /mnt/usb/evidence.tar.gz.hash
```

D)

```
find / -type f -exec cp {} /mnt/usb/evidence/ \; shalsum /mnt/usb/evidence/* > /mnt/usb/evidence/evidence.hash
```

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

Answer: C

Explanation:
Option C shows a device that can perform a forensic copy of a hard drive. A forensic copy, also known as a forensic image or a bit-stream image, is an exact, unaltered digital copy of a piece of digital evidence. A forensic copy captures everything on the hard drive, including active and latent data, and preserves the integrity of the original evidence. A forensic copy can be used for forensic analysis without risking any changes to the original drive1. Option C shows a device that can connect to two hard drives and create a
forensic copy from one drive to another using a write-blocker. A write-blocker is a tool that prevents any data from being written to the destination drive, ensuring that only a read-only copy is made2.

NEW QUESTION 210
A developer is working on a program to convert user-generated input in a web form before it is displayed by the browser. This technique is referred to as:

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

Answer: A

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

NEW QUESTION 211
During an incident investigation, a security analyst discovers the web server is generating an unusually high volume of logs The analyst observes the following response codes:
• 20% of the logs are 403
• 20% of the logs are 404
• 50% of the logs are 200
• 10% of the logs are other codes
The server generates 2MB of logs on a daily basis, and the current day log is over 200MB. Which of the following commands should the analyst use to identify the source of the activity?

A. cat access_log Igrep " 403 "
B. cat access_log Igrep " 200 "
C. cat access_log Igrep " 100 "

D. cat access_log Igrep " 4 04 "
E. cat access_log Igrep " 204 "

Answer: B

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

NEW QUESTION 215
A security analyst is designing firewall rules to prevent external IP spoofing Which of the following explains the firewall rule for mitigation?

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

Answer: B

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

NEW QUESTION 216
A security analyst performs a weekly vulnerability scan on a network that has 240 devices and receives a report with 2.450 pages. Which of the following would most likely decrease the number of false positives?

A. Manual validation
B. Penetration testing
C. A known-environment assessment
D. Credentialed scanning

Answer: D

Explanation:
Credentialed scanning is a method of vulnerability scanning that uses valid user credentials to access the target systems and perform a more thorough and accurate assessment of their security posture. Credentialed scanning can help to reduce the number of false positives by allowing the scanner to access more information and resources on the systems, such as configuration files, registry keys, installed software, patches, and permissions .

NEW QUESTION 218
A cybersecurity analyst inspects DNS logs on a regular basis to identify possible IOCs that are not triggered by known signatures. The analyst reviews the following log snippet:

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

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

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

Answer: B

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

NEW QUESTION 220
A company is building a new internal network. Instead of creating new credentials, the company wants to streamline each employee's authentication. Which of the following technologies would best fulfill this requirement?

A. VPN
B. SSO
C. SAML
D. MFA

Answer: B

Explanation:
SSO stands for Single Sign-On, and it is a technology that allows users to authenticate once and access multiple applications or systems without entering their credentials again. SSO can help streamline each employee's authentication, by reducing the number of passwords they have to remember or enter, and improving their user experience and productivity.

NEW QUESTION 222
A company's Chief Information Officer wants to use a CASB solution to ensure policies are being met during cloud access. Due to the nature of the company's business and risk appetite, the management team elected to not store financial information in the cloud. A security analyst needs to recommend a solution to mitigate the threat of financial data leakage into the cloud. Which of the following should the analyst recommend?

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

Answer: C

Explanation:
"CASB solutions generally offer their own DLP policy engine, allowing you to configure DLP policies in a CASB and apply them to cloud services."
https://www.mcafee.com/blogs/enterprise/cloud-security/how-a-casb-integrates-with-an-on-premises-dlp-solutio
CASB stands for Cloud Access Security Broker, which is a solution that monitors and controls the access and usage of cloud services by an organization's users. DLP stands for Data Loss Prevention, which is a solution that prevents unauthorized disclosure or leakage of sensitive data. Utilizing the CASB to enforce DLP data-in-motion protection for financial information moving to the cloud is the best recommendation for a security analyst to mitigate the threat of financial data leakage into the cloud, because it would prevent users from uploading or transferring financial information to cloud services that are not authorized or secure. Utilizing the CASB to enforce DLP data-at-rest protection for financial information that is stored on premises, not utilizing the CASB solution for this purpose but adding DLP on premises for data in motion or data at rest are other possible recommendations, but they are not as effective or relevant as utilizing the CASB to enforce DLP data-in-motion protection for financial information moving to the cloud. Reference: https://www.csoonline.com/article/3200344/what-is-a-casb-and-why-do-you-need-one.html

NEW QUESTION 223
An organization has specific technical nsk mitigation configurations that must be implemented before a new server can be approved for production Several critical servers were recently deployed with the antivirus missing unnecessary ports disabled and insufficient password complexity Which of the following should the analyst recommend to prevent a recurrence of this risk exposure?

A. Perform password-cracking attempts on all devices going into production
B. Perform an Nmap scan on all devices before they are released to production
C. Perform antivirus scans on all devices before they are approved for production
D. Perform automated security controls testing of expected configurations pnor to production

Answer: D

Explanation:
Automated security controls testing is a method that uses tools or scripts to verify that the security controls of a system or device are configured correctly and comply with the organization's policies and standards. Performing automated security controls testing of expected configurations prior to production would help prevent a recurrence of the risk exposure caused by missing antivirus, unnecessary ports enabled, and insufficient password complexity. Performing password-cracking attempts, Nmap scans, or antivirus scans on all devices before they are released to production are other methods that can help detect some security issues, but they are not as comprehensive or efficient as automated security controls testing. Reference:
https://www.nist.gov/system/files/documents/2017/04/28/sp800-115.pdf

NEW QUESTION 228
Which of the following are important reasons for performing proactive threat-hunting activities7 (Select two).

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

Answer: CE

Explanation:
Proactive threat-hunting is the process of actively searching for unknown threats in the network, rather than waiting for alerts or indicators of compromise. Some of the important reasons for performing proactive
threat-hunting activities are:

- To uncover unknown threats that may have evaded detection by existing security tools or controls, and to mitigate them before they cause damage or data loss.
- To create a new security baseline that reflects the current state of the network, and to identify any anomalies or deviations from the normal behavior or activity.

NEW QUESTION 230
While investigating reports or issues with a web server, a security analyst attempts to log in remotely and recedes the following message:

```
[root@localhost /root]# ssh user1@10.254.2.25
Connection timed out.
```

The analyst accesses the server console, and the following console messages are displayed:

```
Out of memory: Kill process 3448(httpd) score 41 or sacrifice child
Killed process 3448(httpd) totle-vm:74716kB, anon-rss: 23456kB, file-ress:1683kB
Out of memory: Kill process 3449(httpd) score 41 or sacrifice child
Killed process 3449(httpd) totle-vm:74634kB, anon-rss: 20542kB, file-ress:1357kB
Out of memory: Kill process 3452(httpd) score 41 or sacrifice child
Killed process 3452(httpd) totle-vm:73466kB, anon-rss: 29753kB, file-ress:1925kB
```

The analyst is also unable to log in on the console. While reviewing network captures for the server, the analyst sees many packets with the following signature:

```
10.254.2.25.6781 > 128.50.100.23.80
10.254.2.25.6782 > 128.50.100.23.80
10.254.2.25.6783 > 128.50.100.23.80
10.254.2.25.6784 > 128.50.100.23.80
```

Which of the following is the BEST step for the analyst to lake next in this situation?

A. Load the network captures into a protocol analyzer to further investigate the communication with 128.30.100.23, as this may be a botnet command server
B. After ensuring network captures from the server are saved isolate the server from the network take a memory snapshot, reboot and log in to do further analysis.
C. Corporate data is being exfilltrated from the server Reboot the server and log in to see if it contains any sensitive data.
D. Cryptomining malware is running on the server and utilizing an CPU and memor
E. Reboot the server and disable any cron Jobs or startup scripts that start the mining software.

Answer: D

Explanation:
Cryptomining malware, or cryptojacking, is a type of malware that hides on a device and uses its computing resources to mine for valuable online currencies like Bitcoin. Cryptomining malware can cause performance
issues, increased energy consumption, overheating, or hardware damage1
The analyst encountered cryptomining malware on the web server, as indicated by the following signs:

- The analyst was unable to log in remotely or on the console, as the malware blocked access to prevent detection or removal.
- The console messages showed that the server was running out of memory and CPU resources, as the malware consumed all available resources for mining.
- The network captures showed many packets with a signature of “Stratum”, which is a protocol used for
communication between miners and mining pools2

The best step for the analyst to take next is to reboot the server and disable any cron jobs or startup scripts that start the mining software. This can help stop the mining activity and restore access to the server. The analyst should also scan the server for any other traces of malware and remove them.

NEW QUESTION 232
A security analyst is investigating a compromised Linux server. The analyst issues the ps command and receives the following output:

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

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

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

Answer: C

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

NEW QUESTION 237
While conoXicting a cloud assessment, a security analyst performs a Prowler scan, which generates the following within the report:

```
7.74 [extra774] Ensure credentials unused for 30 days or greater are disabled
PASS! User admin has logged into the console in the past 30 days
PASS! User SecOps has logged into the console in the past 30 days
INFO! User CloudDev has not used access key 1 since creation
FAIL! User BusinessUsr has never used access key 1 and not rotated it in 30 days
PASS! No users found with access key 2 enabled
```

Based on the Prowler report, which of the following is the BEST recommendation?

A. Delete Cloud Dev access key 1
B. Delete BusinessUsr access key 1.
C. Delete access key 1.
D. Delete access key 2.

Answer: A

Explanation:
The best recommendation based on the Prowler report is to delete Cloud Dev access key 1. This is because the report shows that this access key has not been used for more than 90 days, which violates the AWS security best practice of rotating access keys every 90 days or less. Deleting unused or inactive access keys can reduce the risk of unauthorized access or compromise of AWS resources.

NEW QUESTION 241
A company's security team recently discovered a number of workstations that are at the end of life. The workstation vendor informs the team that the product is no longer supported and patches are no longer available The company is not prepared to cease its use of these workstations Which of the following would be the BEST method to protect these workstations from threats?

A. Deploy whitelisting to the identified workstations to limit the attack surface
B. Determine the system process centrality and document it
C. Isolate the workstations and air gap them when it is feasible
D. Increase security monitoring on the workstations

Answer: A

Explanation:
Deploying whitelisting to the identified workstations would be the best method to protect these workstations from threats. Whitelisting is a technique that allows only authorized applications, processes, or users to run or access a system or resource. Whitelisting can help limit the attack surface and prevent malware or unauthorized software from running on a system3. Deploying whitelisting to the workstations that are at the end of life can help mitigate the risk of exploitation due to lack of patches or support from the vendor.

NEW QUESTION 245
An analyst Is reviewing a web developer's workstation for potential compromise. While examining the workstation's hosts file, the analyst observes the following:

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

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

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

Answer: D

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

NEW QUESTION 248
A company recently experienced a breach of sensitive information that affects customers across multiple geographical regions. Which of the following roles would be BEST suited to determine the breach notification requirements?

A. Legal counsel
B. Chief Security Officer
C. Human resources
D. Law enforcement

Answer: A

Explanation:
A breach notification is a communication to affected individuals or entities that informs them of a security incident involving their personal or sensitive information. A breach notification may include details such as what information was compromised, when and how the incident occurred, what actions are being taken to mitigate the impact, and what steps the recipients should take to protect themselves3
A breach notification may be required by law or regulation, depending on the type and location of the information involved and the jurisdiction of the affected parties. Different countries or regions may have different breach notification requirements, such as who must be notified, when, how, and what information must be disclosed4
Therefore, the best role to determine the breach notification requirements for a company that experienced a breach of sensitive information affecting customers across multiple geographical regions is legal counsel. Legal counsel can advise the company on its legal obligations and liabilities, as well as help draft and deliver appropriate breach notifications.

NEW QUESTION 251
At which of the following phases of the SDLC shoukJ security FIRST be involved?

A. Design
B. Maintenance
C. Implementation
D. Analysis
E. Planning
F. Testing

Answer: E

Explanation:
The software development life cycle (SDLC) is a process that consists of several phases that guide the development of software applications or systems. Security should be involved in every phase of the SDLC, but especially in the planning phase, which is the first phase where the scope, objectives, requirements, and resources of the project are defined. By involving security in the planning phase, potential risks and threats can be identified and mitigated early in the process, which can save time, money, and effort later on. Design, maintenance, implementation, analysis, and testing are other phases of the SDLC, but they are not the first phase where security should be involved. Reference:
https://www.bmc.com/blogs/software-development-life-cycle-phases/

NEW QUESTION 254
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CS0-002 Practice Exam Features:

* CS0-002 Questions and Answers Updated Frequently

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

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

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