EC-COUNCIL.312-39.v2024-08-29.q80

Exam Code:	312-39
Exam Name:	Certified SOC Analyst (CSA)
Certification Provider:	EC-COUNCIL
Free Question Number:	80
Version:	v2024-08-29
# of views:	829
# of Questions views:	800
https://www.freepdfdumps.com/EC-COUNCIL.312-39.v2024-08-29.q80.html	

NEW QUESTION: 1
Which of the following technique protects from flooding attacks originated from the valid prefixes (IP addresses) so that they can be traced to its true source?
A. Egress Filtering
B. Throttling
C. Rate Limiting
D. Ingress Filtering
Answer: D (LEAVE A REPLY)

NEW QUESTION: 2
Jane, a security analyst, while analyzing IDS logs, detected an event matching Regex /((\%3C)|<)((\%69)|i|(\%
49))((\%6D)|m|(\%4D))((\%67)|g|(\%47))[^\n]+((\%3E)|>)/|.
What does this event log indicate?
A. Directory Traversal Attack
B. Parameter Tampering Attack
C. XSS Attack
D. SQL Injection Attack
Answer: C (LEAVE A REPLY)
The regular expression provided in the question is designed to detect patterns that are typically found in XSS (Cross-Site Scripting) attacks. Here's a breakdown of the regex pattern:
* /((\%3C)|<) - This part of the pattern matches the encoded version of < which is %3C, or the symbol < itself. In HTML, this symbol denotes the start of a tag.
* ((\%69)|i|(\%49)) - This matches the encoded version of i which is %69, the lowercase i, or the encoded version of I which is %49.
* ((\%6D)|m|(\%4D)) - This matches the encoded version of m which is %6D, the lowercase m, or the encoded version of M which is %4D.

* ((\%67)|g|(\%47)) - This matches the encoded version of g which is %67, the lowercase g, or the encoded version of G which is %47.
* [^\n]+ - This part of the pattern matches one or more characters that are not a newline character.
* ((\%3E)|>) - This matches the encoded version of > which is %3E, or the symbol > itself, denoting the end of an HTML tag.
The combination of these patterns is looking for a string that resembles an HTML img tag, which is a common vector for XSS attacks. XSS attacks involve injecting malicious scripts into webpages viewed by other users, exploiting the trust a user has for a particular site. XSS attacks can occur when a web application uses unsanitized user input in the output it generates.
References: The EC-Council's Certified SOC Analyst (CSA) program covers the knowledge required to detect and analyze various types of cyber threats, including XSS attacks. The CSA program's curriculum includes understanding of IDS logs and the ability to interpret and respond to potential security events indicated by such logs. For further study and verification, please refer to the official EC-Council CSA study guides and course materials.

NEW QUESTION: 3
Which of the following technique involves scanning the headers of IP packets leaving a network to make sure that the unauthorized or malicious traffic never leaves the internal network?
A. Rate Limiting
B. Throttling
C. Ingress Filtering
D. Egress Filtering
Answer: D (LEAVE A REPLY)

NEW QUESTION: 4
Which of the following is a report writing tool that will help incident handlers to generate efficient reports on detected incidents during incident response process?
A. Malstrom
B. threat_note
C. IntelMQ
D. MagicTree
Answer: C (LEAVE A REPLY)

NEW QUESTION: 5
Chloe, a SOC analyst with Jake Tech, is checking Linux systems logs. She is investigating files at /var/log/ wtmp.
What Chloe is looking at?
A. Error log
B. System boot log
C. General message and system-related stuff

D. Login records

Answer: (SHOW ANSWER)

The /var/log/wtmp file in Linux systems is used to record all logins and logouts. The wtmp file is a binary file that can be read with tools like last, which can display the login history of all users or a specific user, as well as the times of system reboots and shutdowns. SOC analysts, like Chloe, would inspect this file to track user activities and investigate potential unauthorized access or other security incidents.

References: The EC-Council's Certified SOC Analyst (CSA) course provides extensive training and knowledge on SOC operations, including log management and correlation. The CSA certification emphasizes the importance of understanding various log files and their purposes within a Linux system as part of the SOC analyst's role12. For more detailed information, the EC-Council's official CSA study guides and resources should be consulted.

NEW QUESTION: 6

What does the Security Log Event ID 4624 of Windows 10 indicate?

A. A share was assessed

B. Service added to the endpoint

C. An account was successfully logged on

D. New process executed

Answer: (SHOW ANSWER)

NEW QUESTION: 7

An attacker, in an attempt to exploit the vulnerability in the dynamically generated welcome page, inserted code at the end of the company's URL as follows:

http://technosoft.com.com/<script>alert("WARNING: The application has encountered an error");</script>.

Identify the attack demonstrated in the above scenario.

A. Cross-site Scripting Attack

B. SQL Injection Attack

C. Denial-of-Service Attack

D. Session Attack

Answer: (SHOW ANSWER)

The attack demonstrated in the scenario is a Cross-site Scripting (XSS) attack. This is evident from the attacker's action of inserting a <script> tag into the URL, which is a common technique used in XSS attacks to execute malicious scripts in the context of the victim's browser. The script in the URL is designed to display an alert box with a warning message, which is a typical behavior of XSS to show that the attacker can execute JavaScript in the user's browser session.

References The answer can be verified through EC-Council's Certified SOC Analyst (CSA) course materials and study guides, which cover various types of cyber attacks, including XSS, and their characteristics.

NEW QUESTION: 8
Identify the password cracking attempt involving a precomputed dictionary of plaintext passwords and their corresponding hash values to crack the password.
A. Dictionary Attack
B. Rainbow Table Attack
C. Bruteforce Attack
D. Syllable Attack
Answer: B (LEAVE A REPLY)
A Rainbow Table Attack involves using a precomputed table of hash values for every possible combination of characters for a given password policy. This table, known as a rainbow table, is then used to look up the corresponding plaintext password for a given hash value. The process involves the following steps:
* Precomputation: Generate the rainbow table by computing hash values for all possible password combinations according to the password policy.
* Storage: Store these precomputed hash values in a table, associating each with its plaintext password.
* Lookup: When a hash value is obtained during a password cracking attempt, search the rainbow table for the corresponding plaintext password.
* Match: If a match is found, the plaintext password associated with the hash value is the cracked password.
Rainbow tables are effective because they trade storage space for time, allowing for quicker password cracking compared to brute-force or dictionary attacks, which compute hash values on the fly.
References: The EC-Council's materials on password cracking techniques discuss various methods including dictionary attacks, brute-force attacks, and rainbow table attacks. Specifically, the EC-Council Learning Paths and Skill Packs provide detailed insights into these techniques, emphasizing the use of rainbow tables as a method of cracking passwords by comparing precomputed hash values to those obtained from a system12. Additionally, EC-Council's CyberQ platform offers practical exercises related to password cracking, including the use of rainbow tables2.

NEW QUESTION: 9
Rinni, SOC analyst, while monitoring IDS logs detected events shown in the figure below.
What does this event log indicate?
A. Parameter Tampering Attack
B. SQL Injection Attack
C. XSS Attack
D. Directory Traversal Attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 10

Which attack works like a dictionary attack, but adds some numbers and symbols to the words from the dictionary and tries to crack the password?
A. Birthday Attack
B. Rainbow Table Attack
C. Bruteforce Attack
D. Hybrid Attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 11
Which of the following is a report writing tool that will help incident handlers to generate efficient reports on detected incidents during incident response process?
A. threat_note
B. MagicTree
C. IntelMQ
D. Malstrom
Answer: B (LEAVE A REPLY)
MagicTree is a data management tool designed for penetration testers, incident handlers, and IT security professionals. It is particularly useful for handling the voluminous data typically generated during a security assessment or incident response process. MagicTree allows users to import and aggregate data from various sources, organize it in a structured manner, and generate comprehensive reports. This tool helps in consolidating and making sense of the data, which is crucial for efficient incident handling and reporting.
References: The EC-Council's Certified SOC Analyst (C|SA) program covers various tools and techniques required for effective SOC operations, including report writing and incident handling. While the program's official curriculum does not specifically list MagicTree, it is a well-known tool in the cybersecurity community for such purposes. For more information on SOC Analyst tools and practices, you can refer to the EC-Council's official Certified SOC Analyst Training and resources on Top SIEM Tools for SOC Analysts.
These resources provide insights into the tools and software that are essential for SOC analysts, which would include report writing tools like MagicTree.

NEW QUESTION: 12
Which one of the following is the correct flow for Setting Up a Computer Forensics Lab?
A. Planning and budgeting -> Physical location and structural design considerations -> Work area considerations -> Human resource considerations -> Physical security recommendations -> Forensics lab licensing
B. Planning and budgeting -> Physical location and structural design considerations-> Forensics lab licensing -> Human resource considerations -> Work area considerations -> Physical security recommendations

C. Planning and budgeting -> Forensics lab licensing -> Physical location and structural design considerations -> Work area considerations -> Physical security recommendations -> Human resource considerations
D. Planning and budgeting -> Physical location and structural design considerations -> Forensics lab licensing ->Work area considerations -> Human resource considerations -> Physical security recommendations
Answer: A (LEAVE A REPLY)
The process of setting up a Computer Forensics Lab involves several key steps that must be followed in a logical sequence to ensure the lab is functional, secure, and compliant with legal standards. Here's a breakdown of each step:
* Planning and Budgeting: This initial phase involves defining the scope of the lab, the services it will provide, and the resources required. A detailed budget must be prepared, accounting for all potential costs including equipment, software, personnel, training, and maintenance.
* Physical Location and Structural Design Considerations: Selecting a suitable location is critical. The space must accommodate the necessary equipment and personnel, and also allow for secure evidence storage. The design should facilitate workflow efficiency and include considerations for electrical needs, ventilation, and network infrastructure.
* Work Area Considerations: The layout of the work area should promote a secure and efficient environment for forensic analysis. This includes setting up workstations, secure evidence storage, and areas for examination and documentation.
* Human Resource Considerations: Qualified personnel are essential for the operation of a forensics lab.
This involves hiring experienced forensic analysts, providing ongoing training, and ensuring that staff understand the legal implications of their work.
* Physical Security Recommendations: Security measures must be implemented to protect sensitive data and preserve the integrity of evidence. This includes controlled access to the lab, surveillance systems, and secure storage for evidence.
* Forensics Lab Licensing: Depending on the jurisdiction, a forensics lab may require licensing to operate legally. This step ensures that the lab meets all regulatory requirements and standards for forensic analysis.
References: The verified answer is based on the standard practices and guidelines for setting up a Computer Forensics Lab as outlined in EC-Council's SOC Analyst resources and study guides12.
Please note that while I strive to provide accurate information, it's always best to consult the latest EC-Council SOC Analyst documents and learning resources for the most current and detailed guidance.

NEW QUESTION: 13
John as a SOC analyst is worried about the amount of Tor traffic hitting the network. He wants to prepare a dashboard in the SIEM to get a graph to identify the locations from where the TOR traffic is coming.

Which of the following data source will he use to prepare the dashboard?

A. DNS/ Web Server logs with IP addresses.

B. IIS/Web Server logs with IP addresses and user agent IPtouseragent resolution.

C. DHCP/Logs capable of maintaining IP addresses or hostnames with IPtoName resolution.

D. Apache/ Web Server logs with IP addresses and Host Name.

Answer: (SHOW ANSWER)

NEW QUESTION: 14

Harley is working as a SOC analyst with Powell Tech. Powell Inc. is using Internet Information Service (IIS) version 7.0 to host their website.

Where will Harley find the web server logs, if he wants to investigate them for any anomalies?

A. %SystemDrive%\LogFiles\logs\W3SVCN

B. SystemDrive%\inetpub\logs\LogFiles\W3SVCN

C. SystemDrive%\ inetpub\LogFiles\logs\W3SVCN

D. SystemDrive%\LogFiles\inetpub\logs\W3SVCN

Answer: (SHOW ANSWER)

NEW QUESTION: 15

Which of the following service provides phishing protection and content filtering to manage the Internet experience on and off your network with the acceptable use or compliance policies?

A. Malstrom

B. Apility.io

C. OpenDNS

D. I-Blocklist

Answer: C (LEAVE A REPLY)

NEW QUESTION: 16

Which of the following attack can be eradicated by disabling of "allow_url_fopen and allow_url_include" in the php.ini file?

A. File Injection Attacks

B. URL Injection Attacks

C. LDAP Injection Attacks

D. Command Injection Attacks

Answer: A (LEAVE A REPLY)

Disabling the allow_url_fopen and allow_url_include directives in the php.ini configuration file is a recommended security measure to mitigate the risk of File Injection Attacks in PHP applications. These settings, when enabled, allow PHP scripts to open and include files from remote locations through URL references. This capability can be exploited in File Injection Attacks, where attackers inject malicious files into the application by manipulating inputs to reference external resources. By disabling these directives, you limit PHP's ability to open or include files only to local resources, thus significantly reducing the risk associated with remote file inclusion vulnerabilities.

This specific countermeasure is effective against File Injection Attacks but does not directly impact other types of injection attacks such as URL, LDAP, or Command Injection.
References:
* "PHP: Runtime Configuration," PHP Manual.
* "Preventing Web Attacks with Apache," by Ryan C. Barnett, which discusses various web application vulnerabilities and mitigation strategies.

NEW QUESTION: 17
David is a SOC analyst in Karen Tech. One day an attack is initiated by the intruders but David was not able to find any suspicious events.
This type of incident is categorized into?
A. True Positive Incidents
B. False positive Incidents
C. True Negative Incidents
D. False Negative Incidents
Answer: (SHOW ANSWER)

NEW QUESTION: 18
An attacker exploits the logic validation mechanisms of an e-commerce website. He successfully purchases a product worth $100 for $10 by modifying the URL exchanged between the client and the server.
Original
URL: http://www.buyonline.com/product.aspx?profile=12
&debit=100
Modified URL: http://www.buyonline.com/product.aspx?profile=12
&debit=10
Identify the attack depicted in the above scenario.
A. SQL Injection Attack
B. Denial-of-Service Attack
C. Parameter Tampering Attack
D. Session Fixation Attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 19
Which of the following command is used to view iptables logs on Ubuntu and Debian distributions?
A. $ tailf /var/log/kern.log
B. $ tailf /var/log/sys/kern.log
C. # tailf /var/log/sys/messages
D. # tailf /var/log/messages
Answer: A (LEAVE A REPLY)

NEW QUESTION: 20
Jony, a security analyst, while monitoring IIS logs, identified events shown in the figure below.
What does this event log indicate?
A. Parameter Tampering Attack
B. XSS Attack
C. Directory Traversal Attack
D. SQL Injection Attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 21
What does the HTTP status codes 1XX represents?
A. Client error
B. Success
C. Informational message
D. Redirection
Answer: C (LEAVE A REPLY)

NEW QUESTION: 22
Which of the following is a Threat Intelligence Platform?
A. SolarWinds MS
B. TC Complete
C. Keepnote
D. Apility.io
Answer: B (LEAVE A REPLY)
ThreatConnect Complete (TC Complete) is a Threat Intelligence Platform (TIP) designed to aggregate, analyze, and disseminate threat intelligence data. TIPs like TC Complete enable organizations to understand and act upon threats by providing a comprehensive view of the threat landscape, integrating with other security tools, and facilitating collaboration among security teams. Unlike general management systems like SolarWinds MS, note-taking applications like Keepnote, or threat intelligence APIs like Apility.io, TC Complete is specifically built to handle the lifecycle of threat intelligence, from collection and analysis to sharing and applying intelligence.

This makes it a pivotal tool for organizations looking to enhance their security posture through informed decision-making based on timely and relevant threat intelligence.
References:
* "Threat Intelligence Platforms: Open Source and Commercial Options", by SANS Institute.
* "ThreatConnect Platform Overview", ThreatConnect Official Website.

NEW QUESTION: 23
John, SOC analyst wants to monitor the attempt of process creation activities from any of their Windows endpoints.
Which of following Splunk query will help him to fetch related logs associated with process creation?
A. index=windows LogName=Security EventCode=4678 NOT (Account_Name=*$) .. ..
B. index=windows LogName=Security EventCode=4688 NOT (Account_Name=*$) .. .. ..
C. index=windows LogName=Security EventCode=5688 NOT (Account_Name=*$) ... ...
D. index=windows LogName=Security EventCode=3688 NOT (Account_Name=*$) .. .. ..
Answer: B (LEAVE A REPLY)

NEW QUESTION: 24
Which of the following technique involves scanning the headers of IP packets leaving a network to make sure that the unauthorized or malicious traffic never leaves the internal network?
A. Egress Filtering
B. Throttling
C. Rate Limiting
D. Ingress Filtering
Answer: A (LEAVE A REPLY)
Egress filtering is a network security measure that involves scanning the headers of IP packets as they leave a network. The purpose of this technique is to ensure that unauthorized or malicious traffic does not exit the internal network. This is achieved by implementing rules that define which types of traffic are allowed to leave the network. By filtering outgoing traffic, egress filtering helps prevent data exfiltration and blocks the communication of malware with external command-and-control servers.
References: The EC-Council's Certified SOC Analyst (CSA) program covers the fundamentals of SOC operations, including the importance of egress filtering in protecting a network's perimeter. The CSA training and credentialing program provides in-depth knowledge on various SOC processes, such as log management, SIEM deployment, incident detection, and response, which includes the implementation of egress filtering as a security control12.

NEW QUESTION: 25
Identify the attack, where an attacker tries to discover all the possible information about a target network before launching a further attack.
A. DoS Attack

B. Man-In-Middle Attack
C. Ransomware Attack
D. Reconnaissance Attack
Answer: D (LEAVE A REPLY)
A Reconnaissance Attack is a type of cyber attack where the attacker engages in activities to gather information about a target network before launching further attacks. This preliminary phase involves collecting data that could include network infrastructure details, system vulnerabilities, and other critical information that could be exploited in subsequent stages of an attack. Reconnaissance can be both passive, involving information gathering without directly interacting with the target system, or active, which may include more direct methods like port scanning. References:The concept of Reconnaissance Attacks is detailed in EC-Council's cybersecurity resources, such as the Certified Threat Intelligence Analyst (C|TIA) program and articles on the Cyber Kill Chain, which describe reconnaissance as the first stage in a cyber attack12. These resources outline the methodologies and types of information gathered during reconnaissance, emphasizing its role in identifying potential attack vectors12.

NEW QUESTION: 26
Which of the following threat intelligence helps cyber security professionals such as security operations managers, network operations center and incident responders to understand how the adversaries are expected to perform the attack on the organization, and the technical capabilities and goals of the attackers along with the attack vectors?
A. Strategic Threat Intelligence
B. Analytical Threat Intelligence
C. Tactical Threat Intelligence
D. Operational Threat Intelligence
Answer: C (LEAVE A REPLY)

NEW QUESTION: 27
Which encoding replaces unusual ASCII characters with "%" followed by the character's two-digit ASCII code expressed in hexadecimal?
A. Unicode Encoding
B. UTF Encoding
C. Base64 Encoding
D. URL Encoding
Answer: D (LEAVE A REPLY)
URL encoding, also known as percent-encoding, is a mechanism for encoding information in a Uniform Resource Identifier (URI) under certain circumstances. When characters are not allowed in a URI, they are replaced with a percent sign (%) followed by two hexadecimal digits that represent the ASCII code of the character. For example, a space character is not allowed in a URI and is replaced with %20.

References:The answer is verified as per the EC-Council's Certified SOC Analyst (CSA) course materials and study guides, which discuss various encoding schemes used in cybersecurity practices. URL encoding is specifically mentioned as the method for replacing unusual ASCII characters with a percent sign followed by two hexadecimal digits123.

NEW QUESTION: 28
Identify the event severity level in Windows logs for the events that are not necessarily significant, but may indicate a possible future problem.
A. Failure Audit
B. Warning
C. Error
D. Information
Answer: B (LEAVE A REPLY)
In the context of Windows logs, the event severity level that indicates events that are not necessarily significant but may point to a possible future problem is classified as a "Warning." This level is used to log events that are not immediately harmful, such as an impending disk space shortage or other conditions that could potentially cause problems if not addressed.
References: The EC-Council's Certified SOC Analyst (CSA) program covers the fundamentals of SOC operations, including log management and correlation, which would encompass understanding the severity levels of events in Windows logs1. Additionally, the discussion on the ExamTopics website corroborates that the answer to this question is "Warning"2. Further general information on Windows event logging can be found in resources like Sumo Logic's guide to Windows Event Logging3 and other incident response guides that discuss the importance of monitoring event severity levels within a SOC4.

NEW QUESTION: 29
According to the forensics investigation process, what is the next step carried out right after collecting the evidence?
A. Create a Chain of Custody Document
B. Send it to the nearby police station
C. Set a Forensic lab
D. Call Organizational Disciplinary Team
Answer: A (LEAVE A REPLY)
After collecting the evidence in a forensic investigation, the next critical step is to create a Chain of Custody Document. This document is essential as it records the evidence's chronological history, detailing every person who handled the evidence, the date/time it was collected, transferred, analyzed, or otherwise processed.
This ensures the integrity and security of the evidence, maintaining its admissibility in legal proceedings.
References:
* EC-Council's Computer Forensics Investigation Process1

* EC-Council iLabs Computer Forensics Investigation Process2
* InfraExam 2024, Certified SOC Analyst Part 013
* Digital forensics best practices from various sources4
* Free EC-Council CSA Sample Questions and Study Guide | EDUSUM5

NEW QUESTION: 30
Which of the following is a set of standard guidelines for ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection?
A. HIPAA
B. PCI-DSS
C. DARPA
D. FISMA
Answer: B (LEAVE A REPLY)

NEW QUESTION: 31
David is a SOC analyst in Karen Tech. One day an attack is initiated by the intruders but David was not able to find any suspicious events.
This type of incident is categorized into?
A. True Negative Incidents
B. False positive Incidents
C. False Negative Incidents
D. True Positive Incidents
Answer: A (LEAVE A REPLY)

NEW QUESTION: 32
Which of the following formula is used to calculate the EPS of the organization?
A. EPS = number of correlated events / time in seconds
B. EPS = number of security events / time in seconds
C. EPS = number of normalized events / time in seconds
D. EPS = average number of correlated events / time in seconds
Answer: (SHOW ANSWER)

NEW QUESTION: 33
Which of the following tool is used to recover from web application incident?
A. CrowdStrike FalconTM Orchestrator
B. Symantec Secure Web Gateway
C. Smoothwall SWG
D. Proxy Workbench
Answer: A (LEAVE A REPLY)

NEW QUESTION: 34
What is the process of monitoring and capturing all data packets passing through a given network using different tools?
A. Port Scanning
B. DNS Footprinting
C. Network Sniffing
D. Network Scanning
Answer: (SHOW ANSWER)

NEW QUESTION: 35
Jony, a security analyst, while monitoring IIS logs, identified events shown in the figure below.
What does this event log indicate?
A. Parameter Tampering Attack
B. Directory Traversal Attack
C. XSS Attack
D. SQL Injection Attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 36
Which of the following framework describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering?
A. COBIT
B. SSE-CMM
C. SOC-CMM
D. ITIL
Answer: (SHOW ANSWER)

NEW QUESTION: 37
Which encoding replaces unusual ASCII characters with "%" followed by the character's two-digit ASCII code expressed in hexadecimal?
A. Unicode Encoding
B. Base64 Encoding
C. URL Encoding

D. UTF Encoding
Answer: C (LEAVE A REPLY)

NEW QUESTION: 38
Which of the following data source can be used to detect the traffic associated with Bad Bot User-Agents?
A. Router Logs
B. Switch Logs
C. Web Server Logs
D. Windows Event Log
Answer: C (LEAVE A REPLY)

NEW QUESTION: 39
What does [-n] in the following checkpoint firewall log syntax represents?
fw log [-f [-t]] [-n] [-l] [-o] [-c action] [-h host] [-s starttime] [-e endtime] [-b starttime endtime] [-u unification_scheme_file] [-m unification_mode(initial|semi|raw)] [-a] [-k (alert name|all)] [-g] [logfile]
A. Speed up the process by not performing IP addresses DNS resolution in the Log files
B. Display both the date and the time for each log record
C. Display account log records only
D. Display detailed log chains (all the log segments a log record consists of)
Answer: A (LEAVE A REPLY)
The [-n] option in the Checkpoint firewall log syntax is used to speed up the process by not performing DNS resolution of the IP addresses in the log files. When this option is used, the log file will display IP addresses instead of resolving them to hostnames, which can significantly reduce the time taken to process the logs, especially when dealing with large volumes of data. References: This information is consistent with the Check Point Software documentation, which details the use of the fw log command and its various options for managing and viewing firewall logs1. Understanding these options is crucial for a SOC Analyst, as it allows for more efficient monitoring and analysis of network traffic and potential security events.

NEW QUESTION: 40
Which of the following formula represents the risk?
A. Risk = Likelihood * Consequence * Severity
B. Risk = Likelihood * Impact * Severity
C. Risk = Likelihood * Severity * Asset Value
D. Risk = Likelihood * Impact * Asset Value
Answer: (SHOW ANSWER)

NEW QUESTION: 41
What does [-n] in the following checkpoint firewall log syntax represents?

fw log [-f [-t]] [-n] [-l] [-o] [-c action] [-h host] [-s starttime] [-e endtime] [-b starttime endtime] [-u unification_scheme_file] [-m unification_mode(initial|semi|raw)] [-a] [-k (alert name|all)] [-g] [logfile]
A. Display account log records only
B. Display detailed log chains (all the log segments a log record consists of)
C. Display both the date and the time for each log record
D. Speed up the process by not performing IP addresses DNS resolution in the Log files
Answer: D (LEAVE A REPLY)

NEW QUESTION: 42
InfoSystem LLC, a US-based company, is establishing an in-house SOC. John has been given the responsibility to finalize strategy, policies, and procedures for the SOC.
Identify the job role of John.
A. Security Analyst - L1
B. Chief Information Security Officer (CISO)
C. Security Engineer
D. Security Analyst - L2
Answer: B (LEAVE A REPLY)
The role of finalizing strategy, policies, and procedures for a Security Operations Center (SOC) typically falls under the responsibilities of a Chief Information Security Officer (CISO). The CISO is a senior-level executive within an organization who coordinates and manages the overall strategy and defense mechanisms to protect the organization's information and technology assets. This role involves leadership and strategic decision-making, which includes establishing the SOC's framework, defining its policies, and overseeing its procedures.
References: The EC-Council provides various resources and guides that outline the roles and responsibilities within a SOC. According to the information available, a Security Analyst, whether Level 1 or Level 2, is primarily responsible for monitoring and analyzing the organization's security posture on a continuous basis.
A Security Engineer focuses on the design and implementation of security systems. In contrast, the CISO role encompasses a broader scope of strategic leadership and management, which aligns with the responsibilities described for John in the scenario12.

NEW QUESTION: 43
Emmanuel is working as a SOC analyst in a company named Tobey Tech. The manager of Tobey Tech recently recruited an Incident Response Team (IRT) for his company. In the process of collaboration with the IRT, Emmanuel just escalated an incident to the IRT.
What is the first step that the IRT will do to the incident escalated by Emmanuel?
A. Incident Analysis and Validation
B. Incident Prioritization
C. Incident Classification
D. Incident Recording
Answer: C (LEAVE A REPLY)

NEW QUESTION: 44
According to the Risk Matrix table, what will be the risk level when the probability of an attack is very high, and the impact of that attack is major?
NOTE: It is mandatory to answer the question before proceeding to the next one.
A. High
B. Extreme
C. Low
D. Medium
Answer: B (LEAVE A REPLY)
In a Risk Matrix, risk levels are determined by the intersection of the likelihood of an occurrence (probability) and the consequence of that occurrence (impact). When the probability of an event is very high and the impact is major, it typically falls into the 'Extreme' category. This is because the combination of a high likelihood and major impact represents a scenario where the risk is unacceptable and requires immediate attention and mitigation measures.
References: The EC-Council's Certified SOC Analyst (CSA) course materials and study guides provide detailed information on assessing risks using a Risk Matrix. The course emphasizes the importance of understanding the Risk Matrix for effective security operations center (SOC) analysis. For more in-depth information, refer to the official EC-Council CSA study materials and resources12.

NEW QUESTION: 45
Which of the log storage method arranges event logs in the form of a circular buffer?
A. FIFO
B. LIFO
C. non-wrapping
D. wrapping
Answer: D (LEAVE A REPLY)

NEW QUESTION: 46
John as a SOC analyst is worried about the amount of Tor traffic hitting the network. He wants to prepare a dashboard in the SIEM to get a graph to identify the locations from where the TOR traffic is coming.
Which of the following data source will he use to prepare the dashboard?
A. DHCP/Logs capable of maintaining IP addresses or hostnames with IPtoName resolution.
B. IIS/Web Server logs with IP addresses and user agent IPtouseragent resolution.
C. DNS/ Web Server logs with IP addresses.
D. Apache/ Web Server logs with IP addresses and Host Name.
Answer: (SHOW ANSWER)
To monitor and visualize Tor traffic hitting the network, John would need data sources that can provide detailed information about the source IP addresses of incoming traffic, as well as the

capability to resolve these IP addresses to more identifiable information such as hostnames or geographical locations. DHCP logs, or other log sources capable of maintaining detailed IP address records and facilitating IP-to-Name resolution, would be suitable for this purpose. This data would allow John to create a dashboard in the SIEM system that maps the source IP addresses of Tor traffic to their corresponding locations or identities, providing insights into where the Tor traffic is originating. While web server logs (options B, C, and D) can provide IP addresses, they might not offer the same level of detail or resolution capabilities as DHCP logs or similar network-level logs for this specific use case.
References:
* "Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management" by Anton Chuvakin, Kevin Schmidt, and Chris Phillips.
* "Tor: The Second-Generation Onion Router" by Roger Dingledine, Nick Mathewson, and Paul Syverson.

NEW QUESTION: 47
What does Windows event ID 4740 indicate?
A. A user account was created.
B. A user account was enabled.
C. A user account was disabled.
D. A user account was locked out.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 48
Which of the following attack can be eradicated by converting all non-alphanumeric characters to HTML character entities before displaying the user input in search engines and forums?
A. Session Management Attacks
B. Broken Access Control Attacks
C. Web Services Attacks
D. XSS Attacks
Answer: D (LEAVE A REPLY)

NEW QUESTION: 49
Which of the following contains the performance measures, and proper project and time management details?
A. Incident Response Procedures
B. Incident Response Process
C. Incident Response Tactics
D. Incident Response Policy
Answer: A (LEAVE A REPLY)

NEW QUESTION: 50
Charline is working as an L2 SOC Analyst. One day, an L1 SOC Analyst escalated an incident to her for further investigation and confirmation. Charline, after a thorough investigation, confirmed the incident and assigned it with an initial priority.
What would be her next action according to the SOC workflow?
A. She should formally raise a ticket and forward it to the IRT
B. She should immediately contact the network administrator to solve the problem
C. She should communicate this incident to the media immediately
D. She should immediately escalate this issue to the management
Answer: B (LEAVE A REPLY)

NEW QUESTION: 51
Where will you find the reputation IP database, if you want to monitor traffic from known bad IP reputation using OSSIM SIEM?
A. /etc/siem/ossim/server/reputation.data
B. /etc/ossim/siem/server/reputation/data
C. /etc/ossim/reputation
D. /etc/ossim/server/reputation.data
Answer: C (LEAVE A REPLY)

NEW QUESTION: 52
InfoSystem LLC, a US-based company, is establishing an in-house SOC. John has been given the responsibility to finalize strategy, policies, and procedures for the SOC.
Identify the job role of John.
A. Security Analyst - L1
B. Security Engineer
C. Security Analyst - L2
D. Chief Information Security Officer (CISO)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 53
Juliea a SOC analyst, while monitoring logs, noticed large TXT, NULL payloads.

What does this indicate?
A. DNS Exfiltration Attempt
B. DHCP Starvation Attempt
C. Concurrent VPN Connections Attempt
D. Covering Tracks Attempt
Answer: A (LEAVE A REPLY)

NEW QUESTION: 54
Which of the following attack can be eradicated by using a safe API to avoid the use of the interpreter entirely?
A. Command Injection Attacks
B. SQL Injection Attacks
C. File Injection Attacks
D. LDAP Injection Attacks
Answer: (SHOW ANSWER)
Command Injection Attacks involve the insertion of malicious code into a vulnerable application, which then executes unwanted system commands on the server. The fundamental cause of this vulnerability is the application's use of input data in constructing system commands without proper validation or encoding.
Utilizing a safe API that avoids the use of the interpreter entirely can effectively mitigate this risk by ensuring that commands are executed in a controlled manner, without directly passing user input to the system shell.
Safe APIs typically provide predefined functions and methods that perform the required tasks in a secure way, eliminating the need to construct command strings from user inputs, thus protecting against Command Injection Attacks. This approach contrasts with mitigations for other types of injection attacks, like SQL, File, or LDAP injections, which often involve proper input validation, parameterized queries, or specific encoding techniques.
References:
* OWASP: Command Injection.
* Secure Coding in C and C++, Robert C. Seacord, Addison-Wesley Professional.

NEW QUESTION: 55
An organization is implementing and deploying the SIEM with following capabilities.
What kind of SIEM deployment architecture the organization is planning to implement?
A. Self-hosted, Jointly Managed
B. Cloud, MSSP Managed
C. Self-hosted, Self-Managed
D. Self-hosted, MSSP Managed
Answer: B (LEAVE A REPLY)

NEW QUESTION: 56

Mike is an incident handler for PNP Infosystems Inc. One day, there was a ticket raised regarding a critical incident and Mike was assigned to handle the incident. During the process of incident handling, at one stage, he has performed incident analysis and validation to check whether the incident is a true incident or a false positive.
Identify the stage in which he is currently in.
A. Post-Incident Activities
B. Incident Recording and Assignment
C. Incident Triage
D. Incident Disclosure
Answer: C (LEAVE A REPLY)

NEW QUESTION: 57
Harley is working as a SOC analyst with Powell Tech. Powell Inc. is using Internet Information Service (IIS) version 7.0 to host their website.
Where will Harley find the web server logs, if he wants to investigate them for any anomalies?
A. SystemDrive%\inetpub\logs\LogFiles\W3SVCN
B. SystemDrive%\ inetpub\LogFiles\logs\W3SVCN
C. %SystemDrive%\LogFiles\logs\W3SVCN
D. SystemDrive%\LogFiles\inetpub\logs\W3SVCN
Answer: D (LEAVE A REPLY)

NEW QUESTION: 58
Jane, a security analyst, while analyzing IDS logs, detected an event matching Regex /((\%3C)|<)((\%69)|i|(\% 49))((\%6D)|m|(\%4D))((\%67)|g|(\%47))[^\n]+((\%3E)|>)/|.
What does this event log indicate?
A. XSS Attack
B. Directory Traversal Attack
C. Parameter Tampering Attack
D. SQL Injection Attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 59
Which of the following formula is used to calculate the EPS of the organization?
A. EPS = average number of correlated events / time in seconds
B. EPS = number of normalized events / time in seconds
C. EPS = number of security events / time in seconds
D. EPS = number of correlated events / time in seconds
Answer: D (LEAVE A REPLY)
In the context of a Security Operations Center (SOC), EPS typically refers to "Events Per Second," which is a measure of the number of security events processed in one second. The correct formula for calculating EPS in a SOC environment is the number of correlated events

divided by the time in seconds. Correlated events are those that have been analyzed and aggregated by the SOC's security information and event management (SIEM) system, indicating a potential security incident. This metric helps in understanding the operational load and performance of the SOC.
References: The information is aligned with the EC-Council's Certified SOC Analyst (CSA) course material and best practices, which emphasize the importance of understanding and managing SOC operational metrics such as EPS for effective security monitoring and incident response12.

NEW QUESTION: 60
Which of the following can help you eliminate the burden of investigating false positives?
A. Keeping default rules
B. Not trusting the security devices
C. Treating every alert as high level
D. Ingesting the context data
Answer: D (LEAVE A REPLY)

NEW QUESTION: 61
Which of the following contains the performance measures, and proper project and time management details?
A. Incident Response Policy
B. Incident Response Tactics
C. Incident Response Process
D. Incident Response Procedures
Answer: D (LEAVE A REPLY)
The Incident Response Procedures contain the performance measures and proper project and time management details. These procedures are designed to guide the incident response team through each phase of incident management, ensuring that all activities are performed efficiently and effectively. They include specific steps to follow, roles and responsibilities, timelines, and performance metrics to measure the effectiveness of the response.
References: The answer is verified as per the EC-Council's SOC Analyst documents and learning resources, which outline the structure and content of incident response plans and procedures. For further study, refer to the EC-Council's Certified SOC Analyst (CSA) course material and study guides, which provide detailed information on the incident response lifecycle, including preparation, identification, containment, eradication, recovery, and lessons learned. These resources will offer a comprehensive understanding of the procedures involved in managing and responding to security incidents.

NEW QUESTION: 62
Which of the following fields in Windows logs defines the type of event occurred, such as Correlation Hint, Response Time, SQM, WDI Context, and so on?
A. Source
B. Level
C. Keywords
D. Task Category
Answer: C (LEAVE A REPLY)

NEW QUESTION: 63
Shawn is a security manager working at Lee Inc Solution. His organization wants to develop threat intelligent strategy plan. As a part of threat intelligent strategy plan, he suggested various components, such as threat intelligence requirement analysis, intelligence and collection planning, asset identification, threat reports, and intelligence buy-in.
Which one of the following components he should include in the above threat intelligent strategy plan to make it effective?
A. Threat pivoting
B. Threat trending
C. Threat buy-in
D. Threat boosting
Answer: B (LEAVE A REPLY)
In the context of a threat intelligence strategy plan, 'threat trending' is a critical component that should be included to make the plan effective. Threat trending involves analyzing data over time to identify patterns and trends in cyber threats. This allows an organization to anticipate potential future attacks and prepare accordingly. It is an essential part of a proactive threat intelligence program, enabling the organization to stay ahead of threats rather than just reacting to them.
The other options, while they may be relevant in certain contexts, are not as central to the development of a threat intelligence strategy plan as 'threat trending' is. 'Threat pivoting' refers to the process of using one piece of data to uncover more data (e.g., using an IP address to find related domains). 'Threat buy-in' is not a standard term in threat intelligence, but it could refer to gaining organizational support for threat intelligence efforts. 'Threat boosting' is not a recognized term in the field of cybersecurity.
References: The answer is derived from the components of a threat intelligence strategy as outlined in the EC-Council's Certified SOC Analyst (CSA) training and certification program, which emphasizes the importance of understanding and implementing a threat intelligence-driven SOC12. The CSA program also covers the use of threat intelligence for enhanced incident

detection1. The EC-Council materials highlight the need for SOC analysts to understand various types of cyber threats and the importance of threat intelligence in detecting and responding to these threats2.

NEW QUESTION: 64
Identify the type of attack, an attacker is attempting on www.example.com website.
A. SQL Injection Attack
B. Denial-of-Service Attack
C. Session Attack
D. Cross-site Scripting Attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 65
Which of the following tool is used to recover from web application incident?
A. Symantec Secure Web Gateway
B. CrowdStrike FalconTM Orchestrator
C. Smoothwall SWG
D. Proxy Workbench
Answer: A (LEAVE A REPLY)

NEW QUESTION: 66
Which of the following Windows features is used to enable Security Auditing in Windows?
A. Bitlocker
B. Windows Defender
C. Local Group Policy Editor
D. Windows Firewall
Answer: C (LEAVE A REPLY)

NEW QUESTION: 67
Which of the following are the responsibilities of SIEM Agents?
1.Collecting data received from various devices sending data to SIEM before forwarding it to the central engine.
2.Normalizing data received from various devices sending data to SIEM before forwarding it to the central engine.
3.Co-relating data received from various devices sending data to SIEM before forwarding it to the central engine.
4.Visualizing data received from various devices sending data to SIEM before forwarding it to the central engine.
A. 2 and 3
B. 1 and 2
C. 3 and 1

D. 1 and 4
Answer: D (LEAVE A REPLY)

NEW QUESTION: 68
Which of the following formula represents the risk levels?
A. Level of risk = Consequence × Severity
B. Level of risk = Consequence × Impact
C. Level of risk = Consequence × Likelihood
D. Level of risk = Consequence × Asset Value
Answer: C (LEAVE A REPLY)
The level of risk is typically calculated by considering the consequence (or impact) of an event and the likelihood (or probability) of its occurrence. The formula represents a fundamental risk assessment concept where risk is the product of the two factors:
* Consequence (Impact): The outcome or result if a threat does exploit a vulnerability.
* Likelihood (Probability): The chance that a given threat will exploit a vulnerability.
By multiplying these two factors, one can determine the level of risk, which helps in prioritizing risks and deciding on the appropriate level of controls and mitigation strategies.
References: The EC-Council's Certified SOC Analyst (CSA) course materials and study guides cover the concepts of risk assessment and management, which include the formula for calculating risk levels as the product of consequence and likelihood. These concepts are aligned with industry best practices and standards for security operations centers.

NEW QUESTION: 69
Identify the type of attack, an attacker is attempting on www.example.com website.
A. SQL Injection Attack
B. Cross-site Scripting Attack
C. Denial-of-Service Attack
D. Session Attack
Answer: (SHOW ANSWER)

NEW QUESTION: 70
Which of the following formula represents the risk?
A. Risk = Likelihood × Severity × Asset Value
B. Risk = Likelihood × Consequence × Severity
C. Risk = Likelihood × Impact × Severity
D. Risk = Likelihood × Impact × Asset Value
Answer: (SHOW ANSWER)
Risk is typically calculated as the product of likelihood, impact, and asset value. Likelihood represents the probability of a threat exploiting a vulnerability, impact refers to the potential damage or loss that could result from the threat, and asset value quantifies the importance or worth of the asset to the organization. The formula (\text{Risk} = \text{Likelihood} \times

\text{Impact} \times \text{Asset Value}) captures the essence of risk in terms of these three factors.
References: The EC-Council's Certified SOC Analyst (CSA) program includes training on risk assessment and management, which involves understanding how to calculate and manage risk based on various factors including likelihood, impact, and asset value. The CSA curriculum is designed to align with industry best practices and standards for security operations centers12.

NEW QUESTION: 71
Robin, a SOC engineer in a multinational company, is planning to implement a SIEM. He realized that his organization is capable of performing only Correlation, Analytics, Reporting, Retention, Alerting, and Visualization required for the SIEM implementation and has to take collection and aggregation services from a Managed Security Services Provider (MSSP).
What kind of SIEM is Robin planning to implement?
A. Self-hosted, Self-Managed
B. Self-hosted, MSSP Managed
C. Hybrid Model, Jointly Managed
D. Cloud, Self-Managed
Answer: D (LEAVE A REPLY)

NEW QUESTION: 72
If the SIEM generates the following four alerts at the same time:
I.Firewall blocking traffic from getting into the network alerts
II.SQL injection attempt alerts
III.Data deletion attempt alerts
IV.Brute-force attempt alerts
Which alert should be given least priority as per effective alert triaging?
A. III
B. II
C. IV
D. I
Answer: D (LEAVE A REPLY)

NEW QUESTION: 73
Which of the following factors determine the choice of SIEM architecture?
A. SMTP Configuration
B. DHCP Configuration
C. DNS Configuration
D. Network Topology
Answer: D (LEAVE A REPLY)
The choice of SIEM architecture is influenced by several factors that impact how the SIEM system will collect, manage, and analyze data. Among the options provided, Network Topology is

the most relevant factor. It determines the layout of the network, including the arrangement of nodes and the connections between them, which directly affects how the SIEM system will be integrated into the environment. A well-designed network topology ensures that the SIEM system can efficiently collect and correlate data from across the network.
SMTP Configuration, DHCP Configuration, and DNS Configuration are related to specific services and protocols that may be monitored by a SIEM, but they do not determine the choice of SIEM architecture itself.
References: For further understanding, you can refer to the EC-Council's Certified SOC Analyst course material and study guides, which provide detailed insights into SIEM architectures and the factors influencing their selection. Additionally, resources like Exabeam's "SIEM Architecture: Technology, Process and Data" offer a comprehensive overview of SIEM systems and their components1.

NEW QUESTION: 74
In which of the following incident handling and response stages, the root cause of the incident must be found from the forensic results?
A. Evidence Gathering
B. Evidence Handling
C. Eradication
D. Systems Recovery
Answer: C (LEAVE A REPLY)
The eradication stage is where the root cause of the incident is determined from the forensic results. This stage involves not only removing the threat from the affected systems but also identifying and fixing the vulnerabilities that were exploited. It's crucial to understand how the incident occurred to prevent future occurrences. After the containment stage, where the immediate threat is isolated, eradication ensures that the threat is completely removed and that the root cause is addressed.
References: The EC-Council's Certified Incident Handler (E|CIH) program outlines the stages of incident handling and response, which include preparation, identification, containment, eradication, recovery, and lessons learned. The eradication stage specifically deals with eliminating the threat and addressing the root cause based on forensic analysis. This information is covered in the E|CIH program and can be found in the official EC-Council learning resources1.

NEW QUESTION: 75
According to the Risk Matrix table, what will be the risk level when the probability of an attack is very low and the impact of that attack is major?
A. High
B. Extreme
C. Low
D. Medium
Answer: (SHOW ANSWER)

Explanation
Graphical user interface, application, Teams Description automatically generated

NEW QUESTION: 76
John, a SOC analyst, while monitoring and analyzing Apache web server logs, identified an event log matching Regex /(\.|(%|%25)2E)(\.|(%|%25)2E)(\/|(%|%25)2F|\\|(%|%25)5C)/i.
What does this event log indicate?
A. Parameter Tampering Attack
B. SQL injection Attack
C. XSS Attack
D. Directory Traversal Attack
Answer: (SHOW ANSWER)

NEW QUESTION: 77
According to the Risk Matrix table, what will be the risk level when the probability of an attack is very high, and the impact of that attack is major?
NOTE: It is mandatory to answer the question before proceeding to the next one.
A. Low
B. High
C. Medium
D. Extreme
Answer: (SHOW ANSWER)

NEW QUESTION: 78
Mike is an incident handler for PNP Infosystems Inc. One day, there was a ticket raised regarding a critical incident and Mike was assigned to handle the incident. During the process of incident handling, at one stage, he has performed incident analysis and validation to check whether the incident is a true incident or a false positive.
Identify the stage in which he is currently in.
A. Incident Recording and Assignment
B. Incident Disclosure
C. Incident Triage

D. Post-Incident Activities
Answer: (SHOW ANSWER)

NEW QUESTION: 79
Which of the following contains the performance measures, and proper project and time management details?
A. Incident Response Policy
B. Incident Response Tactics
C. Incident Response Process
D. Incident Response Procedures
Answer: A (LEAVE A REPLY)

NEW QUESTION: 80
Sam, a security analyst with INFOSOL INC., while monitoring and analyzing IIS logs, detected an event matching regex /\\w*((\%27)|(\'))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix.
What does this event log indicate?
A. SQL Injection Attack
B. XSS Attack
C. Parameter Tampering Attack
D. Directory Traversal Attack
Answer: (SHOW ANSWER)