EC-COUNCIL.312-39.v2024-11-29.q83

Exam Code:	312-39
Exam Name:	Certified SOC Analyst (CSA)
Certification Provider:	EC-COUNCIL
Free Question Number:	83
Version:	v2024-11-29
# of views:	756
# of Questions views:	830
https://www.freepdfdumps.com/EC-COUNCIL.312-39.v2024-11-29.q83.html	

NEW QUESTION: 1
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: D (LEAVE A REPLY)
A false negative incident in the context of a Security Operations Center (SOC) is when an actual attack or intrusion occurs, but the SOC analyst fails to detect any suspicious events or indicators of compromise. This means that the security measures in place did not work as intended, and the attack went unnoticed.
In David's case, since an attack was initiated and he was not able to find any suspicious events, it is categorized as a false negative incident. This is a critical type of incident because it indicates a failure in the detection capabilities of the SOC, potentially allowing the intruder to cause harm without being detected.
References: The categorization of incidents is a fundamental part of the SOC Analyst's role, as outlined in the EC-Council's Certified SOC Analyst (CSA) training and certification program. The program covers the different types of incidents that can be encountered in a SOC, including true positives, false positives, true negatives, and false negatives, and how to identify and respond to each12345.

False negative: False negatives are the false result for an activity that actually occurred. It is an attack-negative reply for an actual attack. The false negative is the type of alert which will not raise the alarm even if an attack is taking place on the network. By not defining the rules properly, these kinds of errors in the alerting system will occur. By false positives, actual is not identified, which may lead to cybersecurity breach over the organization. For example, an attacker tried to gain access to an unauthorized network and succeeded by attempting nine times. If the rule in the SIEM is made in such a way that 10 login attempts have to be identified as an alert, then the attempts of the attacker may not be noticed. In this way, false positives can be dangerous for an organization if they are not rectified.

NEW QUESTION: 2

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. Directory Traversal Attack

D. XSS Attack

Answer: (SHOW ANSWER)

NEW QUESTION: 3

Identify the event severity level in Windows logs for the events that are not necessarily significant, but may indicate a possible future problem.

A. Information

B. Warning

C. Failure Audit

D. Error

Answer: B (LEAVE A REPLY)

NEW QUESTION: 4

Which of the following process refers to the discarding of the packets at the routing level without informing the source that the data did not reach its intended recipient?

A. Load Balancing

B. Rate Limiting

C. Black Hole Filtering

D. Drop Requests

Answer: C (LEAVE A REPLY)

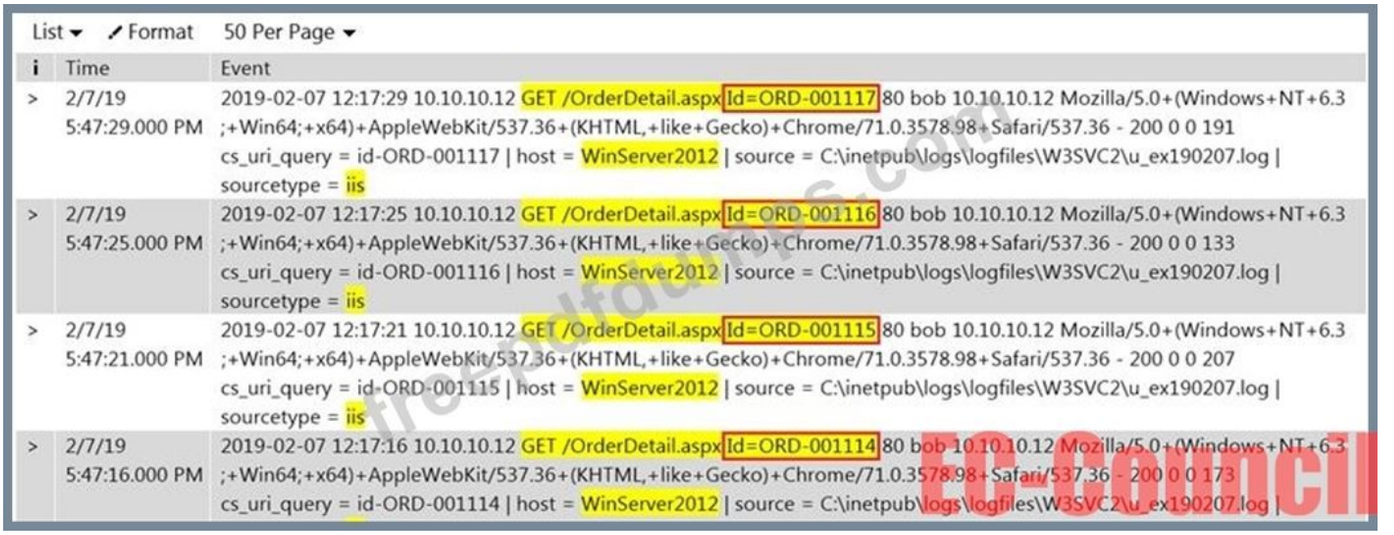
Black hole filtering is a network security measure used to prevent unwanted or malicious traffic from entering a network. It works by directing traffic to a null interface, a non-existent server, or a black hole IP address where the packets are dropped without acknowledgment. This process is typically used to protect against denial-of-service (DoS) attacks, where an overwhelming amount of traffic is sent to a network with the intent to disrupt service.

In the context of a security operations center (SOC), black hole filtering can be an effective strategy for mitigating threats. When a threat is identified, such as a DoS attack, the SOC analyst can configure the network to redirect the suspicious traffic to a black hole, effectively neutralizing the attack by preventing the malicious data packets from reaching their intended target.

References: The EC-Council's Certified SOC Analyst (C|SA) program covers various defensive strategies, including black hole filtering, as part of its curriculum for Tier I and Tier II SOC analysts. The program emphasizes the importance of understanding and implementing network security measures to protect against cyber threats12.

NEW QUESTION: 5

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. XSS Attack

C. Directory Traversal Attack

D. SQL Injection Attack

Answer: (SHOW ANSWER)

NEW QUESTION: 6
According to the forensics investigation process, what is the next step carried out right after collecting the evidence?
A. Set a Forensic lab
B. Send it to the nearby police station
C. Call Organizational Disciplinary Team
D. Create a Chain of Custody Document
Answer: D (LEAVE A REPLY)

NEW QUESTION: 7
Identify the password cracking attempt involving a precomputed dictionary of plaintext passwords and their corresponding hash values to crack the password.
A. Bruteforce Attack
B. Rainbow Table Attack
C. Syllable Attack
D. Dictionary Attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 8
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. Extreme
D. Medium
Answer: (SHOW ANSWER)

NEW QUESTION: 9
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: D (LEAVE A REPLY)
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: 10
An organization wants to implement a SIEM deployment architecture. However, they have the capability to do only log collection and the rest of the SIEM functions must be managed by an MSSP.
Which SIEM deployment architecture will the organization adopt?
A. Self-hosted, Self-Managed
B. Self-hosted, MSSP Managed
C. Self-hosted, Jointly Managed
D. Cloud, MSSP Managed
Answer: B (LEAVE A REPLY)

NEW QUESTION: 11
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. Speed up the process by not performing IP addresses DNS resolution in the Log files
C. Display detailed log chains (all the log segments a log record consists of)
D. Display both the date and the time for each log record
Answer: B (LEAVE A REPLY)

NEW QUESTION: 12
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 Analyst - L2
C. Chief Information Security Officer (CISO)
D. Security Engineer
Answer: C (LEAVE A REPLY)

NEW QUESTION: 13

Which of the following data source will a SOC Analyst use to monitor connections to the insecure ports?

A. Netstat Data

B. IIS Data

C. DNS Data

D. DHCP Data

Answer: A (LEAVE A REPLY)

NEW QUESTION: 14

Which of the following tool can be used to filter web requests associated with the SQL Injection attack?

A. Nmap

B. UrlScan

C. ZAP proxy

D. Hydra

Answer: (SHOW ANSWER)

UrlScan is a security tool that screens all incoming requests to a server and filters these requests based on rules set by the administrator. It is particularly effective against SQL Injection attacks because it can block requests that appear to be malicious, such as those containing SQL syntax or certain keywords often used in SQL Injection.

Nmap is a network scanning tool, not specifically designed for filtering web requests. ZAP Proxy is an open-source web application security scanner, which is used for finding vulnerabilities in web applications but not specifically for filtering requests. Hydra is a password cracking tool, which again, is not used for filtering web requests.

References: The answer is verified as per the EC-Council's SOC Analyst course materials and learning resources, which include training on various security tools and their purposes. Specifically, the EC-Council's SQL Injection Training and other related courses provide insights into the tools and techniques for defending against SQL Injection attacks123.

NEW QUESTION: 15

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 Triage

B. Incident Recording and Assignment

C. Incident Disclosure

D. Post-Incident Activities

Answer: B (LEAVE A REPLY)

NEW QUESTION: 16
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. Analytical Threat Intelligence
B. Tactical Threat Intelligence
C. Strategic Threat Intelligence
D. Operational Threat Intelligence
Answer: B (LEAVE A REPLY)

NEW QUESTION: 17
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. Keywords
B. Task Category
C. Level
D. Source
Answer: (SHOW ANSWER)
The Task Category in Windows logs is used to define the type of event that has occurred. It is a subcategory within the event itself that provides additional context about the event, such as whether it is a Correlation Hint, Response Time, SQM, WDI Context, etc. This categorization helps in filtering and identifying events based on their nature and type.
References: The information is verified as per the SOC Analyst documents and learning resources provided by EC-Council, which emphasize the importance of understanding log management and correlation within a SOC environment12. Additionally, the definition and role of the Task Category field in Windows logs are supported by technical documentation and resources that describe the structure and use of Windows event logs34.

NEW QUESTION: 18

Ray is a SOC analyst in a company named Queens Tech. One Day, Queens Tech is affected by a DoS/DDoS attack. For the containment of this incident, Ray and his team are trying to provide additional bandwidth to the network devices and increasing the capacity of the servers.
What is Ray and his team doing?

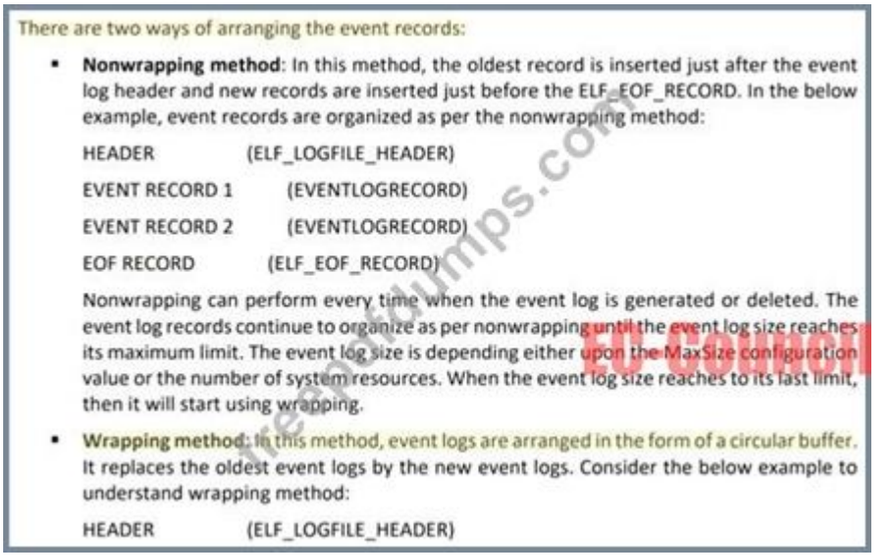
A. Blocking the Attacks
B. Absorbing the Attack
C. Degrading the services
D. Diverting the Traffic
Answer: B (LEAVE A REPLY)

NEW QUESTION: 19
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. Task Category
C. Keywords
D. Level
Answer: (SHOW ANSWER)

NEW QUESTION: 20
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)


There are two ways of arranging the event records:

- **Nonwrapping method**: In this method, the oldest record is inserted just after the event log header and new records are inserted just before the ELF_EOF_RECORD. In the below example, event records are organized as per the nonwrapping method:

  HEADER (ELF_LOGFILE_HEADER)
  EVENT RECORD 1 (EVENTLOGRECORD)
  EVENT RECORD 2 (EVENTLOGRECORD)
  EOF RECORD (ELF_EOF_RECORD)

  Nonwrapping can perform every time when the event log is generated or deleted. The event log records continue to organize as per nonwrapping until the event log size reaches its maximum limit. The event log size is depending either upon the MaxSize configuration value or the number of system resources. When the event log size reaches to its last limit, then it will start using wrapping.

- **Wrapping method**: In this method, event logs are arranged in the form of a circular buffer. It replaces the oldest event logs by the new event logs. Consider the below example to understand wrapping method:

  HEADER (ELF_LOGFILE_HEADER)

NEW QUESTION: 21

Banter is a threat analyst in Christine Group of Industries. As a part of the job, he is currently formatting and structuring the raw data.
He is at which stage of the threat intelligence life cycle?
A. Processing and Exploitation
B. Dissemination and Integration
C. Analysis and Production
D. Collection
Answer: (SHOW ANSWER)

NEW QUESTION: 22
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: D (LEAVE A REPLY)

NEW QUESTION: 23
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)
Ingesting context data can significantly reduce the burden of investigating false positives in a Security Operations Center (SOC). Context data provides additional information that can help differentiate between true threats and benign anomalies. By analyzing context data, such as user behavior, network traffic patterns, and threat intelligence, SOC analysts can apply a more targeted approach to threat detection. This allows for more accurate alerts, reducing the time and resources spent on investigating false positives.
References: The importance of context in threat detection is highlighted in EC-Council's resources, where it is stated that traditional security tools often generate a lot of noise and false positives, making it difficult for SOCs to distinguish real threats from benign events1. Additionally, leveraging threat intelligence and fine-tuning detection rules are recommended strategies for reducing false positives2. These practices are in line with the EC-Council's Certified SOC Analyst (CSA) course and study guides, which emphasize the need for context-aware security measures in modern SOC operations.

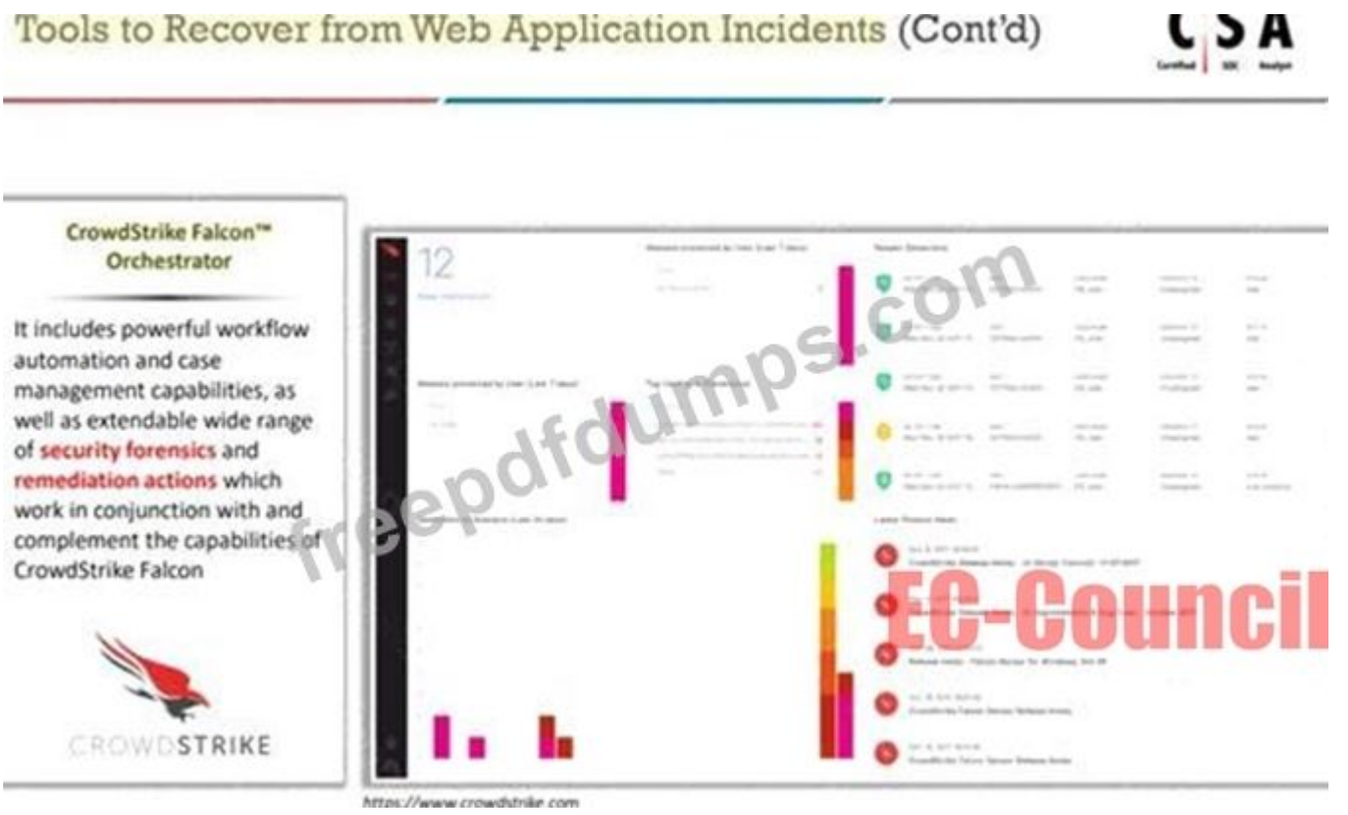
NEW QUESTION: 24
Which attack works like a dictionary attack, but adds some numbers and symbols to the words from the dictionary and tries to crack the password?
A. Birthday Attack
B. Hybrid Attack
C. Rainbow Table Attack
D. Bruteforce Attack
Answer: (SHOW ANSWER)

NEW QUESTION: 25
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: 26
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. 3 and 1
B. 1 and 4
C. 1 and 2
D. 2 and 3
Answer: B (LEAVE A REPLY)

NEW QUESTION: 27
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. Apache/ Web Server logs with IP addresses and Host Name.
C. IIS/Web Server logs with IP addresses and user agent IPtouseragent resolution.
D. DHCP/Logs capable of maintaining IP addresses or hostnames with IPtoName resolution.
Answer: (SHOW ANSWER)

NEW QUESTION: 28
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: 29
In which log collection mechanism, the system or application sends log records either on the local disk or over the network.
A. pull-based
B. rule-based
C. signature-based
D. push-based
Answer: B (LEAVE A REPLY)

NEW QUESTION: 30
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. Rate Limiting
B. Egress Filtering
C. Ingress Filtering
D. Throttling
Answer: (SHOW ANSWER)
Ingress filtering is a technique used to ensure that incoming packets are actually from the networks that they claim to originate from. This is particularly useful in mitigating IP spoofing, where an attacker might use a legitimate IP address to send malicious packets, making it appear as though the packets are coming from a trusted source. By implementing ingress filtering, networks can check that the source IP address of incoming packets is within a range that logically

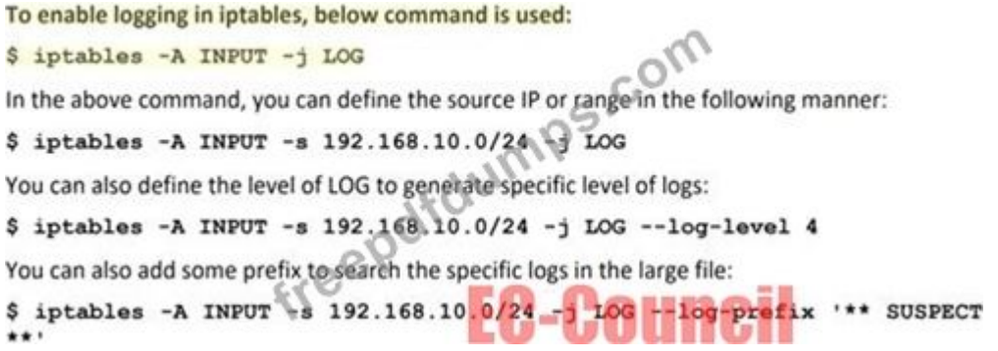
should be entering the network from that point. This helps in tracing back flooding attacks to their true source and is a recommended practice to protect against such attacks.
References: The concept of ingress filtering is covered in EC-Council's Certified SOC Analyst (CSA) training and is a recognized technique for protecting against flooding attacks. It is also mentioned in the context of security operations center (SOC) processes and is a part of the knowledge base required for SOC analysts12.

NEW QUESTION: 31
John, a threat analyst at GreenTech Solutions, wants to gather information about specific threats against the organization. He started collecting information from various sources, such as humans, social media, chat room, and so on, and created a report that contains malicious activity.
Which of the following types of threat intelligence did he use?
A. Strategic Threat Intelligence
B. Operational Threat Intelligence
C. Technical Threat Intelligence
D. Tactical Threat Intelligence
Answer: B (LEAVE A REPLY)

NEW QUESTION: 32
Identify the attack in which the attacker exploits a target system through publicly known but still unpatched vulnerabilities.
A. Slow DoS Attack
B. DHCP Starvation
C. Zero-Day Attack
D. DNS Poisoning Attack
Answer: C (LEAVE A REPLY)
A Zero-Day Attack refers to the exploitation of a publicly known but still unpatched vulnerability. This type of attack occurs when attackers take advantage of a security weakness for which a fix or patch has not yet been released by the vendor. The term "zero-day" refers to the fact that the developers have "zero days" to fix the issue because it has already been exploited in the wild. These attacks are particularly dangerous because they occur before the vulnerability is widely known, giving attackers the opportunity to exploit systems while they are still vulnerable.

References: The EC-Council's Certified SOC Analyst (C|SA) program covers the concept of zero-day vulnerabilities and attacks as part of the training for security operations center analysts. Understanding these attacks is crucial for identifying and responding to incidents that involve unpatched software vulnerabilities. The information is consistent with industry standards and best practices for cybersecurity, as outlined in various EC-Council SOC Analyst study guides and courses1234.

NEW QUESTION: 33
Which of the following command is used to enable logging in iptables?
A. $ iptables -B INPUT -j LOG
B. $ iptables -A OUTPUT -j LOG
C. $ iptables -A INPUT -j LOG
D. $ iptables -B OUTPUT -j LOG
Answer: C (LEAVE A REPLY)
The command to enable logging in iptables for incoming packets is $ iptables -A INPUT -j LOG. This command appends a rule to the INPUT chain that logs the packet information. The -A flag is used to append the rule to the end of the specified chain, which in this case is INPUT, indicating that the rule applies to incoming packets. The -j LOG part of the command specifies the target of the rule, which is LOG, meaning that the packet will be logged.
References:
* EC-Council's Certified SOC Analyst (CSA) training materials and certification guidelines1
* InfraExam 2024, Certified SOC Analyst Part 01, which includes details on iptables commands2

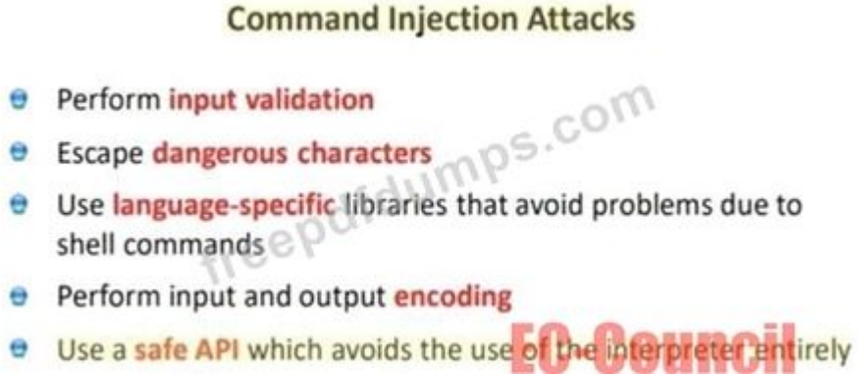


NEW QUESTION: 34
Which of the following data source will a SOC Analyst use to monitor connections to the insecure ports?
A. Netstat Data
B. DNS Data
C. IIS Data
D. DHCP Data
Answer: A (LEAVE A REPLY)
A SOC Analyst would use Netstat Data to monitor connections to insecure ports. Netstat, which stands for network statistics, is a command-line tool that displays incoming and outgoing network

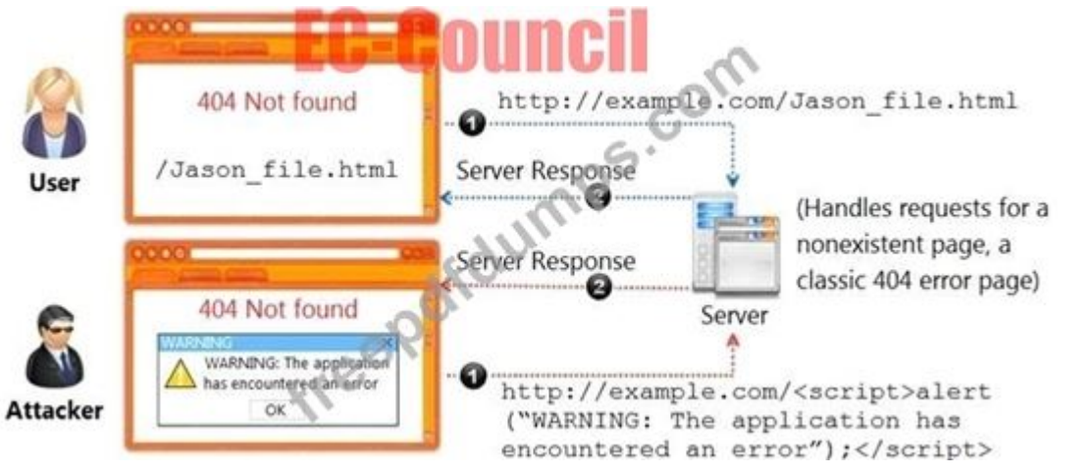
connections (both TCP and UDP), routing tables, and a number of network interface and network protocol statistics. It is available on various operating systems, including Windows, Linux, and Unix, and is used for finding problems in the network and to determine the amount of traffic on the network as a performance measurement.
References: The use of Netstat for monitoring network connections is a common practice and is covered in EC-Council's SOC Analyst curriculum, which provides foundational knowledge for security operations center (SOC) team members on various tools and techniques for monitoring and analyzing network traffic12. Additionally, Netstat's capabilities are well-documented in various technical resources that detail its usage for security analysis purposes34.

NEW QUESTION: 35
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. Parameter Tampering Attack
B. SQL Injection Attack
C. XSS Attack
D. Directory Traversal Attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 36
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: A (LEAVE A REPLY)



NEW QUESTION: 37
Identify the type of attack, an attacker is attempting on www.example.com website.



A. Cross-site Scripting Attack
B. Session Attack
C. Denial-of-Service Attack
D. SQL Injection Attack
Answer: A (LEAVE A REPLY)
The scenario depicted suggests an attacker is injecting a script into the URL of the website "www.example.com" which triggers an alert message. This behavior is characteristic of a Cross-site Scripting (XSS) attack. In XSS attacks, attackers exploit vulnerabilities in web applications to inject malicious scripts into web pages viewed by other users. The injected scripts can steal user data, deface web pages, or redirect users to malicious sites.
The specific attack vector here involves the attacker adding a script to the URL that causes the website to display an alert message. This indicates that the website is not properly sanitizing its inputs, which is how the attacker is able to execute the script in the context of the user's browser session.
References: The EC-Council's Certified SOC Analyst (CSA) program covers various types of cyberattacks, including XSS attacks. The CSA course materials and study guides provide detailed information on identifying, mitigating, and preventing such attacks, as well as best practices for securing web applications against them.

NEW QUESTION: 38
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: 39
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. Parameter Tampering Attack
C. XSS Attack
D. Directory Traversal Attack
Answer: A (LEAVE A REPLY)
The regex pattern /\\w*((\%27)|(\'))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix is designed to detect SQL injection attacks. The pattern looks for common SQL injection payloads which typically include an apostrophe or single quote character (' or %27 when URL-encoded) followed by a logical operator OR (represented by o, %6F, O, %4F, r, %72, R, %52). SQL injection attacks involve inserting or "injecting" a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system, and in some cases, issue commands to the operating system.
References: The explanation provided is based on standard practices of monitoring and analyzing IIS logs for security threats. Information about the regex pattern used for detecting SQL injection attacks can be found in various cybersecurity resources, including OWASP's guide on Testing for SQL Injection1 and Microsoft's documentation on IIS logging2. These resources explain how

regex patterns are used to identify potential security threats in log files and the importance of monitoring logs for unusual patterns that may indicate an attack.

NEW QUESTION: 40
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. SQL Injection Attack
C. Directory Traversal Attack
D. Parameter Tampering Attack
Answer: (SHOW ANSWER)

NEW QUESTION: 41
What type of event is recorded when an application driver loads successfully in Windows?
A. Error
B. Success Audit
C. Warning
D. Information
Answer: D (LEAVE A REPLY)
In Windows, when an application driver loads successfully, it is recorded as an "Information" event in the Event Viewer. This type of event indicates the successful operation of an application or system component, which in this case is the loading of a driver. Information events are typically used to log the normal operations of software and hardware, providing a record that can be useful for troubleshooting and monitoring system activity.
References: The EC-Council's Certified SOC Analyst (C|SA) program covers the types of events recorded in Windows systems, including the significance of Information events. This knowledge is essential for SOC analysts who monitor and analyze logs as part of their role in identifying and responding to security incidents. The details about event types and their implications are included in the official EC-Council SOC Analyst study guides and courses1234.

NEW QUESTION: 42
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\inetpub\logs\W3SVCN
B. SystemDrive%\inetpub\logs\LogFiles\W3SVCN
C. SystemDrive%\ inetpub\LogFiles\logs\W3SVCN
D. %SystemDrive%\LogFiles\logs\W3SVCN
Answer: B (LEAVE A REPLY)

NEW QUESTION: 43
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)
In a Risk Matrix, risk levels are determined by the intersection of the likelihood of an event occurring and the impact that event would have if it did occur. When the probability of an attack is very low, it means that the event is unlikely to happen. However, if the impact of that attack is major, it suggests that the event would have significant consequences if it did occur.
The combination of a very low probability with a major impact typically results in a low risk level. This is because the overall risk is mitigated by the low chance of the event happening, despite the potential for a significant impact. Therefore, even though the impact is major, the risk level is kept low due to the very low likelihood of occurrence.
References: The EC-Council's Certified SOC Analyst (CSA) program covers the concepts of risk assessment and the use of Risk Matrices. The CSA study materials and courses provide detailed explanations on how to evaluate and categorize risks based on their probability and impact, aligning with industry-standard practices123.

NEW QUESTION: 44
Which of the following formula represents the risk levels?
A. Level of risk = Consequence * Asset Value
B. Level of risk = Consequence * Likelihood
C. Level of risk = Consequence * Severity
D. Level of risk = Consequence * Impact
Answer: D (LEAVE A REPLY)

NEW QUESTION: 45
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: 46
Which encoding replaces unusual ASCII characters with "%" followed by the character's two-digit ASCII code expressed in hexadecimal?
A. URL Encoding
B. Unicode Encoding
C. UTF Encoding
D. Base64 Encoding
Answer: (SHOW ANSWER)

NEW QUESTION: 47
Peter, a SOC analyst with Spade Systems, is monitoring and analyzing the router logs of the company and wanted to check the logs that are generated by access control list numbered 210. What filter should Peter add to the 'show logging' command to get the required output?
A. show logging | access 210
B. show logging | forward 210
C. show logging | include 210
D. show logging | route 210
Answer: C (LEAVE A REPLY)
To filter the output of the 'show logging' command to include entries related to a specific access control list, Peter should use the 'include' keyword followed by the access list number. The correct command would be
'show logging | include 210'. This command will display all log entries that contain the string '210', which is the number of the access control list he wants to monitor.
References: The use of the 'include' keyword in Cisco router commands is a standard method for filtering show command outputs to display only lines that contain a specified string or pattern. This is covered in Cisco's documentation and training materials related to router commands and access control list management12.

NEW QUESTION: 48
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: (SHOW ANSWER)
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: 49
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)

NEW QUESTION: 50
What does Windows event ID 4740 indicate?
A. A user account was locked out.
B. A user account was disabled.
C. A user account was enabled.
D. A user account was created.
Answer: A (LEAVE A REPLY)

Event ID 4740 is a security audit event in Windows that indicates a user account has been locked out. This event is generated every time the system locks out a user account due to repeated logon failures, which are typically caused by incorrect password entries. The event is logged on domain controllers, member servers, and workstations where the lockout occurred. It includes details such as the account name, domain, and the computer from which the lockout originated.
References: The information is verified as per Microsoft's official documentation and learning resources related to security auditing and user account management. Specifically, the Microsoft Learn page on security auditing provides comprehensive details on Event ID 47401. Additionally, resources like Ultimate Windows Security offer in-depth explanations of this event and its implications for security monitoring2.

NEW QUESTION: 51
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: 52
Jason, a SOC Analyst with Maximus Tech, was investigating Cisco ASA Firewall logs and came across the following log entry:
May 06 2018 21:27:27 asa 1: %ASA -5 - 11008: User 'enable_15' executed the 'configure term' command What does the security level in the above log indicates?
A. Warning condition message
B. Critical condition message
C. Normal but significant message
D. Informational message
Answer: (SHOW ANSWER)

Cisco ASA Firewall

Cisco ASA firewalls support multiple levels of logging. It helps to address the issue by addressing the most critical events first. These levels of logging are typically labeled 0–7. The logging severity level set for the specific output will not only take logs that configured severity level but also from all the levels above it. For example, if you have configured severity level 7—debugging messages for the console, then level 7 will not only log all debugging messages but also emergencies, alerts, critical errors, warnings, notifications, and informational messages. Always configure critical severity level for the log messages, because higher logging severity level (e.g., 7) generates a large amount of log messages that disturb the CPU and memory usage on the Cisco ASA firewall.

The following table depicts the different levels of logging.

Levels of logging	Description
Emergencies (0)	System unusable messages
Alerts (1)	Immediate action required messages, for examples, failover, power supply, basic RIP, and address verification
Critical (2)	Critical condition messages, for examples, denied packets/connections after basic checks, URL filter server problems, etc.
Errors (3)	Error condition messages, for examples, authentication/authorization failures, CPU and memory resource problems, tunnel problems, routing and NTP problems, etc.
Warnings (4)	Warning condition messages, for examples, fragmentation issues, invalid addresses, auto-update errors, CSPF errors, etc.
Notifications (5)	Normal but significant messages, for examples, commands executed by users, configuration events, and user and session activity

NEW QUESTION: 53

In which log collection mechanism, the system or application sends log records either on the local disk or over the network.

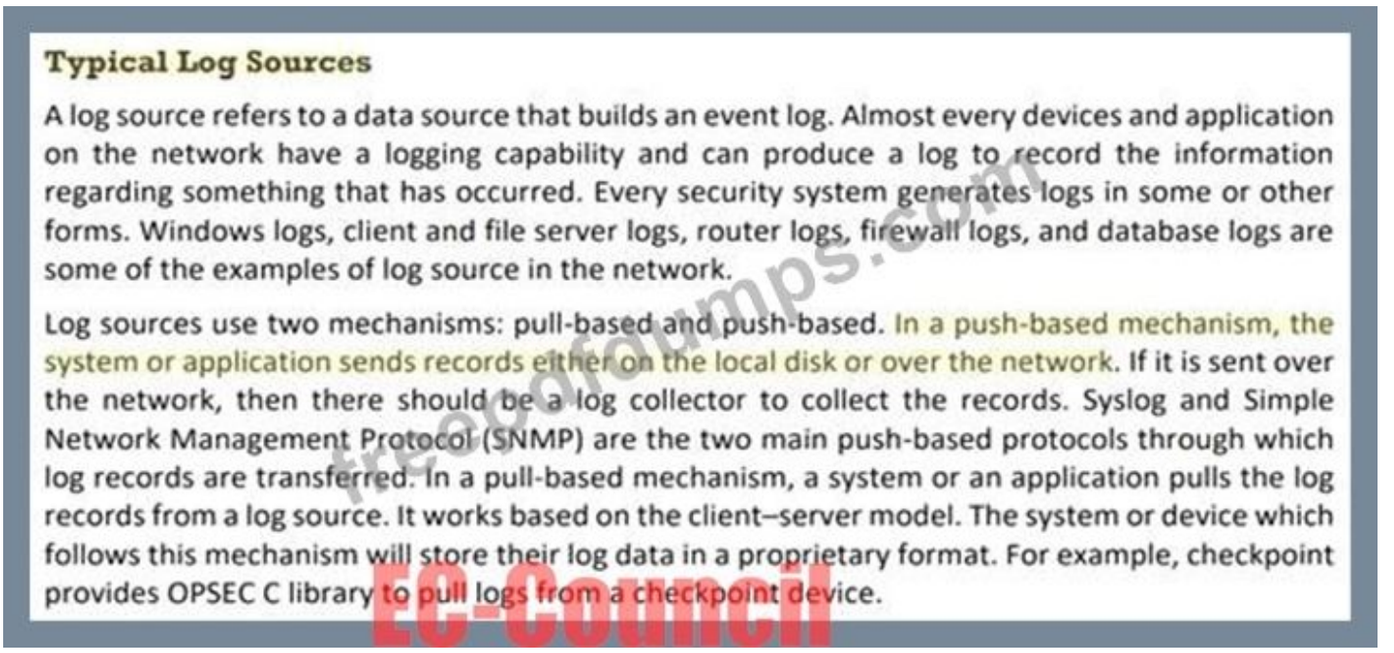
A. rule-based

B. pull-based

C. push-based

D. signature-based

Answer: (SHOW ANSWER)



NEW QUESTION: 54
Jason, a SOC Analyst with Maximus Tech, was investigating Cisco ASA Firewall logs and came across the following log entry:
May 06 2018 21:27:27 asa 1: %ASA -5 - 11008: User 'enable_15' executed the 'configure term' command What does the security level in the above log indicates?
A. Informational message
B. Critical condition message
C. Warning condition message
D. Normal but significant message
Answer: C (LEAVE A REPLY)

NEW QUESTION: 55
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. False positive Incidents
B. False Negative Incidents
C. True Positive Incidents
D. True Negative Incidents
Answer: D (LEAVE A REPLY)

NEW QUESTION: 56
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. Broken Access Control Attacks
B. Web Services Attacks

C. XSS Attacks
D. Session Management Attacks
Answer: C (LEAVE A REPLY)
Converting all non-alphanumeric characters to HTML character entities is a common defense against Cross-Site Scripting (XSS) attacks. Here's how it works:
* User Input Sanitization: When user input is received, the system converts characters like <, >, &, ', and " into their corresponding HTML entities (e.g., <, >, &, ', and ").
* Preventing Script Execution: By converting these characters, the system prevents potentially malicious scripts from being executed in the browser of anyone viewing the content.
* Maintaining Data Integrity: This process allows user-generated content to be displayed without altering the intended message while ensuring the content cannot harm other users or the system.
References:
* EC-Council's Certified SOC Analyst (C|SA) course material covers various cybersecurity threats, including XSS attacks, and the methods used to mitigate them.
* The study guides and resources provided by EC-Council for the SOC Analyst certification include detailed explanations of XSS attacks and the importance of sanitizing user input to prevent such vulnerabilities1234

NEW QUESTION: 57
What does the HTTP status codes 1XX represents?
A. Informational message
B. Client error
C. Success
D. Redirection
Answer: A (LEAVE A REPLY)
The HTTP status codes that fall within the range of 1XX represent informational messages. These are provisional responses that indicate the initial part of a request has been received and has not yet been rejected by the server. The server is informing the client that it has received the header of the request and the client should continue to send the request body if it has not already done so. These status codes are used to provide an interim response to the client while the server processes the full request.
References: The EC-Council's Certified SOC Analyst (C|SA) program includes the study of HTTP status codes as part of understanding web server logs and troubleshooting web server issues. The informational responses (1XX status codes) are covered in the curriculum and can be found in the official EC-Council SOC Analyst study guides and courses. The information is also consistent with the standard definitions provided by the Internet Engineering Task Force (IETF) in RFC 9110, as well as other reputable sources such as MDN Web Docs1 and Wikipedia2.

NEW QUESTION: 58
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. FISMA
B. HIPAA
C. PCI-DSS
D. DARPA
Answer: C (LEAVE A REPLY)

NEW QUESTION: 59
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. SOC-CMM
C. ITIL
D. SSE-CMM
Answer: D (LEAVE A REPLY)

NEW QUESTION: 60
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: D (LEAVE A REPLY)

False negative: False negatives are the false result for an activity that actually occurred. It is an attack-negative reply for an actual attack. The false negative is the type of alert which will not raise the alarm even if an attack is taking place on the network. By not defining the rules properly, these kinds of errors in the alerting system will occur. By false positives, actual is not identified, which may lead to cybersecurity breach over the organization. For example, an attacker tried to gain access to an unauthorized network and succeeded by attempting nine times. If the rule in the SIEM is made in such a way that 10 login attempts have to be identified as an alert, then the attempts of the attacker may not be noticed. In this way, false positives can be dangerous for an organization if they are not rectified.

NEW QUESTION: 61
Identify the attack when an attacker by several trial and error can read the contents of a password file present in the restricted etc folder just by manipulating the URL in the browser as shown:
http://www.terabytes.com/process.php./../../../../etc/passwd
A. Directory Traversal Attack
B. SQL Injection Attack

C. Denial-of-Service Attack

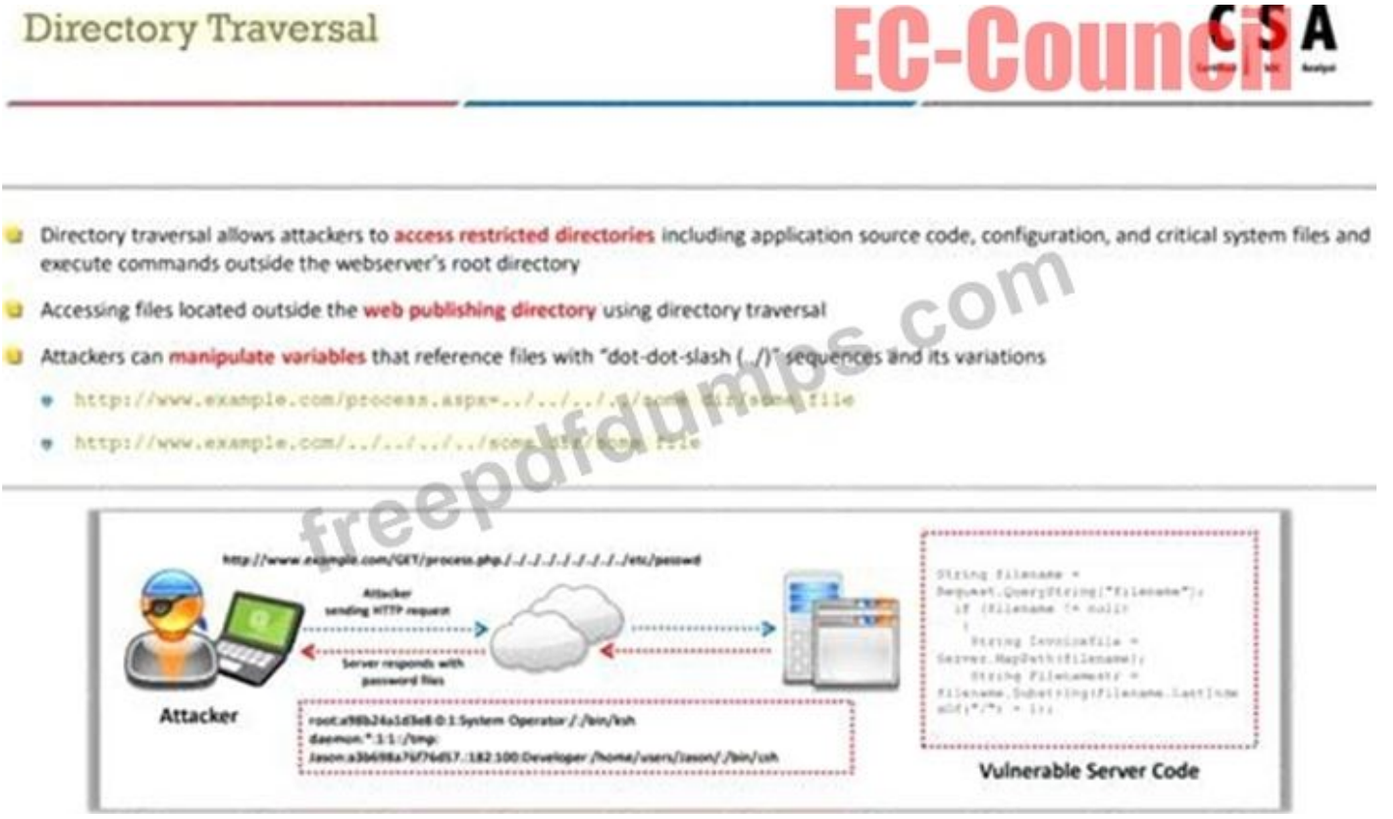
D. Form Tampering Attack

Answer: A (LEAVE A REPLY)

The attack described is a Directory Traversal Attack. This type of attack occurs when an attacker exploits vulnerabilities in a web application (or a web server's software) to gain unauthorized access to files and directories that are stored outside of the web root folder. By manipulating variables that reference files with ../ sequences (also known as dot-dot-slash), the attacker can move up the directory hierarchy and access files or directories that should be restricted. This can lead to information disclosure, such as reading sensitive files like /etc/passwd, which contains user password details in Unix-based systems.

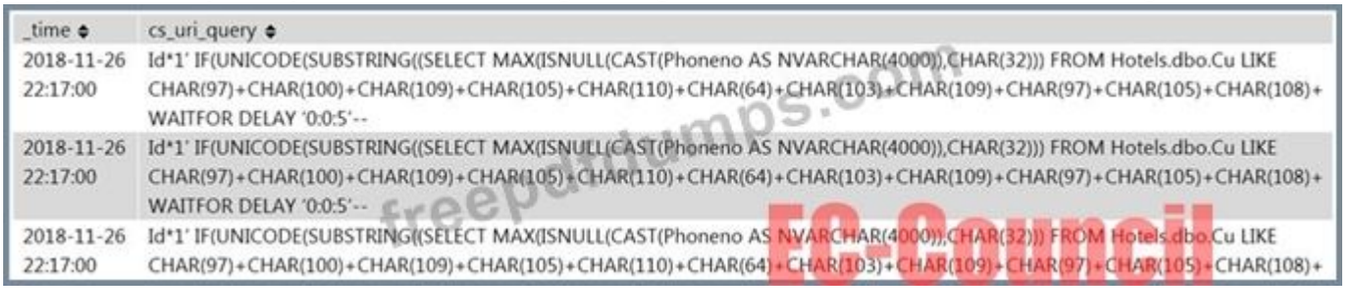
In the given URL http://www.terabytes.com/process.php./../../../../etc/passwd, the attacker uses the ../ pattern to navigate up from the current directory where process.php resides, aiming to reach the root directory and then descend into the /etc/ directory to access the passwd file. This is a classic example of a Directory Traversal Attack.

References: The EC-Council's Certified SOC Analyst course covers various types of cyber attacks, including Directory Traversal Attacks. Specific references to this type of attack can be found in the EC-Council's official training materials for the Certified SOC Analyst (CSA) program, such as the CSA study guide and related courses that discuss web application vulnerabilities and attacks123.



NEW QUESTION: 62
What does HTTPS Status code 403 represents?
A. Unauthorized Error
B. Not Found Error
C. Internal Server Error
D. Forbidden Error
Answer: D (LEAVE A REPLY)
The HTTPS status code 403 represents a Forbidden Error. This error occurs when the server understands the request but refuses to authorize it. Unlike the Unauthorized Error (401), which suggests that the request might be authorized if the client re-authenticates, the Forbidden Error indicates that re-authenticating will make no difference and access is denied regardless of authentication status.
The Forbidden Error is tied to the application logic, such as insufficient rights to a resource or the server being programmed to deny access to a particular resource to the client. It is not related to the client's credentials but rather to the permissions set by the server for the requested resource.
References: The EC-Council SOC Analyst course materials and study guides discuss various HTTP status codes as part of understanding web application security and interpreting web logs within a Security Operations Center (SOC) context. The materials explain the meaning of the 403 Forbidden Error and its implications for cybersecurity analysis123.

NEW QUESTION: 63
Jony, a security analyst, while monitoring IIS logs, identified events shown in the figure below.



_time	cs_uri_query
2018-11-26 22:17:00	Id*1' IF(UNICODE(SUBSTRING((SELECT MAX(ISNULL(CAST(Phoneno AS NVARCHAR(4000)),CHAR(32))) FROM Hotels.dbo.Cu LIKE CHAR(97)+CHAR(100)+CHAR(109)+CHAR(105)+CHAR(110)+CHAR(64)+CHAR(103)+CHAR(109)+CHAR(97)+CHAR(105)+CHAR(108)+ WAITFOR DELAY '0:0:5'--
2018-11-26 22:17:00	Id*1' IF(UNICODE(SUBSTRING((SELECT MAX(ISNULL(CAST(Phoneno AS NVARCHAR(4000)),CHAR(32))) FROM Hotels.dbo.Cu LIKE CHAR(97)+CHAR(100)+CHAR(109)+CHAR(105)+CHAR(110)+CHAR(64)+CHAR(103)+CHAR(109)+CHAR(97)+CHAR(105)+CHAR(108)+ WAITFOR DELAY '0:0:5'--
2018-11-26 22:17:00	Id*1' IF(UNICODE(SUBSTRING((SELECT MAX(ISNULL(CAST(Phoneno AS NVARCHAR(4000)),CHAR(32))) FROM Hotels.dbo.Cu LIKE CHAR(97)+CHAR(100)+CHAR(109)+CHAR(105)+CHAR(110)+CHAR(64)+CHAR(103)+CHAR(109)+CHAR(97)+CHAR(105)+CHAR(108)+

What does this event log indicate?
A. Directory Traversal Attack
B. SQL Injection Attack
C. XSS Attack
D. Parameter Tampering Attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 64

Identify the HTTP status codes that represents the server error.
A. 2XX
B. 4XX
C. 1XX
D. 5XX
Answer: D (LEAVE A REPLY)
HTTP status codes are categorized into five classes, where each class is represented by the first digit of the status code. The 5XX series of status codes indicates server errors, which means that the server is aware that it has encountered an error or is otherwise incapable of performing the request. Common examples of 5XX status codes include 500 (Internal Server Error), 501 (Not Implemented), 502 (Bad Gateway), etc. These indicate that the request was valid, but the server failed to fulfill the request due to some issue on the server side.
References: The EC-Council's Certified SOC Analyst (C|SA) course material and study guides discuss the interpretation and significance of HTTP status codes in the context of security operations. Understanding these codes is crucial for SOC analysts, as they can indicate potential server-side issues that may impact the security posture of an organization12.

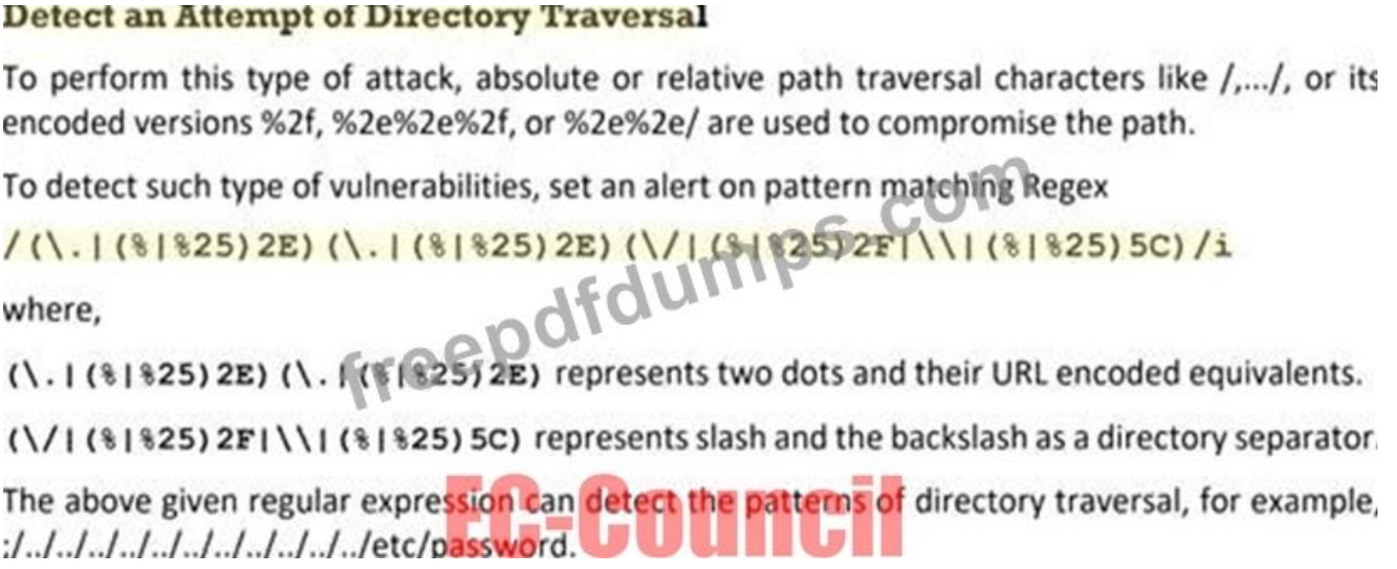
NEW QUESTION: 65
Which of the following command is used to view iptables logs on Ubuntu and Debian distributions?
A. $ tailf /var/log/kern.log
B. # tailf /var/log/sys/messages
C. # tailf /var/log/messages
D. $ tailf /var/log/sys/kern.log
Answer: A (LEAVE A REPLY)

NEW QUESTION: 66
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: 67
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. Systems Recovery
C. Eradication
D. Evidence Handling
Answer: A (LEAVE A REPLY)

NEW QUESTION: 68
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. XSS Attack
B. SQL injection Attack
C. Directory Traversal Attack
D. Parameter Tampering Attack
Answer: (SHOW ANSWER)



NEW QUESTION: 69
Jason, a SOC Analyst with Maximus Tech, was investigating Cisco ASA Firewall logs and came across the following log entry:

May 06 2018 21:27:27 asa 1: %ASA -5 - 11008: User 'enable_15' executed the 'configure term' command What does the security level in the above log indicates?

A. Warning condition message

B. Critical condition message

C. Normal but significant message

D. Informational message

Answer: A (LEAVE A REPLY)

In the context of Cisco ASA Firewall logs, messages are categorized into different severity levels ranging from
0 (emergencies) to 7 (debugging messages). The log entry mentioned specifies a severity level of 5, denoted by "-5-" in the log entry. According to Cisco's documentation, a severity level of 5 corresponds to a
"Notification" level, which indicates a warning condition message. These messages are significant and highlight conditions that could potentially lead to more severe problems if not addressed. The execution of the
'configure term' command by 'enable_15' user, as noted in the log, is an example of a notable event that warrants attention, hence categorized under this severity level.

References:

* "Cisco ASA Series Syslog Messages", Cisco Systems, Inc.
* "Understanding Logging Levels in Cisco ASA Security Appliances", Cisco Community.

NEW QUESTION: 70

The Syslog message severity levels are labelled from level 0 to level 7.

What does level 0 indicate?

A. Notification

B. Debugging

C. Alert

D. Emergency

Answer: A (LEAVE A REPLY)

NEW QUESTION: 71

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. Apility.io

B. Malstrom

C. OpenDNS

D. I-Blocklist

Answer: C (LEAVE A REPLY)

OpenDNS provides extensive phishing protection and content filtering services. It operates by enforcing internet use policies on and off the network, ensuring that users adhere to acceptable use and compliance policies. Here's how OpenDNS achieves this:

* Phishing Protection: OpenDNS uses predictive security to anticipate and prevent threats before they can reach the network. It does this by using DNS to enforce security, which is often quicker and more effective than traditional methods.
* Content Filtering: OpenDNS allows the network administrator to block unwanted content categories, thus enforcing compliance with organizational policies. This is done through DNS queries, which are checked against OpenDNS's database to ensure they comply with the set policies.
* Off-Network Protection: OpenDNS's roaming client allows the same level of protection and filtering even when devices are not connected to the company network, ensuring consistent enforcement of policies.
References:
* EC-Council's Certified SOC Analyst (C|SA) program provides training and certification for SOC analysts, covering the fundamentals of SOC operations, including phishing protection and content filtering 1.
* Additional resources and study guides from the EC-Council elaborate on the role of SOC analysts and the tools they use, including services like OpenDNS for maintaining network security and integrity 23.

NEW QUESTION: 72
Where will you find the reputation IP database, if you want to monitor traffic from known bad IP reputation using OSSIM SIEM?
A. /etc/ossim/reputation
B. /etc/ossim/siem/server/reputation/data
C. /etc/siem/ossim/server/reputation.data
D. /etc/ossim/server/reputation.data
Answer: (SHOW ANSWER)
Explanation
Graphical user interface, text Description automatically generated

NEW QUESTION: 73

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: (SHOW ANSWER)

In the context of log storage, a circular buffer is a data structure that uses a single, fixed-size buffer as if it were connected end-to-end. This structure lends itself to buffering streams of data, where the data is written to the buffer and read from it in a potentially non-sequential manner. When the buffer is full, new data is written starting at the beginning of the buffer, and thus 'wraps' around. This is why the method is referred to as
'wrapping'. FIFO (First In, First Out) and LIFO (Last In, First Out) are queueing methods, and non-wrapping implies that the buffer does not overwrite existing data when full.

References: The answer can be verified through EC-Council's SOC Analyst study materials and official courseware, which detail various log storage methods and their characteristics. Additionally, the concept of a circular buffer is a well-known data structure in computer science, often discussed in the context of system design and memory management.

There are two ways of arranging the event records:

- **Nonwrapping method**: In this method, the oldest record is inserted just after the event log header and new records are inserted just before the ELF_EOF_RECORD. In the below example, event records are organized as per the nonwrapping method:

  HEADER (ELF_LOGFILE_HEADER)

  EVENT RECORD 1 (EVENTLOGRECORD)

  EVENT RECORD 2 (EVENTLOGRECORD)

  EOF RECORD (ELF_EOF_RECORD)

  Nonwrapping can perform every time when the event log is generated or deleted. The event log records continue to organize as per nonwrapping until the event log size reaches its maximum limit. The event log size is depending either upon the MaxSize configuration value or the number of system resources. When the event log size reaches to its last limit, then it will start using wrapping.

- **Wrapping method**: In this method, event logs are arranged in the form of a circular buffer. It replaces the oldest event logs by the new event logs. Consider the below example to understand wrapping method:

  HEADER (ELF_LOGFILE_HEADER)

NEW QUESTION: 74

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)

SIEM Deployment Architecture Options: Cloud, Self-Managed

The cloud, self-managed SIEMs are the kind where only log collection and log aggregation are done in the MSSP, and the remaining methods and techniques like correlation, analytics, reporting, retention, alerting, and visualization of the data are performed inside the organization.

As the data are within the organization, the personalization of the visualization can be done as per the requirement of the staff. The maintenance of the SIEM is done as per the need, and unnecessary updates in the network can be omitted. By implementing the cloud technology in the SIEM, the data are way more secure compared to the storage in the physically accessed hardware storage units which consume a lot of places. These are some of the benefits for the organization by implementing cloud, self-managed SIEM.

Challenges that are faced by the organization if they want to implement this kind of SIEM in their network are that they may not get 24/7 monitoring on the log data. If the organization makes the staff work in shifts, then it will be a fruitful way of implementing a SIEM.

NEW QUESTION: 75

Which of the following can help you eliminate the burden of investigating false positives?

A. Not trusting the security devices

B. Keeping default rules

C. Treating every alert as high level

D. Ingesting the context data

Answer: (SHOW ANSWER)

NEW QUESTION: 76

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: 77

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: D (LEAVE A REPLY)

Explanation

Graphical user interface, application, Teams Description automatically generated

NEW QUESTION: 78

Which of the following is a default directory in a Mac OS X that stores security-related logs?

A. /Library/Logs/Sync

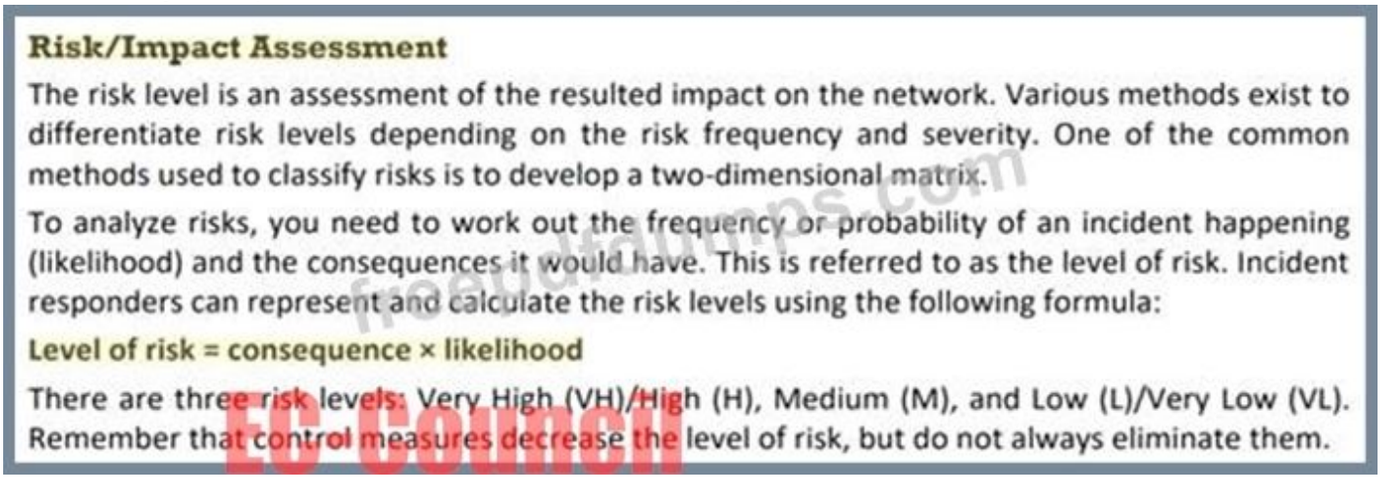
B. /private/var/log

C. /var/log/cups/access_log

D. ~/Library/Logs

Answer: (SHOW ANSWER)

NEW QUESTION: 79
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: (SHOW ANSWER)
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: 80
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 Recording
D. Incident Classification
Answer: D (LEAVE A REPLY)

NEW QUESTION: 81
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: 82
A type of threat intelligent that find out the information about the attacker by misleading them is known as
.
A. Threat trending Intelligence
B. Detection Threat Intelligence
C. Operational Intelligence
D. Counter Intelligence
Answer: D (LEAVE A REPLY)

NEW QUESTION: 83
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)