EC-COUNCIL.312-39.v2022-10-04.q33

Exam Code:	312-39
Exam Name:	Certified SOC Analyst (CSA)
Certification Provider:	EC-COUNCIL
Free Question Number:	33
Version:	v2022-10-04
# of views:	1214
# of Questions views:	330
https://www.freeqas.com/qa/EC-COUNCIL/312-39/EC-COUNCIL.312-39.v2022-10-04.q33.html	

NEW QUESTION: 1
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. OpenDNS
C. Apility.io
D. I-Blocklist
Answer: B (LEAVE A REPLY)

NEW QUESTION: 2
Which of the following security technology is used to attract and trap people who attempt unauthorized or illicit utilization of the host system?
A. Firewall
B. Intrusion Detection System
C. Honeypot
D. De-Militarized Zone (DMZ)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 3
Which of the following event detection techniques uses User and Entity Behavior Analytics (UEBA)?
A. Anomaly-based detection
B. Rule-based detection
C. Signature-based detection
D. Heuristic-based detection

Answer: A (LEAVE A REPLY)

NEW QUESTION: 4
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 trending
B. Threat pivoting
C. Threat boosting
D. Threat buy-in
Answer: D (LEAVE A REPLY)

NEW QUESTION: 5
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. Analysis and Production
B. Collection
C. Processing and Exploitation
D. Dissemination and Integration
Answer: (SHOW ANSWER)

NEW QUESTION: 6
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/server/reputation.data
B. /etc/siem/ossim/server/reputation.data
C. /etc/ossim/reputation
D. /etc/ossim/siem/server/reputation/data
Answer: (SHOW ANSWER)

NEW QUESTION: 7
Which of the following is a default directory in a Mac OS X that stores security-related logs?
A. /private/var/log
B. ~/Library/Logs
C. /var/log/cups/access_log

D. /Library/Logs/Sync
Answer: (SHOW ANSWER)

NEW QUESTION: 8
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. Throttling
B. Rate Limiting
C. Egress Filtering
D. Ingress Filtering
Answer: D (LEAVE A REPLY)

NEW QUESTION: 9
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. XSS Attacks
B. Session Management Attacks
C. Web Services Attacks
D. Broken Access Control Attacks
Answer: A (LEAVE A REPLY)

NEW QUESTION: 10
Which of the following formula represents the risk?
A. Risk = Likelihood * Impact * Asset Value
B. Risk = Likelihood * Consequence * Severity
C. Risk = Likelihood * Impact * Severity
D. Risk = Likelihood * Severity * Asset Value
Answer: B (LEAVE A REPLY)

NEW QUESTION: 11
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. SQL Injection Attack
B. Directory Traversal Attack
C. XSS Attack
D. Parameter Tampering Attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 12

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. DHCP Data

D. IIS Data

Answer: (SHOW ANSWER)

NEW QUESTION: 13

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

A. UrlScan

B. Hydra

C. Nmap

D. ZAP proxy

Answer: (SHOW ANSWER)

NEW QUESTION: 14

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, MSSP Managed

B. Cloud, Self-Managed

C. Self-hosted, Self-Managed

D. Hybrid Model, Jointly Managed

Answer: A (LEAVE A REPLY)

NEW QUESTION: 15

Daniel is a member of an IRT, which was started recently in a company named Mesh Tech. He wanted to find the purpose and scope of the planned incident response capabilities.

What is he looking for?

A. Incident Response Mission

B. Incident Response Resources

C. Incident Response Vision

D. Incident Response Intelligence

Answer: B (LEAVE A REPLY)

NEW QUESTION: 16
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, MSSP Managed
B. Self-hosted, Jointly Managed
C. Cloud, MSSP Managed
D. Self-hosted, Self-Managed
Answer: (SHOW ANSWER)

NEW QUESTION: 17
Juliea a SOC analyst, while monitoring logs, noticed large TXT, NULL payloads.
What does this indicate?
A. Concurrent VPN Connections Attempt
B. Covering Tracks Attempt
C. DHCP Starvation Attempt
D. DNS Exfiltration Attempt
Answer: (SHOW ANSWER)

NEW QUESTION: 18
Which of the following attack inundates DHCP servers with fake DHCP requests to exhaust all available IP addresses?
A. DHCP Cache Poisoning
B. DHCP Spoofing Attack
C. DHCP Starvation Attacks
D. DHCP Port Stealing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 19
Properly applied cyber threat intelligence to the SOC team help them in discovering TTPs.
What does these TTPs refer to?

A. Targets, Threats, and Process
B. Tactics, Techniques, and Procedures
C. Tactics, Targets, and Process
D. Tactics, Threats, and Procedures
Answer: B (LEAVE A REPLY)

NEW QUESTION: 20
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. SQL Injection Attack
B. Directory Traversal Attack
C. Denial-of-Service Attack
D. Form Tampering Attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 21
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. Absorbing the Attack
B. Diverting the Traffic
C. Degrading the services
D. Blocking the Attacks
Answer: A (LEAVE A REPLY)

NEW QUESTION: 22
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. II
B. IV
C. I
D. III
Answer: C (LEAVE A REPLY)

NEW QUESTION: 23
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. Medium
B. Extreme
C. High
D. Low
Answer: D (LEAVE A REPLY)

NEW QUESTION: 24
In which log collection mechanism, the system or application sends log records either on the local disk or over the network.
A. push-based
B. pull-based
C. signature-based
D. rule-based
Answer: (SHOW ANSWER)

NEW QUESTION: 25
What does HTTPS Status code 403 represents?
A. Unauthorized Error
B. Internal Server Error
C. Not Found Error
D. Forbidden Error
Answer: (SHOW ANSWER)

NEW QUESTION: 26
In which of the following incident handling and response stages, the root cause of the incident must be found from the forensic results?
A. Eradication
B. Evidence Gathering
C. Systems Recovery
D. Evidence Handling
Answer: B (LEAVE A REPLY)

NEW QUESTION: 27
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. Critical condition message
B. Informational message
C. Warning condition message
D. Normal but significant message
Answer: (SHOW ANSWER)

NEW QUESTION: 28
Which of the following steps of incident handling and response process focus on limiting the scope and extent of an incident?
A. Identification
B. Data Collection
C. Eradication
D. Containment
Answer: D (LEAVE A REPLY)

NEW QUESTION: 29
What is the correct sequence of SOC Workflow?
A. Collect, Ingest, Document, Validate, Report, Respond
B. Collect, Ingest, Validate, Document, Report, Respond
C. Collect, Respond, Validate, Ingest, Report, Document
D. Collect, Ingest, Validate, Report, Respond, Document
Answer: B (LEAVE A REPLY)

NEW QUESTION: 30
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. Technical Threat Intelligence
C. Operational Threat Intelligence
D. Tactical Threat Intelligence
Answer: (SHOW ANSWER)

NEW QUESTION: 31
Identify the HTTP status codes that represents the server error.
A. 5XX
B. 4XX
C. 2XX
D. 1XX

Answer: (SHOW ANSWER)

NEW QUESTION: 32
Which of the following Windows event is logged every time when a user tries to access the "Registry" key?
A. 4656
B. 4663
C. 4660
D. 4657
Answer: D (LEAVE A REPLY)

NEW QUESTION: 33
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-> Forensics lab licensing -> Human resource considerations -> Work area considerations -> Physical security recommendations
B. Planning and budgeting -> Forensics lab licensing -> Physical location and structural design considerations -> Work area considerations -> Physical security recommendations -> Human resource considerations
C. Planning and budgeting -> Physical location and structural design considerations -> Work area considerations -> Human resource considerations -> Physical security recommendations -> Forensics lab licensing
D. Planning and budgeting -> Physical location and structural design considerations -> Forensics lab licensing ->Work area considerations -> Human resource considerations -> Physical security recommendations
Answer: (SHOW ANSWER)

Valid 312-39 Dumps shared by PrepPdf.com for Helping Passing 312-39 Exam! PrepPdf.com now offer the **newest 312-39 exam dumps**, the PrepPdf.com 312-39 exam **questions have been updated** and **answers have been corrected** get the