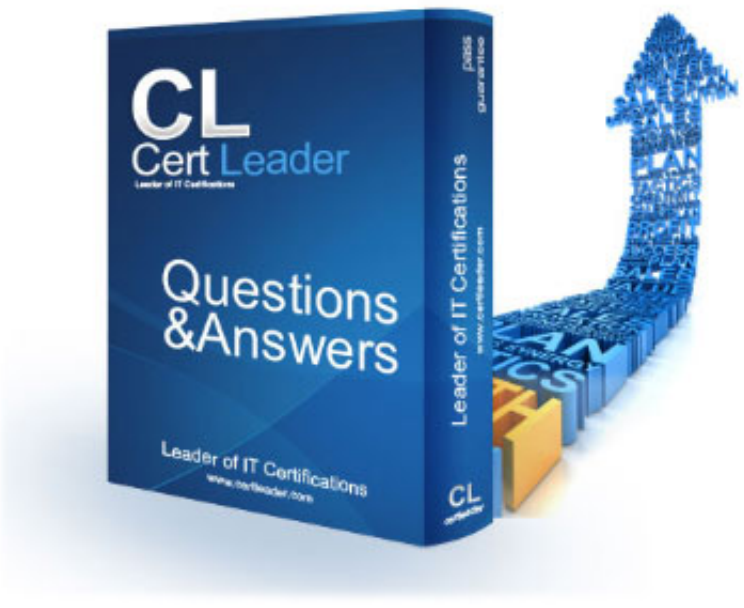
312-39 Dumps

Certified SOC Analyst (CSA)

https://www.certleader.com/312-39-dumps.html



NEW QUESTION 1
What is the correct sequence of SOC Workflow?

A. Collect, Ingest, Validate, Document, Report, Respond
B. Collect, Ingest, Document, Validate, Report, Respond
C. Collect, Respond, Validate, Ingest, Report, Document
D. Collect, Ingest, Validate, Report, Respond, Document

Answer: A

NEW QUESTION 2
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. Tactical Threat Intelligence
D. Operational Threat Intelligence

Answer: D

NEW QUESTION 3
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

NEW QUESTION 4
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/Sync
C. /var/log/cups/access_log
D. ~/Library/Logs

Answer: D

NEW QUESTION 5
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

NEW QUESTION 6
What does the Security Log Event ID 4624 of Windows 10 indicate?

A. Service added to the endpoint
B. A share was assessed
C. An account was successfully logged on
D. New process executed

Answer: C

NEW QUESTION 7
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

NEW QUESTION 8
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

NEW QUESTION 9
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: B

NEW QUESTION 10
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

NEW QUESTION 10
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: C

NEW QUESTION 14
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: C

NEW QUESTION 19
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

NEW QUESTION 23
Which of the following data source can be used to detect the traffic associated with Bad Bot User-Agents?

A. Windows Event Log
B. Web Server Logs
C. Router Logs
D. Switch Logs

Answer: B

NEW QUESTION 28
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

NEW QUESTION 31
Which of the following attack inundates DHCP servers with fake DHCP requests to exhaust all available IP addresses?

A. DHCP Starvation Attacks
B. DHCP Spoofing Attack
C. DHCP Port Stealing
D. DHCP Cache Poisoning

Answer: A

NEW QUESTION 34
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: B

NEW QUESTION 36
What does HTTPS Status code 403 represents?

A. Unauthorized Error
B. Not Found Error
C. Internal Server Error
D. Forbidden Error

Answer: D

NEW QUESTION 39
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

NEW QUESTION 44
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 Intelligence
B. Incident Response Mission
C. Incident Response Vision
D. Incident Response Resources

Answer: D

NEW QUESTION 45
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: A

NEW QUESTION 46
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: B

NEW QUESTION 49
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. ITIL
C. SSE-CMM
D. SOC-CMM

Answer: C

NEW QUESTION 52
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

NEW QUESTION 56
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 immediately escalate this issue to the management
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 formally raise a ticket and forward it to the IRT

Answer: B

NEW QUESTION 59
In which phase of Lockheed Martin's – Cyber Kill Chain Methodology, adversary creates a deliverable malicious payload using an exploit and a backdoor?

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

Answer: B

NEW QUESTION 64
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

NEW QUESTION 65
Which of the following is a Threat Intelligence Platform?

A. SolarWinds MS
B. TC Complete
C. Keepnote
D. Apility.io

Answer: A

NEW QUESTION 66
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: B

NEW QUESTION 68
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: A

NEW QUESTION 72
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: A

NEW QUESTION 75
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 312-39 Exam with Our Prep Materials Via below:

https://www.certleader.com/312-39-dumps.html