

EC-Council

Exam Questions 312-39

Certified SOC Analyst (CSA)



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

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: B

NEW QUESTION 3

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 4

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

- A. Tactics, Techniques, and Procedures
- B. Tactics, Threats, and Procedures
- C. Targets, Threats, and Process
- D. Tactics, Targets, and Process

Answer: A

NEW QUESTION 5

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 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/reputation
- B. /etc/ossim/siem/server/reputation/data
- C. /etc/siem/ossim/server/reputation.data
- D. /etc/ossim/server/reputation.data

Answer: A

NEW QUESTION 7

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

NEW QUESTION 8

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: B

NEW QUESTION 9

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: A

NEW QUESTION 10

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. Diverting the Traffic
- C. Degrading the services
- D. Absorbing the Attack

Answer: D

NEW QUESTION 10

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 12

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 17

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 18

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

NEW QUESTION 21

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 23

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 25

Which of the following tool is used to recover from web application incident?

- A. CrowdStrike Falcon™ Orchestrator
- B. Symantec Secure Web Gateway
- C. Smoothwall SWG
- D. Proxy Workbench

Answer: B

NEW QUESTION 30

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

NEW QUESTION 31

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

NEW QUESTION 34

Juliea a SOC analyst, while monitoring logs, noticed large TXT, NULL payloads. What does this indicate?

- A. Concurrent VPN Connections Attempt
- B. DNS Exfiltration Attempt
- C. Covering Tracks Attempt
- D. DHCP Starvation Attempt

Answer: B

NEW QUESTION 36

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 37

Which of the following attacks causes sudden changes in file extensions or increase in file renames at rapid speed?

- A. Ransomware Attack
- B. DoS Attack
- C. DHCP starvation Attack
- D. File Injection Attack

Answer: A

NEW QUESTION 41

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 44

Wesley is an incident handler in a company named Maddison Tech. One day, he was learning techniques for eradicating the insecure deserialization attacks. What among the following should Wesley avoid from considering?

- A. Deserialization of trusted data must cross a trust boundary
- B. Understand the security permissions given to serialization and deserialization
- C. Allow serialization for security-sensitive classes
- D. Validate untrusted input, which is to be serialized to ensure that serialized data contain only trusted classes

Answer: C

NEW QUESTION 48

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 52

Which of the following is a Threat Intelligence Platform?

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

Answer: A

NEW QUESTION 53

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 56

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 57

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: A

NEW QUESTION 61

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

312-39 Practice Exam Features:

- * 312-39 Questions and Answers Updated Frequently
- * 312-39 Practice Questions Verified by Expert Senior Certified Staff
- * 312-39 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 312-39 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 312-39 Practice Test Here](#)