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
The Syslog message severity levels are labelled from level 0 to level 7. What does level 0 indicate?

A. Alert
B. Notification
C. Emergency
D. Debugging

Answer: B

NEW QUESTION 4
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. Cloud, MSSP Managed
B. Self-hosted, Jointly Managed
C. Self-hosted, MSSP Managed
D. Self-hosted, Self-Managed

Answer: C

NEW QUESTION 5
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 6
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. Dissemination and Integration
B. Processing and Exploitation
C. Collection
D. Analysis and Production

Answer: B

NEW QUESTION 7
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 8
Which of the following event detection techniques uses User and Entity Behavior Analytics (UEBA)?

A. Rule-based detection
B. Heuristic-based detection
C. Anomaly-based detection
D. Signature-based detection

Answer: C

NEW QUESTION 9
Which of the following stage executed after identifying the required event sources?

A. Identifying the monitoring Requirements
B. Defining Rule for the Use Case
C. Implementing and Testing the Use Case
D. Validating the event source against monitoring requirement

Answer: D

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
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

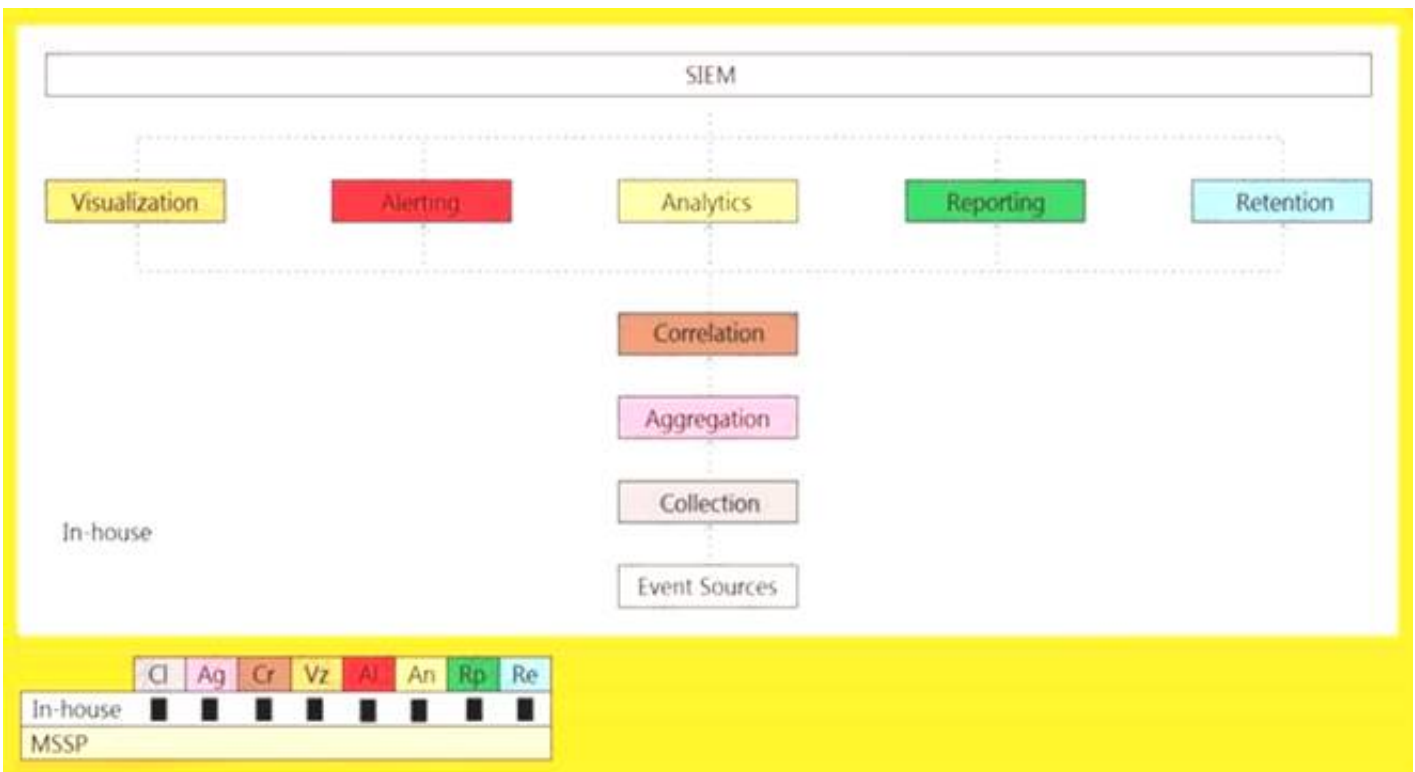
Answer: C

NEW QUESTION 13
Which of the following threat intelligence is used by a SIEM for supplying the analysts with context and "situational awareness" by using threat actor TTPs, malware campaigns, tools used by threat actors.
* 1. Strategic threat intelligence
* 2.Tactical threat intelligence
* 3.Operational threat intelligence
* 4.Technical threat intelligence

A. 2 and 3
B. 1 and 3
C. 3 and 4
D. 1 and 2

Answer: A

NEW QUESTION 16
An organization is implementing and deploying the SIEM with following capabilities.



What kind of SIEM deployment architecture the organization is planning to implement?

A. Cloud, MSSP Managed
B. Self-hosted, Jointly Managed
C. Self-hosted, Self-Managed
D. Self-hosted, MSSP Managed

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 22
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 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 27
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 31
What is the process of monitoring and capturing all data packets passing through a given network using different tools?

A. Network Scanning

B. DNS Footprinting
C. Network Sniffing
D. Port Scanning

Answer: C

NEW QUESTION 34
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: B

NEW QUESTION 36
Which of the following factors determine the choice of SIEM architecture?

A. SMTP Configuration
B. DHCP Configuration
C. DNS Configuration
D. Network Topology

Answer: C

NEW QUESTION 40
Rinni, SOC analyst, while monitoring IDS logs detected events shown in the figure below.

What does this event log indicate?

A. Directory Traversal Attack
B. XSS Attack
C. SQL Injection Attack
D. Parameter Tampering Attack

Answer: D

NEW QUESTION 45
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. 1 and 2
B. 2 and 3
C. 1 and 4
D. 3 and 1

Answer: C

NEW QUESTION 48
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 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

NEW QUESTION 52
Which of the following Windows features is used to enable Security Auditing in Windows?

A. Bitlocker
B. Windows Firewall
C. Local Group Policy Editor
D. Windows Defender

Answer: C

NEW QUESTION 57
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

NEW QUESTION 59
Which of the following is a correct flow of the stages in an incident handling and response (IH&R) process?

A. Containment –> Incident Recording –> Incident Triage –> Preparation –> Recovery –> Eradication –> Post-Incident Activities
B. Preparation –> Incident Recording –> Incident Triage –> Containment –> Eradication –> Recovery –> Post-Incident Activities
C. Incident Triage –> Eradication –> Containment –> Incident Recording –> Preparation –> Recovery –> Post-Incident Activities
D. Incident Recording –> Preparation –> Containment –> Incident Triage –> Recovery –> Eradication –> Post-Incident Activities

Answer: B

NEW QUESTION 63
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 67
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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 FirstTry

* 312-39 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year