EC-Council

Exam Questions 312-39

Certified SOC Analyst (CSA)

NEW QUESTION 1
Which of the following Windows Event Id will help you monitors file sharing across the network?

A. 7045
B. 4625
C. 5140
D. 4624

Answer: C

NEW QUESTION 2
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 3
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 4
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 5
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 6
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 7
Which of the following directory will contain logs related to printer access?

A. /var/log/cups/Printer_log file
B. /var/log/cups/access_log file
C. /var/log/cups/accesslog file
D. /var/log/cups/Printeraccess_log file

Answer: A

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. Rate Limiting
B. Egress Filtering
C. Ingress Filtering
D. Throttling

Answer: C

NEW QUESTION 9
What does the HTTP status codes 1XX represents?

A. Informational message
B. Client error
C. Success
D. Redirection

Answer: A

NEW QUESTION 10
Which of the following steps of incident handling and response process focus on limiting the scope and extent of an incident?

A. Containment
B. Data Collection
C. Eradication
D. Identification

Answer: A

NEW QUESTION 10
Identify the HTTP status codes that represents the server error.

A. 2XX
B. 4XX
C. 1XX
D. 5XX

Answer: D

NEW QUESTION 12
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 15
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 17
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 19
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: C

NEW QUESTION 24
Which of the following formula is used to calculate the EPS of the organization?

A. EPS = average number of correlated events / time in seconds
B. EPS = number of normalized events / time in seconds
C. EPS = number of security events / time in seconds
D. EPS = number of correlated events / time in seconds

Answer: A

NEW QUESTION 26
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 29
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. DHCP/Logs capable of maintaining IP addresses or hostnames with IPtoName resolution.
B. IIS/Web Server logs with IP addresses and user agent IPtouseragent resolution.
C. DNS/ Web Server logs with IP addresses.
D. Apache/ Web Server logs with IP addresses and Host Name.

Answer: D

NEW QUESTION 30
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 Recording
C. Incident Classification
D. Incident Prioritization

Answer: C

NEW QUESTION 33
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 38
John, SOC analyst wants to monitor the attempt of process creation activities from any of their Windows endpoints.
Which of following Splunk query will help him to fetch related logs associated with process creation?

A. index=windows LogName=Security EventCode=4678 NOT (Account_Name=*$) .. ..
B. index=windows LogName=Security EventCode=4688 NOT (Account_Name=*$) .. .. ..
C. index=windows LogName=Security EventCode=3688 NOT (Account_Name=*$) .. .. ..
D. index=windows LogName=Security EventCode=5688 NOT (Account_Name=*$) ... ...

Answer: B

NEW QUESTION 42
......

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

100% Actual & Verified — Instant Download, Please Click
Order The 312-39 Practice Test Here