312-39Q&As

Certified SOC Analyst (CSA)

Pass EC-COUNCIL 312-39 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/312-39.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

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

Correct Answer: C

Reference: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=5140

QUESTION 2

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

Correct Answer: D

QUESTION 3

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

Correct Answer: D

Reference: https://blog.eccouncil.org/phases-of-an-incident-response-plan/

QUESTION 4

Which of the following is a set of standard guidelines for ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection?

A. FISMA

B. HIPAA

C. PCI-DSS

D. DARPA

Correct Answer: C

Reference: https://library.educause.edu/topics/policy-and-law/pci-dss

QUESTION 5

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

Correct Answer: A

QUESTION 6

Which of the following factors determine the choice of SIEM architecture?

A. SMTP Configuration

B. DHCP Configuration

C. DNS Configuration

D. Network Topology

Correct Answer: C

QUESTION 7

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

Correct Answer: A

QUESTION 8

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

Correct Answer: A

Reference: https://www.eccouncil.org/wp-content/uploads/2019/02/ECIH-V2-Brochure.pdf

QUESTION 9

What type of event is recorded when an application driver loads successfully in Windows?

A. Error

B. Success Audit

C. Warning

D. Information

Correct Answer: D

Reference: https://www.manageengine.com/network-monitoring/Eventlog_Tutorial_Part_I.html

QUESTION 10

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

Correct Answer: C

Reference: https://www.moheri.gov.om/userupload/Policy/IT%20Risk%20Management%20Framework.pdf

(17)

QUESTION 11

Jane, a security analyst, while analyzing IDS logs, detected an event matching Regex /((\%3C)|)/|.

What does this event log indicate?

A. Directory Traversal Attack

B. Parameter Tampering Attack

C. XSS Attack

D. SQL Injection Attack

Correct Answer: C

Reference: https://books.google.com.pk/books?id=PDR4nOAP8qUCandpg=PA87andlpg=PA87anddq=regex+/((%5C%253C)%7C)/%7Candsource=blandots=kOBHNfJmtqandsig=ACfU3U2CG_hELc1HMb1chdc9OS4ooXPIMgandhl=enandsa=Xandved=2ahUKEwjYwJmlt_buAhUFShUIHTBNAs8Q6AEwBXoECAUQAw#v=onepageandqandf=false

QUESTION 12

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

Correct Answer: B

QUESTION 13

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

Correct Answer: B

QUESTION 14

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

Correct Answer: A

QUESTION 15

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

Correct Answer: C