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.geekcert.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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

Correct Answer: A

Reference: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=001f5e09-88b4-4a9a-b310-4c20578eecf9andCommunityKey=1ecf5f55-9545-44d6-b0f44e4a7f5f5e68andtab=librarydocuments

QUESTION 2

Identify the event severity level in Windows logs for the events that are not necessarily significant, but may indicate a possible future problem.

A. Failure Audit

B. Warning

C. Error

D. Information

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/windows/win32/eventlog/event-types

QUESTION 3

Which of the following is a Threat Intelligence Platform?

A. SolarWinds MS

B. TC Complete

C. Keepnote

D. Apility.io

Correct Answer: A

Reference: https://www.esecurityplanet.com/products/threat-intelligence-platforms/

QUESTION 4

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

Correct Answer: C

Reference: https://en.wikipedia.org/wiki/Black_hole_(networking)#:~:text=In%20networking%2C%20black%20holes%20refer,not%20reach%20its%20intended%20recipient.

QUESTION 5

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

Correct Answer: C

Reference: https://www.iso.org/standard/44716.html