312-39^{Q&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

SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

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 2

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 3

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 4

Which of the following formula represents the risk levels?

A. Level of risk = Consequence x Severity

B. Level of risk = Consequence x Impact

C. Level of risk = Consequence x Likelihood

D. Level of risk = Consequence x Asset Value

Correct Answer: B

QUESTION 5

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

Correct Answer: C

Reference: https://resources.infosecinstitute.com/topic/how-to-audit-windows-10-application-logs/

[312-39 PDF Dumps](link)   [312-39 Practice Test](link)   [312-39 Braindumps](link)