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.pass2lead.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

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

Correct Answer: A

QUESTION 2

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

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

If the SIEM generates the following four alerts at the same time:

I. Firewall blocking traffic from getting into the network alerts

II. SQL injection attempt alerts

III. Data deletion attempt alerts

IV. Brute-force attempt alerts

Which alert should be given least priority as per effective alert triaging?

A. III

B. IV

C. II

D. I

Correct Answer: D

QUESTION 5

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