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.passapply.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

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 2

Which of the following service provides phishing protection and content filtering to manage the Internet experience on and off your network with the acceptable use or compliance policies?

A. Apility.io

B. Malstrom

C. OpenDNS

D. I-Blocklist

Correct Answer: C

Reference: https://www.spamtitan.com/web-filtering/category/cybersecurity-advice/

QUESTION 3

Which of the following are the responsibilities of SIEM Agents?

1.

Collecting data received from various devices sending data to SIEM before forwarding it to the central engine.

2.

Normalizing data received from various devices sending data to SIEM before forwarding it to the central engine.

3.

Co-relating data received from various devices sending data to SIEM before forwarding it to the central engine.

4.

Visualizing data received from various devices sending data to SIEM before forwarding it to the central engine.

A. 1 and 2

B. 2 and 3

C. 1 and 4

D. 3 and 1

Correct Answer: C

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

Juliea a SOC analyst, while monitoring logs, noticed large TXT, NULL payloads. What does this indicate?

A. Concurrent VPN Connections Attempt

B. DNS Exfiltration Attempt

C. Covering Tracks Attempt

D. DHCP Starvation Attempt

Correct Answer: B

Reference: https://www.google.com/url?sa=tandrct=jandq=andesrc=sandsource=webandcd=andved=2ahUKEwj8gZaKq_PuAhWGi1wKHfQTC0oQFjAAegQIARADandurl=https%3A%2F%2Fconf.splunk.com%2Fsession%2F2014%2Fconf2014_FredWilmotSanfordOwings_Splunk_Security.pdfandusg=AOvVaw3ZLfzGqM-VUG7xKtze67ac