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

Charline is working as an L2 SOC Analyst. One day, an L1 SOC Analyst escalated an incident to her for further investigation and confirmation. Charline, after a thorough investigation, confirmed the incident and assigned it with an initial priority.

What would be her next action according to the SOC workflow?

A. She should immediately escalate this issue to the management

B. She should immediately contact the network administrator to solve the problem

C. She should communicate this incident to the media immediately

D. She should formally raise a ticket and forward it to the IRT

Correct Answer: B

QUESTION 2

What does Windows event ID 4740 indicate?

A. A user account was locked out.

B. A user account was disabled.

C. A user account was enabled.

D. A user account was created.

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4740#:~:text=For%204740(S)%3A%20A,Security%20ID"%20is%20not%20SYSTEM.

QUESTION 3

John as a SOC analyst is worried about the amount of Tor traffic hitting the network. He wants to prepare a dashboard in the SIEM to get a graph to identify the locations from where the TOR traffic is coming. Which of the following data source will he use to prepare the dashboard?

A. DHCP/Logs capable of maintaining IP addresses or hostnames with IPtoName resolution.

B. IIS/Web Server logs with IP addresses and user agent IPtouseragent resolution.

C. DNS/ Web Server logs with IP addresses.

D. Apache/ Web Server logs with IP addresses and Host Name.

Correct Answer: D

QUESTION 4

Bonney\\'s system has been compromised by a gruesome malware.

What is the primary step that is advisable to Bonney in order to contain the malware incident from spreading?

A. Complaint to police in a formal way regarding the incident

B. Turn off the infected machine

C. Leave it to the network administrators to handle

D. Call the legal department in the organization and inform about the incident

Correct Answer: B

QUESTION 5

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