

EC Council

112-56

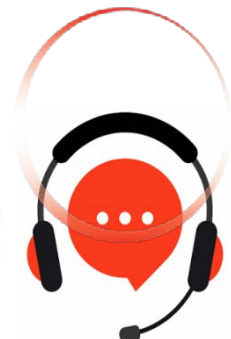
EC-Council SOC Essentials (SCE)

For More Information – Visit link below:

<https://www.examsempire.com/>

Product Version

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/112-56>

Latest Version: 6.0

Question: 1

What does triaging alerts involve in the context of a SOC?

- A. Deciding the priority and severity of alerts
- B. Sorting emails by importance
- C. Organizing social events
- D. Categorizing company products

Answer: A

Question: 2

During which phase is the root cause of an incident thoroughly investigated?

- A. Preparation
- B. Identification
- C. Eradication
- D. Post-Incident Analysis

Answer: D

Question: 3

Identify a common characteristic of 'insider attacks'.

- A. They are always intentional and malicious
- B. They originate outside the organization
- C. They may involve employees abusing their access rights
- D. They are less harmful than external attacks

Answer: C

Question: 4

How does a 'Trojan horse' typically present itself?

- A. As a legitimate software
- B. As an email from a friend
- C. As a network service
- D. As an antivirus update

Answer: A

Question: 5

Identify the network topology that is highly fault-tolerant due to the direct connection between each pair of nodes.

- A. Ring
- B. Mesh
- C. Star
- D. Bus

Answer: B

Question: 6

Which aspect of SOC focuses on the people involved in operations?

- A. Infrastructure
- B. Processes
- C. Technologies
- D. People

Answer: D

Question: 7

How does threat hunting differ from automated threat detection?

- A. Threat hunting is a reactive process based solely on known threats
- B. Threat hunting is a proactive and iterative approach to search for hidden threats
- C. Threat hunting uses only automated tools without human intervention
- D. Threat hunting is focused on improving team morale

Answer: B

Question: 8

Which SOC model is particularly useful for organizations with limited security budgets?

- A. Fully outsourced SOC
- B. In-house SOC
- C. Hybrid SOC
- D. Virtual SOC

Answer: A

Question: 9

What type of network is typically used to connect devices within a single building?

- A. WAN
- B. MAN
- C. LAN
- D. PAN

Answer: C

Question: 10

Which protocol operates at the Internet layer of the TCP/IP model?

- A. Ethernet
- B. ARP
- C. UDP
- D. IP

Answer: D

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

**Check our Customer Testimonials and ratings
available on every product page.**

Visit our website.

<https://examsempire.com/>