Free Questions for 312-39 by vceexamstest

Shared by Anthony on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

A- Apility.io

B- Malstrom

C- OpenDNS

D- I-Blocklist

Answer:

C

Question 2

Question Type: MultipleChoice

InfoSystem LLC, a US-based company, is establishing an in-house SOC. John has been given the responsibility to finalize strategy, policies, and procedures for the SOC.

Identify the job role of John.

Options:

A- Security Analyst -- L1

B- Chief Information Security Officer (CISO)

C- Security Engineer

D- Security Analyst -- L2

Answer:

B

Question 3

Question Type: MultipleChoice

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

1. 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?

Options:

A- III

B- IV

C- II

D- 1

Answer:

D

Question 4

Question Type: **MultipleChoice**

Which of the following threat intelligence helps cyber security professionals such as security operations managers, network operations center and incident responders to understand how the adversaries are expected to perform the attack on the organization, and the technical capabilities and goals of the attackers along with the attack vectors?

Options:

A- Analytical Threat Intelligence

B- Operational Threat Intelligence

C- Strategic Threat Intelligence

D- Tactical Threat Intelligence

Answer:

D

Question 5

Question Type: **MultipleChoice**

Which of the following data source will a SOC Analyst use to monitor connections to the insecure ports?

Options:

A- Netstat Data

B- DNS Data

C- IIS Data

D- DHCP Data

Answer:

A

Question 6

Question Type: **MultipleChoice**

Which of the following steps of incident handling and response process focus on limiting the scope and extent of an incident?

Options:

A- Containment

B- Data Collection

C- Eradication

D- Identification

Answer:

A

Question 7

Question Type: **MultipleChoice**

Which of the following stage executed after identifying the required event sources?

Options:

A- Identifying the monitoring Requirements

B- Defining Rule for the Use Case

C- Implementing and Testing the Use Case

D- Validating the event source against monitoring requirement

Answer:

D