200-201 Q&As

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

Pass Cisco 200-201 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/200-201.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

Which metric should be used when evaluating the effectiveness and scope of a Security Operations Center?

A. The average time the SOC takes to register and assign the incident.

B. The total incident escalations per week.

C. The average time the SOC takes to detect and resolve the incident.

D. The total incident escalations per month.

Correct Answer: C

QUESTION 2

An information security analyst inspects the .pcap file and observes encrypted unusual SSH traffic flow over nonstandard ports. Which technology makes this behavior feasible?

A. NAT

B. tunneling

C. P2P

D. TOR

Correct Answer: B

QUESTION 3

How does agentless monitoring differ from agent-based monitoring?

A. Agentless can access the data via API. while agent-base uses a less efficient method and accesses log data through WMI.

B. Agent-based monitoring is less intrusive in gathering log data, while agentless requires open ports to fetch the logs

C. Agent-based monitoring has a lower initial cost for deployment, while agentless monitoring requires resource-intensive deployment.

D. Agent-based has a possibility to locally filter and transmit only valuable data, while agentless has much higher network utilization

Correct Answer: D

Agent-based monitoring: With agent-based monitoring, software agents are installed on the monitored systems or devices. These agents collect data locally, perform filtering or preprocessing of the data, and then transmit the relevant or valuable information to the monitoring system. Agent-based monitoring allows for local processing and filtering, which

can reduce network utilization by only transmitting essential data.

Agentless monitoring: Agentless monitoring, on the other hand, does not require software agents to be installed on the monitored systems or devices. Instead, it relies on leveraging existing protocols and interfaces, such as APIs (Application Programming Interfaces) or SNMP (Simple Network Management Protocol), to remotely access and retrieve monitoring data from the target systems. Agentless monitoring generally involves higher network utilization as the monitoring system needs to gather data from remote systems over the network.

QUESTION 4

Which two elements of the incident response process are stated in NIST Special Publication 800-61 r2? (Choose two.)

A. detection and analysis

B. post-incident activity

C. vulnerability management

D. risk assessment

E. vulnerability scoring

Correct Answer: AB

Reference: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

QUESTION 5

What is a difference between a threat and a risk?

A. A threat can be people, property, or information, and risk is a probability by which these threats may bring harm to the business.

B. A risk is a flaw or hole in security, and a threat is what is being used against that flaw.

C. A risk is an intersection between threat and vulnerabilities, and a threat is what a security engineer is trying to protect against.

D. A threat is a sum of risks, and a risk itself represents a specific danger toward the asset.

Correct Answer: C