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.leads4pass.com/200-201.html

100% Passing Guarantee
100% Money Back Assurance

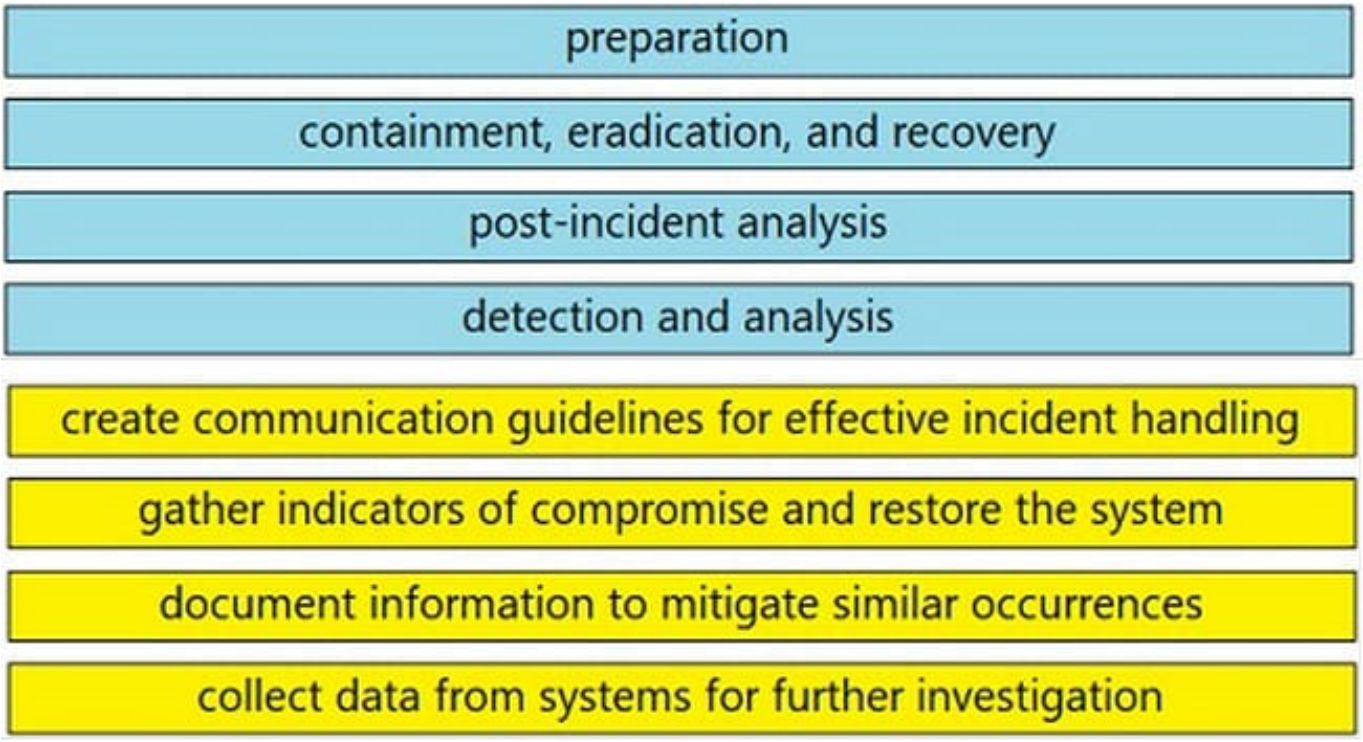
Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

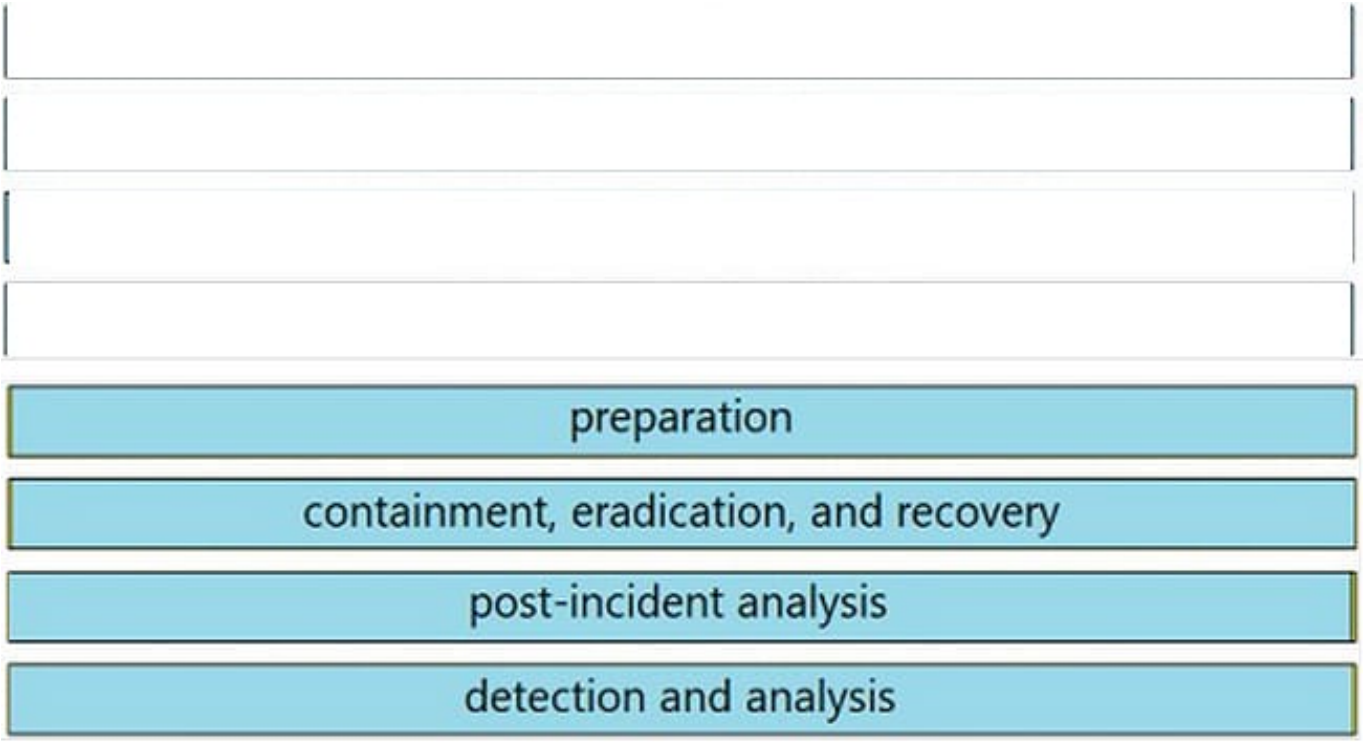
DRAG DROP

Drag and drop the elements from the left into the correct order for incident handling on the right.

Select and Place:



Correct Answer:



QUESTION 2

What is the difference between inline traffic interrogation and traffic mirroring?

A. Inline interrogation is less complex as traffic mirroring applies additional tags to data.

B. Traffic mirroring copies the traffic rather than forwarding it directly to the analysis tools

C. Inline replicates the traffic to preserve integrity rather than modifying packets before sending them to other analysis tools.

D. Traffic mirroring results in faster traffic analysis and inline is considerably slower due to latency.

Correct Answer: B

Inline inspection - Inline traffic interrogation is a technique in which traffic flows through a device that inspects the traffic and makes decisions about how to handle it. The inspection takes place in real-time and in-line with the traffic flow.

Traffic mirroring - Traffic mirroring, also known as port mirroring or SPAN (Switched Port Analyzer), is a technique for forwarding a copy of network traffic to a monitoring device. The copy of the traffic is sent to a separate tool for analysis, security or other purposes.

QUESTION 3

What are two denial of service attacks? (Choose two.)

A. MITM

B. TCP connections

C. ping of death

D. UDP flooding

E. code red

Correct Answer: CD

QUESTION 4

How does an attacker observe network traffic exchanged between two users?

A. port scanning

B. man-in-the-middle

C. command injection

D. denial of service

Correct Answer: B

QUESTION 5

What should an engineer use to aid the trusted exchange of public keys between user tom0411976943 and dan1968754032?

A. central key management server

B. web of trust

C. trusted certificate authorities

D. registration authority data

Correct Answer: C