

# 210-255<sup>Q&As</sup>

Cisco Cybersecurity Operations

## Pass Cisco 210-255 Exam with 100% Guarantee

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

<https://www.leads4pass.com/210-255.html>

100% Passing Guarantee  
100% Money Back Assurance

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

- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers



## QUESTION 1

What is accomplished in the identification phase of incident handling?

- A. determining the responsible user
- B. identifying source and destination IP addresses
- C. defining the limits of your authority related to a security event
- D. determining that a security event has occurred

Correct Answer: D

---

## QUESTION 2

Which of the following are the three broad categories of cybersecurity investigations?

- A. Public, private, and individual investigations
- B. Judiciary, private, and individual investigations
- C. Public, private, and corporate investigations
- D. Government, corporate, and private investigations

Correct Answer: A

---

## QUESTION 3

Which element is part of an incident response plan?

- A. organizational approach to incident response
- B. organizational approach to security
- C. disaster recovery
- D. backups

Correct Answer: A

---

## QUESTION 4

Which component of the NIST SP800-61 r2 incident handling strategy reviews data?

- A. preparation
- B. detection and analysis

C. containment, eradication, and recovery

D. post-incident analysis

Correct Answer: D

---

## QUESTION 5

Which CVSSv3 Attack Vector metric value requires the attacker to physically touch or manipulate the vulnerable component?

A. local

B. physical

C. network

D. adjacent

Correct Answer: B

[210-255 PDF Dumps](#)

[210-255 Study Guide](#)

[210-255 Braindumps](#)