



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

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





QUESTION 1

What is the functionality of an IDS?

- A. forensic tool used to perform an in-depth analysis and debugging
- B. software or device which monitors and identifies malicious network activity
- C. device or software that detects and blocks suspicious files
- D. endpoint protection software that prevents viruses and malware

Correct Answer: B

QUESTION 2

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 3

Which type of data consists of connection level, application-specific records generated from network traffic?

- A. transaction data
- B. location data
- C. statistical data
- D. alert data

Correct Answer: A

QUESTION 4

What matches the regular expression `c(rgr)+e`?

- A. `c(rgr)e`



B. crgrgre

C. crgr+e

D. ce

Correct Answer: B

QUESTION 5

Which risk approach eliminates activities posing a risk exposure?

A. risk acknowledgment

B. risk reduction

C. risk retention

D. risk avoidance

Correct Answer: D

[200-201 VCE Dumps](#)

[200-201 Study Guide](#)

[200-201 Braindumps](#)