

210-255^{Q&As}

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

Which of the following statements is true about processes and threads?

- A. Each thread starts with a single process, known as the primary process, but can also create additional processes from any of its services.
- B. Each service starts with a single hive, known as the primary hive, but can also create additional threads from any of its hives.
- C. Each process starts with a single thread, known as the primary thread, but can also create additional threads from any of its threads.
- D. Each hive starts with a single thread, known as the primary thread, but can also create additional threads from any of its threads.

Correct Answer: C

QUESTION 2

Which technology generates events utilizing proxy logs?

- A. Firepower
- B. Email Security Appliance
- C. Stealthwatch
- D. Web Security Appliance

Correct Answer: D

QUESTION 3

How do you verify that one of your hosts is potentially compromised based on their communication destinations?

- A. Search the communication destinations of the host in the Talos IP and Domain Reputation Center.
- B. Analyze how much traffic the host sent and received from each IP address or domain.
- C. See if any Stealthwatch alarms were triggered for the host communicating with internal hosts.
- D. Check the Firepower appliance to see if malicious files were downloaded.

Correct Answer: A

QUESTION 4

Which identifies both the source and destination location?

- A. IP address
- B. URL
- C. ports
- D. MAC address

Correct Answer: A

QUESTION 5

Choose the option that best describes NIST data integrity

- A. use only sha-1
- B. use only md5
- C. you must hash data and backup and compare hashes
- D. no need to hash data and backup and compare hashes

Correct Answer: C

[Latest 210-255 Dumps](#)

[210-255 VCE Dumps](#)

[210-255 Braindumps](#)