



# 210-250<sup>Q&As</sup>

Cisco Cybersecurity Fundamentals

## Pass Cisco 210-250 Exam with 100% Guarantee

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

<https://www.pass4itsure.com/210-250.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 two of the following statements best describe the reasons that web proxy logs are important? (Choose two.)

- A. Web proxy logs can show the activity of CnC bot traffic or evidence of dropper files.
- B. Web proxy logs can only show legitimate HTTP traffic.
- C. Web proxy devices such as the Cisco WSA can decrypt HTTPS traffic and enter it into the log for review later.
- D. Web proxies TCP\_HIT log messages can identify DoS attacks.

Correct Answer: AC

---

#### QUESTION 2

Which definition of a daemon on Linux is true?

- A. error check right after the call to fork a process
- B. new process created by duplicating the calling process
- C. program that runs unobtrusively in the background
- D. set of basic CPU instructions

Correct Answer: C

---

#### QUESTION 3

Which security monitoring data type requires the most storage space?

- A. full packet capture
- B. transaction data
- C. statistical data
- D. session data

Correct Answer: A

---

#### QUESTION 4

Cisco AMP for Endpoints takes advantage of which of the following?

- A. Telemetry from big data, continuous analysis, and advanced analytics provided by Cisco ESA and WSA in order to detect, analyze, and stop advanced malware across endpoints



- B. Advanced analytics provided by antivirus software in order to detect, analyze, and stop advanced malware across endpoints
- C. Telemetry from big data, continuous analysis, and advanced analytics provided by Cisco threat intelligence in order to detect, analyze, and stop advanced malware across endpoints
- D. Telemetry from big data, continuous analysis, and advanced analytics provided by Cisco next-generation firewalls in order to detect, analyze, and stop advanced malware across endpoints.

Correct Answer: C

---

#### QUESTION 5

Which three of the following options are methods that are used by an attacker while gathering network data? (Choose three.)

- A. unplug network devices
- B. packet sniffer
- C. ping sweeps
- D. port scans

Correct Answer: BCD

[210-250 PDF Dumps](#)

[210-250 Exam Questions](#)

[210-250 Braindumps](#)