



600-199^{Q&As}

Securing Cisco Networks with Threat Detection and Analysis

Pass Cisco 600-199 Exam with 100% Guarantee

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

<https://www.geekcert.com/600-199.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

When investigating potential network security issues, which two pieces of useful information would be found in a syslog message? (Choose two.)

- A. product serial number
- B. MAC address
- C. IP address
- D. product model number
- E. broadcast address

Correct Answer: BC

QUESTION 2

As a part of incident response, which action should be performed?

- A. watch to see if the incident reoccurs
- B. custody of information
- C. maintain data security and custody for future forensics use
- D. classify the problem

Correct Answer: C

QUESTION 3

Which two measures would you recommend to reduce the likelihood of a successfully executed network attack from the Internet? (Choose two.)

- A. Completely disconnect the network from the Internet.
- B. Deploy a stateful edge firewall.
- C. Buy an insurance policy against attack-related business losses.
- D. Implement a password management policy for remote users.

Correct Answer: BD

QUESTION 4

Which action is recommended to prevent an incident from spreading?



- A. Shut down the switch port.
- B. Reboot the system.
- C. Reboot the switch.
- D. Reboot the router.

Correct Answer: A

QUESTION 5

Which is considered to be anomalous activity?

- A. an alert context buffer containing traffic to amazon.com
- B. an alert context buffer containing SSH traffic
- C. an alert context buffer containing an FTP server SYN scanning your network
- D. an alert describing an anonymous login attempt to an FTP server

Correct Answer: C

[600-199 Study Guide](#)

[600-199 Exam Questions](#)

[600-199 Braindumps](#)



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

<https://www.geekcert.com/allproducts>

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



 <p>One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p>Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © geekcert, All Rights Reserved.