600-199 Q&As

Securing Cisco Networks with Threat Detection and Analysis

QUESTION 1

Which publication from the ISO covers security incident response?

A. 1918

B. 2865

C. 27035

D. 25012

Correct Answer: C

QUESTION 2

Which describes the best method for preserving the chain of evidence?

A. Shut down the machine that is infected, remove the hard drive, and contact the local authorities.

B. Back up the hard drive, use antivirus software to clean the infected machine, and contact the local authorities.

C. Identify the infected machine, disconnect from the network, and contact the local authorities.

D. Allow user(s) to perform any business-critical tasks while waiting for local authorities.

Correct Answer: C

QUESTION 3

Which step should be taken first when a server on a network is compromised?

A. Refer to the company security policy.

B. Email all server administrators.

C. Determine which server has been compromised.

D. Find the serial number of the server.

Correct Answer: A

QUESTION 4

In what sequence do the proper eradicate/recovery steps take place? 1) Re-image2) Restore3) Patch4) Backup

A. 1, 2, 3, 4

B. 4, 3, 2, 1

C. 1, 3, 4, 2

D. 4, 1, 3, 2

Correct Answer: D

QUESTION 5

Which would be classified as a remote code execution attempt?

A. OLE stack overflow detected

B. null login attempt

C. BitTorrent activity detected

D. IE ActiveX DoS

Correct Answer: A

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

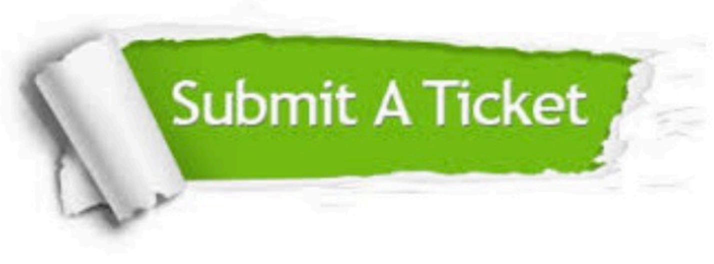
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

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:



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.

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.

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.

Any charges made through this site will appear as Global Simulators Limited.