C2150-196^{Q&As}

IBM Security QRadar SIEM V7.1 Implementation

Pass IBM C2150-196 Exam with 100% Guarantee

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

https://www.geekcert.com/C2150-196.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IBM Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

What are three default charting options available within the Report wizard? (Choose three.)

A. Delta

B. Flows

C. Identity

D. Anomaly

E. Events/Logs

F. Asset Vulnerabilities

Correct Answer: BEF

QUESTION 2

What must be done first when changing the network settings on a console in a multi- system deployment?

A. install new patches

B. reset the SIM model

C. remove all managed hosts

D. install a new license for the new IP address

Correct Answer: C

QUESTION 3

Which IBM Security QRadar SIEM V7.1 DSM protocol supports the collection of Microsoft SMTPI OWA, and message tracking logs?

A. MicrosoftIS

B. Microsoft DHCP

C. Microsoft Exchange

D. Microsoft Security Event Log

Correct Answer: C

QUESTION 4

When adding a managed host using encryption, which network port must be openbi- directionally between the console and new host?

A. 22

B. 115

C. 443

D. 445

Correct Answer: A

QUESTION 5

Which statement best describes the advantages of implementing NetFlow monitoring?

A. If antivirus software signatures fail todetect malware infection, NetFlow monitoring can help identify malware propagation by using its own signatures.

B. NetFlow provides the ability to detect suspicious log activity. Each log contains the number of bytes and packets transferred by both the SRC and DST allowing for volume- based reporting of network traffic.

C. NetFlow provides deep packet inspection, from layers three to seven of the OSI model, increasing visibility into applications; whereas, traditional flow monitoring only provides visibility at layers three and four.

D. NetFlow provides the ability to detect suspicious network activity, e.g. identify a potential botnet when Local to Remote traffic is matched to an IP address configured in a corresponding Remote Network group.

Correct Answer: D

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: