# C2150-196$^{\text{Q\&As}}$

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.pass4lead.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**

The ip_context_menu.xml file was edited in order to access additional details for selected IP addresses. Which service must be restarted for the changes to take effect?

A. tomcat

B. webmin

C. syslog-ng

D. hostcontext

Correct Answer: A

**QUESTION 2**

By default how often are events forwarded from an event collector to an event processor?

A. every hour

B. continuously

C. every 2 hours

D. it does not forward until the forwarding schedule is set

Correct Answer: B

**QUESTION 3**

When creating a new IBM Security QRadar SIEMV7.1 user account, the administrator did not give access to the log source group (called MS Domain Security Logs) that contains Microsoft Security Event logs. What happens if the user attempts to run a shared saved search for failed login attempts to a domain?

A. The user is not able to see any results from that search.

B. Since the user is part of the domain, they are able to see the data in the search results.

C. The user is notified that they do not have the proper permissions to run that search and are requested to contact their administrator.

D. The search will run but since the user was not given access to the MS Domain Security Logs group, the user cannot see results from those log sources contained in that group.

Correct Answer: D

**QUESTION 4**

Which group of tests is used to test the sequence of rulesthat have been triggered by events or flows?

A. DateyTime tests

B. Behavioral tests

C. Common Property tests

D. Function Sequence tests

Correct Answer: D

**QUESTION 5**

Which method does WinCollect use to collect Windows 2008 events?

A. It uses Windows file sharing to pull the Windows 2008 event logs.

B. It uses the syslog forwarding facility of Windows 2008 Event Logger.

C. It uses the native Windows 2008 event log API to access the log records.

D. It uses SNARE toconvert the Windows 2008 events to syslog messages.

Correct Answer: C

C2150-196 PDF Dumps C2150-196 Exam Questions C2150-196 Braindumps

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

# Try our product !

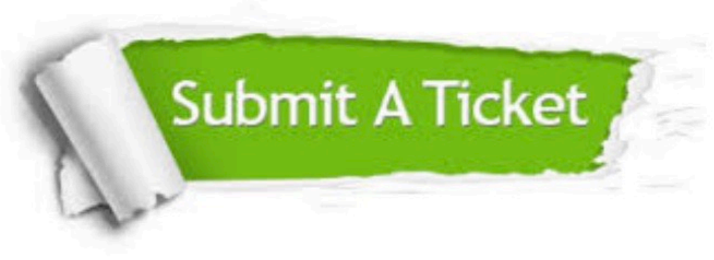
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

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.pass4lead.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.
All trademarks are the property of their respective owners.
Copyright © pass4lead, All Rights Reserved.