



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.lead4pass.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

Given that ICMP pings from all hosts are dropped, which rule(s) allows ICMP pings and responses only from and to host 10.35.100.23?

- A. iptables -A INPUT-p icmp -j ACCEPT
- B. iptables -A OUTPUT-s 10.35.100.23-p icmp -j ACCEPT
- C. iptables -A OUTPUT-p icmp--icmp-type echo-reply-j ACCEPT
- D. iptables -A INPUT-s 10.35.100.23 -p icmp --icmp-type echo-request-i ACCEPT

Correct Answer: D

QUESTION 2

What is a defining characteristic of an asymmetric flow?

- A. It is evidenced by receiving varying length NetFlow records.
- B. It describes network traffic that is configured to take alternate paths for inbound and outbound traffic.
- C. It describes where traffic volumes are significantly skewed towards either inbound or outbound communication.
- D. It describes network traffic that commonly resolves to a Superflow in the IBM Security QRadar QFlow appliance.

Correct Answer: B

QUESTION 3

Prior to installing IBM Security QRadar SIEM V7.1 on customer provided hardware, Red Hat Enterprise Linux must be installed. SELinux must be set to which option?

- A. Enforce
- B. Enabled
- C. Disabled
- D. Permissive

Correct Answer: C

QUESTION 4

What would be considerations for defining a Threshold Rule in the Automated Anomaly Analysis?

- A. a change value and a length of time for accumulation



- B. a time window during the day and a moving averagesmoothing value
- C. a time interval for accumulation and a relative weight for the current observation
- D. a seasonal component, a trend component, and a delta or incremental change value

Correct Answer: A

QUESTION 5

How are values mapped in a LSXto parse data from a payload for a UDSM?

- A. quotes (\"')
- B. back tics(`)
- C. regular expressions
- D. comma separated (,)

Correct Answer: C

[Latest C2150-196 Dumps](#)

[C2150-196 VCE Dumps](#)

[C2150-196 Exam Questions](#)



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.lead4pass.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 © lead4pass, All Rights Reserved.