



VMware

5V0-94.22

VMware Carbon Black Cloud Enterprise EDR Skills

Questions & Answers PDF

For More Information:

<https://www.certswarrior.com/>

Features:

- 90 Days Free Updates
- 30 Days Money Back Guarantee
- Instant Download Once Purchased
- 24/7 Online Chat Support
- Its Latest Version

Latest Version: 6.0

Question: 1

Which of the following is a use case of VMware Carbon Black Enterprise EDR in supporting compliance and legal investigations?

Response:

- A. Providing a secure messaging platform for internal communications
- B. Generating real-time alerts for stock market fluctuations
- C. Capturing and storing detailed logs of all endpoint activities
- D. Automating the distribution of security policies

Answer: C

Question: 2

During a system upgrade, what is crucial to ensure continuity and minimize downtime?

Response:

- A. Immediate shutdown of all services
- B. Performing upgrades during peak hours
- C. Backing up critical data
- D. Ignoring deprecated features

Answer: C

Question: 3

What design principle does Carbon Black Cloud follow to ensure scalability in threat data analysis?

Response:

- A. Monolithic architecture
- B. Peer-to-peer network topology
- C. Service-oriented architecture
- D. Elastic cloud computing

Answer: D

Question: 4

An essential part of managing operational tasks in VMware Carbon Black Cloud is understanding the impact of dismissing alerts. Dismissing an alert:

Response:

- A. Permanently deletes all data associated with the alert
- B. Marks the alert as reviewed, keeping it accessible for future reference
- C. Automatically resolves any underlying security issues
- D. Notifies the threat actor that their activity has been detected

Answer: B

Question: 5

How can administrators prioritize IOCs within a report to focus on the most critical threats?

Response:

- A. By assigning a severity level to each IOC
- B. Using color codes for different IOCs
- C. Organizing IOCs alphabetically
- D. Grouping IOCs by the date they were added

Answer: A

Question: 6

When configuring a firewall, what is a best practice?

Response:

- A. Allow all inbound traffic by default
- B. Disable logging for improved performance
- C. Implement least privilege access rules
- D. Use a single, complex password for all access

Answer: C

Question: 7

In managing a high-priority security incident, which Live Response command is most crucial for isolating an endpoint?

Response:

- A. netstat to review active connections
- B. kill to terminate suspicious processes
- C. isolate to prevent network communication
- D. cp to copy important files for analysis

Answer: C

Question: 8

When noticing an increase in false positives related to encrypted traffic analysis, what is the best course of action for tuning the watchlist?

Response:

- A. Ignoring all encrypted traffic to reduce false positives
- B. Refining the watchlist to better differentiate between normal and suspicious encrypted traffic
- C. Decreasing the overall sensitivity of the watchlist
- D. Focusing solely on unencrypted traffic for monitoring

Answer: B

Question: 9

Given a scenario where an environment experiences seasonal traffic peaks, how should the watchlist be adjusted?

Response:

- A. By temporarily disabling the watchlist during peak periods
- B. Adjusting the watchlist criteria to account for expected changes in traffic patterns
- C. Keeping the watchlist criteria static for consistency
- D. Focusing the watchlist on perimeter defenses only

Answer: B

Question: 10

Which of the following are notification methods supported by VMware Carbon Black Cloud?
(Choose two)

Response:

-
- A. SMS messages
 - B. Email alerts
 - C. Push notifications to mobile devices
 - D. Automated phone calls

Answer: B,C



CERTSWARRIOR

FULL PRODUCT INCLUDES:

Money Back Guarantee



Instant Download after Purchase



90 Days Free Updates



PDF Format Digital Download



24/7 Live Chat Support



Latest Syllabus Updates



For More Information – Visit link below:

<https://www.certswarrior.com>

16 USD Discount Coupon Code: U89DY2AQ