Ultimate IT Test Preparation Material

Splunk

SPLK-5001
Splunk Certified Cybersecurity Defense Analyst

- **Up to Date products, reliable and verified.**
- **Questions and Answers in PDF Format.**

Full Version Features:

- **90 Days Free Updates**
- **30 Days Money Back Guarantee**
- **Instant Download Once Purchased**
- **24 Hours Live Chat Support**

For More Information:

https://www.testsexpert.com/

- **Product Version**

Visit us at

Latest Version: 6.0

Question: 1

When should adaptive response actions be used in threat hunting?
Response:

A. Adaptive response actions should always be used for any security incident.
B. Adaptive response actions are optional and not necessary for threat hunting.
C. Adaptive response actions should only be used for low-risk threats.
D. Adaptive response actions should be used to automate responses to security incidents.

Answer: D

Question: 2

How does Splunk Enterprise Security (ES) interact with Common Information Model (CIM) and Data Models?
Response:

A. CIM is used to accelerate Data Models for faster searching
B. CIM provides a framework for categorizing data, and Data Models are used to normalize the data
C. CIM and Data Models are the same thing and can be used interchangeably
D. Data Models are used to enrich the data stored in CIM

Answer: B

Question: 3

Which Splunk resource provides pre-built content for assessing data sources and threat intelligence capabilities?
Response:

A. Splunk Enterprise Security (ES)
B. Splunk Security Essentials
C. Splunk Lantern
D. Splunk Add-on for Microsoft Exchange

Answer: B

Question: 4

In Splunk SPL, which command is used to filter and group results based on specific fields?
Response:

A. eval
B. filter
C. stats
D. fields

Answer: C

Question: 5

What is the main difference between a Denial of Service (DoS) attack and a Distributed Denial of Service (DDoS) attack?
Response:

A. The DoS attack targets a single device, while the DDoS attack targets multiple devices.
B. The DoS attack is carried out by a single threat actor, while the DDoS attack involves multiple threat actors.
C. The DoS attack aims to exfiltrate sensitive data, while the DDoS attack aims to disrupt services by overwhelming resources.
D. The DoS attack is illegal, while the DDoS attack is a legal form of cybersecurity testing.

Answer: A

Question: 6

In the context of cybersecurity, what does the term "SIEM" stand for?
Response:

A. Security Incident and Event Management.
B. Secure Internet and Email Management.
C. Systematic Intrusion and Event Monitoring.
D. Safety Intranet and Event Maintenance.

Answer: A

Question: 7

How are SOAR playbooks used in threat hunting?
Response:

A. To define and test hypotheses related to security incidents.
B. To monitor the network for anomalies and indicators of compromise.
C. To automate response actions based on specific security scenarios.
D. To analyze historical data for patterns of abnormal behavior.

Answer: C

Question: 8

Which of the following are correct statements about Splunk Enterprise Security annotations?
Response:

A. Annotations help enrich data with additional information.
B. Annotations can be used to mark notable events in the investigation.
C. Annotations are used for visual representation only and do not affect search results.
D. Annotations are applied automatically to all incoming data.

Answer: A,B

Question: 9

What is the recommended approach when handling a security incident?
Response:

A. Take immediate actions based on intuition.
B. Ignore the incident if it seems minor.
C. Follow a pre-defined incident response plan.
D. Rely solely on antivirus software.

Answer: C

Question: 10

What do frameworks and standards help accomplish in the cybersecurity landscape?
Response:

A. Create new vulnerabilities.
B. Improve interoperability and consistency.

C. Decrease the number of data sources.
D. Promote isolation between security teams.

Answer: B

For More Information – **Visit link below:**

https://www.testsexpert.com/

16$ Discount Coupon: 9M2GK4NW

Features:

- Money Back Guarantee……..……...…. 

- 100% Course Coverage…… 

- 90 Days Free Updates…… 

- Instant Email Delivery after Order……