Splunk

SPLK-5001
Splunk Certified Cybersecurity Defense Analyst

For More Information – Visit link below:
https://www.examsempire.com/

Product Version

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

https://examsempire.com/

Latest Version: 6.1

Question: 1

Which of the following are examples of common cyber industry controls and frameworks?
Response:

A. NIST Cybersecurity Framework
B. ISO/IEC 27001
C. CIS Controls
D. OWASP Top Ten

Answer: A,B,C

Question: 2

In Splunk Enterprise Security, which framework is used to represent information about assets and their attributes?
Response:

A. CIM
B. Data Models
C. Asset framework
D. Identity framework

Answer: C

Question: 3

What is one of the best practices for efficient searching in Splunk?
Response:

A. Using vague search terms to get broader results.
B. Using the 'NOT' operator to exclude all events.
C. Using wildcards in every search term.
D. Utilizing field filters to narrow down results.

Answer: D

Question: 4

What is the primary purpose of the TSTATS command in Splunk?
Response:

A. To create a time-based statistical summary of events.
B. To extract fields from unstructured data using regular expressions.
C. To perform a search and replace operation on events.
D. To look up additional information from an external data source.

Answer: A

Question: 5

Which of the following are common social engineering tactics used by attackers?
(Select all that apply)
Response:

A. Phishing
B. Patching
C. Shoulder surfing
D. Firewall configuration

Answer: A,C

Question: 6

Which of the following best describes correlation in cybersecurity?
Response:

A. A process of encrypting data to protect it from unauthorized access.
B. A method of combining data from multiple sources to identify meaningful patterns.
C. The act of preventing malware attacks from entering the network.
D. The process of gathering information about potential attackers.

Answer: B

Question: 7

What best describes the motivation behind Advanced Persistent Threats (APTs)?

Response:

A. Random attacks on different targets.
B. Financial gain through ransomware attacks.
C. Short-term disruption of services.
D. Long-term espionage and data exfiltration.

Answer: D

Question: 8

What are common sourcetypes for on-premises deployments in Splunk?
Response:

A. syslog, winEventLog, json
B. cloudTrail, aws:s3, cloudwatch
C. apache, iis, nginx
D. cisco:asa, cisco:ios, juniper:firewall

Answer: A,C,D

Question: 9

Which of the following is a form of social engineering attack?
Response:

A. A distributed denial-of-service (DDoS) attack.
B. A phishing email attempting to trick the recipient into revealing personal information.
C. A network intrusion using a botnet.
D. A direct attempt to exploit a software vulnerability.

Answer: B

Question: 10

What is an "Adaptive Response Action" in Splunk Enterprise Security?
Response:

A. A manual response taken by an analyst in response to a security incident.
B. An automated action taken by Splunk to respond to a security threat.
C. A predefined action that requires approval from management to execute.
D. An action taken to escalate a notable event to a higher priority.

Answer: B

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/