Splunk
SPLK-5001
Splunk Certified Cybersecurity Defense Analyst

Latest Version: 10.1

Question: 1

Which of the following is the primary benefit of using the CIM in Splunk?

A. It allows for easier correlation of data from different sources.
B. It improves the performance of search queries on raw data.
C. It enables the use of advanced machine learning algorithms.
D. It automatically detects and blocks cyber threats.

Answer: A

Question: 2

Which of the following data sources would be most useful to determine if a user visited a recently identified malicious website?

A. Active Directory Logs
B. Web Proxy Logs
C. Intrusion Detection Logs
D. Web Server Logs

Answer: B

Question: 3

Which of the following is a tactic used by attackers, rather than a technique?

A. Gathering information about a target.
B. Establishing persistence with a scheduled task.
C. Using a phishing email to gain initial access.
D. Escalating privileges via UAC bypass.

Answer: A

Question: 4

Enterprise Security has been configured to generate a Notable Event when a user has quickly authenticated from multiple locations between which travel would be impossible. This would be considered what kind of an anomaly?

A. Access Anomaly
B. Identity Anomaly
C. Endpoint Anomaly
D. Threat Anomaly

Answer: A

Question: 5

An analyst is investigating a network alert for suspected lateral movement from one Windows host to another Windows host. According to Splunk CIM documentation, the IP address of the host from which the attacker is moving would be in which field?

A. host
B. dest
C. src_nt_host
D. src_ip

Answer: D

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer