Boost up Your Certification Score

cisco

SPK-501

Splunk Certified Cybersecurity Defense Analyst

Exams Boost

For More Information – Visit link below:

https://www.examsboost.com/

Product Version

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

Visit us at: https://www.examsboost.com/test/spk-501

Latest Version: 6.0

Question: 1

Which of the Enterprise Security frameworks provides additional automatic context and correlation to fields that exist within raw data?

A. Adaptive Response
B. Threat Intelligence
C. Risk
D. Asset and Identity

Answer: D

Explanation:
The Asset and Identity framework correlates event fields with asset and identity records to add context during a search.

Question: 2

An analyst is not sure that all of the potential data sources at her company are being correctly or completely utilized by Splunk and Enterprise Security.
Which of the following might she suggest using, in order to perform an analysis of the data types available and some of their potential security uses?

A. Splunk ITSI
B. Security Essentials
C. SOAR
D. Splunk Intelligence Management

Answer: B

Explanation:
Splunk Security Essentials helps analysts map data sources to security content. Its Data Source Check dashboard can verify whether the sources needed for an example are available.

Question: 3

Splunk SOAR uses what feature to automate security workflows so that analysts can spend more time performing analysis and investigation?

A. Workbooks
B. Analytic Stories

C. Adaptive Actions
D. Playbooks

Answer: D

Explanation:
Playbooks link actions into an automated workflow that can support triage and investigation.

Question: 4

Which of the following Splunk Enterprise Security features allows industry frameworks such as CIS Critical Security Controls, MITRE ATT&CK, and the Lockheed Martin Cyber Kill Chain® to be mapped to Correlation Search results?

A. Annotations
B. Playbooks
C. Comments
D. Enrichments

Answer: A

Explanation:
Annotations add industry framework mappings to correlation search results, giving analysts context for the detection.

Question: 55

An organization is using Risk-Based Alerting (RBA). During the past few days, a user account generated multiple risk observations. Splunk refers to this account as what type of entity?

A. Risk Factor
B. Risk Index
C. Risk Analysis
D. Risk Object

Answer: D

Explanation:
A user account can be a risk object. Enterprise Security associates risk events and scores with that object when evaluating risk-based alerts.

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

