ExamsNest

Your Ultimate Exam Preparation Hub

Vendor: Splunk

Code: SPLK-5001

Exam: Splunk Certified Cybersecurity Defense Analyst

https://www.examsnest.com/exam/splk-5001/

QUESTIONS & ANSWERS

DEMO VERSION

Version: 4.0

Question: 1

Which Enterprise Security framework provides a mechanism for running preconfigured actions within the Splunk platform or integrating with external applications?

A. Asset and Identity

B. Notable Event

C. Threat Intelligence

D. Adaptive Response

Answer: D

Question: 2

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

Question: 3

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: 4

Tactics, Techniques, and Procedures (TTPs) are methods or behaviors utilized by attackers. In which framework are these categorized?

A. NIST 800-53

B. ISO 27000

C. CIS18

D. MITRE ATT&CK

Answer: D

Question: 5

A threat hunter executed a hunt based on the following hypothesis:

As an actor, I want to plant rundll32 for proxy execution of malicious code and leverage Cobalt Strike for Command and Control.

Relevant logs and artifacts such as Sysmon, netflow, IDS alerts, and EDR logs were searched, and the hunter is confident in the conclusion that Cobalt Strike is not present in the company's environment.

Which of the following best describes the outcome of this threat hunt?

A. The threat hunt was successful because the hypothesis was not proven.

B. The threat hunt failed because the hypothesis was not proven.

C. The threat hunt failed because no malicious activity was identified.

D. The threat hunt was successful in providing strong evidence that the tactic and tool is not present in the environment.

Answer: D

ExamsNest

Your Ultimate Exam Preparation Hub

Thank You for trying the PDF Demo

Vendor: Splunk

Code: SPLK-5001

Exam: Splunk Certified Cybersecurity Defense Analyst

https://www.examsnest.com/exam/splk-5001/

Use Coupon "**SAVE15**" for extra 15% discount on the purchase of Practice Test Software. Test your Exam preparation with actual exam questions.

Start Your Preparation