Splunk SPLK-5001

Splunk Cybersecurity Defense Analyst Certification Questions & Answers

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

SPLK-5001

Splunk Certified Cybersecurity Defense Analyst

60 Questions Exam – 700 / 1000 Cut Score – Duration of 75 minutes

Table of Contents:

Discover More about the Splunk SPLK-5001 Certification

Are you interested in passing the Splunk SPLK-5001 exam? First discover, who benefits from the SPLK-5001 certification. The SPLK-5001 is suitable for a candidate if he wants to learn about Enterprise Security. Passing the SPLK-5001 exam earns you the Splunk Certified Cybersecurity Defense Analyst title.

While preparing for the SPLK-5001 exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The SPLK-5001 PDF contains some of the most valuable preparation tips and the details and instant access to useful **SPLK-5001 study materials just at one click.**

Splunk SPLK-5001 Cybersecurity Defense Analyst Certification Details:

Exam Name	Splunk Certified Cybersecurity Defense Analyst
Exam Code	SPLK-5001
Exam Price	$130 (USD)
Duration	75 mins
Number of Questions	60
Passing Score	700 / 1000
Schedule Exam	**Pearson VUE**
Sample Questions	**Splunk Cybersecurity Defense Analyst Sample Questions**
Practice Exam	**Splunk SPLK-5001 Certification Practice Exam**

Splunk SPLK-5001 Syllabus:

Topic	Details	Weights
The Cyber Landscape, Frameworks, and Standards	- Summarize the organization of a typical SOC and the tasks belonging to Analyst, Engineer and Architect roles. - Recognize common cyber industry controls, standards and frameworks and how Splunk incorporates those frameworks. - Describe key security concepts surrounding information assurance	10%

Topic	Details	Weights
	including confidentiality, integrity and availability and basic risk management.	
Threat and Attack Types, Motivations, and Tactics	- Recognize common types of attacks and attack vectors. - Define common terms including supply chain attack, ransomware, registry, exfiltration, social engineering, DoS, DDoS, bot and botnet, C2, zero trust, account takeover, email compromise, threat actor, APT, adversary. - Identify the common tiers of Threat Intelligence and how they might be applied to threat analysis. - Outline the purpose and scope of annotations within Splunk Enterprise Security. - Define tactics, techniques and procedures and how they are regarded in the industry.	20%
Defenses, Data Sources, and SIEM Best Practices	- Identify common types of cyber defense systems, analysis tools and the most useful data sources for threat analysis. - Describe SIEM best practices and basic operation concepts of Splunk Enterprise Security, including the interaction between CIM, Data Models and acceleration, Asset and Identity frameworks, and common CIM fields that may be used in investigations. - Describe how Splunk Security Essentials and Splunk Enterprise Security can be used to assess data sources, including common sourcetypes for on-prem and cloud based deployments and how to find content for a given sourcetype.	20%
Investigation, Event Handling, Correlation, and Risk	- Describe continuous monitoring and the five basic stages of investigation according to Splunk. - Explain the different types of analyst performance metrics such as MTTR and dwell time. - Demonstrate ability to recognize	20%

Topic	Details	Weights
	common event dispositions and correctly assign them. - Define terms and aspects of Splunk Enterprise Security and their uses including SPL, Notable Event, Risk Notable, Adaptive Response Action, Risk Object, Contributing Events. - Identify common built-in dashboards in Enterprise Security and the basic information they contain. - Understand and explain the essentials of Risk Based Alerting, the Risk framework and creating correlation searches within Enterprise Security.	
SPL and Efficient Searching	- Explain common SPL terms and how they can be used in security analysis, including TSTATS, TRANSACTION, FIRST/LAST, REX, EVAL, FOREACH, LOOKUP, and MAKERESULTS. - Give examples of Splunk best practices for composing efficient searches. - Identify SPL resources included within ES, Splunk Security Essentials, and Splunk Lantern.	20%
Threat Hunting and Remediation	- Identify threat hunting techniques including configuration, modeling (anomalies), indicators, and behavioral analytics. - Define long tail analysis, outlier detection, and some common steps of hypothesis hunting with Splunk. - Determine when to use adaptive response actions and configure them as needed. - Explain the use of SOAR playbooks and list the basic ways they can be triggered from Enterprise Security.	10%

Broaden Your Knowledge with Splunk SPLK-5001 Sample Questions:

Question: 1

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

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: 2

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

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

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: 4

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

a) Create new vulnerabilities.
b) Improve interoperability and consistency.
c) Decrease the number of data sources.
d) Promote isolation between security teams.

Answer: b

Question: 5

When should adaptive response actions be used in threat hunting?

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: 6

How are SOAR playbooks used in threat hunting?

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: 7

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

a) Splunk Security Essentials
b) Splunk Enterprise Security (ES)
c) Splunk Lantern
d) Splunk Add-on for Microsoft Exchange

Answer: a

Question: 8

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

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: 9

What is the recommended approach when handling a security incident?

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

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

a) eval
b) filter
c) fields
d) stats

Answer: d

Avail the Study Guide to Pass Splunk SPLK-5001 Cybersecurity Defense Analyst Exam:

- Find out about the SPLK-5001 syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **Splunk SPLK-5001 syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk out the best plan for yourself to cover each part of the syllabus in a hassle-free manner.

- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the **Cybersecurity Defense Analyst training.** Joining the Splunk provided training for this Splunk certification exam helps a candidate to strengthen his practical knowledge base from the certification.
- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **Splunk SPLK-5001 sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. SPLK-5001 practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

Passing the Splunk SPLK-5001 exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.

Here Is the Trusted Practice Test for the Splunk SPLK-5001 Certification

CertFun.Com is here with all the necessary details regarding the SPLK-5001 exam. We provide authentic practice tests for the SPLK-5001 exam. What do you gain from these practice tests? You get to experience the real exam-like questions made by industry experts and get a scope to improve your performance in the actual exam. Rely on CertFun.Com for rigorous, unlimited two-month attempts on the **SPLK-5001 practice tests**, and gradually build your confidence. Rigorous practice made many aspirants successful and made their journey easy towards grabbing the Splunk Certified Cybersecurity Defense Analyst.

Start Online practice of Splunk SPLK-5001 Exam by visiting URL
https://www.certfun.com/splunk/splk-5001-splunk-certified-cybersecurity-defense-analyst