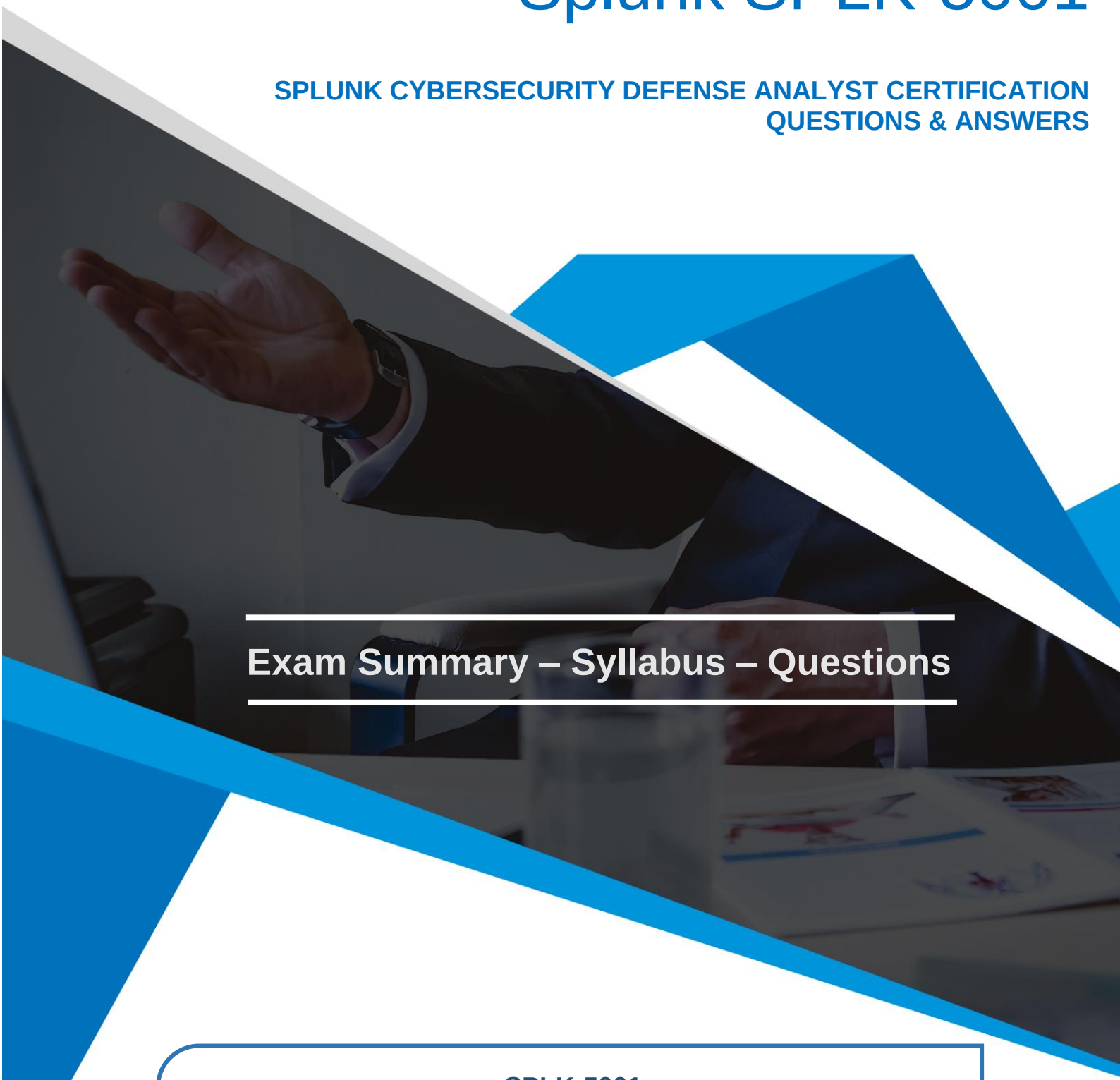
Splunk SPLK-5001

SPLUNK CYBERSECURITY DEFENSE ANALYST CERTIFICATION QUESTIONS & ANSWERS



Exam Summary – Syllabus – Questions

SPLK-5001

Splunk Certified Cybersecurity Defense Analyst

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

www.CertFun.com

Table of Contents

Know Your SPLK-5001 Certification Well:

The SPLK-5001 is best suitable for candidates who want to gain knowledge in the Splunk Enterprise Security. Before you start your SPLK-5001 preparation you may struggle to get all the crucial Cybersecurity Defense Analyst materials like SPLK-5001 syllabus, sample questions, study guide.

But don't worry the SPLK-5001 PDF is here to help you prepare in a stress free manner.

The PDF is a combination of all **your queries like**-

- What is in the SPLK-5001 syllabus?
- How many questions are there in the SPLK-5001 exam?
- Which Practice test would help me to pass the SPLK-5001 exam at the first attempt?

Passing the SPLK-5001 exam makes you Splunk Certified Cybersecurity Defense Analyst. Having the Cybersecurity Defense Analyst certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

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	66
Passing Score	700 / 1000
Schedule Exam	**Pearson VUE**
Sample Questions	**Splunk Cybersecurity Defense Analyst Sample Questions**
Practice Exam	**Splunk SPLK-5001 Certification Practice Exam**

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 including confidentiality, integrity and availability and basic risk management.	10%
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	20%

Topic	Details	Weights
	deployments and how to find content for a given sourcetype.	
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 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.	20%
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%

Splunk SPLK-5001 Sample Questions:

Question: 1

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: 2

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: 3

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

Question: 4

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: 5

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: 6

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: 7

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: 8

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: 9

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: 10

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

Study Guide to Crack Splunk Cybersecurity Defense Analyst SPLK-5001 Exam:

- Getting details of the SPLK-5001 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the SPLK-5001 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the Splunk provided training for SPLK-5001 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the SPLK-5001 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on SPLK-5001 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for SPLK-5001 Certification

Make CertFun.com your best friend during your Splunk Certified Cybersecurity Defense Analyst exam preparation. We provide authentic practice tests for the SPLK-5001 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual SPLK-5001 exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the SPLK-5001 exam.

Start Online Practice of SPLK-5001 Exam by Visiting URL

https://www.certfun.com/splunk/splk-5001-splunk-certified-cybersecurity-defense-analyst