



SPLUNK SPLK-2003 STUDY GUIDE

PDF

Grab the Splunk SOAR Automation Developer Certification
PDF Questions & Answers

[Details of the Exam-Syllabus-Questions](#)

SPLK-2003

[Splunk SOAR Certified Automation Developer](#)

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

www.CertFun.com

Table of Contents:

Get an Overview of the SPLK-2003 Certification:.....	2
Why Should You Earn the Splunk SPLK-2003 Certification?	2
What Is the Splunk SPLK-2003 SOAR Automation Developer Certification Exam Structure?.....	2
Enhance Knowledge with SPLK-2003 Sample Questions:	3
What Study Guide Works Best in Acing the Splunk SPLK- 2003 SOAR Automation Developer Certification?	6
Explore the Syllabus Topics and Learn from the Core:	6
Make Your Schedule:	6
Get Expert Advice from the Training:.....	6
Get Access to the PDF Sample Questions:	6
Avoid Dumps and Utilize the Splunk SPLK-2003 Practice Test:	7

Get an Overview of the SPLK-2003 Certification:

Who should take the [SPLK-2003 exam](#)? This is the first question that comes to a candidate's mind when preparing for the SOAR Automation Developer certification. The SPLK-2003 certification is suitable for candidates who are keen to earn knowledge on the SOAR and grab their Splunk SOAR Certified Automation Developer. When it is about starting the preparation, most candidates get confused regarding the study materials and study approach. But SPLK-2003 study guide PDF is here to solve the problem. SPLK-2003 PDF combines some effective sample questions and offers valuable tips to pass the exam with ease.

Why Should You Earn the Splunk SPLK-2003 Certification?

There are several reasons why one should grab the SPLK-2003 certification.

- The SOAR Automation Developer certification proves to be one of the most recognized certifications.
- The certification badge proves the knowledge of the candidate regarding subject matters and makes his resume presentable to potential candidates.
- Thus earning the [Splunk SOAR Certified Automation Developer](#) is a powerful qualification for a prosperous career.

What Is the Splunk SPLK-2003 SOAR Automation Developer Certification Exam Structure?

Exam Name	Splunk SOAR Certified Automation Developer
Exam Code	SPLK-2003
Exam Price	\$130 (USD)
Duration	60 mins
Number of Questions	45
Passing Score	700 / 1000

Schedule Exam	Pearson VUE
Sample Questions	Splunk SOAR Automation Developer Sample Questions
Practice Exam	Splunk SPLK-2003 Certification Practice Exam

Enhance Knowledge with SPLK-2003 Sample Questions:

Question: 1

When using case management in a SOAR platform, how does it contribute to collaboration and knowledge sharing among incident response teams?

- a) By automatically running playbooks based on predefined actions
- b) By integrating with external security tools and threat intelligence feeds
- c) By generating real-time reports on incident trends and patterns
- d) By providing a centralized location to track and manage incident-related data

Answer: d

Question: 2

The architecture of a SOAR platform typically involves the integration of which key components?

- a) Firewalls, intrusion detection systems, and antivirus software
- b) Threat intelligence feeds, analytics engines, and email clients
- c) Orchestration engine, automation capabilities, and case management
- d) Operating systems, databases, and network devices

Answer: c

Question: 3

How are filters utilized in a SOAR platform?

- a) Filters prevent unauthorized access to the platform.
- b) Filters are used to automate the data ingestion process.
- c) Filters facilitate the integration of external security tools into the platform.
- d) Filters are applied to search results to narrow down the displayed data.

Answer: d

Question: 4

What action is taken when invoking child playbooks from a parent playbook in a SOAR platform?

- a) Child playbooks are merged into a single playbook for execution.
- b) Child playbooks are executed sequentially in a predefined order.
- c) Child playbooks are executed in parallel concurrently.
- d) Child playbooks are automatically shared with all platform users.

Answer: c

Question: 5

Which search feature in a SOAR platform allows analysts to search for specific keywords within incident notes and case descriptions?

- a) Full-text search
- b) Metadata search
- c) Natural language search
- d) Advanced search

Answer: a

Question: 6

In the context of a SOAR platform, what is the primary benefit of using the visual playbook editor?

- a) It automatically runs playbooks without human intervention.
- b) It provides real-time monitoring of system health.
- c) It enables users to design and modify playbooks graphically.
- d) It generates automated reports on incident trends and patterns.

Answer: c

Question: 7

What is the primary purpose of using the Analyst Queue in a SOAR platform?

- a) To manage the installation and upgrade options of the platform
- b) To create custom filters for data analysis
- c) To prioritize and assign security incidents to analysts
- d) To configure data ingestion assets for real-time monitoring

Answer: c

Question: 8

When configuring data ingestion assets in a SOAR platform, what is the main purpose of defining data parsers?

- a) Ensuring data is encrypted during transmission
- b) Converting raw data into a standardized format for analysis
- c) Assigning data access permissions to specific users
- d) Facilitating data replication across multiple servers

Answer: b

Question: 9

Which of the following actions can be taken by analysts in the Case Management and Workbooks section of Splunk SOAR?

(Select all that apply)

- a) Closing cases and marking them as resolved
- b) Creating and editing playbooks
- c) Adding notes and comments to cases
- d) Assigning cases to other analysts

Answer: a, c, d

Question: 10

How can a user test a new playbook before deploying it in a production environment in a SOAR platform?

- a) By using the visual playbook editor to design the playbook workflow.
- b) By executing the playbook on actual incidents and monitoring the results.
- c) By customizing severity levels and status values within the playbook.
- d) By using the I2A2 design methodology to validate the playbook design.

Answer: b

What Study Guide Works Best in Acing the Splunk SPLK-2003 SOAR Automation Developer Certification?

The SPLK-2003 study guide is a combination of some proven study tips and the combination of all valuable study materials like sample questions, syllabus and practice tests in one place.

Explore the Syllabus Topics and Learn from the Core:

If you are determined to earn success in the SOAR Automation Developer exam, getting in full touch of the [syllabus](#) is mandatory. During preparation, you might not like all syllabus sections or topics, but try to get at least the fundamental knowledge from the sections you don't like. The more you possess knowledge on all syllabus sections, the more is the chance to attempt maximum number of questions during the actual exam.

Make Your Schedule:

Studying and completing the syllabus becomes easier, if you work on the syllabus topics after making a schedule. Your syllabus must mention what areas you want to cover and within what time. Once you make a schedule and follow it regularly, syllabus completion becomes easier and preparation becomes smoother.

Get Expert Advice from the Training:

Do not forget to join the Splunk SPLK-2003 training if it is providing any. Training enhances the practical knowledge of a candidate, which helps them to work well in the practical field during projects.

Get Access to the PDF Sample Questions:

If your study material is in a [PDF format](#) or the materials are mobile-friendly, what could be better than that? Get access to the free sample questions and keep enhancing your knowledge beyond the syllabus.

Avoid Dumps and Utilize the Splunk SPLK-2003 Practice Test:

Why should you rely on practice tests? The reason is simple: you must get familiar with the exam pattern before reaching the exam hall. An aspirant aware of the exam structure and time management during the exam preparation can perform well in the actual exam and attempt the maximum number of questions during the exam.

Many aspirants prefer to read from dumps, but they miss out on the self assessment method. Therefore, SPLK-2003 practice tests always stand out to be the better choice than dumps PDF.

Avail the Proven SPLK-2003 Practice Test for Success!!!

Do you want to pass the SPLK-2003 exam on your first attempt? Stop worrying; we, CertFun.com are here to provide you the best experience during your Splunk SOAR Certified Automation Developer preparation. Try out our free mock tests to get a glimpse of our quality study materials, and build your confidence with the premium [SPLK-2003 practice tests](#). Our expert-designed questions help you to improve performance and pass the exam on your first attempt.