Splunk SPLK-2003

Splunk SOAR Automation Developer Certification Questions & Answers

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

SPLK-2003

Splunk SOAR Certified Automation Developer

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

Table of Contents:

Discover More about the Splunk SPLK-2003 Certification

Are you interested in passing the Splunk SPLK-2003 exam? First discover, who benefits from the SPLK-2003 certification. The SPLK-2003 is suitable for a candidate if he wants to learn about SOAR. Passing the SPLK-2003 exam earns you the Splunk SOAR Certified Automation Developer title.

While preparing for the SPLK-2003 exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The SPLK-2003 PDF contains some of the most valuable preparation tips and the details and instant access to useful **SPLK-2003 study materials just at one click.**

Splunk SPLK-2003 SOAR Automation Developer Certification Details:

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

Splunk SPLK-2003 Syllabus:

Topic	Details	Weights
Deployment, Installation, and Initial Configuration	- Describe SOAR operating concepts - Identify documentation and community resources - Identify installation and upgrade options - Describe SOAR architecture - Configure licenses, administration, and product settings	5%

Topic	Details	Weights
User Management	- Configure authentication options - Add users - Add roles	5%
Apps, Assets, and Playbooks	- Configure apps - Configure assets - Configure data ingestion assets - Configure labels and SLAs - Manage playbooks	5%
Analyst Queue	- Use the Analyst Queue - Use search features - Create filters - Use the indicator view	5%
The Investigation Page	- Use the Investigation page to work on events - Manually run actions and examine action results - Manually run playbooks - Use the file tab to store related files	10%
Case Management and Workbooks	- Use case management for complex investigations - Use workbooks - Mark items as evidence	5%
Customizations	- Customize severity levels - Customize CEF fields - Customize status values - Customize workbooks - Add global custom fields to containers	5%
System Maintenance	- Run reports - Use system health displays - Examine health logs	5%
Introduction to Playbooks	- Understand automation best practices - Describe playbook capabilities - Determine available app actions - Use I2A2 design methodology	5%
Visual Playbook Editor	- Use the visual playbook editor - Execute actions from a playbook - Test new playbooks	5%
Logic, Filters, and User Interaction	- Use decision blocks - Use filter blocks to process data - Describe the use of different join options - Interact with users during playbook execution	5%

Topic	Details	Weights
Formatted Output and Data Access	- Use Format blocks to structure data - Understand the structure of action results - Compose datapaths to access data - Use the utility block to modify containers	5%
Modular Playbook Development	- Design modular solutions with interacting playbooks - Invoke child playbooks from a parent - Exchange data between playbooks	5%
Custom Lists and Data Routing	- Create custom lists - Access lists from playbooks - Use filters to control data flow	5%
Configuring External Splunk Search	- Describe the benefits of externalizing search to Splunk - Configure the SOAR instance for externalization - Configure the Splunk instance for externalization - Use reindex to push existing content to the Splunk instance - Use the Splunk app for Phantom Reporting	5%
Integrating SOAR into Splunk	- Install the Splunk App for SOAR Export - Send Enterprise Security notables to SOAR - Install and configure the Splunk app in SOAR - Use Splunk search from playbooks	10%
Custom Coding	- Describe when and when not to use the global block - Use custom function blocks - Write and test custom SOAR code	5%
Using REST	- Describe the capabilities of SOAR REST API - Use Django queries to search for data in SOAR - Use SOAR REST from other systems to access SOAR data	5%

Broaden Your Knowledge with Splunk SPLK-2003 Sample Questions:

Question: 1

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: 2

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: 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 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: 5

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: 6

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: 7

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: 8

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: 9

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: 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

Avail the Study Guide to Pass Splunk SPLK-2003 SOAR Automation Developer Exam:

- Find out about the SPLK-2003 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-2003 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 **SOAR Automation Developer 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-2003 sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. SPLK-2003 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-2003 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.