Splunk SOAR Certified Automation Developer

The Splunk SOAR Certified Automation Developer exam is the final step towards completion of the Splunk SOAR Certified Automation Developer certification track—formerly referred to as Splunk Phantom Certified Admin.

45 Questions	Professional-Level	60* Minutes

Total exam time* ***includes 3 minutes* *to review the* ***exam agreement.***

Exam Content

The following topics are general guidelines for the content likely to be included on the exam; however, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

1.0 Deployment, Installation, and Initial Configuration 5%

1.1 Describe SOAR operating concepts
1.2 Identify documentation and community resources
1.3 Identify installation and upgrade options
1.4 Describe SOAR architecture
1.5 Configure licenses, administration, and product settings

2.0 User Management 5%

2.1 Configure authentication options
2.2 Add users
2.3 Add roles

3.0 Apps, Assets, and Playbooks 5%

3.1 Configure apps
3.2 Configure assets
3.3 Configure data ingestion assets
3.4 Configure labels and SLAs
3.5 Manage playbooks

4.0 Analyst Queue 5%

4.1 Use the Analyst Queue
4.2 Use search features
4.3 Create filters
4.4 Use the indicator view

5.0 The Investigation Page 10%

5.1 Use the Investigation page to work on events
5.2 Manually run actions and examine action results
5.3 Manually run playbooks
5.4 Use the file tab to store related files

6.0 Case Management and Workbooks 5%

6.1 Use case management for complex investigations
6.2 Use workbooks
6.3 Mark items as evidence

7.0 Customizations 5%

7.1 Customize severity levels
7.2 Customize CEF fields
7.3 Customize status values
7.4 Customize workbooks
7.5 Add global custom fields to containers

8.0 System Maintenance 5%

8.1 Run reports
8.2 Use system health displays
8.3 Examine health logs

9.0 Introduction to Playbooks 5%

9.1 Understand automation best practices
9.2 Describe playbook capabilities
9.3 Determine available app actions
9.4 Use I2A2 design methodology

10.0 Visual Playbook Editor 5%

10.1 Use the visual playbook editor
10.2 Execute actions from a playbook
10.3 Test new playbooks

11.0 Logic, Filters, and User Interaction 5%

11.1 Use decision blocks
11.2 Use filter blocks to process data
11.3 Describe the use of different join options
11.4 Interact with users during playbook execution

12.0 Formatted Output and Data Access 5%

12.1 Use Format blocks to structure data
12.2 Understand the structure of action results
12.3 Compose datapaths to access data
12.4 Use the utility block to modify containers

13.0 Modular Playbook Development 5%

13.1 Design modular solutions with interacting playbooks
13.2 Invoke child playbooks from a parent
13.3 Exchange data between playbooks

14.0 Custom Lists and Data Routing 5%

14.1 Create custom lists
14.2 Access lists from playbooks
14.3 Use filters to control data flow

15.0 Configuring External Splunk Search 5%

15.1 Describe the benefits of externalizing search to Splunk
15.2 Configure the SOAR instance for externalization
15.3 Configure the Splunk instance for externalization
15.4 Use reindex to push existing content to the Splunk instance
15.5 Use the Splunk app for Phantom Reporting

16.0 Integrating SOAR into Splunk 10%

16.1 Install the Splunk App for SOAR Export
16.2 Send Enterprise Security notables to SOAR
16.3 Install and configure the Splunk app in SOAR
16.4 Use Splunk search from playbooks

17.0 Custom Coding 5%

17.1 Describe when and when not to use the global block
17.2 Use custom function blocks
17.3 Write and test custom SOAR code

18.0 Using REST 5%

18.1 Describe the capabilities of SOAR REST API
18.2 Use Django queries to search for data in SOAR
18.3 Use SOAR REST from other systems to access SOAR data

Exam Preparation

Candidates may reference the Splunk How-To YouTube Channel, Splunk Docs, and draw from their own Splunk experience.

The following is a ***suggested and non-exhaustive*** list of training from the SOAR Certified Automation Developer Learning Path that may cover topics listed in the above blueprint:

❏ Administering SOAR*

❏ Investigating Splunk Incidents with SOAR*

❏ Developing SOAR Playbooks

❏ Advanced SOAR Implementation

**The 9-hour legacy course, Administering SOAR, also presented the topics covered in this exam. The 9-hour legacy course is now broken down into two shorter courses: Administering SOAR and Investigating Splunk Incidents with SOAR.*

There are no prerequisite exams for this certification.

Schedule this exam >