Splunk Certified Cybersecurity Defense Engineer

The Splunk Certified Cybersecurity Defense Engineer exam is the final step toward completion of the Splunk Certified Cybersecurity Defense Engineer certification.

60 Questions	Professional-Level	75* 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 Data Engineering — 10%

- 1.1 Perform effective data review and analysis.
- 1.2 Create and maintain performant data indexing.
- 1.3 Understand and apply Splunk methods of data normalization.

2.0 Detection Engineering — 40%

- 2.1 Create and tune detections (i.e. Correlation Search).
- 2.2 Incorporate context into detections (i.e. Correlation Search).
- 2.3 Understand and create risk-based modifiers and detections.
- 2.4 Generate effective Notable Events/findings.
- 2.5 Create and maintain a detection lifecycle.

3.0 Building Effective Security Processes and Programs — 20%

- 3.1 Research, incorporate and develop threat intelligence.

3.2 Use common methodologies for risk and detection prioritization.
3.3 Generate documentation and standard operating procedures.

4.0 Automation and Efficiency 20%

4.1 Develop automation and orchestration for standard operating procedures.
4.2 Optimize Case Management.
4.3 Describe and utilize REST APIs.
4.4 Automate responses using SOAR playbooks.
4.5 Compare and validate integrations and automation capabilities of Enterprise Security and SOAR.

5.0 Auditing and Reporting on Security Programs 10%

5.1 Develop and optimize security metrics.
5.2 Build and populate effective security reports.
5.3 Build and populate dashboards for program analytics.

Exam Preparation

Candidates may reference the Splunk YouTube Channel, Splunk Docs, Splunk Blogs especially Splunk Threat Research Team (STRT) and Splunk Boss of the SOC (BOTS) Blog, and draw from their own Splunk experience.

In addition to the courses listed for Splunk Certified Cybersecurity Defense Analyst, the following is a ***suggested and non-exhaustive*** list of training from our Course Catalog that may cover topics listed in the above blueprint:

- ❏ Using Splunk Enterprise Security
- ❏ Developing SOAR Playbooks
- ❏ Introduction to Splunk Security Essentials
- ❏ Administering Splunk Enterprise Security

- ❏ Splunk Enterprise Data Administration

Please Note: *It is strongly recommended that candidates have Power User level knowledge of Splunk Enterprise and familiarity with Administrator tasks in Splunk Cloud or Splunk Enterprise.*

The prerequisite exams for this certification are:

- ☐ Splunk Certified Cybersecurity Defense Analyst