Splunk Certified Cybersecurity Defense Analyst

The Cybersecurity Defense Analyst exam is the final step toward completion of the Splunk Cybersecurity Defense Analyst Certification.

66 Questions	Intermediate-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 The Cyber Landscape, Frameworks, and Standards 10%

1.1 Summarize the organization of a typical SOC and the tasks belonging to Analyst, Engineer and Architect roles.

1.2 Recognize common cyber industry controls, standards and frameworks and how Splunk incorporates those frameworks.

1.3 Describe key security concepts surrounding information assurance including confidentiality, integrity and availability and basic risk management.

2.0 Threat and Attack Types, Motivations, and Tactics 20%

2.1 Recognize common types of attacks and attack vectors.

2.2 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.

2.3 Identify the common tiers of Threat Intelligence and how they might be applied to threat analysis.

2.4 Outline the purpose and scope of annotations within Splunk Enterprise Security.

2.5 Define tactics, techniques and procedures and how they are regarded in the industry.

3.0 Defenses, Data Sources, and SIEM Best Practices 20%

3.1 Identify common types of cyber defense systems, analysis tools and the most useful data sources for threat analysis.

3.2 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.

3.3 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 deployments and how to find content for a given sourcetype.

4.0 Investigation, Event Handling, Correlation, and Risk 20%

4.1 Describe continuous monitoring and the five basic stages of investigation according to Splunk.

4.2 Explain the different types of analyst performance metrics such as MTTR and dwell time.

4.3 Demonstrate ability to recognize common event dispositions and correctly assign them.

4.4 Define terms and aspects of Splunk Enterprise Security and their uses including SPL, Notable Event, Risk Notable, Adaptive Response Action, Risk Object, Contributing Events.

4.5 Identify common built-in dashboards in Enterprise Security and the basic information they contain.

4.6 Understand and explain the essentials of Risk Based Alerting, the Risk framework and creating correlation searches within Enterprise Security.

5.0 SPL and Efficient Searching 20%

5.1 Explain common SPL terms and how they can be used in security analysis, including TSTATS, TRANSACTION, FIRST/LAST, REX, EVAL, FOREACH, LOOKUP, and MAKERESULTS.

5.2 Give examples of Splunk best practices for composing efficient searches.

5.3 Identify SPL resources included within ES, Splunk Security Essentials, and Splunk Lantern.

6.0 Threat Hunting and Remediation 10%

6.1 Identify threat hunting techniques including configuration, modeling (anomalies), indicators, and behavioral analytics.

6.2 Define long tail analysis, outlier detection, and some common steps of hypothesis hunting with Splunk.

6.3 Determine when to use adaptive response actions and configure them as needed.

6.4 Explain the use of SOAR playbooks and list the basic ways they can be triggered from Enterprise Security.

Exam Preparation

Candidates may reference the Splunk How-To YouTube Channel, Splunk Docs, Splunk Boss of the SOC (BOTS) Blog, and draw from their own Splunk experience.

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

- ❏ The Cybersecurity Landscape
- ❏ Understanding Threats and Attacks
- ❏ Security Operations and the Defense Analyst

- ❑ Intro to Splunk
- ❑ Data and Tools for Defense Analysts
- ❑ Introduction to Enterprise Security
- ❑ Search under the hood
- ❑ The Art of investigation
- ❑ SOC Essentials: Investigating with Splunk ES
- ❑ SOC Essentials: Introduction to Threat Hunting
- ❑ Using Splunk Enterprise Security

Just getting started? Below are recommended Splunk How-To Youtube videos:

- ❑ **Introduction to Security Domain (Part 1) - A Little History**
- ❑ **Intro to the Security Domain (Part 2)**

There are no prerequisite exams for this certification but it's recommended to have Power User Level Knowledge of Splunk Enterprise.

Schedule this exam >