# Splunk Certified Cybersecurity Defense Architect

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

**The Splunk Certified Cybersecurity Defense Architect often has 5-7 years of experience with the sections and objectives outlined below. Candidates should be eager to help organizations mature and scale their defense capabilities through strategizing, planning, and building security controls.**

| 120 Questions | Expert-Level | 120* Minutes |
|---|---|---|

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

## Exam Content

**Exam will be launched in its beta phase in March of 2026.*

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 Advanced Threat Intelligence and Analysis | 5% |
|---|---|
| 1.1 Develop and implement customized threat intelligence strategies, including both open source and commercial intelligence providers.<br>1.2 Integrate threat intelligence, including all aspects of the lifecycle (evaluation, curation, maintenance, sources, confidence scoring, etc.), into broader security operations.<br>1.3 Integrate intelligence-informed advanced adversary emulation and threat modeling. | |
| **2.0 Security Data Management** | **20%** |
| 2.1 Explain how to develop and implement integration strategies for data-driven security operations. | |

| | |
|---|---|
| 2.2 Identify data sources critical to cybersecurity operations, such as event sources, identity directories, asset management systems, and vulnerability assessments. This can include non-security data sources, eg. observability tools.<br>2.3 Identify high value / high signal / high noise data sources (e.g. Windows process vs EDR process flow, or network/VPC flow vs packet capture) and how they support security operations use cases.<br>2.4 Identify strategies to monitor an environment that requires nonstandard or out-of-band instrumentation and sensors, e.g. legacy data sources, OT/IC infrastructure environments.<br>2.5 Develop a data lifecycle management strategy, including retention, storage tiering, summarization, data residency, and access control.<br>2.6 Describe the value of data normalization in order to support integration into cybersecurity defense programs, such as security monitoring and threat hunting, e.g. with CIM, CEF.<br>2.7 Implement security analytics strategies beyond traditional SIEM such as advanced techniques like data science, machine learning, behavioral analysis, and AI.<br>2.8 Explain how cybersecurity defense data architectures scale using technologies and capabilities such as data mesh, data lakes, message bus, message routing, and federated search. | |
| **3.0 Advanced Incident Response and Management** | **10%** |
| 3.1 Align cybersecurity incident response with an organization's incident management, change management, and other ITSM/ITIL processes.<br>3.2 Develop a process to manage, coordinate, and communicate responses to large-scale security incidents.<br>3.3 Ensure appropriate technologies and processes are in place to support various forensics investigations. | |
| **4.0 Advanced Automation and Orchestration** | **10%** |
| 4.1 Understand how an organization's technical architectures, e.g. network design, enable or constrain security orchestration.<br>4.2 Develop complex/cross platform automation to orchestrate workflows for cybersecurity operations such as investigation, detection, and incident response.<br>4.3 Describe the benefits of an autonomous SOC, and strategies, processes, and technologies to develop one.<br>4.4 Leverage AI/ML for automated threat detection and response. | |
| **5.0 Scaling Cybersecurity Defenses and DevSecOps** | **15%** |
| 5.1 Develop scalable strategies for agile and DevOps-driven cybersecurity defenses, such as detection as code. | |

| | |
|---|---|
| 5.2 Describe how to integrate security sensors and controls into DevOps workflows.<br>5.3 Describe how to create and leverage a SBOM (Software Bill of Materials) in cybersecurity defenses.<br>5.4 Describe continuous integration & deployment strategies for security data management and engineering solutions.<br>5.5 Describe how to develop and implement patterns, architecture blueprints, and "paved roads" to enable cybersecurity defenses to scale.<br>5.6 Understand how application and infrastructure architectures support cybersecurity defenses. | |
| **6.0 Governance, Risk, and Compliance** | **10%** |
| 6.1 Explain how governmental directives and regulations guidance publications like NIST CSF help influence the design of defense capabilities.<br>6.2 Explain how regulations like GDPR affect cyber defense architecture in relation to data privacy impact on logging, data sovereignty, and data residency.<br>6.3 Explain how industry standard security frameworks (PCI, HIPAA, OT/IC, others) affect cyber defense architecture.<br>6.4 Define how security controls contribute to business operating cost and offsetting risk.<br>6.5 Explain how security technologies and controls fit into the organization's Governance, Risk, and Compliance program and overall risk management. | |
| **7.0 Measuring and Improving Security Program Effectiveness** | **15%** |
| 7.1 Explain how to define, measure, and report on metrics to assess and monitor a security program's effectiveness.<br>7.2 Explain how a business's risk tolerance informs a security program's metrics.<br>7.3 Explain how Continuous Process Improvement can enrich and expand a metrics driven security program's efficacy.<br>7.4 Explain how security controls are continually tested and gaps are remediated. | |
| **8.0 Security Capability Selection, Placement, Configuration** | **15%** |
| 8.1 Identify organizational coverage for prevention, detection, response and recovery capabilities.<br>8.2 Determine how coverage gaps can be mitigated by architecture changes, config changes, or process changes.<br>8.3 Affect organizational and company priorities and budgets based on key capabilities required for security that are aligned to security and business goals.<br>8.4 Explain methodologies used to select security technologies aligned to business need, organizational technology landscape, and security controls.<br>8.5 Define technology implementation strategies to provide desired capabilities. | |

| | | |
|---|---|---|
| 8.6 | Ensure that resilient solutions aligned to the business and operational requirements are selected and deployed. | |

## Exam Preparation

Candidates may reference the Splunk YouTube Channel, Splunk Docs, Splunk Lantern Security Use Cases, 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 and Splunk Certified Cybersecurity Defense Engineer, the following is a ***suggested and non-exhaustive*** list of training from our Course Catalog that may cover topics listed in the above blueprint:

- ❑ Administering Splunk Enterprise
- ❑ Splunk Cloud Administration
- ❑ Architecting Splunk Enterprise Deployments
- ❑ Troubleshooting Splunk Enterprise
- ❑ Mastering Splunk Data Management Techniques
- ❑ Splunk Distributed Search
- ❑ Administering Splunk SOAR
- ❑ SOAR Advanced Implementation
- ❑ Using Splunk UEBA to Detect Insider Threats

**There are no prerequisite exams for this certification.**

Schedule this exam