

# Splunk Education Learning Path for Enterprise Security Administrators

Splunk Education programs help you get the most out of Splunk. The curriculum is comprised of lecture, demos, hands-on lab exercises and assessments to test your knowledge. Courses are concise and designed for Splunk users, administrators, developers, architects and partners and are structured for rapid learning. We offer a variety of delivery methods including instructor-led virtual and onsite training as well as self-paced training that provides flexibility to attend at anytime from anywhere. Whether you just downloaded Splunk or have been using it for years, Splunk Education courses deliver value and accelerate success.

## Splunk Enterprise Security Administrators

Learn to install, configure, manage, and use the Splunk App for Enterprise Security. This path is intended for Splunk Administrators that manage Splunk Enterprise Security deployments.

### Splunk Fundamentals 1

This self-paced course teaches you how to search and navigate in Splunk, use fields, get statistics from your data, create reports, dashboards, lookups, and alerts. It will also introduce you to Splunk's datasets features and Pivot interface.

### Splunk Fundamentals 2

This course focuses on additional SPL commands, using field aliases and calculated fields, creating tags and event types, using macros, creating workflow actions and data models, and normalizing data with the CIM.

### Creating Dashboards with Splunk

This course is designed for power users who want to learn best practices for building dashboards and forms. It focuses on improving performance, using tokens and global searches; customizing charts, creating dynamic behaviors and adding extensions for JavaScript and CSS.

### Splunk Fundamentals 3

This course focuses on additional search commands as well as on advanced use of knowledge objects. Major topics include advanced statistics and eval commands, advanced lookup topics, advanced alert actions, using regex and erex to extract fields, using spath to work with self-referencing data, creating nested macros and macros with event types, and accelerating reports and data models.

### Advanced Searching and Reporting with Splunk

This course takes the Splunk search language to the next level. Learn powerful advanced commands and lookup methods.

### Splunk Enterprise System Administration

This course is designed for system administrators who manage a Splunk Enterprise environment. Topics include Splunk license manager, indexers and search heads, configuration, management, and monitoring.

### Splunk Enterprise Data Administration

This course is for data administrators who are responsible for getting data into Splunk. The course provides content about

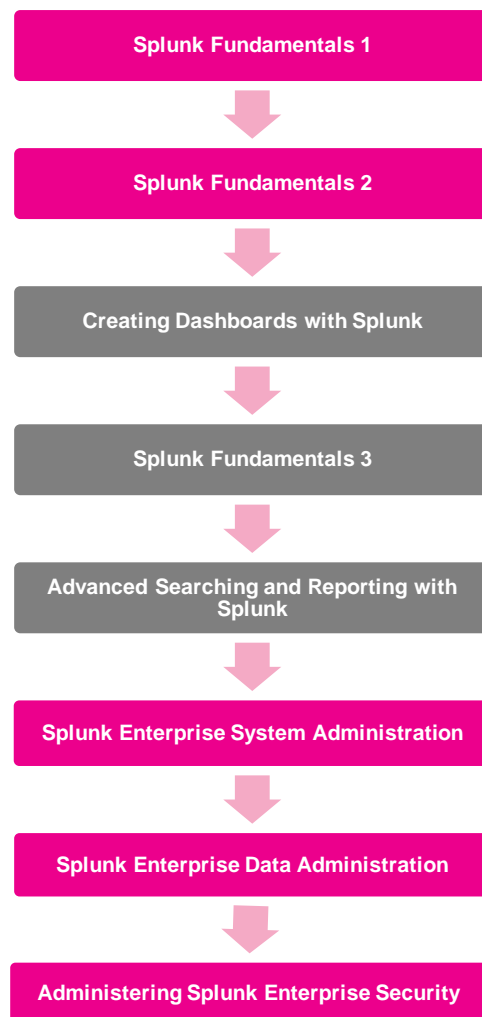
Splunk forwarders and methods to get remote data into Splunk.

### Architecting Splunk Enterprise Deployments

This course focuses on large enterprise deployments. Learn best practices for planning, data collection, sizing and documenting a distributed deployment.

### Administering Splunk Enterprise Security

This course prepares architects and systems administrators to install, configure and manage Splunk Enterprise Security. It covers ES event processing and normalization, deployment requirements, technology add-ons, settings, risk analysis settings, threat intelligence and protocol intelligence configuration, and customizations.



Required Course  
Recommended Course