splunk>

Administering ES 5.2

This 13.5 hour 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.

Course Topics

- Identify normal ES use cases
- Examine deployment requirements for typical ES installs
- Learn how to install ES and gather information for lookups
- Learn the steps to setting up inputs using technology add-ons
- Create custom correlation searches
- Configure ES risk analysis, threat and protocol intelligence
- Fine tune ES's settings and other customizations

Course Prerequisites

Required: Splunk Fundamentals 1, Splunk Fundamentals 2, Splunk System Administration, Splunk Data Administration

Note: For Splunk Cloud customers, Splunk Cloud Administration can replace Splunk System Administration and Splunk Data Administration

Recommended: Architecting Spunk Enterprise Deployments

Class Format

Instructor-led lecture with labs. Delivered via virtual classroom or at your site.

Course Objectives

Module 1 – ES Introduction

- Overview of ES features and concepts

Module 2 – Monitoring and Investigation

- Security Posture
- Incident Review
- Notable events management
- Managing Investigations

Module 3 – Security Intelligence

- Overview of security intel tools

Module 4 – Forensics, Glass Tables and Navigation Control

- Explore forensics dashboards
- Examine glass tables
- Configure navigation and dashboard permissions

Module 5 – ES Deployment

- Identify deployment topologies
- Examine the deployment checklist
- Understand indexing strategy for ES
- Understand ES Data Models

Module 6 – Installation and Configuration

- Prepare a Splunk environment for installation
- Download and install ES on a search head
- Test a new install
- Understand ES Splunk user accounts and roles
- Post-install configuration tasks

Module 7 – Validating ES Data

- Plan ES inputs
- Configure technology add-ons

Module 8 – Custom Add-ons

- Design a new add-on for custom data
- Use the Add-on Builder to build a new add-on

Module 9 – Tuning Correlation Searches

- Configure correlation search scheduling and sensitivity
- Tune ES correlation searches

Module 10 – Creating Correlation Searches

- Create a custom correlation search
- Configuring adaptive responses
- Search export/import

Module 11 – Lookups and Identity Management

- Identify ES-specific lookups
- Understand and configure lookup lists

Module 12 – Threat Intelligence Framework

- Understand and configure threat intelligence
- Configure user activity analysis

About Splunk Education

Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.

Certification Tracks

Our certification tracks provide comprehensive education for Splunk customer and partner personnel according to their areas of responsibility.

To view all of Splunk Education's course offerings, or to register for a course, go to http://www.splunk.com/goto/education

To contact us, email education_AMER@splunk.com

About Splunk

Splunk is software that indexes, manages and enables you to search data from any application, server or network device in real time.

Visit our website at www.splunk.com to download your own free copy.

Splunk Inc.
270 Brannan
San Francisco, CA 94107
866.GET.SPLUNK
(866.438.7758)
sales@splunk.com
support@splunk.com