Introduction to Enterprise Security

This 40-minute, free eLearning course provides an introduction to Splunk Enterprise Security (ES). Students will learn about the anatomy of a security incident, and how ES can help you identify, combat, and prevent future threats to your organization.

Course Topics

- Anatomy of a kill chain/APT attack
- ES use cases
- ES workflow
- Correlation searches and notable events
- ES user interface and dashboard overview

Prerequisite Knowledge

To be successful, students should have a working understanding of the following courses:

- What is Splunk?
- Intro to Splunk
- Using Fields
- Visualizations
- Intro to Knowledge Objects

Course Format

eLearning

Course Objectives

Topic 1 – Anatomy of a Security Incident

- Kill chain methodology
- Advanced Persistent Threats (APTs)
- ES use cases

Topic 2 – Enterprise Security Workflow

- Correlation searches
- Notable events
- Accelerated data models

Topic 3 – Enterprise Security Dashboards

- Security Posture dashboard
- Incident Review dashboard
- Executive Summary dashboards
- Risk-based alerting

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

To contact us, email Education_AMER@splunk.com

Splunk, Inc.

270 Brannan St. San Francisco, CA 94107

+1 866.GET.SPLUNK (1 866.438.7758)

Contact sales