splunk>

Using ES 4.5

This 13.5 hour course prepares security practitioners to use Splunk Enterprise Security (ES). Students will use ES to identify and track security incidents, analyze security risks, use predictive analytics, and threat discovery.

Course Topics

- ES concepts
- Security monitoring and Incident investigation
- Assets and identities
- Detecting known types of threats
- Monitoring for new types of threats
- Using analytical tools
- Analyze user behavior for insider threats
- Use risk analysis and threat intelligence tools
- Use protocol intelligence and live stream data
- Use investigation timelines and journal tools
- Build glass tables to display security status

Course Prerequisites

Using Splunk, Creating Knowledge Objects, Searching and Reporting with Splunk (recommended).

Class Format

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

Course Objectives

Module 1 - Getting Started with ES

- Provide an overview of the Splunk App for Enterprise Security (ES)
- Identify the differences between traditional security threats and new adaptive threats
- Describe correlation searches, data models and notable events
- Describe user roles in ES
- Log on to ES

Module 2 - Security Monitoring and Incident Investigation

- Use the Security Posture dashboard to monitor enterprise security status
- Use the Incident Review dashboard to investigate notable events
- Take ownership of an incident and move it through the investigation workflow
- Use adaptive response actions during incident investigation
- Create notable events
- Suppress notable events

Module 3 – Investigation Timelines

- Use ES investigation timelines to manage, visualize and coordinate incident investigations
- Use timelines and journals to document breach analysis and mitigation efforts

Module 4 – Forensic Investigation with ES

- Investigate access domain events
- Investigate endpoint domain events
- Investigate network domain events
- Investigate identity domain events

Module 5 – Risk and Network Analysis

- Understand and use Risk Analysis
- Use the Risk Analysis dashboard
- Assign risk scores

Module 6 – Web Intelligence

- Use HTTP Category Analysis, HTTP User Agent Analysis, New Domain Analysis, and Traffic Size Analysis to spot new threats
- Filter and highlight events

Module 7 – User Intelligence

- Evaluate the level of insider threat with the user activity and access anomaly dashboards
- Understand asset and identity concepts
- Use the Asset Investigator to analyze events related to an asset
- Use the Identity Investigator to analyze events related to an identity
- Examine asset and identity lookup tables

Module 8 – Threat Intelligence

- Use the Threat Activity dashboard to analyze traffic to or from known malicious sites
- Inspect the status of your threat intelligence content with the threat artifact dashboard

Module 9 - Protocol Intelligence

- Use ES predictive analytics to make forecasts and view trends

Module 10 – Glass Tables

- Build glass tables to display security status information
- Create new key indicators for metrics on glass tables

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