

Introduction to Detection Engineering with Splunk

Summary




This course is for mature detection engineers and Security Operations Center (SOC) teams with experience in detection development, tuning, and familiarity with attack simulation tools, who are ready to implement automated development, testing, and deployment pipelines for their detection engineering process.

The course covers an introduction to the basics of detection creation, tools, and recommendations for detection engineering with Splunk. It also explores how Splunk supports detection engineering through a variety of open source tools and frameworks. By the end of this course, you will be able to:

- Describe the Splunk Threat Research Team's detection engineering process.
- Explain considerations for designing, building, and testing detections.
- Identify common tools and frameworks used in detection engineering.
- Define Detection-as-Code.
- Explain the Detection Lifecycle.

Prerequisites

- To be successful, students must have completed these Splunk Education course(s) or have equivalent working knowledge:
 - Intro to Splunk
 - Using Fields
 - Introduction to Knowledge Objects
 - Creating Knowledge Objects
 - Creating Field Extractions
- Additional courses and/or knowledge in these areas are highly recommended:
 - Introduction to Splunk Security Essentials
 - Administering Splunk Enterprise Security

	Format: <ul style="list-style-type: none">• Self-paced eLearning
	Estimated Duration: 2.5 Hours
	Audience: <ul style="list-style-type: none">• Detection Engineers• Splunk Enterprise Security Administrators

Course Outline

Module 1 – SOC Maturity

- Describe the Prescriptive Adoption Model
- Describe Assets and Identities
- List common SOC metrics

Module 2 – Detection Engineering with Splunk

- Describe a detection engineering cycle
- Explain the Splunk Threat Research Team's detection engineering process
- Introduce open source resources for detection engineering

Module 3 – Getting Ready

- Explain the process for designing effective detections
- Understand data normalization

Module 4 – Preparing your Data and Environment

- Understand Data Models
- Explain data management components in Splunk
- Review index and search time processes

Module 5 – Building Detections

- Define detections and findings
- Explore detection scheduling
- Establish thresholds

Module 6 – Testing and Tuning

- Explore the Splunk Attack Range
- Explain the use of adversary simulation
- Identify tools for adversary simulation
- Explain optimizing search queries

Module 7 – Risk-based Alerting

- Describe Risk-Based Alerting (RBA)
- List the key components of RBA

Module 8 – Detection-as-Code

- Define Detection-as-Code (DaC)
- Identify components of DaC systems
- Understand the benefits of a detection lifecycle

Module 9 – Summary

- Review course objectives

About Splunk Education

With Splunk Education, you and your teams can learn to optimize Splunk through self-paced eLearning and instructor-led training, supported by hands-on labs. Explore learning paths and certifications to meet your goals. Splunk courses cover all product areas, supporting specific roles such as Splunk Platform Search Expert, Splunk Enterprise or Cloud Administrator, SOC Analyst or Administrator, DevOps or Site Reliability Engineer, and more. To learn more about our flexible learning options, full course catalog, and Splunk Certification, please visit <http://www.splunk.com/education>.

To contact us, email education@splunk.com.

