SOC Essentials: Investigating and Threat Hunting (SEITH)

ID SEITH **Price** CHF 1,100.—(excl. VAT) **Duration** 9 hours

Who should attend

- SOC Analysts
- Defense Engineers
- Splunk Admins who support these roles

Prerequisites

To be successful students should have a basic understanding of common cyber technologies and concepts including:

- OSI Model
- Networking concepts and common security tools
- Common Operative Systems like Windows and Linux

The following Splunk courses are also highly recommended:

- Intro to Splunk (eLearning)
- Using Fields (SUF)
- Previous courses in the Defense Analyst learning path

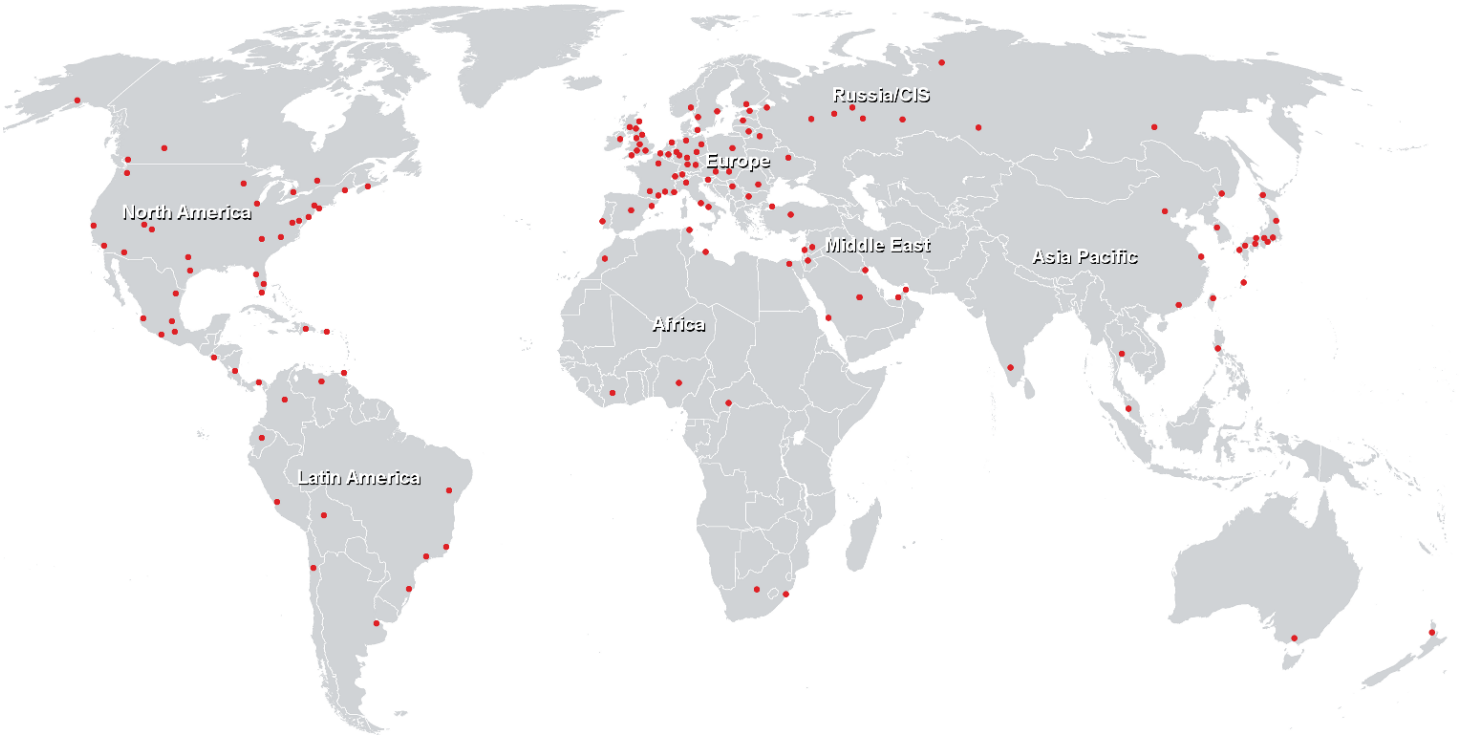
Course Objectives

At the end of this course you should be able to:

- Describe SIEM best practices and basic operation concepts of Splunk Enterprise Security, including the interaction between CIM, Data Models, and acceleration, and common CIM fields that may be used in investigations
- Carry out a typical triage and investigation process using Splunk Enterprise Security
- Describe the purpose of the Asset and Identity, and Threat Intelligence frameworks in ES
- Define Splunk ES elements like Notable Event, Risk Notable, Adaptive Response Action, Risk Object, Contributing Events.
- Identify common built-in dashboards in Enterprise Security and the basic information they contain.
- Explain the use of SOAR playbooks and list the basic ways they can be triggered from Enterprise Security
- Explain the essentials of Risk-based Alerting and the Risk framework
- List the common high-level steps of threat hunting using the PEAK framework and practice some common steps of hypothesis hunting with Splunk.

SOC Essentials: Investigating and Threat Hunting (SEITH)

Training Centres worldwide





Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch