KOENIG SOLUTIONS · COURSE OUTLINE

Advanced SOAR Implementation

Learn to integrate Splunk with SOAR and build custom playbooks, from external search configuration to REST-based data access.

6	23
MODULES	TOPICS

COURSE OVERVIEW

This course covers the implementation of Splunk and SOAR together, including the concepts, data flows and prerequisites for integration. It addresses configuring external Splunk search, sending Splunk events to SOAR through CIM to CEF field mapping and notable triggers, and accessing Splunk data and notable events from within SOAR playbooks. It also covers writing custom functions and code using the SOAR API with persistent data storage, and using Django queries, REST and the HTTP app to access SOAR data from playbooks.

WHO THIS COURSE IS FOR

- **SOC Analysts**
- **Security Engineers**
- **SOAR Administrators**
- **Splunk Administrators**
- **Automation Developers**
- **Incident Responders**

LEARNING OBJECTIVES

- Describe interactions and data flows between Splunk and SOAR
- Configure external Splunk search for a SOAR instance
- Configure the SOAR Add-on for Splunk and map CIM to CEF
- Implement automatic playbook triggers for Splunk notables
- Ingest Splunk events and update notables from SOAR playbooks
- Apply SOAR coding best practices in custom functions
- Develop custom code using the SOAR API and persistent data
- Use REST, Django queries and the HTTP app in SOAR

COURSE SYLLABUS

6 Modules, 23 Topics

01

Implementing Splunk and SOAR

TOPICS

Review of SOAR UI and concepts · Describe interactions between Splunk and SOAR · Identify key concepts and data flows · Pre-requisites for integration

02

Configuring External Splunk Search

TOPICS

- Describe the benefits of externalizing search to Splunk
- Configure the SOAR instance for externalization
- Configure the Splunk instance for externalization
- Use the Splunk app for SOAR Reporting

03

Sending Splunk Events to SOAR

TOPICS

- Configure the SOAR Add-on for Splunk
- Map CIM fields to CEF
- Send Enterprise Security notables to SOAR
- Automatically trigger SOAR playbooks for Splunk notables

04

Accessing Splunk from SOAR

TOPICS

Install and configure the SOAR App for Splunk · Ingest Splunk events into SOAR · Use Splunk search from playbooks · Update Splunk notable events

05

Custom Coding in Playbooks

TOPICS

SOAR coding best practices · Writing, using and managing custom functions · Using the SOAR API in custom code · Store and retrieve persistent data

06

Using SOAR REST

TOPICS

- Use Django queries to search for data in SOAR
- Use REST to access SOAR data
- Use the HTTP app to execute REST from playbooks

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training | Live Online Classes (ILO) | Fly-Me-A-Trainer (FMAT) | Flexi (Self-Paced) | 1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com | info@koenig-solutions.com