KOENIG
step forward

KOENIG SOLUTIONS · COURSE OUTLINE

Advanced Phantom Implementation 4.10

Learn to integrate Splunk and Phantom, configure external search, exchange events, and extend playbooks with custom code and REST.

6	23
MODULES	TOPICS

COURSE OVERVIEW

This course covers the integration of Splunk and Phantom, including the interactions, data flows, and pre-requisites involved. It then addresses configuring external Splunk search on both the Phantom and Splunk instances, and sending Splunk events to Phantom through the Phantom Add-on, CIM to CEF field mapping, and automated playbook triggers. It also covers accessing Splunk data from Phantom, including ingesting events, searching from playbooks, and updating notable events. Finally, it addresses writing custom functions and code within playbooks, and using Phantom REST through Django queries and the HTTP app.

WHO THIS COURSE IS FOR

Security Analysts **SOC Engineers** **Splunk Administrators** **Phantom Developers**

Security Automation Engineers

LEARNING OBJECTIVES

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

COURSE SYLLABUS

6 Modules, 23 Topics

01

Implementing Splunk and Phantom

TOPICS

- Review of Phantom UI and concepts
- Describe interactions between Splunk and Phantom
- 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 Phantom instance for externalization
- Configure the Splunk instance for externalization
- Use the Splunk app for Phantom Reporting

03

Sending Splunk Events to Phantom

TOPICS

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

04

Accessing Splunk from Phantom

TOPICS

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

05

Custom Coding in Playbooks

TOPICS

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

06

Using Phantom REST

TOPICS

- Use Django queries to search for data in Phantom
- Use REST from other systems to access Phantom 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