KOENIG
step forward

KOENIG SOLUTIONS · COURSE OUTLINE

Administering Splunk Enterprise Security 6.6

Learn to install, configure and administer Splunk Enterprise Security, from correlation searches to asset and threat intelligence management.

12
MODULES

41
TOPICS

COURSE OVERVIEW

This course covers the functions and data models of Splunk Enterprise Security, including security monitoring dashboards, risk-based alerting and incident investigation workflows. It then addresses installation, initial configuration and validation of ES data, along with building custom add-ons. Further topics include tuning and creating correlation searches, managing asset and identity information, and configuring the threat intelligence framework.

WHO THIS COURSE IS FOR

- **Splunk Administrators**
- **Security Analysts**
- **Security Operations Engineers**
- **Incident Responders**
- **SIEM Administrators**

LEARNING OBJECTIVES

- Explain how ES functions and uses data models
- Configure ES roles and permissions
- Customise Security Posture and Incident Review dashboards
- Create notable events and notable event suppressions
- Describe risk-based alerting and risk scores
- Manage investigations using the Investigation Workbench
- Install and configure ES on a search head
- Create and tune correlation searches

COURSE SYLLABUS

12 Modules, 41 Topics

01

Introduction to ES

TOPICS

Review how ES functions · Understand how ES uses data models · Configure ES roles and permissions

02

Security Monitoring

TOPICS

- Customize the Security Posture and Incident Review dashboards
- Create ad hoc notable events
- Create notable event suppressions

03

Risk-Based Alerting

TOPICS

- Give an overview of risk-based alerting
- View Risk Notables and risk information on the Incident Review dashboard
- Explain risk scores and how an ES admin can change an object's risk score
- Review the Risk Analysis dashboard
- Describe annotations

04

Incident Investigation

TOPICS

Review the Investigations dashboard · Customize the Investigation Workbench · Manage investigations

05

Installation

TOPICS

Prepare a Splunk environment for installation · Download and install ES on a search head · Test a new install · Post-install configuration tasks

06

Initial Configuration

TOPICS

Set general configuration options · Add external integrations · Configure local domain information · Customize navigation · Configure Key Indicator searches

07

Validating ES Data

TOPICS

- Verify data is correctly configured for use in ES
- Validate normalization configurations
- Install additional add-ons

08

Custom Add-ons

TOPICS

Design a new add-on for custom data · Use the Add-on Builder to build a new add-on

09

Tuning Correlation Searches

TOPICS

- Configure correlation search scheduling and sensitivity
- Tune ES correlation searches

10

Creating Correlation Searches

TOPICS

Create a custom correlation search · Manage adaptive responses · Export/Import content

11

Asset & Identity Management

TOPICS

- Review the Asset and Identity Management interface
- Describe Asset and Identity KV Store collections
- Configure and add asset and identity lookups to the interface
- Configure settings and fields for asset and identity lookups
- Explain the asset and identity merge process
- Describe the process for retrieving LDAP data for an asset or identity lookup

12

Threat Intelligence Framework

TOPICS

- Understand and configure threat intelligence
- Use the Threat Intelligence Management interface to configure a new threat list

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