KOENIG SOLUTIONS · COURSE OUTLINE

Administering Splunk Enterprise Security 7.0

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

12
MODULES

40
TOPICS

COURSE OVERVIEW

This course covers how Splunk Enterprise Security functions, including its use of data models, roles and permissions, security monitoring dashboards, and risk-based alerting. It then addresses incident investigation, installation, initial configuration and validating data for use in ES. Further modules cover building custom add-ons, tuning and creating correlation searches, and managing asset, identity and threat intelligence information.

WHO THIS COURSE IS FOR

- **Security Analysts**
- **Splunk Administrators**
- **Security Operations Engineers**
- **Incident Responders**
- **Threat Intelligence Analysts**

LEARNING OBJECTIVES

- Explain how Splunk Enterprise Security functions and uses data models
- Configure ES roles, permissions and general settings
- Customize Security Posture, Incident Review and Investigation dashboards
- Create notable events, suppressions and ad hoc alerts
- Install Splunk Enterprise Security and perform post-install configuration
- Validate data normalization and install additional add-ons
- Develop custom add-ons and correlation searches for ES
- Configure asset, identity and threat intelligence management

COURSE SYLLABUS

12 Modules, 40 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

Explain Risk-Based Alerting · Explain risk scores · Review the Risk Analysis dashboard · Use 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

Manage Threat Intelligence

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