KOENIG SOLUTIONS · COURSE OUTLINE

SIEM Systems: AlienVault & Splunk

Learn to deploy and manage SIEM systems using AlienVault and Splunk, from log collection to correlation and reporting.

COURSE OVERVIEW

This course covers the fundamentals of SIEM, including network threats, architecture, deployment, logs and events, event correlation, and intrusion detection and prevention. It then covers installing and configuring AlienVault SIEM, including its web interface, sensors, loggers, servers, network inventory, vulnerability scanning, signature updates, policy management and tickets. It concludes with Splunk, covering machine data, its user interface, searching and saving results, and creating reports and visualisations.

WHO THIS COURSE IS FOR

- **SIEM Administrators**
- **Security Analysts**
- **Network Security Engineers**
- **SOC Analysts**
- **IT Security Professionals**

LEARNING OBJECTIVES

- Explain core SIEM concepts and network threats
- Describe SIEM architecture and deployment options
- Identify methods for log and event collection
- Apply event correlation and correlation rules
- Analyse forensically ready data for investigations
- Configure AlienVault sensors, loggers and servers
- Configure network inventory and vulnerability scanning
- Develop reports and visualisations using Splunk

COURSE SYLLABUS

24 Topics

TOPICS

- Introduction to SIEM
- Network Threats
- SIEM Architecture
- SIEM Deployment
- Logs and Events
- Event Collection and Event Correlation
- Correlation Rules
- Forensically Ready Data
- Intrusion Detection, Prevention and Tolerance
- Properties of a Robust SIEM
- Installing Alien Vault SIEM
- Using Web Interface
- Configuring Sensor, Logger and Server
- Configuring Network Inventory
- Configuring Vulnerability Scanning
- Configuring Signature Updates
- Policy Management
- Configuring Tickets
- Introduction to SPLUNK
- Overview of machine data
- How Splunk works with machine data
- Introduction to Splunk's user interface
- Searching and saving results
- Creating reports and visualizations

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