4-Day Splunk Enterprise Security Admin Training TOC

Day 1: Splunk Core Essentials (Pre-requisite for ES)

> ***Objective: Ensure foundational knowledge of Splunk required to work with ES.***

- - Introduction to Splunk Platform
- - Navigating Splunk Web UI
- - Search Processing Language (SPL) Basics
- - Using Fields, Tags, and Event Types
- - Creating and Managing Alerts
- - Dashboards and Visualizations
- - Overview of Knowledge Objects
- - Indexes and Sourcetypes Basics
- - Forwarders and Data Ingestion Overview
- - Basic User Roles & Permissions

Day 2: Introduction to Enterprise Security (ES) & Architecture

> ***Objective: Understand ES components, architecture, and integration points.***

- - What is Splunk Enterprise Security?
- - ES Architecture and Data Flow
- - Installing and Configuring ES App
- - ES Data Onboarding Requirements (CIM compliance)
- - Overview of Notable Events
- - Incident Review and Investigation Workflows
- - Understanding Correlation Searches
- - ES Navigation: Security Posture, Threat Intelligence, etc.

Day 3: Administering and Tuning ES

> ***Objective: Perform administrative tasks, tune ES components, and manage data sources.***

- - Customizing and Managing Correlation Searches
- - Tuning Risk-Based Alerting (RBA)
- - Creating and Managing Lookups
- - Managing Threat Intelligence Feeds
- - Maintaining CIM Data Models
- - Tuning and Suppressing Notable Events
- - Identity and Asset Framework Configuration
- - Deployment Best Practices

Day 4: Advanced Administration, Maintenance & Troubleshooting

Objective: Deep-dive into ES maintenance, performance tuning, and troubleshooting.

- - Managing ES Updates and Upgrades
- - Monitoring Performance of ES
- - Troubleshooting Correlation Searches and Data Models
- - Custom Use Case Development
- - Backup and Recovery Best Practices
- - Working with Data Model Acceleration
- - Role-Based Access Control in ES
- - Case Studies & Real-World Use Cases
- - Final Q&A and Wrap-up