



Enterprise Computing Solutions - Education Services

## TRAINING OFFERING

---

**Du kan nå oss här**

Kronborgsgränd 7, 164 46 Kista

Email: [edu.ecs.se@arrow.com](mailto:edu.ecs.se@arrow.com)

Phone: +46 8 555 188 00



# Administering Splunk Enterprise Security

CODE:	LENGTH:	PRICE:
SPL_ASES7	24 Hours (3 days)	kr16,000.00

## Description

This 13.5 hour course prepares architects and systems administrators to install and configure Splunk Enterprise Security (ES). It covers ES event processing and normalization, deployment requirements, technology add-ons, dashboard dependencies, data models, managing risk, and customizing threat intelligence.

## Objectives

- Examine how ES functions including data models, correlation searches, notable events and dashboards
- Create custom correlation searches -Customize the Investigation Workbench -Learn how to install or upgrade ES
- Learn the steps to setting up inputs using technology add-ons -Fine tune ES Global Settings
- Customize risk and configure threat intelligence

## Prerequisites

To be successful, students should have a solid understanding of the following:

- Splunk Enterprise System Administration
- Splunk Enterprise Data Administration

OR the following single-subject courses:

- What Is Splunk?
- Intro to Splunk
- Using Fields
- Scheduling Reports and Alerts
- Visualizations
- Leveraging Lookups and Subsearches
- Search Under the Hood
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions
- Enriching Data with Lookups
- Data Models

- Introduction to Dashboards

- Dynamic Dashboards

Students should also have completed the following courses:

- Splunk System Administration

- Splunk Data Administration

## Programme

### Module 1 – Introduction to ES

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

### Module 2 – Security Monitoring

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

### Module 3 – Risk-Based Alerting

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

### Module 4 – Incident Investigation

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

### Module 5 – Installation

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

### Module 6 – Initial Configuration

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

### Module 7 – Validating ES Data

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

### Module 8 – Custom Add-ons

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

### Module 9 – Tuning Correlation Searches

- Configure correlation search scheduling and sensitivity

- Tune ES correlation searches

#### Module 10 – Creating Correlation Searches

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

#### Module 11 – Asset & Identity Management

- 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

#### Module 12 – Manage Threat Intelligence

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

### **Session Dates**

På begäran, [kontakta oss](#)

### **Ytterligare information**

[Denna utbildning finns också som utbildning på plats. Kontakta oss för mer information.](#)