Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss här

Kronborgsgränd 7, 164 46 Kista

Email: edu.ecs.se@arrow.com
Phone: +46 8 555 188 00

Prerequisites Fast Start

CODE:	LENGTH:	PRICE:
SPL_PREREQ	24 Hours	Free

Description

What is Splunk : This eLearning course introduces students to what machine data is—and how Splunk can leverage operational intelligence to investigate and respond to incidents in their organizations.
To register to this course , please use this link :https://www.splunk.com/en_us/training/courses/what-is-splunk.html
Intro to Splunk : This eLearning course teaches students how to use Splunk to create reports and dashboards and explore events using Splunk's Search Processing Language. Students will learn the basics of Splunk's architecture, user roles, and how to navigate the Splunk Web interface to create robust searches, reports, visualizations, and dashboards.
To register to this course , please use this link :https://www.splunk.com/en_us/training/courses/intro-to-splunk.html
Using Fields : This three-hour course is for power users who want to learn about fields and how to use fields in searches. Topics will focus on explaining the role of fields in searches, field discovery, using fields in searches, and the difference between persistent and temporary fields. The last topic will introduce how fields from other data sources can be used to enrich search results.
To register to this course , please use this link :https://www.splunk.com/en_us/training/courses/using-fields.html
Visualizations : This eLearning course teaches students how to create visualizations in Splunk, using Splunk's Search Processing Language as well as the Splunk Web interface. Students will learn commands that allow data to be displayed on charts and graphs, transform geographic data into maps, create single value visualizations, and use Splunk's visual formatting options to change the look of statistical tables.
To register to this course , please use this link : https://www.splunk.com/en_us/training/courses/visualizations.html
Intro to Knowledge Objects : This eLearning course teaches students about how different types of knowledge objects to extract additional insights from their data. Students will learn the basics of how to create knowledge objects, define their settings, edit, and manage existing knowledge objects.
To register to this course , please use this link :https://www.splunk.com/en_us/training/courses/intro-to-knowledge-objects.html
Search Under the Hood : This eLearning course gives students additional insight into how Splunk processes searches. Students will learn about Splunk architecture, how components of a search are broken down and distributed across the pipeline, and how to troubleshoot searches when results are not returning as expected.
To register to this course , please use this link :https://www.splunk.com/en_us/training/courses/search-under-the-hood.html

Objectives

What is Splunk : Topic 1 – What Is Machine Data?

- Understand the basics of machine data

Topic 2 – Operational Intelligence

- Scenario-based introduction to investigating a customer issue without operational intelligence

Topic 3 – What Is Splunk?

- Identify the core features of Splunk
- Understand how Splunk's features work together to explore organizational data

Intro to Splunk : Topic 1 – Intro to Splunk

- Splunk components
- Basic Splunk functions

Topic 2 – Using Splunk

- Define Splunk Apps

- Understand Splunk user roles
- Searching & Reporting app
- Splunk Web interface

Topic 3 – Using Search

- Run basic searches
- Set the time range of a search
- Save search results
- Identify the contents of search results
- Work with events
- Share search jobs
- Export search results
- Select search modes
- Control a search job

Topic 4 – Exploring Events

- Refine searches
- Understand timestamps
- Use the events tab to add and remove terms from a search

Topic 5 – Search Processing Language

- Use wildcards to search for multiple terms
- Understand case sensitivity in searches
- Use booleans to include and exclude search criteria
- Use special character with search terms

Topic 6 – What Are Commands?

- Understand the anatomy of Splunk's search language:
- Search terms
- Commands
- Functions
- Arguments
- Clauses
- Understand bestpractices for writing searches

Topic 7 – What Are Knowledge Objects?

- Identify the five categories of knowledge objects:
- Data interpretation
- Data classification

- Data enrichment
- Data normalization
- Data models
- Understand types of knowledge objects

Topic 8 – Creating Reports and Dashboards

- Save a search as a report
- Edit reports
- Use transforming commands to create visualizations
- Create a dashboard
- Add a report to a dashboard
- Edit a dashboard

Using Fields : Topic 1 - What are Fields?

- Understand fields and field auto-extraction
- Explore the Fields sidebar
- Add fields to the Selected Fields list
- Explore and generate reports from the Fields window

Topic 2 - What is Field Discovery?

- Understand Field Discovery
- Explore search modes and their effect on search results

Topic 3 - Using Fields in Searches

- Use fields correctly in basic searches
- Use fields with operators
- Use the rename command
- Use the fields command to improve search performance

Topic 4 - Comparing Temporary versus Persistent Fields

- Differentiate between temporary and persistent fields
- Create temporary fields with the eval command
- Extract temporary fields with the erex and rex commands

Topic 5 - Enriching Data

- Understand how fields from lookups, calculated fields, field aliases, and field extractions enrich data

Visualizations : Module 1 – Title

- The fields command
- The table command
- The dedup command
- The addtotals command

- The fieldformat command

Module 2 – Title

- Explore visualization types
- Use transforming commands to order results into a data table:
- top
- rare
- stats
- chart
- timechart
- trendline
- Understand when to use different transforming commands

Module 3 – Title

- Explore geographic visualization types
  - Use commands specific to geographic data
  - iplocation
  - geostats
  - geom
- Prepare data for use in a choropleth map

Module 4 – Title

- Use visual formatting options for single value visualizations
- Add a sparkline to a single value visualization
- Use the Trellis layout to split visualizations
- Use the gauge command
- Use the radial, filler, and marker gauge visualization types

Module 5 – Title

- Explore formatting options for statistical tables
- Create a chart overlay
- Explore formatting options for different types of visualizations

Intro to Knowledge Objects Topic 1 – What Are Knowledge Objects?

- Understand the different types of knowledge objects:
- Fields
- Field Extractions
- Field aliases

- Calculated fields
- Lookups
- Event types
- Tags
- Workflow actions
- Reports
- Alerts
- Macros
- Data models

Topic 2 – Knowledge Object Settings

- Define naming conventions
- Define role-based permissions for knowledge objects

Topic 3 – Managing Knowledge Objects

- Edit knowledge objects
- Reassign knowledge objects
  - Use commands specific to geographic data
  - iplocation
  - geostats
  - geom
- Prepare data for use in a choropleth map

Module 4 – Title

- Use visual formatting options for single value visualizations
- Add a sparkline to a single value visualization
- Use the Trellis layout to split visualizations
- Use the gauge command
- Use the radial, filler, and marker gauge visualization types

Module 5 – Title

- Explore formatting options for statistical tables
- Create a chart overlay
- Explore formatting options for different types of visualizations

Intro to Knowledge Objects Topic 1 – What Are Knowledge Objects?

- Understand the different types of knowledge objects:
- Fields
- Field Extractions

- Field aliases
- Calculated fields
- Lookups
- Event types
- Tags
- Workflow actions
- Reports
- Alerts
- Macros
- Data models

Topic 2 – Knowledge Object Settings

- Define naming conventions
- Define role-based permissions for knowledge objects

Topic 3 – Managing Knowledge Objects

- Edit knowledge objects
- Reassign knowledge objects

Search Under the Hood : Topic 1 – Investigating Searches

- Use the Search Job Inspector to examine how a search was processed and troubleshoot performance
- Use SPL commenting to help identify and isolate problems

Topic 2 – Splunk Architecture

- Understand the role of search heads, indexers, and forwarders in a Splunk deployment
- Understand how the components of a bucket (.tsidx and journal.gz files) are used
- Understand how bloom filters are used to improve search speed

Topic 3 – Streaming and Non-Streaming Commands

- Describe the parts of a search string
- Understand the use of centralized vs. distributable commands
- Create more efficient searches

Topic 4 – Breakers and Segmentation

- Understand how segmenters are used in Splunk
- Use lispy to reduce the number of events read from disk

Topic 5 – Commands and Functions for Troubleshooting

- Using the fieldsummary command
- Using the makeresults command
- Using information functions with the eval command

- the isnull function
- the typeof function

Prerequisites

Classes:

- None

Skills:

- None

Programme

Test and Certification

Certification : Splunk Core Certified Power User
To pass this certification , you need to follow next step : Power User Fast Start course

Further Information

Network Security Data Intelligence AI Cloud

Session Dates

Date	Location	Time Zone	Language	Type	Guaranteed	PRICE
18 Jul 2024			English	Web based Training		Free

Ytterligare information

Denna utbildning finns också som utbildning på plats. Kontakta oss för mer information.