ExecuTrain

Impulsamos tu talento tecnológico

- Aplicaciones Móviles
- Colaboración
- Mejores Practicas
- Sistemas Operativos
- Bases de datos
- Cloud Computing
- Office
- Virtualización
- Big Data
- Desarrollo
- Seguridad

Tel: 33 3647 6622
ventas@executrain.com.mx
www.executrain.com.mx

¿Por qué ExecuTrain?

ExecuTrain es un proveedor de entrenamiento corporativo a nivel internacional y líder mundial en la capacitación empresarial. Contamos con 30 años y más de 72 mil personas capacitadas en México.

¿Por qué ExecuTrain?

Te guiamos en la definición de tus requerimientos de capacitación, en las diferentes etapas:

- Detección de necesidades, evaluación de conocimientos, plan de capacitación y seguimiento posterior para elegir el plan de capacitación como tú lo necesitas.
- El más amplio catálogo de cursos, desde un nivel básico hasta los niveles de conocimientos más especializados.
- En ExecuTrain el material y la metodología están diseñados por expertos en aprendizaje humano. Lo que te garantiza un mejor conocimiento en menor tiempo.
- Tú puedes confiar y estar seguro del aprendizaje porque nuestro staff de instructores es de primer nivel, algunos de los cuales son consultores en reconocidas empresas.
- No pierdas tu tiempo, los cursos están diseñados para un aprendizaje práctico.
- Nuestra garantía: Nuestro compromiso es que tú aprendas, si no quedas satisfecho con los resultados del programa, podrás volver a tomar los cursos hasta tu entera satisfacción o la devolución de tu dinero.

Modalidad de servicio

- Cursos de Calendario
- Cursos Privados: On site y en nuestras instalaciones.
- Cursos Personalizados: Adaptamos el contenido del curso y su duración dependiendo de la necesidad del cliente.
- E-Training: cursos a distancia de forma interactiva, mejorando la capacidad de aprendizaje de nuestros participantes guiados por un instructor en vivo.

Duración: 4 días

Splunk / Splunk Fast Start Core Power User

Working with Time

This three-hour course is for power users who want to become experts at using time in searches. Topics will focus on searching and formatting time in addition to using time commands and working with time zones.

> Description

- Searching with Time
- Formatting Time
- Comparing Index Time versus Search Time
- Using Time Commands
- Working with Time Zones

> Prerequisites

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

- How Splunk works
- Creating Search queries
- The eval command

> Audience

- Search Experts Knowledge Managers

> Objectives

Topic 1 – Searching with Time

- Understand the_time field and timestamps
- View and interact with the event Timeline
- Use the earliest and latest time modifiers
- Use the bin command with the _time field

Topic 2 – Formatting Time

- Use various date and time eval functions to format time

Topic 3 – Using Time Commands

- Use the timechart command
- Use the timewrap command

Topic 4 – Working with Time Zones

- Understand how time and timezones are represented in your data
- Determine the time zone of your server
- Use strftime to correct timezones in results

Statistical Processing

This three-hour course is for power users who want to identify and use transforming commands and eval functions to calculate statistics on their data. Topics will cover data series types, primary transforming commands, mathematical and statistical eval functions, using eval as a function, and the rename and sort commands.

> Description

- What is Data Series
- Transforming Data
- Manipulating Data with eval
- Formatting Data

> Prerequisites

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

- How Splunk works
- Creating Search queries

> Audience

- Search Experts Knowledge Managers

> Objectives

Topic 1 – What is a Data Series

- Introduce data series
- Explore the difference between single-series, multi-series, and time series data series

Topic 2 – Transforming Data

- Use the chart, timechart, top, rare, and stats commands to transform events into data tables
- Explore search modes and their effect on search results

Topic 3 – Manipulating Data with eval Command

- Understand the eval command
- Explore and perform calculations using mathematical and statistical eval functions
- Perform calculations and concatenations on field values
- Use the eval command as a function with the stats command

Topic 4 – Formatting Data

- Use the rename command
- Use the sort command

Comparing Values

This three-hour course is for power users who want to learn how to compare field values using eval functions and eval expressions. Topics will focus on using the comparison and conditional functions of the eval command, and using eval expressions with the fieldformat and where commands.

> Description

- Using eval to Compare
- Filtering with where

> Prerequisites

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

- How Splunk works
- Creating Search queries

> Audience

- Search Experts Knowledge Managers

> Objectives

Topic 1 – Using eval to Compare

- Understand the eval command
- Explain evaluation functions
- Identify and use comparison and conditional functions
- Use the fieldformat command to format field values

Topic 2 – Filtering with where

- Use the where command to filter results
- Use wildcards with the where command
- Filter fields with the information functions, isnull and isnotnull

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

Result Modification

This three-hour course is for power users who want to use commands to manipulate output and normalize data. Topics will focus on specific commands for manipulating fields and field values, modifying result sets, and managing missing data. Additionally, students will learn how to use specific eval command functions to normalize fields and field values across multiple data sources.

> Description

- Manipulating Output
- Modifying Result Sets
- Managing Missing Data
- Modifying Field Values
- Normalizing with eval

> Prerequisites

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

- How Splunk works
- Creating Search queries
- Knowledge Objects

> Audience

- Search Experts Knowledge Managers

> Objectives

Topic 1 – Manipulating Output

- Convert a 2-D table into a flat table with the untable command
- Convert a flat table into a 2-D table with thexyseries command

Topic 2 – Modifying Result Sets

- Append data to search results with the appendpipe command
- Calculate event statistics with the eventstats command
- Calculate "streaming" statistics with the streamstats command
- Modify values to segregate events with the bin command

Topic 3 – Managing Missing Data

- Find missing and null values with the fillnull command

Topic 4 – Modifying Field Values

- Understand the eval command
- Use conversion and text eval functions to modify field values
- Reformat fields with the foreach command

Topic 5 – Normalizing with eval

- Normalize data with eval functions
- Identify eval functions to use for data and field normalization

Correlation Analysis

This three-hour course is for power users who want to learn how to calculate co occurrence between fields and analyze data from multiple datasets. Topics will focus on the transaction, append, appendcols, union, and join commands.

> Description

- Calculate Co-Occurences Between Fields
- Analyze Multiple Datasets

> Prerequisites

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

- How Splunk works
- Creating Search queries
- Lookups

> Audience

- Search Experts Knowledge Managers

> Objectives

Topic 1 – Calculate Co-Occurrence Between Fields

- Understand transactions
- Explore the transaction command

Topic 2 – Analyze Multiple Data Source

- Understand subsearch
- Use the append, appendcols, union, and join commands to combine, analyze, and compare multiple data sources

Creating Knowledge Objects

This three-hour course is for knowledge managers who want to learn how to create knowledge objects for their search environment using the Splunk web interface. Topics will cover types of knowledge objects, the search-time operation sequence, and the processes for creating event types, workflow actions, tags, aliases, search macros, and calculated fields.

> Description

- Knowledge Objects and Search-time Operations
- Creating Event Types
- Using Event Type Builder
- Creating Workflow Actions
- Creating Tags and Aliases
- Creating Serach Macros

> Prerequisites

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

- How Splunk works
- Knowledge Objects

> Audience

- Search Experts Knowledge Managers

> Objectives

Topic 1 – Knowledge Objects & Search-time Operations

- Understand role of knowledge objects for enriching data
- Define search-time operation sequence

Topic 2 – Creating Event Types

- Define event types
- Create event types using three methods
- Tag event types
- Compare event types and reports

Topic 3 – Creating Workflow Actions

- Identify what are workflow actions
- Create a GET, POST, and search workflow action
- Test workflow actions

Topic 4 – Creating Tags and Aliases

- Describe field aliases and tags
- Create field aliases and tags
- Search with field aliases and tags

Topic 5 – Creating Search Macros

- Explain search macros
- Create macros with and without arguments
- Validate macro arguments
- Use and preview macros at search time
- Create and use nested macros
- Use macros with other knowledge objects

Topic 6 – Creating Calculated Fields

- Explain calculated fields
- Create a calculated field
- Use a calculated field in search

Creating Field Extractions

This three-hour course is for knowledge managers who want to learn about field extraction and the Field Extractor (FX) utility. Topics will cover when certain fields are extracted and how to use the FX to create regex and delimited field extractions.

> Description

- Using the Field Extractor
- Creating Regex Field Extractions
- Creating Delimited Field Extractions

> Prerequisites

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

- How Splunk works
- Knowledge Objects

> Audience

- Search Experts Knowledge Managers

> Objectives

Topic 1 – Using the Field Extractor

- Understand types of extracted fields and when they are extracted
- Explore the Splunk Web Field Extractor (FX)

Topic 2 – Creating Regex Field Extractions

- Identify basics of regular expressions (regex)
- Understand the regex field extraction workflow
- Edit regex for field extractions

Topic 3 – Creating Delimited Field Extractions

- Identify delimited field values in event data
- Understand the delimited field extraction workflow

Data Models

This three-hour course is for knowledge managers who want to learn how to create and accelerate data models. Topics will cover datasets, designing data models, using the Pivot editor, and accelerating data models.

> Description

- Introducing Data Model Datasets
- Designing Data Models
- Creating a Pivot
- Accelerating Data Models

> Prerequisites

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

- How Splunk works
- Creating Search queries
- Knowledge Objects

> Audience

- Search Experts Knowledge Managers

> Objectives

Topic 1 – Introducing Data Model Datasets

- Understand data models
- Add event, search, and transaction datasets to data models
- Identify event objects hierarchy and constraints
- Add fields based on eval expressions to transaction datasets

Topic 2 – Designing Data Models

- Create a data model
- Add root and child datasets to a data model
- Add fields to data models
- Test a data model
- Define permissions for a data model
- Upload/download a data model for backup and sharing

Topic 3 – Creating a Pivot

- Identify benefits of using Pivot
- Create and configure a Pivot
- Visualize a Pivot
- Save a Pivot
- Use Instant Pivot
- Access underlying search for Pivot

Topic 4 – Accelerating Data Model

- Understand the difference between ad-hoc and persistent data model acceleration
- Accelerate a data model
- Describe the role of tsidx files in data model acceleration
- Describe the role of tsidx files in data model acceleration
- Review considerations about data model acceleration

Topic 5 – Enriching Data

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