

## Splunk Power User Fast Start

Dieser Kurs richtet sich an Splunk Power User, die Experten in den folgenden Splunk-Themen werden wollen:

### Arbeiten mit Zeit :

für Power-User, die Experten im Umgang mit der Zeit in der Suche werden wollen. Die Themen konzentrieren sich auf die Suche und Formatierung der Zeit sowie auf die Verwendung von Zeitbefehlen und die Arbeit mit Zeitzonen.

### Statistische Verarbeitung :

Identifizierung und Verwendung von Transformationsbefehlen und Eval-Funktionen zur Berechnung von Statistiken über ihre Daten. Die Themen umfassen Typen von Datenreihen, primäre Transformationsbefehle, mathematische und statistische eval-Funktionen, die Verwendung von eval als Funktion sowie die Befehle Umbenennen und Sortieren.

### Werte vergleichen:

Sie lernen, wie man Feldwerte mit eval-Funktionen und eval-Ausdrücken vergleicht. Die Themen konzentrieren sich auf die Verwendung der Vergleichs- und Bedingungsfunktionen des eval-Befehls und die Verwendung von eval-Ausdrücken mit den Befehlen Feldformat und Wo.

### Modifizierung von Ergebnissen:

Verwendung von Befehlen zur Manipulation von Ausgaben und zur Normalisierung von Daten. Die Themen konzentrieren sich auf spezifische Befehle zur Bearbeitung von Feldern und Feldwerten, zur Änderung von Ergebnismengen und zur Verwaltung fehlender Daten. Darüber hinaus lernen die Teilnehmer, wie sie spezifische eval-Befehlsfunktionen zur Normalisierung von Feldern und Feldwerten über mehrere Datenquellen hinweg verwenden können.

### Korrelationsanalyse:

Die Teilnehmer lernen, wie man das gemeinsame Auftreten von Feldern berechnet und Daten aus mehreren Datensätzen analysiert. Die Themen konzentrieren sich auf die Befehle transaction, append, appendcols, union und join.

### Erstellen von Wissensobjekten:

Die Teilnehmer lernen, wie sie mithilfe der Splunk-Webschnittstelle Wissensobjekte für ihre Suchumgebung erstellen können. Die Themen umfassen die Arten von Wissensobjekten, die Reihenfolge der Suchvorgänge und die Prozesse zur Erstellung von Ereignistypen, Workflow-Aktionen, Tags, Aliases, Suchmakros und berechneten Feldern.

### Erstellen von Feldextraktionen:

Sie lernen etwas über Feldextraktion und das Dienstprogramm Field Extractor (FX). Es wird behandelt, wann bestimmte Felder extrahiert werden und wie man den FX verwendet, um Regex- und begrenzte Feldextraktionen zu erstellen.

### Datenmodelle:

Sie lernen, wie Sie Datenmodelle erstellen und beschleunigen können. Die Themen umfassen Datensätze, den Entwurf von Datenmodellen, die Verwendung des Pivot-Editors und die Beschleunigung von Datenmodellen.

### Kursinhalt

- Working with Time
- Statistical Processing
- Comparing Values
- Result Modification
- Correlation Analysis
- Creating Knowledge Objects
- Creating Field Extractions
- Data Models

### Zielgruppe

Der Kurs richtet sich an Splunk Power User.

### Voraussetzungen

Um erfolgreich zu sein, sollten die Studierenden ein solides Verständnis der folgenden Punkte haben:

- Wie Splunk funktioniert
- Erstellen von Suchanfragen

Die Voraussetzungen können mit kostenlosem E-Learning erworben werden. Für den Zugriff auf die E-Learnings ist eine Registrierung bei Splunk erforderlich, falls noch kein Account existiert:

- What is Splunk (Video)
- Intro to Splunk
- Using Fields
- Visualizations
- Intro to Knowledge Objects
- Search Under the Hood

### Kursziel

Certification: Splunk Core Certified Power User

Stand 24.04.2025

### Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link:  
[www.experteach.de/go/SPUF](http://www.experteach.de/go/SPUF)

### Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

### Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

### Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

### Training

Preise zzgl. MwSt.

**Termine in Deutschland** 4 Tage € 4.000,-

**Online Training** 4 Tage € 4.000,-

**Termin/Kursort** Kurssprache Deutsch

19.05.-22.05.25 Online 06.10.-09.10.25 München

23.06.-26.06.25 Online 06.10.-09.10.25 Online

21.07.-24.07.25 München 01.12.-04.12.25 München

21.07.-24.07.25 Online 01.12.-04.12.25 Online

01.09.-04.09.25 Online

# Inhaltsverzeichnis

## Splunk Power User Fast Start

<b>Working with Time :</b>	Convert a 2-D table into a flat table with the untble command	Validate macro arguments
<b>Module 1 - Searching with Time</b>	Convert a flat table into a 2-D table with the xyseries command	Use and preview macros at search time
Understand the _time field and timestamps		Create and use nested macros
View and interact with the Event Timeline		Use macros with other knowledge objects
Use the earliest and latest time modifiers		
Use the bin command with the _time field		
<b>Module 2 - Formatting Time</b>	<b>Module 2 - Modifying Result Sets</b>	<b>Topic 6 – Creating Calculated Fields</b>
Use various date and time eval functions to format time	Append data to search results with the appendpipe command	Explain calculated fields
	Calculate event statistics with the eventstats command	Create a calculated field
	Calculate "streaming" statistics with the streamstats command	Use a calculated field in search
	Modify values to segregate events with the bin command	
<b>Module 3 - Using Time Commands</b>	<b>Module 3 - Managing Missing Data</b>	<b>Creating Field Extractions</b>
Use the timechart command	Find missing and null values with the fillnull command	<b>Module 1 - Using the Field Extractor</b>
Use the timewrap command		Understand types of extracted fields and when they are extracted
<b>Module 4 - Working with Time Zones</b>	<b>Module 4 - Modifying Field Values</b>	Explore the Splunk Web Field Extractor (FX)
Understand how time and timezones are represented in your data	Understand the eval command	
Determine the time zone of your server	Use conversion and text eval functions to modify field values	<b>Module 2 - Creating Regex Field Extractions</b>
Use strftime to correct timezones in results	Reformat fields with the foreach command	Identify basics of regular expressions (regex)
<b>Statistical Processing :</b>	<b>Module 5 - Normalizing with eval</b>	Understand the regex field extraction workflow
<b>Module 1 - What is a Data Series</b>	Normalize data with eval functions	Edit regex for field extractions
Introduce data series	Identify eval functions to use for data and field normalization	
Explore the difference between single-series, multi-series, and time series data series	<b>Correlation Analysis</b>	<b>Module 3 - Creating Delimited Field Extractions</b>
<b>Module 2 - Transforming Data</b>	<b>Module 1 - Calculate Co-Occurrence Between Fields</b>	Identify delimited field values in event data
Use the chart, timechart, top, rare, and stats commands to transform events into data tables	Understand transactions	Understand the delimited field extraction workflow
<b>Module 3 - Manipulating Data with eval Command</b>	Explore the transaction command	<b>Data Models</b>
Understand the eval command	<b>Module 2 - Analyze Multiple Data Sources</b>	<b>Module 1 - Introducing Data Model Datasets</b>
Explore and perform calculations using mathematical and statistical eval functions	Understand subsearch	Understand data models
Perform calculations and concatenations on field values	Use the append, appendcols, union, and join commands to combine, analyze, and compare multiple data sources	Add event, search, and transaction datasets to data models
Use the eval command as a function with the stats command	Creating Knowledge Objects	Identify event object hierarchy and constraints
<b>Module 4 - Formatting Data</b>	<b>Topic 1 – Knowledge Objects &amp; Search-time Operations</b>	Add fields based on eval expressions to transaction datasets
Use the rename command	Understand role of knowledge objects for enriching data	<b>Module 2 - Designing Data Models</b>
Use the sort command	Define search-time operation sequence	Create a data model
<b>Comparing Values</b>	<b>Topic 2 – Creating Event Types</b>	Add root and child datasets to a data model
<b>Module 1 - Using eval to Compare</b>	Define event types	Add fields to data models
Understand the eval command	Create event types using three methods	Test a data model
Explain evaluation functions	Tag event types	Define permissions for a data model
Identify and use comparison and conditional functions	Compare event types and reports	Upload/download a data model for backup and sharing
Use the fieldformat command to format field values	<b>Topic 3 – Creating Workflow Actions</b>	<b>Module 3 - Creating a Pivot</b>
<b>Module 2 - Filtering with where</b>	Identify what are workflow actions	Identify benefits of using Pivot
Use the where command to filter results	Create a GET, POST, and search workflow action	Create and configure a Pivot
Use wildcards with the where command	Test workflow actions	Visualize a Pivot
Filter fields with the information functions, isnull and isnotnull	<b>Topic 4 – Creating Tags and Aliases</b>	Save a Pivot
<b>Result Modification</b>	Describe field aliases and tags	Use Instant Pivot
<b>Module 1 - Manipulating Output</b>	Create field aliases and tags	<b>Access underlying search for Pivot</b>
	▪ Search with field aliases and tags	<b>Module 4 - Accelerating Data Models</b>
	<b>Topic 5 – Creating Search Macros</b>	Understand the difference between ad-hoc and persistent data model acceleration
	Explain search macros	Accelerate a data model
	Create macros with and without arguments	Describe the role of tsidx files in data model acceleration
		Review considerations about data model acceleration

