مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ - ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

Splunk Fundamentals ۲

یادگیری جست‌وجوهای پیشرفته، مصورسازی داده‌ها و ایجاد Knowledge Objectها در Splunk.

مروری بر دوره

دوره ۲ **Splunk Fundamentals** ادامه‌ی مسیر یادگیری Splunk پس از گذراندن سطح مقدماتی (ndamentals ۱) است و به شرکت‌کنندگان کمک می‌کند تا مهارت‌های پیشرفته‌تری در جست‌وجو، تحلیل و مدیریت داده‌ها در محیط Splunk به‌دست آورند.

در این دوره، تمرکز بر استفاده از دستورات **Transforming** و **Visualization** برای نمایش داده‌ها، فیلتر و قالب‌بندی نتا همبستگی رخدادها (**Event Correlation**) و ساخت **Knowledge Object**ها مانند فیلدهای محاسباتی، برچسبه (Tags)، نوع رخداد (Event Types)، ماکروها و اکشن‌های Workflow است.

همچنین شرکت‌کنندگان با مفاهیم پیشرفته‌ای مانند **Data Models** و **Common Information Model** (**CIM**) آشنا می‌شوند که برای استانداردسازی داده‌ها و تحلیل یکپارچه در محیط Splunk به‌کار می‌روند.
این دوره برای کسانی طراحی شده است که می‌خواهند از Splunk نه‌تنها برای جست‌وجو، بلکه برای تحلیل هوشمند داده‌ها و توسعه دانش سازمانی بهره ببرند.

آنچه در این دوره خواهید آموخت

- استفاده از دستورات Transforming برای تحلیل و مصورسازی داده‌ها
- فیلتر و قالب‌بندی نتایج جست‌وجو
- همبسته‌سازی رخدادها (Correlate Events) در قالب تراکنش‌ها
- ایجاد و مدیریت **Knowledge Object**ها
- ساخت و مدیریت فیلدهای استخراج‌شده، فیلدهای جایگزین و فیلدهای محاسباتی
- ایجاد **Tags** و **Event Types** برای دسته‌بندی داده‌ها

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ - ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- طراحی و استفاده از **Macros** و **Workflow Actions**
- ایجاد و مدیریت **Data Models**
- استفاده از **CIM** (**Splunk Common Information Model**) برای نرمال‌سازی داده‌ها

سرفصل ها

Module ۱: Beyond Search Fundamentals

Module ۲: Using Transforming Commands for Visualization

Module ۳: Using Trendlines, Mapping, and Single Value Commands

Module ۴: Filtering Results and Manipulating Data

Module ۵: Correlating Events

Module ۶: Understanding Knowledge Objects

Module ۷: Creating and Managing Fields

Module ۸: Creating Field Aliases and Calculated Fields

Module ۹: Creating Tags and Event Types

Module ۱۰: Creating and Using Macros

Module ۱۱: Creating Data Models

Module ۱۲: Using the Common Information Model (CIM) Add-on

مخاطبان دوره

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- تحلیلگران داده و امنیت که دوره Fundamentals ۱ را گذرانده‌اند
- مدیران و کارشناسان IT، مانیتورینگ و SOC
- توسعه‌دهندگان و متخصصان داده که با Splunk کار می‌کنند
- کاربرانی که قصد دارند در ساخت مدل‌های داده و استانداردسازی اطلاعات در Splunk مهارت یابند