SEMATEC
IT Professional Training Center

Splunk Fundamentals 1 & 2

خلاصه دوره : اسپلانک یکی از نرم افزارهای برتر در حوزه ی مانیتورینگ و مراکز امنیت (SOC) می باشد که کاربران بخش امنیت سازمان ها و شرکت ها از آن برای ذخیره ی Logها و سپس جستجو، ایجاد گزارش و داشبورد سازی، ایجاد هشدار، Threat Hunting و SOAR استفاده میکنند. استفاده از تمام قابلیت ها و جزییات موجود در اسپلانک دانشی گسترده در این زمینه نیاز دارد که باعث شده تعداد متخصصین این نرم افزار در دنیا بسیار کم باشند.

مدت دوره : ۴۰ ساعت برای هر ۲ دوره

پیش نیاز : آشنایی با مفاهیم شبکه و امنیت

مخاطب :

- کارشناسان و مدیران حوزه امنیت
- افراد علاقه مند به کار در حوزه SOC
- کارشناسان Splunk که میتوانند با استفاده از این دوره دید کافی در مورد نرم افزار اسپلانک بدست بیاورند و یا هدف آن ها فعالیت در حوزه ی کارشناس SOC شوند.

اهداف دوره : در ابتدا با اسپلانک، Big Data و نحوه ی استفاده از آن آشنا میشویم سپس اسپلانک را در محیط های مختلف نصب می کنیم و با Search، Report، Fieldها به صورت عملی کار خواهد شد. در مورد Best Practiceهای قابل انجام، زبان SPL، دستورهای Transformer، Pivot، DataSetها صحبت خواهیم کرد و در ادامه در مورد Lookup ها و نحوه ی Enrich کردن، بحث خواهد شد و در انتهای دوره Fundamental 1 به Alertها ، Report و نحوه ی ایجاد Automation و Action خواهیم پرداخت.

در دوره ی Fundamental 2 به مباحث دیگر Search و Job Inspector ، ایجاد گزارش های گرافیکی توسط دستورات Transforming، ایجاد گزارش آماری با توجه به نقشه ی جغرافیایی، فیلترینگ نتایج جستجو، Correlat کردن داده ها، ایجاد Knowledge Objectها، استفاده از RegEx برای استخراج Fieldها، تغییر در نام گذاری Fieldها ، ایجاد Tag و Event Typeها، ایجاد Macro و نحوه ی استفاده از آن، ایجاد Data Modelها و در نهایت استفاده از Common Information Model (CIM) خواهیم پرداخت.

IT Professional Training Center

در انتهای این دوره دانشجویان قادر خواهند بود :

در انتهای دوره دانشجویان میتوانند اسپلانک را برای دریافت داده، ایجاد دستورات برای جستجو در داده ها، ایجاد داشبورد، گزارشگیری، هشدار و پاسخ به رخدادها ، تنظیم و کانفیگ نمایند و در امتحان Splunk Core Certified User شرکت نمایند.

سرفصل دوره :

Splunk Fundamental 1

Module 2 – What is Splunk?

- **Splunk components**
- **Installing Splunk**
- **Getting data into Splunk**

Module 3 – Introduction to Splunk's User Interface

- **Understand the uses of Splunk**
- **Define Splunk Apps**
- **Customizing your user settings**
- **Learn basic navigation in Splunk**

Module 4 – Basic Searching

- **Run basic searches**
- **Use autocomplete to help build a search**
- **Set the time range of a search**
- **Identify the contents of search results**
- **Refine searches**
- **Use the timeline**
- **Work with events**
- **Control a search job**
- **Save search results**

Module 5 – Using Fields in Searches

- **Understand fields**
- **Use fields in searches**
- **Use the fields sidebar**

Module 6 – Search Language Fundamentals

- **Review basic search commands and general search**
- **practices**
- **Examine the search pipeline**
- **Specify indexes in searches**
- **Use autocomplete and syntax highlighting**
- **Use the following commands to perform searches:**
- **tables**
- **rename**
- **fields**
- **dedup**
- **sort**

Module 7 – Using Basic Transforming Commands

- **The top command**
- **The rare command**
- **The stats command**

Module 8 – Creating Reports and Dashboards

- **Save a search as a report**
- **Edit reports**
- **Create reports that include visualizations such as charts and**
- **tables**

- **Create a dashboard**
- **Add a report to a dashboard**

- **Edit a dashboard**

Module 9 – Datasets and the Common Information Model

- **Naming conventions**
- **What are datasets?**
- **What is the Common Information Model (CMI)?**

Module 10 – Creating and Using Lookups

- **Describe lookups**
- **Create a lookup file and create a lookup definition**
- **Configure an automatic lookup**

Module 11 – Creating Scheduled Reports and Alerts

- **Describe scheduled reports**
- **Configure scheduled reports**
- **Describe alerts**
- **Create alerts**
- **View fired alerts**

Module 12 - Using Pivot

- **Describe Pivot**
- **Understand the relationship between data models and pivot**
- **Select a data model object**
- **Create a pivot report**
- **Create an instant pivot from a search**
- **Add a pivot report to a dashboard**

IT Professional Training Center

Splunk Fundamental 2

Module 2 – Beyond Search Fundamentals

- **Search fundamentals review**
- **Case sensitivity**
- **Using the job inspector to view search performance**

Module 3 – Using Transforming Commands for

- **Visualizations**
- **Explore data structure requirements**
- **Explore visualization types**
- **Create and format charts and timecharts**

Module 4 – Using Mapping and Single Value Commands

- **The iplocation command**
- **The geostats command**
- **The geom command**
- **The addtotals command**

Module 5 –Filtering and Formatting Results

- **The eval command**
- **Using the search and where commands to filter results**
- **The filnull command**

Module 6 – Correlating Events

- **Identify transactions**
- **Group events using fields**
- **Group events using fields and time**
- **Search with transactions**

- **Report on transactions**
- **Determine when to use transactions vs. stats**

Module 7 – Introduction to Knowledge Objects

- **Identify naming conventions**
- **Review permissions**
- **Manage knowledge objects**

Module 8 – Creating and Managing Fields

- **Perform regex field extractions using the Field Extractor (FX)**
- **Perform delimiter field extractions using the FX**

Module 9 – Creating Field Aliases and Calculated Fields

- **Describe, create, and use field aliases**
- **Describe, create and use calculated fields**

Module 10 – Creating Tags and Event Types

- **Create and use tags**
- **Describe event types and their uses**
- **Create an event type**

Module 11 – Creating and Using Macros

- **Describe macros**
- **Create and use a basic macro**
- **Define arguments and variables for a macro**
- **Add and use arguments with a macro**

Module 12 – Creating Data Models

- **Describe the relationship between data models and pivot**
- **Identify data model attributes**
- **Create a data model**
- **Use a data model in pivot**

IT Professional Training Center

Module 13 – Using the Common Information Model (CIM)

- **Add-On**
- **Describe the Splunk CIM**
- **List the knowledge objects included with the Splunk CIM**
- **Add-On**
- **Use the CIM Add-On to normalize data**

منبع درسی: https://docs.splunk.com/Documentation