Splunk Fundamental

مقدمه

Splunk یک پلت فرم نرم افزاری برای جستجو، تجزیه و تحلیل و تجسم داده های تولید شده توسط ماشین جمع آوری شده از وب سایت ها، برنامه ها، حسگرها، دستگاه ها و غیره است که زیرساخت فناوری اطلاعات و تجارت شما را تشکیل می دهند.

Splunk یک فناوری پیشرفته، مقیاس پذیر و مؤثر است که پرونده های ثبت شده در یک سیستم را فهرست بندی و جستجو می کند. اسپلانک این داده های تولید شده توسط ماشین را تجزیه و تحلیل می کند تا بر مبنای هوش ماشین برنامه عملیاتی را ارائه دهد.

مدت زمان دوره:

32 ساعت – حضوری / آنلاین

اهداف دوره:

- ارزیابی وضعیت امنیت، مانیتورینگ، کنترل رویداد و هشدار
- تحلیل و بررسی نقض داده ها
- پاسخ گویی به تهدیدات پیش رو
- همبستگی های بین رویداد ها
- جستجو های زمینه ای
- تحلیل و شناسایی سریع تهدیدات پیشرفته
- ساده سازی روند مدیریت تهدیدات

سرفصل دوره ی آموزشی:

- **Splunk Fundamental**
- Introducing Splunk
- Understand the uses of Splunk
- Define Splunk Apps
- Learn basic navigation in Splunk
- **Searching**
- Run basic searches
- Use autocomplete to help build a search
- Set the time range of a search
- Identify the contents of search results

Splunk Fundamental

- **The stats command**

Creating and Using Lookups

- Describe lookups
- Examine a lookup file example
- Create a lookup file and create a lookup definitio
- Configure an automatic lookup
- Use the lookup in searches

Creating Scheduled Reports and Alerts

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

- Use the timeline
- **Work with events**
- **Control a search job**
- **2 Save search results**

Using Fields in Searches

- **Understand fields**
- **Use fields in searches**
- **Use the fields sidebar**
- **Use search modes (fast, verbose, and smart)**

Creating Reports and Dashboards

- **Save a search as a report**
- **Edit reports**
- **Create reports that display statistics (tables)**
- **Create reports that display visualizations (charts)**
- **Create a dashboard**
- **Add a report to a dashboard**
- **Edit a dashboard**

Splunk's Search Language Fundamentals

- **Understand the search pipeline**
- **Understand search syntax concepts**
- **Use the following commands to perform searches:**
- **Tables**
- **Rename**
- **Fields**
- **Dedup**
- **sort**

Using Basic Transforming Commands

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

پیش نیازهای دوره

Network+ و Lpic1 از پیش نیاز های این دوره آموزشی می باشد

درباره ی مدرک

به شرکت کنندگان در این دوره ی آموزشی گواهی حضور از سوی موسسه ITHOUSE اعطا خواهد شد.

درباره ی IT HOUSE

تیم مدیریتی IT House از سال ۱۳۸۷ به صورت جدی به منظور ارائه‌ی خدمات مشاوره‌ای و آموزشی در حوزه‌ی چارچوب‌های مدیریتی فناوری اطلاعات پا به عرصه‌ی ظهور گذاشت. این گروه در ابتدا تحت نام‌های تجاری دیگری همچون NIS ICT شروع به فعالیت نموده که در سال ۱۳۹۸ به منظور ارائه‌ی خدمات جدید و متفاوت برند IT House را ایجاد نموده‌اند. IT House با اتکا به توانمندی نیروهای متخصص داخلی و همینطور حمایت شبکه‌ای گسترده از شرکای بین‌المللی، همچون گذشته آمادگی دارد سبد کاملی از خدمات مورد نیاز سازمان‌ها را در حوزه‌های استانداردها و چارچوب‌های مدیریت فناوری اطلاعات و امنیت اطلاعات، ارائه نماید. حوزه‌های اصلی فعالیت این شرکت چارچوب‌ها و استانداردها و بهروش‌های مدیریتی فناوری اطلاعات از جمله و نه محدود به موارد مندرج در دیاگرام‌های ذیل است که در هر یک از چارچوب‌های درج شده خدمات مرتبط با:

- آموزش
- مشاوره
- نرم‌افزار
- ممیزی و صدورگواهینامه
- ارزیابی

بسته به نوع محصول، ارائه می‌شود.

تماس با IT HOUSE

آدرس:
تهران، سهروردی شمالی،کوچه تهمتن، پلاک 6 واحد 7
تلفن: + 98 (0) 21 88731466
فکس: + 98 (0) 21 86031447
وبسایت: www.it-house.me