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

دوره مقدماتی اسپلانک دژبان

پکیج جامع Splunk شامل سه بخش عملیاتی و امنیتی، آموزش جستجو، داشبورد، گزارش‌گیری، Knowledge Objects و دفاع سایبری برای تحلیل داده و SOC.

مروری بر دوره

این پکیج جامع آموزشی شما را از مفاهیم پایه تا مباحث پیشرفته و امنیتی در **Splunk** هدایت می‌کند و شامل سه بخش اصلی است که با تمرین‌های عملی و سناریو محور، توانایی شما در تحلیل داده، گزارش‌گیری، مدیریت اطلاعات و دفاع سایبری افزایش می‌دهد.

۱ Splunk Fundamentals

این بخش به شما آموزش می‌دهد چگونه در Splunk جستجو و پیمایش کنید، از فیلدها استفاده کنید، آمار داده‌های خود را استخراج کنید، گزارش و داشبورد بسازید، Lookups و Alerts ایجاد کنید. مثال‌های مبتنی بر سناریو و تمرین‌های عملی به شما امکان می‌دهد جستجوها، گزارش‌ها و نمودارهای قدرتمند بسازید. همچنین قابلیت‌های datasets و Pivot Splunk معرفی می‌شوند.

۲ Splunk Fundamentals

این بخش بر دستورات جستجو و گزارش‌گیری و همچنین ایجاد Knowledge Objects تمرکز دارد. مباحث اصلی شامل استفاده از دستورات transforming و Visualizations، فیلتر و فرمت نتایج، همبستگی رویدادها، ایجاد Knowledge Objects، استفاده از Field Aliases و Calculated Fields، ایجاد Tags و Event Types، استفاده از Workflow Actions، Macros و Data Models و نرمال‌سازی داده‌ها با Common Information Model (CIM) است.

Splunk Certified Cybersecurity Defense Analyst

در این بخش با چشم‌انداز سایبری، چارچوب‌ها و استانداردها، انواع تهدیدات و حملات، دفاع‌ها، منابع داده و بهترین شیوه‌های SIEM، بررسی، همبستگی و مدیریت ریسک، زبان جستجوی SPL و تکنیک‌های Threat Hunting و Remediation آشنا

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

می‌شوید.

آنچه در این دوره خواهید آموخت

۱ Splunk Fundamentals

- شناسایی مفاهیم پایه Splunk، کاربردها و پیمایش آن
- اجرای جستجوهای پایه و تحلیل نتایج
- استفاده از فیلدها در جستجو
- مدیریت گزارش‌ها و داشبوردها
- درک syntax و Search Pipeline
- استفاده از دستورات top، stats و rare
- ایجاد Lookup File، تعریف Lookup و Automatic Lookup
- ایجاد گزارش‌ها و Alerts زمان‌بندی‌شده
- Identify basic Splunk concepts, use cases, and navigation
- Run basic searches and identify the contents of search results
- Understand fields and use them in searches
- Manage reports and dashboards
- Understand search language syntax and the search pipeline
- Use the stats, top, and rare commands
- Create a lookup file, a lookup definition, and an automatic lookup
- Create scheduled reports and alerts

۲ Splunk Fundamentals

- استفاده از transforming commands و Visualizations
- فیلتر و فرمت نتایج جستجو
- همبستگی رویدادها به تراکنش‌ها

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

- ایجاد و مدیریت Knowledge Objects
- ایجاد و مدیریت Field Aliases، Extracted Fields و Calculated Fields
- ایجاد Tags و Event Types
- استفاده از Macros و Workflow Objects
- ایجاد و مدیریت Data Models
- استفاده از Common Information Model (CIM)
- Use transforming commands and visualizations
- Filter and format the results of a search
- Correlate events into transactions
- Create and manage Knowledge Objects
- Create & manage extracted fields, field aliases, and calculated fields
- Create tags and event types
- Create and use macros and workflow objects
- Create and manage data models
- Use the Splunk Common Information Model (CIM)

Splunk Certified Cybersecurity Defense Analyst

- چشم‌انداز امنیت سایبری و چارچوب‌ها
- درک تهدیدات و انواع حملات
- عملیات امنیتی و نقش Defense Analyst
- مقدمه‌ای بر Splunk و داده‌ها برای تحلیلگران امنیتی
- معرفی Enterprise Security و جستجوهای پیشرفته
- مهارت‌های بررسی و تحلیل رویدادها
- اصول SOC و استفاده از Splunk ES

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

- تهدیدیابی و مدیریت اقدامات اصلاحی
- The Cybersecurity Landscape
- Understanding Threats and Attacks
- Security Operations and the Defense Analyst
- Intro to Splunk
- Data and Tools for Defense Analysts
- Introduction to Enterprise Security
- Search under the hood
- The Art of investigation
- SOC Essentials: Investigating with Splunk ES
- SOC Essentials: Introduction to Threat Hunting
- Using Splunk Enterprise Security

سرفصل ها

Splunk Fundamentals ۱

❑ Module ۱: Introducing Splunk

❑ Module ۲: Searching

❑ Module ۳: Using Fields in Searches

❑ Module ۴: Creating Reports and Dashboards

❑ Module ۵: Splunk’s Search Language

❑ Module ۶: Transforming Commands

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

❑ Module ۷: Creating and Using Lookups

❑ Module ۸: Creating Scheduled Reports and Alerts

Splunk Fundamentals ۲

❑ 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

Splunk Certified Cybersecurity Defense Analyst

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

- ❑ The Cybersecurity Landscape
- ❑ Understanding Threats and Attacks
- ❑ Security Operations and the Defense Analyst
- ❑ Intro to Splunk
- ❑ Data and Tools for Defense Analysts
- ❑ Introduction to Enterprise Security
- ❑ Search under the hood
- ❑ The Art of investigation
- ❑ SOC Essentials: Investigating with Splunk ES
- ❑ SOC Essentials: Introduction to Threat Hunting
- ❑ Using Splunk Enterprise Security

مخاطبان دوره

- تحلیلگران داده و علاقه‌مندان به **Data Analytics**
- علاقه‌مندان و متخصصان امنیت سایبری و **SOC**
- افرادی که می‌خواهند مهارت‌های عملی در **Splunk**، گزارش‌گیری و داشبوردسازی کسب کنند
- مدیران فناوری اطلاعات و کارشناسان شبکه که به دنبال مدیریت داده‌ها و امنیت عملیاتی هستند
- دانشجویان و فارغ‌التحصیلانی که قصد ورود به حوزه‌های تحلیل داده و امنیت اطلاعات را دارند