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

کمپ نوروزی Splunk
Fundamentals & Enterprise Sys Admin

دوره جامع Splunk

مروری بر دوره

این دوره که دوره جامع Splunk شناخته می شود به آموزش سرفصل های مقدماتی تا پیشرفته Splunk خواهد پرداخت تا در انتها از شما یک متخصص حوزه کار با Splunk بسازد. سرفصل این دوره متشکل از دوره های زیر می باشد:

- Splunk Fundamentals ۱&۲
- Splunk Enterprise System & Data Administration

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
- Module ۷: Creating and Using Lookups
- Module ۸: Creating Scheduled Reports and Alerts

Splunk Fundamentals ۲

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

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

Splunk Enterprise System Administration

- Module ۱: Splunk Deployment Overview
- Module ۲: License Management
- Module ۳: Splunk Apps
- Module ۴: Splunk Configuration Files
- Module ۵: Splunk Indexes
- Module ۶: Splunk Index Management
- Module ۷: Splunk User Management
- Module ۸: Configuring Basic Forwarding

Splunk Enterprise Data Administration

- Module ۱: Introducing Splunk Data Administration
- Module ۲: Getting Data In – Staging
- Module ۳: Forwarder Configuration

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

- Module ۴: Heavy Forwarders & Forwarder Management
- Module ۵: Monitor Inputs
- Module ۶: Network and Scripted Inputs Module
- Module ۷: Fine-tuning Inputs
- Module ۸: Parsing Phase and Data Preview
- Module ۹: Manipulating Raw Data

Using Splunk Enterprise Security

- Getting Started with Enterprise Security
- Security Monitoring and Incident Investigation
- Investigations
- Using Security Domain Dashboards
- Risk Analysis
- Web Intelligence
- User Intelligence
- Threat Intelligence
- Protocol Intelligence

Administering Splunk Enterprise Security

- Introduction to ES
- Security Monitoring
- Incident Investigation
- Analyst Tools & Dashboards
- ES On-prem Deployment
- Installation
- Initial Configuration

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

- Validating ES Data
- Tuning Correlation Searches
- Creating Correlation Searches
- Asset & Identity Management
- Threat Intelligence Framework