Carrier Digit

کاریارارقام

مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی

و برگزارکننده دوره های آموزشی

Splunk

Splunk

مدت(ساعت): ۴۰ **پیش نیاز:** مبانی اولیه امنیت **اعتبار دهنده:** ندارد

معرفی دوره :

در این دوره نحوه کار با پلتفرم تحلیل داده های Splunk با رویکرد امنیتی ارایه خواهد شد. دانشجویان در این دوره ضمن فراگیری کار با Splunk، با متدهای تحلیل داده های امنیتی (لاگ و ترافیک شبکه) نیز آشنا خواهند شد. عمده مباحث این دوره به صورت عملیاتی آموزش داده می شود.

امتیازات دوره :

- اعطای مدرک فارسی و انگلیسی با مجوز رسمی از :
  - مجوز از اداره کل نظام مدیریت امنیت اطلاعات (نما)
  - سازمان مدیریت و برنامه ریزی کشور (معاونت توسعه مدیریت و سرمایه انسانی رئیس جمهوری سابق)
  - شورای عالی انفورماتیک
  - قابلیت ترجمه وتایید قوه قضاییه وامور خارجه
- بهره گیری از اساتید مجرب و تأیید شده با سابقه حضور در پروژه‌های ملی

اهداف دوره :

- آشنایی با مولفه ها و معماری Splunk
- آشنایی با انواع داده های مورد نیاز تحلیل
- آموزش عملیاتی کار با Splunk و جستجوی پیشرفته
- آموزش بصری سازی و تولید گزارش در Splunk
- آموزش عملیاتی نحوه تشخیص تهدیدات و تکنیک های تحلیل داده

مخاطبان دوره :

- تحلیلگران امنیت
- کارشناسان مرکز عملیات امنیت
- مدیران سیستم و شبکه
- کاربران Splunk
- کارشناسان تحلیل نفوذ و حملات سایبری

محتوای دوره :

Log Analysis with Splunk (Advanced Searching)
- Advanced Searching
- Log Analysis Techniques
- Correlating events
- Sample APT Detection using SPL
- Sample Ransomware Detection Using SPL

Splunk Administration
- Splunk Deployment Overview
- License Management
- Splunk Apps
- Splunk Configuration Files
- Users, Roles, and Authentication
- Distributed Search

Course Outline :

Introduction and Components
- Introduction to Splunk's interface
- Introduction To Splunk Components (Forwarder, Indexer, Search Head)
- Basic searching and SPL Queries
- Using fields in searches
- Creating reports and dashboards
- Datasets
- The Common Information Model (CIM)
- Creating and using lookups
- Scheduled Reports
- Alerts
- Using Pivot

تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳،۸ فاکس: ۸۸۰۶۵۲۲۲