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

تحلیل گر سطح یک مرکز عملیات امنیت با splunk

آموزش عملی تحلیل رخدادهای امنیتی با Splunk؛ ورود به نقش تحلیلگر SOC با مهارت‌های پایش، تشخیص تهدید و پاسخ سریع در محیط‌های واقعی.

مروری بر دوره

در این دوره، شرکت‌کنندگان با وظایف، ابزارها و فرآیندهای کلیدی یک تحلیلگر امنیتی در سطح مقدماتی Security Operations Center) SOC) آشنا می‌شوند. تمرکز دوره بر درک چرخه‌ی کشف، تحلیل و پاسخ به رخدادهای امنیتی است و با بهره‌گیری از Splunk به عنوان پلتفرم SIEM اصلی، مهارت‌های عملی تحلیل داده‌های امنیتی و تشخیص تهدیدها تمرین خواهد شد.

دوره با رویکردی کاملاً عملی طراحی شده است تا دانشجویان بتوانند لاگ‌ها را جست‌وجو، هم‌بسته سازی (correlate) و تحلیل کنند، الگوهای رفتاری مشکوک را شناسایی نمایند و گزارشی حرفه‌ای از یافته‌های خود ارائه دهند.

در پایان دوره، فراگیران درک عمیقی از نقش SOC، انواع هشدارها و حملات رایج، و نحوه‌ی کار با Splunk برای پایش و پاسخ‌گویی سریع به رویدادهای امنیتی خواهند داشت.

آنچه در این دوره خواهید آموخت

- آشنایی با ساختار، مأموریت و نقش‌های مختلف در مرکز عملیات امنیت (SOC)
- درک مسئولیت‌های تحلیلگر SOC لایه ۱ (Tier ۱ Analyst)
- شناخت مفاهیم SIEM و چرایی استفاده از Splunk
- جست‌وجوی لاگ‌ها و استفاده از SPL (Search Processing Language) در Splunk
- تحلیل لاگ‌های امنیتی از منابع مختلف (فایروال، AD، endpoint، IDS/IPS و غیره)

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

- تشخیص الگوهای مشکوک و تحلیل هشدارها (alerts)
- دسته‌بندی و اولویت‌بندی رویدادها بر اساس شدت و تأثیر
- گزارش‌دهی و مستندسازی رخدادها در SOC
- آشنایی مقدماتی با فرایند Incident Response و Escalation
- کار با داشبوردها و ساخت گزارش‌های خودکار در Splunk

سرفصل ها

- مقدمه و مبانی SOC
- مفاهیم پایه امنیت سایبری
- ساختار و نقش‌های SOC
- مدل سه‌لایه ۳-۱ Tier) SOC)
- مفاهیم SIEM و معرفی Splunk
- اصول SIEM و نیاز به همبستگی لاگ‌ها
- نصب و معماری Splunk
- مفاهیم Index، Source type، و Data Input
- کار با Splunk و SPL (Search Processing Language)
- جست‌وجوی پایه و پیشرفته در Splunk
- فیلترها، فیلدها، و عملگرها
- آشنایی با stats، eval، timechart و lookup
- تحلیل داده‌های امنیتی در Splunk
- تحلیل لاگ فایروال، Windows Event، IDS و Syslog
- تشخیص فعالیت‌های غیرعادی (Anomalies)
- تشخیص brute force، phishing، lateral movement
- کار با داشبوردها و گزارش‌ها

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

- ایجاد داشبورد و پنل‌های نظارتی
- ساخت هشدارها (Alerts) و Thresholdها
- گزارش‌دهی خودکار و مستندسازی
- مدیریت هشدارها و واکنش اولیه (Tier ۱ Response)
- تحلیل هشدار، triage و escalation
- مستندسازی رخدادها در Ticketing System
- تعامل با تیم‌های Tier ۲/۳
- تمرین عملی و سناریوهای واقعی
- تحلیل سناریوی حمله واقعی در Splunk
- شناسایی و پاسخ اولیه به compromise indicators

مخاطبان دوره

- تحلیلگران تازه‌وارد به تیم SOC
- دانشجویان رشته‌های امنیت سایبری و شبکه
- کارشناسان IT و Helpdesk علاقه‌مند به ورود به حوزه امنیت
- افراد متقاضی شغل “Security Operations Analyst (Tier ۱)”

پیش نیاز ها

- آشنایی مقدماتی با مفاهیم شبکه (TCP/IP، Ports، Protocols)
- درک اولیه از مفاهیم امنیت اطلاعات (CIA، Threats، Vulnerabilities)