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

دوره سطح پیشرفته مرکز عملیات امنیت (SOC) | آموزش سطح پیشرفته SOC

شامل کد دوره های SEC۵۱۱، SEC۵۰۳ و SEC۵۳۰

مروری بر دوره

این دوره ضمن ارائه دانش فنی لازم همراه با آموزش های عملی، به صورت تخصصی و عمیق مهارت های شما در حوزه امنیت را تقویت می کند تا در دفاع از شبکه خود با اطمینان بیشتری عمل کنید.

شما در این دوره می آموزید که چگونه در مدل مرجع TCP/IP و پرکاربردترین پروتکل های کاربردی مانند HTTP ترافیک شبکه را به صورت هوشمند برای نشانه های نفوذ بررسی کنید. در این دوره شما ضمن فراگیری دانش IDS و انواع آن به صورت عملی و تخصصی، با نگاه و رویکردی جدید به موضوع معماری امنیت به صورت مستمر به ارزیابی وضعیت فعلی معماری امنیتی خواهید پرداخت.

آشنایی کامل با مفاهیم SIEM و کسب تسلط هر چه بیشتر در معماری های امنیتی و طراحی آنها مثل Zero Trust از جمله مفاهیمی خواهد بود که شما به عنوان مهندس امنیت در ادامه این دوره با آن آشنا خواهید شد.

سرفصل ها

- SEC۵۰۳: Intrusion Detection In-Depth
- SEC۵۰۳.۱: Fundamentals of Traffic Analysis: Part I
- SEC۵۰۳.۲: Fundamentals of Traffic Analysis: Part II
- SEC۵۰۳.۳: Signature Based Detection
- SEC۵۰۳.۴: Anomalies and Behaviors
- SEC۵۰۳.۵: Modern and Future Monitoring: Forensics, Analytics, and Machine Learning
- SEC۵۰۳.۶: IDS Capstone Challenge

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

- SEC۵۱۱: Continuous Monitoring and Security Operations
- SEC۵۱۱.۱: Current State Assessment, Security Operations Centers, and Security Architecture
- SEC۵۱۱.۲: Network Security Architecture
- SEC۵۱۱.۳: Network Security Monitoring
- SEC۵۱۱.۴: Endpoint Security Architecture
- SEC۵۱۱.۵: Automation and Continuous Security Monitoring
- SEC۵۱۱.۶: Capstone: Design, Detect, Defend

- SEC۵۳۰: Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise
- SEC۵۳۰.۱: Defensible Security Architecture and Engineering: A Journey Towards Zero Trust
- SEC۵۳۰.۲: Network Security Architecture and Engineering
- SEC۵۳۰.۳: Network-Centric Application Security Architecture
- SEC۵۳۰.۴: Data-Centric Application Security Architecture
- SEC۵۳۰.۵: Zero-Trust Architecture: Addressing the Adversaries Already in Our Networks
- SEC۵۳۰.۶: Hands-On Secure the Flag Challenge

پیش نیاز ها

- شرکت در دوره مقدماتی SOC و یا برخورداری از دانشی معادل با آن