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

پکیج مقدماتی تا پیشرفته تشخیص نفوذ

شامل دوره های SEC۴۰۱, SEC۵۰۳, SEC۵۵۵

مروری بر دوره

دانشجویان با شرکت در این دوره جامع ضمن فراگیری مباحث مربوط به مانیتورینگ و تشخیص نفوذ، بینش و دانش کافی جهت تشخیص حملات را کسب خواهند نمود. این دوره که در قالب پک ارائه خواهد شد به طور جامع از مقدماتی ترین تا پیشرفته ترین مطالب حوزه تشخیص نفوذ را پوشش خواهد داد.

سرفصل ها

SEC۴۰۱

- SEC۴۰۱.۱: Network Security Essentials
- SEC۴۰۱.۲: Defense-in-Depth
- SEC۴۰۱.۳: Vulnerability Management and Response
- SEC۴۰۱.۴: Data Security Technologies
- SEC۴۰۱.۵: Windows Security
- SEC۴۰۱.۶: Linux, Mac and Smartphone Security

SEC۵۰۳

- 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

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

Learning

- SEC۵۰۳.۶: IDS Capstone Challenge

SEC۵۵۵

- SEC۵۵۵.۱: SIEM Architecture
- SEC۵۵۵.۲: Service Profiling with SIEM
- SEC۵۵۵.۳: Advanced Endpoint Analytics
- SEC۵۵۵.۴: Baselining and User Behavior Monitoring
- SEC۵۵۵.۵: Tactical SIEM Detection and Post-Mortem Analysis
- SEC۵۵۵.۶: Capstone: Design, Detect, Defend

مخاطبان دوره

- مدیران فناوری اطلاعات
- مدیران امنیت اطلاعات
- کارشناسان امنیت
- کارشناسان واحد پاسخگویی به حوادث
- کارشناسان واحد مرکز عملیات امنیت

پیش نیاز ها

- برای شرکت در این دوره پیشنیازی لازم نیست و مباحث مقدماتی لازم در پکیج گنجانده شده است.