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

دوره پیشرفته شکار تهدیدات (FOR ۵۰۸)

ADVANCED THREATS ARE IN YOUR NETWORK–IT'S TIME TO GO HUNTING

مروری بر دوره

تاکتیک‌ها و روش های شکار تهدید و پاسخ به حوادث در چند سال گذشته به سرعت تکامل یافته‌اند. تیم شما دیگر نمی‌تواند از تکنیک‌های قدیمی واکنش به حادثه و شکار تهدید استفاده کند که به درستی سیستم‌های در معرض خطر را شناسایی نمی‌کنند. نکته کلیدی این است که دائماً به دنبال حملاتی باشید که سیستم‌های امنیتی را پشت سر می‌گذارند، و نفوذهای در حال انجام را شناسایی کنید، نه اینکه مهاجمان اهداف خود را تکمیل کرده و آسیب بدتری به سازمان وارد کنند. برای تیم واکنش به حادثه، این فرآیند به عنوان "شکار تهدید" شناخته می شود.این دوره ، مهارت‌های پیشرفته‌ای برای شکار، شناسایی، مقابله و بازیابی از طیف گسترده‌ای از تهدیدات در شبکه‌های سازمانی، از جمله دشمنان حملات APT، جرایم سازمان‌یافته، و فعالیت های هکرها را آموزش می‌دهد.

سرفصل ها

- Advanced Incident Response & Threat Hunting
- Intrusion Analysis
- Memory Forensics in Incident Response & Threat Hunting
- Timeline Analysis
- Incident Response & Hunting Across the Enterprise

پیش نیاز ها

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

دوره ۱ soc یا

دوره های ۴۰۱,۵۰۴ sans حتما گذرانده شده باشد