مؤسسه آموزش عالی آزاد

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

دوره آموزشی SANS FOR۵۷۲

FOR۵۷۲: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response

مروری بر دوره

Whether you handle an intrusion incident, data theft case, employee misuse scenario, or are engaged in proactive adversary discovery, the network often provides an unparalleled view of the incident. SANS FOR۵۷۲ covers the tools, technology, and processes required to integrate network evidence sources into your investigations to provide better findings, and to get the job done faster.

سرفصل ها

- FOR۵۷۲.۱: Off the Disk and Onto the Wire
- FOR۵۷۲.۲: Core Protocols & Log Aggregation/Analysis
- FOR۵۷۲.۳: NetFlow and File Access Protocols
- FOR۵۷۲.۴: Commercial Tools, Wireless, and Full-Packet Hunting
- FOR۵۷۲.۵: Encryption, Protocol Reversing, OPSEC, and Intel
- FOR۵۷۲.۶: Network Forensics Capstone Challenge

مخاطبان دوره

Incident response team members and forensicators

Hunt team members

Law enforcement officers, federal agents, and detectives

Security Operations Center (SOC) personnel and information security practitioners

Network defenders

Information security managers

Network engineers

Information technology professionals

Anyone interested in computer network intrusions and investigations

پیش نیاز ها

دوره Security Essentials : SEC۴۰۱