

Give your security professionals the core practical and theoretical skills, tools and knowledge they need to perform in-depth network forensic analysis.

Network Forensic Analysis

When an organization's network is hit by a cyberattack, network forensic analysis can help uncover the source of the security breach. It can also be used to proactively identify suspicious traffic or an impending attack, so that steps can be taken to keep the network secure.

This intensive three-day training session for security professionals provides the core practical and theoretical skills, tools and knowledge required to perform in-depth network forensic analysis. Participants learn how to investigate and detect network attack traces, map attack stages, and identify and assess the potential future damage of an ongoing APT.



Participants

- SOC Analysts
- Tier 1 Security Analysts
- Incident Response Team Members



Prerequisites

- Understanding of basic information security concepts and tools
- Familiarity with networking principles, architecture and protocols



Training Outcomes

- Acquisition of the necessary skills, methodology and practical experience required to become a Network Forensics expert
- Ability to expertly manage and investigate ongoing, complex cyberattacks and their consequences, in organizations of all sizes



Duration

- 24 hours (3 x 8-hour days)