

Give your cyber teams the highly-specialized expertise required to optimize SIEM systems, including rule configuration, data correlation, and system optimization.

SOC Intrusion – Advanced Detection Tactics

In monitoring your network environment, your Security Operations Center (SOC) team will rely on your Security Information and Event Management (SIEM) platform to help prevent data breaches and learn about present or future cyber events.

This practical program provides the highly-specialized expertise required to optimize SIEM systems, including rule configuration, data correlation, and system optimization. Participants will refine their detection and investigation skills through real-life, real-time cyberattacks in our secure cyberwarfare arena, analyzing case studies, and taking part in hands-on exercises, which require the practical use of advanced SIEM systems and techniques.



Participants

- SOC Analysts
- Incident Response Team Members



Prerequisites

- Excellent SIEM operation and configuration knowledge
- Good understanding of data communications
- Understanding of basic information security concepts and tools



Training Outcomes

- Improved capabilities for detecting and analyzing intrusions and data breaches
- Enhanced SIEM configuration and optimization skills
- Insights into the hacker's perspective and mindset, through live cyberattacks
- Ability to execute well-designed procedures during an actual cyberattack



Duration

- 24 hours (3 x 8-hour days)