



CYBER THREATS DETECTION AND MITIGATION

COURSE DESCRIPTION

Cyber threats are increasing at an alarming rate and the ability for organizations to defend against large scaled attacks quickly and effectively is becoming essential. Organizations must adapt by becoming more automated to make them capable of characterizing attacks across hundreds or thousands of IP sessions. The result will be the enhanced capability to recognize attack commonalities fast, which then enables prioritization, and isolation of the critical threats. Taught by leaders in the computer security industry, this course demonstrates how to defend large-scale network infrastructures by building and maintaining advanced intrusion detection systems.

THE STUDENT WILL LEARN:

- + How to identify the best defensive measures to effectively protect a network
- + How to setup and maintain an intrusion detection system
- + How to analyze and respond to intrusion attempts
- + How to recover from a successful intrusion

PREREQUISITES:

- + General understanding of computer networks and networking protocols
- + General knowledge of computer and O/S fundamentals is recommended

COURSE INFORMATION:

5 days, MF, 40 hours. A certificate of completion will be given at the end of the course. Each student will be provided with a preconfigured laptop with all course training software.