



The Cybersecurity Expert course is designed to provide a comprehensive understanding of the advanced concepts and practical skills required to start a career in Cybersecurity. This program is ideal for individuals aspiring to become senior cybersecurity experts, cybersecurity lead or manager equipping them with the knowledge and hands-on experience required to deploy advanced technologies like SIEM, Data Loss Prevention, Endpoint Detection & Response and to handle security incidents in a network.

Key Topics:

- SIEM Deployment & integration
- Endpoint Detection & Response
- Data Loss Prevention
- Incident handling

Cybersecurity Expert



Module 1: SIEM

- What is SIEM
- Functions of SIEM
- SIEM architecture
- Different SIEM applications
- Installation of SIEM solution
- Integration of SIEM solution with existing network resources
- Collecting and analysing event logs
- Fine tuning and alert generation
- · Creating and assigning alert tickets

Module 2 : Endpoint Detection and Response (EDR)

- What is EDR
- Installation of EDR
- Deployment of EDR
- Analysing EDR alerts

Module 3: Data Loss Prevention (DLP)

- What is DLP
- Installation of DLP
- Deployment of DLP
- Analysisng DLP alerts

Module 4: Incident Response

- What is incident response
- Incident response policy
 - What is incident response policy
 - Elements of incident response policy
 - Different types of incident response teams
 - Role of incident response manager
 - What does incident response team do
- Incident Handling
 - What is incident handling
 - CIRC team
 - The REACT principle
 - Maintaining integrity of scene following an accident

- Legal aspects of Incident Response
 - Legal considerations of incident response
 - Expectation of privacy
 - Personally Identifiable Information (PII)
 - Giving notice to individuals
 - Benefits of information sharing
- Forensics of incident response
 - Forensics in support of an incident response
 - Phases of Investigation
 - Capturing of data
 - Volatile data considerations
 - Volatile memory capture
 - Imaging concepts
 - Forensic acquisition of data from PC
 - Obtaining BitLocker keys
 - Analysis of forensic data
- Insider threat
 - What is insider threat
 - Indicators to identify an insider threat
 - Automated processes to look for indicators of in insider threats
 - Policies and procedures
 - Policy enforcement
- Malware
 - Malware incidents
 - Malware analysis
- Incident Recovery