SecOps Training and Certification Course

Curriculum 2 Days

Day - 1

-
  - Brief overview of the objectives for the workshop
  - Introduction of the participants and their roles
-
  - Definition and objectives of SecOps
  - The importance of SecOps in a modern IT environment
  - Overview of key security frameworks and standards (e.g. NIST, ISO, etc.)
-
  - Introduction to incident response planning
  - Understanding the phases of incident response (preparation, detection and analysis, containment, eradication and recovery)
  - Best practices for incident response planning
-
  - Introduction to threat intelligence and analysis
  - Understanding the different types of threats (e.g. malware, social engineering, insider threats, etc.)
  - Best practices for threat intelligence and analysis
-
  - Introduction to security monitoring and alerting
  - Understanding the different types of monitoring (e.g. network, endpoint, application, etc.)
  - Best practices for security monitoring and alerting
-
  - Introduction to security metrics and reporting
  - Understanding the different types of metrics (e.g. vulnerability metrics, incident metrics, compliance metrics, etc.)
  - Best practices for security metrics and reporting