Technical and Operational IT Security Concepts

**Course Description**

IT systems and networks containing and processing highly sensitive information and data, as well as IT infrastructure in support of business-critical processes or national critical infrastructure, require higher security mechanisms than normal regarding confidentiality, integrity and availability. Based on specific “Protection Profiles,” highly sophisticated tools, mechanisms and procedures need to be designed, implemented, configurated and operated. Through this course, the student will learn to evaluate a given IT infrastructure, support the security design of new IT systems and networks by developing specific Protection Profiles, and evaluate which technical and operational security measures and applications are required and how these are integrated, configured and operated.

**Contents**

1. Network Analysis and Evaluation
   1. Layer-Specific Threats and Vulnerabilities
   2. Data Flow, Interdependencies, and Interrelationships
   3. Vulnerability Scanning and Detection
   4. Supporting Tools and Techniques
2. Protection Profiles
   1. Reference Architecture Technology and Networking
   2. Risk Assessment, Residual Risk, and Risk Management
   3. Security Requirements and Safeguards
   4. Security Evaluation of IT Security Products
   5. Accreditation of IT Systems and Networks
3. Intrusion Detection Systems
   1. Detection Strategy
   2. Data Sources; Sensors
   3. Analytics
   4. Indicators of Compromise
4. Network Monitoring
   1. Threat Protection Systems
   2. Wireless Sensor Networks Technology
   3. Threat Information Sharing
5. Security Information and Event Management (SIEM)
   1. Technical and Operational Data Sources
   2. Data Fusion
   3. Network Norm Behavior
   4. Big Data Analysis – Transferring Technical Data for Operational Information
   5. Security Situation Picture; Situational Awareness
   6. Incident Response Strategies and Automated Responses
6. IT Security Evaluation and Assessment

6.1 IT Security Metrics

1. IT Security Assessment