MICAD LIMITED
Advanced Industrial Security Supervisor Training

Lesson 2.4: Risk Prioritization and Mitigation Strategies

Here's an example of completing a threat modeling exercise for a SCADA (Supervisory Control and Data Acquisition) system using the STRIDE methodology:

Threat Modeling Exercise for a SCADA System
System: The SCADA system is utilized to control and monitor industrial processes in a manufacturing facility. It communicates with field devices and collects data for real-time operational insights.

Methodology: STRIDE

1. Identified Threats and Vulnerabilities

Threat Identification:

Using the STRIDE methodology, we categorize potential threats as follows:

- **Spoofing:**
  - Unauthorized access through credential theft or impersonation.
- **Tampering:**
  - Alteration of control signals to machinery, leading to unsafe operations.
- **Repudiation:**
  - Users denying actions taken within the SCADA system, complicating accountability.
- **Information Disclosure:**
  - Sensitive data like operational parameters and employee information being exposed due to weak encryption.
- **Denial of Service:**

    - Attacks causing system downtime, impacting production activities.
- **Elevation of Privilege:**
    - Users exploiting software vulnerabilities to gain higher access levels than permitted.

2. Vulnerability Assessment

- Weak passwords for user accounts.
- Lack of network segmentation between SCADA and corporate networks.
- Outdated software and firmware on field devices.
- Insufficient logging and monitoring capabilities for actions taken within the system.

3. Risk Analysis

Threat	Likelihood	Impact	Mitigation Strategy
Spoofing	Medium	High	Implement multi-factor authentication and regular password updates.
Tampering	Medium	High	Use secure coding best practices and rigid access control measures to limit user permissions.
Denial of Service	Low	High	Deploy DDoS protection and ensure system redundancy and backups.
Information Disclosure	High	Medium	Utilize end-to-end encryption for sensitive data in transit and at rest.
Elevation of Privilege	Medium	Medium	Regular conduct software updates and vulnerability scans on the SCADA system and its components.

5. Documentation in Threat Register

Threat Register:

Threat	Description	Identified Vulnerabilities	Mitigation Strategies
Spoofing	Unauthorized access to the SCADA system	Weak passwords	Implement multi-factor authentication
Tampering	Alteration of control signals	Poor access controls	Secure coding practices, limit user permissions
Information Disclosure	Exposure of sensitive data	Weak data encryption	Employ end-to-end encryption for data
Denial of Service	System downtime due to attacks	Lack of redundancy	Deploy DDoS protection, ensure backups
Elevation of Privilege	Exploiting vulnerabilities for access	Outdated software	Conduct regular software updates and vulnerability scanning