MICAD LIMITED
Advanced Industrial Security Supervisor Training

Lesson 2.1: Threat Modeling and Analysis Techniques

Here are examples of threat modeling exercises for two different industrial systems, demonstrating the application of the STRIDE methodology. Remember that this is a simplified example; a real-world threat model would be far more extensive and detailed.

Example 1: Threat Modeling a SCADA System
System: A Supervisory Control and Data Acquisition (SCADA) system controlling a water treatment plant.
Methodology: STRIDE

Threat Register:

Threat Category	Specific Threat	Vulnerability	Likelihood	Impact	Mitigation Strategy
Spoofing	Spoofing SCADA commands	Weak authentication on SCADA network devices	Medium	High	Implement strong authentication (multi-factor)

Tampering	Modifying SCADA data	Lack of data integrity checks	Medium	High	Implement data integrity checks and digital signatures
Repudiation	Unauthorized changes	Lack of audit logging	Low	Medium	Implement comprehensive audit logging
Information Disclosure	Data breach	Unencrypted communication	High	Critical	Implement encryption (TLS/SSL) for all communications
Denial of Service	Network outage	Single point of failure in network infrastructure	Low	High	Implement redundancy and failover mechanisms
Elevation of Privilege	Unauthorized access	Default credentials on SCADA devices	Medium	Critical	Change default credentials and implement access control

Example 2: Threat Modeling a Manufacturing Process (Automated Assembly Line)

System: Automated assembly line in a car manufacturing plant.

Methodology: STRIDE

Threat Register:

Threat Category	Specific Threat	Vulnerability	Likelihood	Impact	Mitigation Strategy
Spoofing	Spoofing robotic commands	Weak authentication on robot controllers	Low	High	Implement strong authentication and access control
Tampering	Physical tampering	Lack of physical security around robots	Medium	High	Install security cameras and access control to the area
Repudiation	Unauthorized modifications	Lack of logging for robot actions	Low	Medium	Implement logging and auditing of robot actions
Information Disclosure	Data theft	Inadequate protection of production data (PLC)	Low	Medium	Implement network segmentation, data encryption, access control

Denial of Service	Robot malfunction	Lack of redundancy in robot control system	Medium	High	Implement redundancy in the robot control system
Elevation of Privilege	Unauthorized control	Unsecured access to robot programming interfaces	Low	Critical	Secure access to robot programming interfaces using strong authentication

Important Considerations:

- **Context Matters:** The likelihood and impact of threats are context-dependent. Factors like the criticality of the system, the organization's security posture, and the threat landscape should all be considered when assigning these values.
- **Mitigation Strategy Effectiveness:** The effectiveness of a mitigation strategy should also be assessed. For example, a simple password change might be insufficient protection against sophisticated attacks.
- **Continuous Improvement:** Threat modeling should be a recurring process, updated as systems evolve and new threats emerge.
- **Documentation:** A well-maintained threat register is essential for tracking threats, vulnerabilities, mitigation strategies, and their effectiveness over time. This document should be regularly reviewed and updated.

These examples illustrate how the STRIDE methodology can be used to systematically identify and analyze threats. Remember to adapt these models to specific systems, considering the unique characteristics and vulnerabilities of each industrial setting. The

use of specific software or tools for visualizing threat models (e.g., threat modeling software) is beneficial in a real-world application.