Threat Modeling for Operational Technology (OT) Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The rapidly accelerating convergence of Information Technology (IT) and Operational Technology (OT) has introduced unprecedented cyber risk to critical industrial environments. While traditional IT threat modeling focuses on data confidentiality, OT security prioritizes safety, integrity, and availability the fundamental pillars of Industrial Control Systems (ICS). Sophisticated nation-state and criminal threat actors are increasingly targeting vulnerabilities in legacy OT assets and the Industrial Internet of Things (IIoT), leading to catastrophic physical and financial consequences. Mastering OT Threat Modeling is no longer optional; it's an imperative for maintaining operational resilience and defending global Critical Infrastructure.

Threat Modeling for Operational Technology (OT) Training Course provides a practical, hands-on methodology to secure highly sensitive OT/ICS environments. You'll move beyond generic IT security principles to master specialized frameworks like the Purdue Model, ISA/IEC 62443, and adapted threat analysis methods like STRIDE for ICS. The course is structured around real-world case studies from energy grid attacks to water treatment system compromise equipping security, engineering, and compliance professionals with the analytical skills to proactively identify, model, and mitigate threats across SCADA, PLC, and Distributed Control Systems (DCS). Elevate your organization?ÇÖs cyber-physical security posture and become an essential OT Security Architect and defender.

Programme Curriculum

Threat Modeling for Operational Technology (OT) Training Course

Introduction

The rapidly accelerating convergence of Information Technology (IT) and Operational Technology (OT) has introduced unprecedented cyber risk to critical industrial environments. While traditional IT threat modeling focuses on data confidentiality, OT security prioritizes safety, integrity, and availability the fundamental pillars of

Industrial Control Systems (ICS). Sophisticated nation-state and criminal threat actors are increasingly targeting vulnerabilities in legacy OT assets and the Industrial Internet of Things (IIoT), leading to catastrophic physical and financial consequences. Mastering OT Threat Modeling is no longer optional; it's an imperative for maintaining operational resilience and defending global Critical Infrastructure.

Threat Modeling for Operational Technology (OT) Training Course provides a practical, hands-on methodology to secure highly sensitive OT/ICS environments. You'll move beyond generic IT security principles to master specialized frameworks like the Purdue Model, ISA/IEC 62443, and adapted threat analysis methods like STRIDE for ICS. The course is structured around real-world case studies from energy grid attacks to water treatment system compromise equipping security, engineering, and compliance professionals with the analytical skills to proactively identify, model, and mitigate threats across SCADA, PLC, and Distributed Control Systems (DCS). Elevate your organization?ÇÖs cyber-physical security posture and become an essential OT Security Architect and defender.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Differentiate between IT and OT security models, emphasizing safety, integrity, and availability in cyber-physical systems.
2. Decompose complex OT architectures using the Purdue Model and ISA/IEC 62443 zone and conduit concepts.
3. Apply the adapted STRIDE for ICS methodology to systematically identify industrial control system threats.
4. Analyze proprietary industrial protocols for inherent security weaknesses and attack vectors.
5. Map OT threats to the MITRE ATT&CK for ICS framework to understand attacker TTPs.
6. Develop robust Data Flow Diagrams (DFDs) that accurately represent trust boundaries and data movement in SCADA environments.
7. Evaluate system risks using quantitative methods like PASTA or qualitative methods like DREAD tailored for OT environments.
8. Formulate prioritized mitigation strategies that balance security requirements with operational continuity and uptime.
9. Identify and secure vulnerabilities in legacy systems and Human-Machine Interfaces (HMIs) common in older plants.
10. Implement network segmentation and compensating controls to minimize the impact of breaches across the IT/OT boundary.
11. Conduct a complete OT threat modeling workshop aligned with the system's Secure Development Lifecycle (SDLC) or maintenance cycle.
12. Integrate threat modeling output with organizational Risk Management frameworks and regulatory mandates.
13. Propose effective Zero Trust Architecture (ZTA) principles and technologies for modernizing an existing OT network.

Target Audience Roles

1. OT/ICS Security Engineers
2. Cybersecurity Architects and Security Analysts

3. Industrial Automation/Control Engineers
4. Plant Managers and Operations/Maintenance Personnel
5. IT/OT Network & Infrastructure Professionals
6. Compliance and Risk Managers
7. Product Security Teams designing and integrating IIoT devices
8. Penetration Testers and Vulnerability Assessors focused on industrial environments

Course Modules with 5 Bullets and Case Studies

Module 1: OT/ICS Architecture and Security Fundamentals

- The IT/OT Convergence Challenge
- Detailed breakdown of the Purdue Enterprise Reference Architecture and its security implications.
- Understanding core OT components.
- Introduction to key OT Standards and Frameworks
- Defining Zones and Conduits and establishing Trust Boundaries for threat scoping.
- Case Study: Analyzing a real-world IT-to-OT breach via the DMZ and failure to enforce a security conduit.

Module 2: The Threat Modeling Process for OT

- The 4-Question Framework adapted for OT
- System Decomposition.
- Identifying Critical Assets and defining the system's Mission and Objectives.
- Selecting the right methodology.
- Scoping the threat model based on lifecycle phase
- Case Study: Threat modeling a new remote access solution for vendor maintenance on a SCADA system.

Module 3: OT Threat Identification and Analysis

- Applying STRIDE for ICS.
- Deep dive into Attack Vectors targeting common industrial protocols
- Leveraging MITRE ATT&CK for ICS to simulate real-world attacker TTPs
- Identifying physical security gaps that enable cyber-physical attacks
- Introduction to advanced threat models like PASTA in an OT context.
- Case Study: Modeling the attack path used in the Triton/TRISIS safety-instrumented system attack.

Module 4: Risk Scoring and Prioritization

- Methods for Risk Rating in OT.
- Qualitative Risk Scoring using models like DREAD or customized severity matrices for OT.
- Quantitative risk estimation
- Prioritization based on Operational Impact and Safety Integrity Level.
- Developing clear, actionable Vulnerability and Threat Remediation Plans.
- Case Study: Calculating the business impact of a hypothetical DoS attack on a utility's primary DNP3 communication link.

Module 5: Mitigation Strategy: Controls and Compensating Measures

- Designing Defense-in-Depth strategies tailored for the Purdue Model.
- Implementing Network Segmentation and Unidirectional Gateways at the IT/OT boundary.

- Securing Industrial Protocols using deep-packet inspection and protocol whitelisting.
- Applying Hardening Best Practices for PLCs and HMIs.
- The role of Zero Trust Architecture principles in modern OT environments.
- Case Study: Designing and threat modeling a micro-segmentation solution for a critical cell/area zone

Module 6: Securing the Industrial Internet of Things (IIoT)

- Threats unique to IIoT devices and wireless industrial sensor networks.
- Modeling the Supply Chain Risk from vendor-supplied hardware and software.
- Securing Cloud Connectivity for industrial data and remote monitoring services.
- Managing Authentication and Identity for machine-to-machine and device-to-cloud communications.
- Applying threat modeling to embedded systems and firmware updates.
- Case Study: Identifying vulnerabilities in a newly deployed smart factory sensor array and its cloud dashboard interface.

Module 7: Documentation, Review, and Automation

- Creating a comprehensive Threat Model Report that is accessible to both engineers and management.
- Integrating threat modeling artifacts with organizational Governance, Risk, and Compliance programs.
- Developing a process for Model Maintenance and review during system changes or patches.
- Introduction to Threat Modeling Tools for OT-specific diagrams.
- Mapping mitigations back to compliance requirements like NERC CIP and Gartner's Adaptive Security Architecture.
- Case Study: Validating the completeness of a threat model against the security requirements of the ISA/IEC 62443-3-3 standard.

Module 8: Hands-On OT Threat Modeling Workshop

- Decomposing a functional water treatment plant SCADA architecture.
- Collaborative Brainstorming Session to identify threats using the ATT&CK for ICS framework.
- Practical exercise in prioritizing threats based on simulated system failure and environmental impact.
- Developing and presenting a prioritized mitigation roadmap for the WTP.
- Final Review: Assessing the quality and effectiveness of the completed threat model
- Case Study: Full-cycle threat model of the Colonial Pipeline attack scenario mapping initial access through to OT disruption.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com