Threat Modeling for Defense Systems Training Course

Professional Development Training Course Outline

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

Course Introduction

Threat modeling for defense systems is a critical discipline that enables defense and security professionals to proactively identify, assess, and mitigate potential threats to military and national security infrastructures. As cyber warfare, advanced surveillance, and technological espionage become more sophisticated, defense organizations require structured frameworks and analytical methods to anticipate vulnerabilities, prioritize risks, and design resilient countermeasures. Threat Modeling for Defense Systems Training Course provides participants with practical skills to apply threat modeling techniques across defense systems, integrating intelligence analysis, system architecture review, and adversary profiling to enhance operational security and mission readiness.

The course combines theoretical foundations with hands-on exercises, enabling participants to map potential threat scenarios, evaluate system weaknesses, and develop robust mitigation strategies. Participants will gain expertise in leveraging industry-standard methodologies, leveraging digital tools, and applying risk-based approaches to real-world defense systems. By the end of this training, learners will be able to implement a structured threat modeling process that strengthens defense system integrity, improves decision-making, and ensures mission-critical assets are protected against evolving threats.

Programme Curriculum

Threat Modeling for Defense Systems Training Course

Introduction

Threat modeling for defense systems is a critical discipline that enables defense and security professionals to proactively identify, assess, and mitigate potential threats to military and national security infrastructures. As cyber warfare, advanced surveillance, and technological espionage become more sophisticated, defense organizations require structured frameworks and analytical methods to anticipate vulnerabilities, prioritize risks,

and design resilient countermeasures. Threat Modeling for Defense Systems Training Course provides participants with practical skills to apply threat modeling techniques across defense systems, integrating intelligence analysis, system architecture review, and adversary profiling to enhance operational security and mission readiness.

The course combines theoretical foundations with hands-on exercises, enabling participants to map potential threat scenarios, evaluate system weaknesses, and develop robust mitigation strategies. Participants will gain expertise in leveraging industry-standard methodologies, leveraging digital tools, and applying risk-based approaches to real-world defense systems. By the end of this training, learners will be able to implement a structured threat modeling process that strengthens defense system integrity, improves decision-making, and ensures mission-critical assets are protected against evolving threats.

Course Objectives

1. Understand the principles and frameworks of threat modeling in defense systems.
2. Identify and categorize potential threats across multiple defense domains.
3. Analyze system architectures to detect vulnerabilities and attack vectors.
4. Apply risk assessment techniques to prioritize threats based on impact and likelihood.
5. Develop mitigation strategies for identified vulnerabilities.
6. Utilize threat intelligence and adversary profiling in threat modeling.
7. Integrate threat modeling into defense system lifecycle management.
8. Evaluate defensive controls and countermeasure effectiveness.
9. Conduct scenario-based simulations to validate threat models.
10. Apply structured methodologies such as STRIDE, DREAD, and PASTA.
11. Improve decision-making using quantitative and qualitative threat analysis.
12. Enhance cross-team collaboration and information sharing on threat risks.
13. Develop actionable threat mitigation plans aligned with operational objectives.

Organizational Benefits

- Improved operational resilience against emerging threats
- Strengthened security posture of defense systems
- Enhanced risk management and mitigation strategies
- Increased situational awareness for defense personnel
- Better integration of threat intelligence into decision-making
- Reduced vulnerability exposure across mission-critical assets
- Improved compliance with national and international security standards
- Enhanced collaboration across defense and security teams
- Efficient allocation of resources for threat prevention and response
- Strengthened organizational reputation in defense and cybersecurity

Target Audiences

- Defense system architects and engineers
- Military intelligence officers and analysts
- Cybersecurity and network defense professionals
- Risk and compliance officers in defense organizations
- Defense operations planners and strategists
- Security auditors and inspectors
- Defense technology consultants and advisors

- Military training and simulation specialists

Course Duration: 5 days

Course Modules

Module 1: Introduction to Threat Modeling

- Principles of threat modeling for defense systems
- Understanding threat actors and adversary capabilities
- Overview of threat modeling frameworks and methodologies
- Identifying defense system assets and critical components
- Common vulnerabilities and risk scenarios in defense systems
- Case Study: Identifying critical threats in a defense command system

Module 2: System Architecture Analysis

- Mapping system components, networks, and communication flows
- Identifying potential attack vectors and weak points
- Analyzing interdependencies and critical paths
- Evaluating security controls and redundancies
- Assessing the impact of system failures or breaches
- Case Study: Architecture vulnerability analysis of a missile defense system

Module 3: Threat Identification & Classification

- Categorizing threats by type, source, and likelihood
- Understanding insider versus external threats
- Cyber, physical, and hybrid attack scenarios
- Prioritizing threats based on operational impact
- Incorporating threat intelligence feeds and historical data
- Case Study: Threat classification in an integrated air defense system

Module 4: Risk Assessment & Prioritization

- Quantitative and qualitative risk assessment approaches
- Applying DREAD, STRIDE, and other risk scoring models
- Determining likelihood, impact, and exposure levels
- Scenario analysis and probability modeling
- Evaluating existing mitigation measures
- Case Study: Risk prioritization exercise for a naval defense system

Module 5: Mitigation Strategies & Countermeasures

- Developing technical, procedural, and operational countermeasures
- Aligning mitigation strategies with system architecture and objectives
- Evaluating cost-effectiveness and feasibility of controls
- Planning layered defense mechanisms
- Continuous monitoring and adjustment of mitigation measures
- Case Study: Implementing countermeasures in a satellite communication system

Module 6: Threat Modeling Methodologies

- STRIDE methodology for threat categorization
- DREAD model for risk scoring and prioritization
- PASTA (Process for Attack Simulation and Threat Analysis)
- Integrating multiple methodologies for comprehensive analysis
- Best practices for consistent application across defense projects
- Case Study: Comparative application of STRIDE and PASTA in a cyber defense scenario

Module 7: Simulation & Scenario-Based Exercises

- Designing realistic threat scenarios for defense systems
- Conducting red team / blue team exercises
- Evaluating system response and resilience
- Applying lessons learned to improve threat models
- Reporting and documenting scenario outcomes
- Case Study: Simulation of an electronic warfare attack

Module 8: Governance, Reporting & Continuous Improvement

- Integrating threat modeling into defense system governance
- Reporting protocols for identified threats and mitigation actions
- Continuous evaluation and update of threat models
- Stakeholder engagement and cross-functional collaboration
- Establishing organizational threat intelligence sharing mechanisms
- Case Study: Threat model governance framework for a joint defense operation

Training Methodology

- Instructor-led sessions and expert presentations
- Hands-on exercises and group threat modeling workshops
- Scenario simulations and red team/blue team activities
- Case study reviews and peer discussions
- Practical templates, checklists, and assessment tools
- Action plan development and facilitator feedback

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
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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