OWASP THREAT DRAGON TRAINING

Level - OWASP

Email – contact@DevOpsSchool.com

TRAINING AGENDA

DAY 1

Introduction to OWASP Threat Dragon

- Overview of Threat Dragon and its purpose
- Importance of threat modeling in modern SDLC
- OWASP Foundation context and standardization
- Key benefits of adopting Threat Dragon in security planning

Threat Modeling Concepts

- Fundamentals of threat modeling
- Identifying assets, attackers, and security objectives
- STRIDE methodology and risk categorization
- Mapping threats to mitigation strategies

OWASP Threat Dragon Architecture & Features

- Understanding Threat Dragon interface (desktop & web versions)

- Project setup and navigation
- Diagram creation and asset representation
- Import/export and integration capabilities

Creating Threat Models - Hands-On Lab

- Setting up sample application projects
- Drawing data flow diagrams (DFDs) in Threat Dragon
- Identifying entry points, assets, and trust boundaries
- Annotating threats and vulnerabilities

Threat Analysis Techniques

- Assigning threat ratings and risk levels
- Understanding attack vectors and threat likelihood
- Prioritizing threats for mitigation
- Hands-on exercises analyzing sample threats

Recap & Q&A

- Summary of threat modeling fundamentals
- Review of hands-on exercises
- Open discussion and knowledge sharing

DAY 2

Advanced Threat Dragon Features

- Managing multiple threat models and projects
- Collaboration features for teams
- Templates and custom threat libraries

- Integrating Threat Dragon into SDLC pipelines

Mitigation Strategies & Security Controls

- Mapping threats to countermeasures
- Developing actionable mitigation plans
- Prioritizing and tracking mitigation effectiveness
- Hands-on lab: applying mitigations in Threat Dragon

Case Studies & Real-World Examples

- Threat modeling of web applications
- Threat modeling of APIs and microservices
- Lessons learned from industry scenarios
- Group discussion and practical insights

Reporting & Documentation

- Generating threat model reports
- Communicating findings to stakeholders
- Integrating reports into risk management and compliance processes
- Hands-on lab: creating a professional threat report

Threat Modeling in Agile & DevSecOps

- Incorporating threat modeling in iterative development
- Aligning Threat Dragon with CI/CD and DevSecOps workflows
- Automating threat tracking and mitigation validation

Practical Workshop - End-to-End Threat Modeling

- Conduct full threat modeling for a sample application

- Identify threats, assign risk levels, and propose mitigations
- Peer review and feedback session
- Applying best practices for enterprise adoption

Final Review & Knowledge Assessment

- Recap of OWASP Threat Dragon functionalities and methodologies
- Knowledge check with practical scenarios
- Q&A and recommendations for real-world implementation