Practical DevSecOps

Threat Modeling Professional

COURSE

www.practical-devsecops.com

Practical DevSecOps

Threat Modeling Professional

A Practical Approach to Agile and Automation Techniques in Threat Modeling.

Course Objective

As information security threats continue to explode, your ability to build models becomes increasingly important, because building better models means creating better defenses for your organization—defenses that often increase an application's resilience against external threats and insider threats alike.

The **Certified Threat Modeling Professional (CTMP)** is a vendor-neutral course and certification program that is designed to assess and improve the threat modeling expertise of a security professional.

More and more organizations are increasingly seeking threat modeling as an indispensable skill. This course is designed to give students a practical understanding of Threat modeling, covering not only the theory but immediately applicable tools and techniques. The course is project-oriented, with 20+ hands-on labs that will put your newly gained knowledge into action and guide you along the way.

Course Prerequisites

1. Course participants should know basic security fundamentals like Confidentiality, Integrity, and Availability (CIA).
2. Basic knowledge of application development is preferred but is not necessary.

Learning Objectives

The following are the course's objectives.

1. Build a solid foundation that is required to understand Threat modeling.
2. Gain a practical understanding of threat modeling and the tools to automate it.
3. Understand and implement the modern ways of scaling threat modeling.

Course Syllabus

The curriculum focuses on educating students on Security requirements in agile environments, Agile Threat modeling, Threat Modeling as Code, and Secure Design Principles to help you ensure security in the design phase of systems development.

The following topics are covered as part of the course.

1. Overview to Threat Modeling.
2. Threat Modeling Basics.
3. Agile Threat Modeling.
4. Reporting and Deliverables.
5. Secure Design Principles and Cloud Threat modeling.

Threat Modeling Professional

A Practical Approach to Agile and Automation Techniques in Threat Modeling.

What Will Students be Provided?

The students will be provided with

1. Course videos and Checklists.
2. Course Manual.
3. 30 days Online Lab Access.
4. 30+ Guided Exercises.
5. Access to a dedicated Mattermost channel.
6. One exam attempt for Certified Threat Modeling Professionl Certification.

Course Duration

The participant can complete the course in 20 hours. That includes 5 hours of video lectures and 15 hours of hands-on practice. However, a participant has lifetime access to the on-demand course with 30 days of online lab access.

Learn more

To learn more about our courses, certifications and pricing, please visit **our courses** or **contact us**

Who Should Take This Course?

This course is aimed at professionals interested in performing threat modeling in agile/ cloud/ DevOps environments like Security Professionals, Penetration Testers, Red Teamers, Application Security Engineers, IT managers, Developers, and DevOps Engineers.

Software and Hardware Requirements

Our state-of-the-art Training Platform works within your browser. You can even do the labs from your mobile devices like iPad and Android phones. All you need is a modern browser on a laptop or desktop.

Threat Modeling Professional

Practical DevSecOps

Detailed Syllabus

DAY 1

1 Overview of Threat Modeling

1. What is Threat Modelling?
2. Key Concepts and Terminology
3. Uses, Benefits, and its challenges
4. Threat Modelling vs. Other Security Practices
5. Threat modeling Frameworks and Methodologies
    a. List/Library Centric Threat modeling
    b. Asset/Goal Centric Threat Modelling
    c. Threat Actor/Attacker Centric Threat Modelling
6. Trust Boundaries vs. Attack Surfaces
7. Threat modeling approaches for Agile and DevOps
8. Strategies for Risk Management with Examples
    a. Avoiding Risks
    b. Accepting Risks
    c. Mitigating Risks
    d. Transferring Risks
9. **Hands-on Exercises**:
    a. Breakout sessions to identify threats for a multi-tiered application

Threat Modeling Professional

Detailed Syllabus

2 Threat Modeling Basics

1. Threat modeling and security requirements
2. Threat modeling vs. Threat Rating
3. Introduction to List based modeling approach
4. Exploring the STRIDE Model
    - a. Spooring
    - b. Tampering
    - c. Repudiation
    - d. Information Disclosure
    - e. Denial of service
    - f. Elevation of privileges
5. Pros and Cons of STRIDE technique
6. STRIDE defenses
    - a. Authentication
    - b. Integrity
    - c. Non-Repudiation
    - d. Confidentiality
    - e. Availability
    - f. Authorization
7. STRIDE Threat examples
8. Goal/Asset Based modeling Approach
    - a. Attack Trees
    - b. Attack Tree Analysis
9. Threat actor centric modeling Approach
    - a. Using MITRE ATT&CK for attacker centric approach
10. Other Threat modeling methodologies
    - a. PASTA
    - b. VAST
    - c. Hybrid Threat modeling
    - d. RTMP

11. Gamified approaches for Threat Modelling
    - a. Virtual Card Games
    - b. Adversary Card Games
12. Introduction to Threat Rating
    - a. Pros and Cons of DREAD for threat rating
    - b. Pros and Cons of CVSS for threat rating
13. Defensive tactics for building secure systems
14. **Hands-on Exercises**:
    - a. Each of the above topics includes a hands-on exercise

3 Agile Threat Modeling

1. Modern Agile Threat Modelling Approaches
2. Transforming security requirements to code with BDD Security
3. Exploring the events and rituals of Agile Software Development through Scrum
4. Writing security requirements for Agile Software Development
5. Writing User cases and Abuse use cases
6. The Role of Privacy Impact Assessments in Security Requirements
7. Modern Threat modeling approaches
    - a. Rapid Risk Assessment
    - b. Rapid Threat Modelling prototyping
8. **Hands-on Exercises**:
    - a. Exploring UML as Code
    - b. Exploring Threat Modelling as Code
    - c. BDD - Security

Threat Modeling Professional

Practical DevSecOps

Detailed Syllabus

DAY 2

4 Reporting and Deliverables

1. How to manage threat models
    a. Documentation (excel, pdf)
    b. Backlog
    c. Bugs/Tickets
    d. Code
    e. Automation
2. Open source templates and tools
3. Validating threat models
4. Hands-on Exercises:

5 Secure Design Principles and Cloud Threat modeling

1. Case Study of Kubernetes Threat Model
2. Case Study of DNS Threat model
3. Case Study of AWS S3 Threat model
4. Exploring principles of Secure Design with examples
    a. Secure by Design
        i. Authentication
        ii. Authorization
        iii. Confidentiality
        iv. Integrity
        v. Availability
        vi. Defense in Depth
    b. Secure by Default
        i. Least Privilege
    c. Securing Deployment
        i. Hardened
        ii. Secure
    d. Trust with Reluctance

Threat Modeling Professional

Practical DevSecOps

Certification Process

✓ Exam and certification process

Our certifications are well recognized in the industry as we ensure our students gain practical skills to implement DevSecOps. To ensure we deliver on our promise, we have a rigorous certification program.

CTMP exam is an online, task-oriented exam where you attempt to solve **5 challenges** (tasks) in a span of **6 hours**. The exam is based on the content covered in the course but might require further research to pass the exam. Once the exam is done, you have **24 hours** to send us the exam report.

> ***Please note***
> it's not an MCQ or tests your memory type of exam but practical applicability of the content covered in the course.

✓ Exam Pass percentage

The student needs to achieve at least 80 points (80%) to achieve the CTMP certification.

✓ Exam Challenges/tasks

The exam has 5 challenges for the exam, each of these challenges provides you points based on how complete or partial your solution was. You would need to score 80 points out of 100 (80%) to achieve the CTMP certification.

✓ Exam documentation

After the exam, you have about 24 hours to send us the exam report via email.

✓ Steps Involved

A typical certification flow involves 5 steps.

1. The student schedules the exam.
2. The student will receive an exam guide that includes challenges via email. Our instructors will be there to assist you if you face any difficulty while connecting to the exam lab.
3. The student will connect to the exam lab using the above details and attempts the exam.
4. After the exam, the student will have 24 hours to send us the exam report.
5. Practical DevSecOps team will evaluate the report and share the result (pass/fail) with the student.

Practical
DevSecOps

About us

Practical DevSecOps (a Hysn Technologies Inc company) offers vendor-neutral, practical, and hands-on DevSecOps training and certification programs for IT Professionals. Our online training and certifications are focused on modern areas of information security, including DevOps Security, Cloud-Native Security, Cloud Security & Container security. The certifications are achieved after rigorous tests (12-24 hour exams) of skill and are considered the most valuable in the information security field.

@pdevsecops

@pdevsecops

Practical DevSecOps

USA

+1 (415) 800 4768
trainings@practical-devsecops.com
201 Spear St #1100, San Francisco, CA 94105

India

+91 81216 77008
apac@practical-devsecops.com
Hyderabad, India

Singapore

+65 85042132
apac@practical-devsecops.com
531A Upper Cross Street #04-95
Hong Lim Complex Singapore 051531

Practical DevSecOps