TOREON

Online training: Hands-on threat modeling and tooling for DevSecOps

Toreon CVBA
Grotehondstraat 44 1/1, B-2018 Antwerpen, Belgium | T +32 33 69 33 96
VAT BE0542.795.568 info@toreon.com | www.toreon.com

Table of contents

1 Online Hands-on threat modeling and tooling for DevSecOps 3
2 Hands-on threat modeling course 4
2.1 Threat modeling trainers 4
2.2 Course topics (1-day training online in-person) 5
2.3 Student package 7
2.4 Threat modeling – real world use cases 7
2.5 Training prerequisites 8
3 Get in touch 9

1 Online Hands-on threat modeling and tooling for DevSecOps

Based on our OWASP, O'Reilly and Black Hat training experience, we developed **an action-packed 1-day online Threat Modeling course** specifically for DevOps Engineers to improve reliability and security of delivered software. We will teach an iterative and incremental threat modeling method that is integrated in the development and deployment pipeline.

As speed of delivery is crucial with shorter development cycles, increased deployment frequency, and more dependable releases we focus on a **risk-based unified threat modeling practice** that is in close alignment with business objectives. The training material and hands-on workshops with real life use cases are provided by Toreon. The students will be challenged to perform practical threat modeling covering the different stages of threat modeling. Exercises are built upon a fictional Acme Hotel Booking (AHB) system, where we migrate a legacy client-server system towards a cloud based, micro service stack using AWS services:

- Sprint 1: Modeling a hotel booking web and mobile application, sharing a REST backend
- Sprint 2: Threat identification as part of migrating the booking system application to AWS
- Sprint 3: AWS threat mitigations for the booking system build on microservices
- Sprint 4: Building an attack library for CI/CD pipelines

After each hands-on workshop, the results are discussed, and students receive a documented solution.

Some feedback from our O'Reilly, OWASP and Black Hat training attendees:

- *"Sebastien delivered! One of the best workshop instructors I've ever had."*
- *"Very nice training course, one of the best I ever attended."*
- *"I feel that this course is one of the most important courses to be taken by a security professional."*
- *"The group hands-on practical exercises truly helped."*

Keywords:

- Threat modeling
- Secure application design
- Technical architecture risk analysis
- Privacy by design

This course is aimed at product managers, software developers, architects, DevOps engineers or application security professionals. Before attending this course, students should be familiar with basic knowledge of web and mobile applications, databases, and cloud development.

We adapted the training content, exercises and supporting tools to **allow remote online delivery of this training**. So far, we successfully delivered several inhouse remote trainings, Online Live Training for O'Reilly and an online training as part of OWASP Virtual AppSec Days.

2 Hands-on threat modeling course

Threat modeling is the primary security analysis task performed during the software design stage. Threat modeling is a structured activity for identifying and evaluating application threats and vulnerabilities. The security objectives, threats, and attacks modeling activities during the threat modeling are designed to help you find vulnerabilities in your application and the supporting architecture. You can use the identified vulnerabilities to help shape your design and direct and scope your security testing.

Threat modeling allows you to consider, document, and discuss the security implications of designs in the context of their planned operational environment and in a structured fashion. It also allows consideration of security issues at the component or application level. The threat modeling course will teach you to perform threat modeling through a series of workshops, where our trainer will guide you through the different stages of a practical threat model.

2.1 Threat modeling trainers

Toreon provides our experienced Threat Modeling trainers to share our practical threat model experience:

- **Sebastien Deleersnyder** led engagements in the domain of ICT-security, Web and Mobile Security with several customers in the private and public sector. Sebastien is the Belgian OWASP Chapter Leader, served as vice-chair of the global OWASP Foundation Board and performed several public presentations on Web Application, Mobile and Web Services Security. Furthermore, Sebastien co-founded the yearly BruCON conference.
- **Steven Wierckx** is a software and security tester with 15 years of experience in programming, security testing, source code review, test automation, functional and technical analysis, development, and database design, Steven shares his passion for web application security through writing and training on testing software for security problems, secure coding, security awareness, security testing, and threat modeling. He is the project leader for the OWASP Threat Modeling Project and organizes the BruCON student CTF. Last year, he spoke at Hack in the Box Amsterdam, hosted a workshop at BruCON and delivered threat modeling trainings at OWASP AppSec USA and O'Reilly Security New York.
- **Thomas Heyman** is an application security expert with 14 years of experience in both academia and industry. He has a PhD in secure software engineering, and has experience in threat modeling, secure architecture and coding, secure design reviews, and assessing the performance and scalability of distributed systems. He co-founded a software product company that helps highly regulated companies apply data analytics to improve their identity and access management. Thomas is passionate about application security, and strongly believes that proper security requires a holistic perspective, for which a good threat model is key.

2.2 Course topics (1-day training online in-person)

Threat modeling introduction

- Threat modeling in a secure development lifecycle
- What is threat modeling?
- Why perform threat modeling?
- Threat modeling stages

Diagrams – what are you building?

- Understanding context
- Data flow diagrams
- Trust boundaries
- **Hands-on: diagram B2B web and mobile applications, sharing the same REST backend**

Identifying threats – what can go wrong?

- STRIDE introduction
- Spoofing threats
- Tampering threats
- Repudiation threats
- Information disclosure threats
- Denial of service threats
- Elevation of privilege threats
- Threat tables
- **Hands-on: STRIDE analysis of AHB API migration to AWS cloud**

Addressing each threat

- How to address threats
- Authentication: mitigating spoofing
- Integrity: mitigating tampering
- Non-repudiation: mitigating repudiation
- Confidentiality: mitigating information disclosure
- Availability: mitigating denial of service
- Authorization: mitigating elevation of privilege
- Risk calculation
- **Hands-on: Threat mitigation of microservices and S3 buckets**

Practical threat modeling

- Effective threat model workshops
- Communicating threat models
- Updating threat models
- Soft skills for threat modelers
- Threat modeling from home
- Remote threat modeling
- **Hands-on: Threats & mitigations for a CI/CD pipeline**

Threat modeling tooling and resources

- Open-Source / free tools
- Commercial tools
- Threat modeling as code
- Threat modeling resources
- OWASP Threat Modeling Playbook

2.3 Student package

The course students receive the following package as part of the course:

- Hand-outs of the presentations
- Work sheets of the use cases,
- Detailed solution descriptions of the use cases
- Template to document a threat model
- Template to calculate risk levels of identified threats
- Toreon Whiteboard Hacking survival guide
- OWASP Threat Modeling Playbook

2.4 Threat modeling – real world use cases

As highly skilled professionals with years of experience under our belts we know that there is a gap between academic knowledge of threat modeling and the real world.

In order to minimize that gap we have developed practical Use Cases, based on real world projects. Each use case includes a description of the environment, together with questions and templates to build a threat model. Using this methodology for the hands-on workshops we provide our students with a robust training experience and the templates to incorporate threat modeling best practices in their daily work.

The students will be challenged to perform the threat modeling on the different stages of threat modeling on:

- Sprint 1: Modeling a hotel booking web and mobile application, sharing a REST backend
- Sprint 2: Threat identification as part of migrating the booking system application to AWS
- Sprint 3: AWS threat mitigations for the booking system build on microservices
- Sprint 4: Building an attack library for CI/CD pipelines

After each hands-on workshop, the results are discussed, and the students receive a documented solution.

2.5 Training prerequisites

Important pre-requisites for the training room are:

- Stable Internet access for the students
- Students should have their own laptop or tablet available
- Students should be able to participate in MS Teams virtual meetings
- Students should be able to participate in a dedicated private Slack channels created for this training.

3 Get in touch

To learn more about this training check out our threat modeling training offering on:

https://www.toreon.com/threatmodeling/

Or contact us at:

Sebastien Deleersnyder

seba@toreon.com

+32 478 504 117