TOREON

In-house training: Hands-on threat modeling for medical device manufacturers

Toreon BV
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

Revision control

Version	Date	Author	Comments
1.0	13-Apr-19	Sebastien Deleersnyder	Version Black Hat 2019
1.1	4-Oct-19	Sebastien Deleersnyder	In-house training version
1.2	28-Apr-20	Sebastien Deleersnyder	Adapted for medical device manufacturers

1 Hands-on threat modeling for medical device manufacturers

International regulators (such as the FDA) as well as customers are expecting Medical Device Manufacturers to deliver proactively secured devices. This is in part a question of technology, but equally a question of security engineering best practices applied during the product development lifecycle. This includes applying a mature Cybersecurity Risk Assessment methodology during the Risk Management process. One powerful technique available to engineers is threat modeling.

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.

To minimize that gap we have developed a 2-day course with 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. Students will be challenged in groups of 3 to 4 people to perform the different stages of threat modeling on the following:

- E-health web and mobile applications, sharing the same REST backend
- A CT scanner deployment in a hospital connected to a DICOM network
- OAuth scenarios for a wearable device supported by a web portal
- Privacy of a new data logging feature of a wearable health monitor

After each hands-on workshop, the results are discussed, and students receive a documented solution. This training is based on our advanced threat modeling training given at premium events such as Black Hat USA but tailored for medical device manufacturers.

Some feedback from our 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 software developers, architects, system managers, and people involved in quality/design assurance for medical devices. Before attending this course, students should be familiar with basic knowledge of web and mobile Applications, databases & Single sign on (SSO) principles.

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, 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 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

Threat modeling introduction

- Threat modeling in a secure development lifecycle
- FDA regulation “security by design”
- What is threat modeling?
- Why perform threat modeling?
- Threat modeling stages
- Different threat modeling methodologies
- Document a threat model

Diagrams – what are you building?

- Understanding context
- Doomsday scenarios
- Data flow diagrams
- Trust boundaries
- Sequence and state diagrams
- Advanced diagrams
- **Hands-on: diagram E-health 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
- Attack trees
- Attack libraries
- **Hands-on: STRIDE analysis of a CT scanner deployment in a hospital connected to a DICOM network**

Addressing each threat

- Mitigation patterns
- Authentication: mitigating spoofing
- Integrity: mitigating tampering
- Non-repudiation: mitigating repudiation

- Confidentiality: mitigating information disclosure
- Availability: mitigating denial of service
- Authorization: mitigating elevation of privilege
- Specialist mitigations
- **Hands-on: threat mitigations OAuth scenarios for a wearable device supported by a web portal**

Privacy threat modeling

- GDPR
- Privacy by design
- Privacy impact assessment (PIA)
- Privacy threats
- LINDUNN
- Mitigating privacy threats
- **Hands-on: Privacy of a new data logging feature of a wearable health monitor**

Advanced threat modeling

- Typical steps and variations
- Validation threat models
- Effective threat model workshops
- Communicating threat models
- Updating threat models
- **Threat models examples from other domains: automotive, industrial control systems, IoT and Cloud**

Threat modeling resources

- Open-Source tools
- Commercial tools
- General tools
- Threat modeling tools compared

Examination

- Hands-on examination
- Grading and certification

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
- Receive certificate: Following a successful exam (passing grade defined at 70%) the student will receive certification for successful completion of course

2.4 Threat modeling – real world use cases

International regulators as well as customers are expecting Medical Device Manufacturers to deliver proactively secured devices. This is in part a question of technology, but equally a question of security engineering best practices applied during the product development lifecycle. This includes activities such as threat modeling, as part of a mature Cybersecurity Risk Assessment methodology during the Risk Management process. However, 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 in groups of 3 to 4 people performing the different stages of threat modeling on:

- E-health web and mobile applications, sharing the same REST backend
- A CT scanner deployment in a hospital connected to a DICOM network
- OAuth scenarios for a wearable device supported by a web portal
- Privacy of a new data logging feature of a wearable health monitor

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:

- Internet access for the trainer and the students
- Projector
- White board
- One flip chart per 4 students
- Room setup in groups of 4 students
- Power adapters

The students should bring their own laptop or tablet to read and use the training handouts and exercise descriptions.

2.6 Training variations

We can also propose the following threat modeling training variations:

1) Whiteboard hacking
This is the general variation of the training, with a broad range of use cases from many domains. Perfect for companies that are not bound by domain specific regulation! As given at Black Hat USA: https://www.blackhat.com/us-19/training/schedule/#advanced-whiteboard-hacking---aka-hands-on-threat-modeling-14282

2) Offensive Whiteboard hacking for pen testers
Focus is on threat modeling as part of security testing. As given at BruCON: https://www.brucon.org/2018/brucon-2018-training/offensive-whiteboard-hacking-for-penetration-testers/

3) Hands-on Threat Modeling and tooling for DevSecOps
Focus is on defensive threat modeling as part of a secure development life cycle and tooling. As given at O'Reilly Velocity: https://conferences.oreilly.com/velocity/vl-ca/public/schedule/detail/74641

4) Privacy by design and threat modeling for IT
Focus is on integrating privacy by design and GDPR risk patterns with threat modeling as part of a secure development life cycle.

5) Threat modeling for ICS/OT
Focus is on using threat modeling in industrial, manufacturing, and operational technologies environments. As given at CS3STHLM: https://cs3sthlm.se/program/trainings/jasper-hooft/

3 Training options

3.1 Training customization

As an option we provide the possibility to use one of your applications for the training exercises.

Adapting the training with one of your own applications has some considerable benefits:

- The attendees will relate to the exercise, as it covers a real application of your organisation.
- The security awareness of the attendees on security design will increase, as the attendees will be exposed to your own organisation risks.
- The implications of doing threat modeling and how to integrate that in your project methodology and technology stack will be better understood by the participants.
- During the exercises some extra security threats and design flaws might be discovered for the selected application.

As input for this option we will need the following information for the representative and selected application:

- Business context and value
- Use cases
- Applicable security and regulatory requirements
- A diagram, with a detailed description of the components and flows.
- Any known security or privacy risks identified so far
- A contact to ask questions and review the exercise

The outcome will be the adapted exercises of the training based on your application.

3.2 Threat modeling coaching

An important next step after our training is to put your gained knowledge into practice. Therefore we propose to complement your training with our threat modeling coaching.

Our threat modeling coaching consists of the following activities:

- Introduce threat modeling templates in your development tooling
- Align threat modeling with your project methodology and security governance
- Facilitate and support threat modeling workshops with your teams
- Be a soundboard for your security champions and architects on threat modeling
- Validate new or updated threat models
- Start and improve threat model risk patterns for your organisation
- Assist in selection and introduction of threat modeling tools

Our goal is to measure, start and improve your threat modeling practice towards the level that is appropriate for your organisation risk exposure and appetite.

4 Get in touch

To learn more about this training, contact us at:

Sebastien Deleersnyder

seba@toreon.com

+32 478 504 117