TOREON

Agile Whiteboard Hacking aka Hands-on Threat Modeling Training

TOREON

Business driven cyber consulting

Build more secure products!

We teach threat modeling based on practical experience and have been offering our training annually at OWASP since 2016 and Black Hat Trainings since 2017. Our Black Hat training average score is 4.7/5 with excellent feedback!

Get a **Threat Modeling Practitioner Certificate**

You can get your Threat Modeling Practitioner Certificate with our internal training options: the **2-day "Agile Whiteboard Hacking" (this training)** or the 20-hour "Threat Modeling Practitioner" blended course. You will also receive our Threat Modeling Playbook, one-year online learning access, and a one-hour personal coaching session.

You can choose to have this training on-site or remote. We can adapt this training to fit your technology stack, products, or way of working.

Contact us by reaching out to:

Sebastien Deleersnyder

CTO Toreon

seba@toreon.com

+32 478 50 41 17

Schedule a call directly

Agile Whiteboard Hacking - aka hands-on Threat Modeling

This Training is taught in English, available in-person, on-site or remote.

This 2-day training is based on our 10th edition of our Black Hat trainings. We improved our threat modeling training with the exclusive threat modeling war game with red and blue threat modeling teams. Engaged in capture the flag style threat modeling challenges your team will battle for control over an offshore wind turbine park. Based on our experience in securing real-world Operational Technology (OT) infrastructure we deliver this war game as part of this training.

Also, in this edition we enhanced the section on privacy by design, compliance, and added a section on threat modeling medical devices. All participants get our Threat Modeling Playbook plus one-year access to our online threat modeling learning platform. As part of this training, you will be asked to **create your own threat model**, on which you will get individual feedback. **One month after the training we organize an online review session with all the participants**.

As highly skilled professionals with years of experience under our belts, we're intimately familiar with the gap between academic knowledge of threat modeling and real-world practice. To minimize that gap, we have developed practical use cases, based on real-life 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 challenging training experience and the templates to incorporate threat modeling best practices in their daily work. Students will be challenged in groups of 3 to 4 people to perform the different stages of threat modeling on the following:

◆ Diagramming techniques applied on a travel booking service

◆ Identification threats cloud-based update service IoT kiosk

◆ Attack Tree to break into a nuclear research facility

◆ SOC Risk Based Alerting system with MITRE ATT&CK

◆ Mitigate threats in a payment service

◆ Threat Modeling a Machine Learning-Powered Chatbot

◆ Apply Threat Modeling Playbook to agile development

◆ Threat Modeling the CI/CD pipeline

◆ Threat modeling wargame: "Zwarte Wind" battle for control

After each hands-on workshop, the results are discussed, and students receive a documented solution. Based on our successful trainings in the last years and the great and positive feedback, we release this updated advanced threat modeling training at Black Hat USA.

Some feedback from our Black Hat training attendees:

"Sebastien delivered! One of the best workshops 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."

"Hands-on labs are very well designed, and the solutions are also very smart!"

Keywords:

◆ Threat Modeling

◆ Secure application design

◆ Technical architecture risk analysis

◆ Privacy by design

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.

This course is aimed at software developers, architects, system managers or security professionals. Before attending this course, students should be familiar with basic knowledge of web and mobile applications, databases & security principles.

Course topics

Threat modeling introduction

◆ Threat modeling in a secure development lifecycle

◆ 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

◆ Advanced diagrams

◆ **Hands-on: Diagramming techniques applied on a travel booking service**

Identifying threats - what can go wrong?

◆ STRIDE

◆ **Hands-on: identification threats cloud-based update service IoT kiosk**

◆ Attack trees

◆ **Hands-on: Attack Tree to break into a nuclear research facility**

◆ Attack libraries

◆ **Hands-on: SOC Risk Based Alerting system with MITRE ATT&CK**

Addressing each threat

◆ How to address threats

◆ Mitigation patterns

◆ Setting priorities through risk calculation

◆ Risk management

◆ Threat agents

◆ **Hands-on: Mitigate threats in a payment service**

Threat modeling, compliance, and machine learning

◆ How to marry threat modeling with compliance

◆ GDPR and Privacy by design

◆ LINDUNN and Mitigating privacy threats

◆ Threat modeling medical devices

◆ Threat modeling Industrial Control Systems (IEC 62443)

◆ Mapping threat modeling on compliance frameworks

◆ AI related threats and countermeasures

◆ **Hands-on: Threat modeling a Machine Learning-Powered Chatbot**

Threat modeling practice

◆ Soft skills for threat modelers

◆ Threat modeling in sprints

◆ OWASP Threat Modeling Playbook

◆ **Hands on: Apply Threat Modeling Playbook to agile development**

◆ Threat modeling at scale

◆ SAMM and threat modeling

◆ Lessons learned

◆ **Hands-on: Threat Modeling the CI/CD pipeline**

◆ **Threat modeling wargame: "Zwarte Wind" battle for control**

Threat modeling tooling and resources

◆ Open-Source tools

◆ Commercial tools

◆ General tools

◆ Threat modeling tools compared

◆ Threat Modeling Manifesto and Capabilities

◆ Example threat models

Review session (online session after 4-6 weeks)

◆ Hand-in of your own threat model

◆ Individual feedback on your threat model

◆ Review session

Student package

Your bonus training package includes:

◆ Following the demonstration of handed-in threat model: Threat Modeling Practitioner Certificate.

◆ One year of access to our threat modeling e-learning platform

◆ Presentation handouts

◆ Tailored use case solution descriptions

◆ Detailed use case solution descriptions

◆ Threat model documentation template

◆ Template for calculating identified threat risk severity

◆ Threat modeling playbook

◆ STRIDE mapped on compliance standards

Course topics

Important pre-requisites for the training room are:

◆ Internet access for the trainer and the students

◆ Projector

◆ White board

◆ One flip chart with 3M sheets 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.

Training options

Training customization

Optionally we provide the possibility to use your applications or systems for the training exercises.

Adapting the training with your own applications has considerable benefits:

◆ The attendees will relate to the exercises, as it covers a real application of your organization.

◆ The security awareness of the attendees on security design will increase, as the attendees will be exposed to your own organization 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 applications.

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.

Threat modeling coaching

An important next step after our training is to put your trained 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 organization

◆ 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 organization risk exposure and appetite.

Threat Modeling Trainers

Our experienced Threat Modeling trainers share their practical threat model experience:

Sebastien 'Seba' Deleersnyder

Sebastien (Seba) Deleersnyder is co-founder and CTO of Toreon and a proponent of application security as a holistic approach. He started the Belgian OWASP chapter, was an OWASP Foundation Board member, and has given numerous public presentations on Application Security. Seba also co-founded Belgium's annual BruCON security & hacker conference and training sessions. With a development background and years of security experience, he has trained countless developers to create more secure software. Having led OWASP projects such as OWASP SAMM, he has genuinely helped make the world a safer place. What's he currently up to? Right now, he's busy adapting application security models to the evolving field of DevOps and is also focused on getting the word out on Threat Modeling to a broader audience.

Steven Wierckx

Steven Wierckx is a seasoned 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 web application security passion by writing about and through training on testing software for security problems, secure coding, security awareness, security testing, and threat modeling. He's the OWASP Threat Modeling Project Lead and organises the BruCON student CTF. Last year, he spoke at Hack in the Box Amsterdam, hosted a workshop at BruCON, and provided threat modeling training at OWASP AppSec USA and O'Reilly Security New York.

Thomas Heyman

Thomas Heyman is an application security expert with 14 years of experience in academia and industry. He has a PhD in secure software engineering and has worked 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 firmly believes that good security requires a holistic perspective, which should always have a sound threat model at the base.

Georges Bolssens

Georges Bolssens embarked on his coding journey in the early 1990s and delved into the realm of application security in 2017. With an inherent passion for teaching, Georges is not only a seasoned developer but also an adept communicator. His unique talent lies in simplifying intricate subjects through relatable analogies, making him an engaging and effective speaker. Having undertaken numerous consulting assignments, Georges has assumed the role of a cybersecurity educator for a diverse spectrum of professionals. His guidance has illuminated the path for individuals ranging from legal experts at renowned "Big 4" consulting firms to ethical hackers and all those in between.In his capacity as an Application Security Consultant at Toreon, Georges has been instrumental in assisting numerous clients in constructing comprehensive threat models for their digital assets

Get in touch!

You can choose to have this training on-site or remote. We can adapt this training to fit your technology stacks, products, or way of working.

Contact us by reaching out to:

Sebastien Deleersnyder

CTO Toreon

seba@toreon.com

+32 478 50 41 17

Schedule a call directly

Supplier Information

Name:	Toreon
Legal Entity:	BV
Nationality:	Belgian
Address:	Grotehondstraat 44 1/1 B-2018 Antwerpen Belgium
Administrative email:	administratie@toreon.com
VAT:	BE 0542.795.568
IBAN:	BE10 0017 1351 5104
Financial Institution:	BNP Paribas Fortis
Telephone:	+32 3 369 33 96
Contract Responsible(s)	SEBASTIEN DELEERSNYDER
Mail Address:	sebastien.deleersnyder@toreon.com
Telephone:	+32 478 504 117

References

These are some of our Threat Modeling (TM) reference customers. Further details are available upon request.

- Euroclear - TM coaching
- Standard Chartered Bank - TM training
- Banque Lombard Odier & CIE SA - TM training
- Lloyds Banking Group - IriusRisk TM training and coaching
- BP - TM training

- Sage - IriusRisk TM training and coaching
- Costo Wholesale - TM training
- Accenture USA - TM training
- LinkedIn - TM training
- Booking.com - TM training
- SD Worx - TM execution
- Barco - Appsec Support / Threat modeling

- ENTSO-E - Appsec Support / Threat modeling
- Atlas Copco - Appsec Support / Threat modeling
- UCB - Appsec Support / Threat modeling / TM training
- Blackhat USA and Europe 2017 - 2023 - TM trainings
- O'Reilly, OWASP, BruCON, ... - TM trainings

Terms & Conditions

1 Object

Toreon delivers services in accordance with the General Sales Conditions and the specific conditions set out in the offer. The agreement between the Client and Toreon consists of the General Sales Conditions and the Toreon offer ("Agreement").

2 Toreon offer and purchase order

The Toreon offer is valid for a maximum period of thirty (30) calendar days. This version of the offer prevails over earlier versions. It supersedes all prior agreements, whether oral or written, between the parties with respect to such matter.

The Client accepts the Toreon offer by signing a purchase order or by the acceptance of the commencement of the performance of the services.

3 Rights and obligations

3.1 Information. The Client shall make all information, files, documents and other relevant material required for proper performance of the Agreement available to Toreon no later than two (2) Working Days (any day except a Saturday, Sunday or official Belgian holiday) after receipt of a request from Toreon.

3.2 Cooperation. The Client shall provide immediately upon request of Toreon all facilities, assistance, and cooperation for the proper performance of the Agreement.

The Client shall give access to the premises, buildings, or other facilities during and after normal office hours for the purposes of performance of the Agreement.

The Client shall provide to Toreon the security procedures and instructions and prepare the environment to enable the delivery of services, prior to the performance of the Agreement.

The Client shall appoint a contact person, who will be responsible for the communication with Toreon and who shall take the decisions related to the execution of the Agreement in a timely fashion.

3.3 Toreon material. The Client shall be liable for the loss of or damage to Toreon's material used in the execution of the Agreement, except if the loss or damage results exclusively from fault or negligence by Toreon.

4 Delivery and acceptance

4.1 Delivery. Toreon undertakes reasonable commercial effort to deliver services at the agreed point in time.

4.2 Acceptance. The Client has accepted the services unless he has notified Toreon in writing of any problem within five (5) Working Days as from delivery.

5 Prices and payment

5.1 Prices are quoted in EURO. The prices mentioned in the Toreon offer do not include VAT or any other expenses or duties. Toreon may adapt the prices if the costs for the services increase before the placement of the purchase order by the Client.

5.2 Additional administrative cost. The Client shall make a separate payment per invoice, clearly stating the invoice number. If payments are lumped together, Toreon may charge an administrative cost of €65.

5.3 The Client shall bear all costs due to the payment of the invoice. In the event of overdue payment, Toreon shall be entitled to interest at the legal rate without prior written notice. Should the Client not pay timely, Toreon may suspend the performance of the Agreement until full payments has been made or may consider the Agreement as terminated.

5.4 The Client shall have accepted the invoices, unless Toreon has received Client's complaint related to the invoice within fifteen (15) calendar days of invoice date.

5.5 Travel and stay expenses outside of Belgium will be invoiced at cost with an additional 8% administration cost with a minimum of 100€ per one-way trip per person. Travel time of consultants will be billed at 60% of agreed hourly tariffs.

6 Intellectual property

6.1 Intellectual property rights. All intellectual property rights related to the products/services shall vest in Toreon or its suppliers. It is understood that Client receives no title or ownership of intellectual property rights, unless otherwise explicitly specified in the Agreement.

6.2 Software licenses. All software shall be delivered subject to the software license agreement of the manufacturer of the software.

7 Copyright and intellectual property

All software, programs, studies, systems, and all other documents developed in the framework of the present Agreement shall be deemed to be property and will stay property of Toreon.

The Client will provide the necessary ownership and user rights when Toreon is considered to use software, or other material, subject to copyrights, owned by the customer. The Client shall indemnify Toreon completely of any expenses and/or costs (incl. Legal expenses) and damage that occurs from a third-party claim with regards to ownership and copy- and user rights of software or material as described above.

8 Confidentiality

Parties shall undertake all reasonable measures to treat the confidential information exchanged in the frame of the Agreement ("Confidential Information") in a confidential manner. Parties shall not disclose Confidential Information to third parties without the prior written approval of the other party. Confidential Information may be disclosed only to staff and/or subcontractors of the receiving party who reasonably require access to such information for the purpose of the performance of the Agreement.

Confidential Information does not include: (i) information received outside the scope of the Agreement and without restriction on disclosure; (ii) information independently developed by the receiving party; (iii) information which is publicly known.

9 Liability

Toreon's liability under the Agreement shall be limited to the total amounts that the Client paid over the 6 months preceding the cause of the damage. Toreon shall not be liable for unforeseeable or indirect damages, including but not limited to suspension of Client's activities, loss of revenue, loss of information, data, or programs, third party claims.

Any claim for damages should be filed ultimately six (6) months after occurrence of the damages and ultimately six (6) months after termination of the Agreement.

10 Termination

If the term of the Agreement is indefinite, either party may terminate the Agreement by notice in writing to the other party with a notice period of 3 months.

Either party may terminate the Agreement at any time, directly without referral to the courts, by notifying the other party, if the latter seriously violates any of its essential obligations under this Agreement and the violation is not rectified within thirty (30) calendar days of written notification thereof.

The Agreement shall automatically be terminated if one of the parties ceases its activities, becomes insolvent or bankrupt, is dissolved or is subject of a similar procedure.

11 Miscellaneous

11.1 Toreon may entrust performance of its obligations under this Agreement to a subcontractor or transfer all or part of its rights and obligations under this Agreement without Client's prior consent.

11.2 The Client to whom Toreon delivers services, shall not engage directly or indirectly any of Toreon employees or any subcontractor who is or has been directly involved in the performance of the Agreement without the prior written consent of Toreon, independent of whether the Client had direct contact with the employee or subcontractor. This prohibition applies during the Agreement and for a period of six (6) months after the termination of all contractual agreements between Toreon and the Client.

In the event of non-compliance with the aforementioned prohibition, the Client must pay Toreon compensation equal to twelve times the global monthly cost that Toreon bears for the performance of the relevant employee or subcontractor. The global monthly cost is determined based on the average of the months, limited to a period of twelve months, prior to the violation of the prohibition, subject to Toreon's right to claim a higher compensation claim if the actual damage suffered would be greater.

11.3 The Agreement replaces any previous agreement, oral or written, between the parties with respect to the purchase order.

11.4 The fact a party does not exercise his rights under this Agreement, shall not be interpreted as a waiver of that party's rights.

11.5 Either party shall be excused from the performance of any of its obligations under the Agreement, if the performance is prevented or delayed by a cause beyond the affected party's control which, without limitation, includes fire, flood, accident, storm, natural disaster, war, riot, act of government or strike. The obligations of Toreon under the Agreement shall be extended by a reasonable period.

11.6 Communications under the Agreement shall be in writing and sent by registered mail, courier, fax, or e-mail, handed over to the general counsel at the registered office of the party to whose attention the message is sent.

11.7 The Agreement shall be governed by Belgian law.

In case of a dispute between both Parties concerning the Agreement, which cannot be solved by negotiations, both Parties commit themselves to resolve the dispute by mediation by means of the instruction guide of bMediation (Louizalaan 500 – 1050 Brussel).

In the event of a dispute which cannot be resolved by mediation within a month of the first request for mediation, the Antwerp courts have the exclusive jurisdiction.