
TOREON
Threat modeling
done right

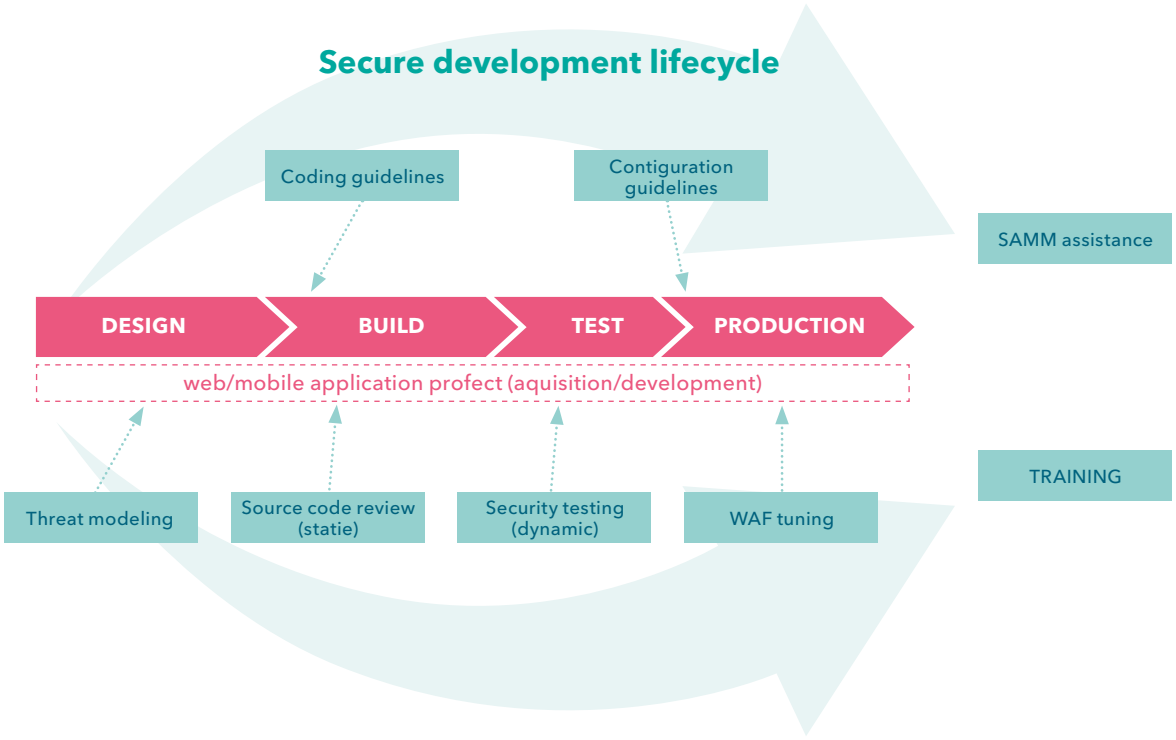
Table of Contents

Creating trust for a safer digital society

Stop shooting in the dark

You may have heard of threat modeling as a structured activity for identifying and managing application threats. And that's exactly what it is. Threat modeling – also called **Architectural Risk Analysis** – is an essential step in the development of your application. Without it, your protection is a shot in the dark.

Multiple security issues, a timely approach



When you create a piece of software, you will face multiple security issues in different phases of the lifecycle; such as security design flaws, security coding bugs and security configuration errors.

Reducing risks effectively equals starting with threat modeling as soon as possible. That is why it is typically done during the **design stage** of a new application. Threat modeling allows you to find vulnerabilities and to consider, document and discuss the security implications of design, code and configurations.

Threat modeling is typically performed in 4 steps:

- **Diagram**: what are we building?
- **Identify threats**: what can go wrong?
- **Mitigate**: what are we doing to defend against threats?
- **Validate**: validation of the previous steps and act upon them.

Do you want more details about the 4 steps? Just turn the page. You'll find it on page 5.

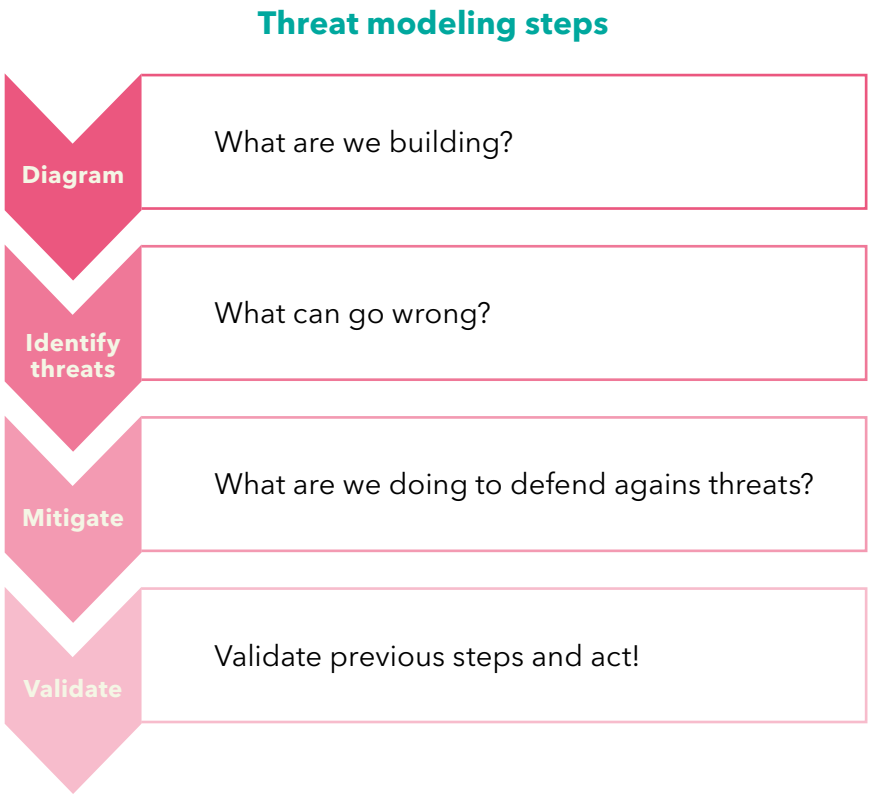
Why you should start with threat modeling

One of the major advantages of threat modeling is that you prevent security flaws when there is time to fix them: in the design phase. But there are many more reasons to start with threat modeling today; such as:

- You select a mitigation strategy and mitigation techniques based on identified, documented and rated threats.
- You identify and address the greatest risks.
- You are able to prioritize development efforts within a project team based on risk weighing.
- You increase risk awareness and understanding.
- You use mechanisms for reaching consensus and better trade-off decisions.
- You also make use of threat modeling to communicate results.
- You benefit from cost justification and support for needed controls.
- You use artefacts to document due diligence for each software project.

Threat modeling in 4 steps

Where do you start? And how?
Threat modeling is performed through a series of **workshops**. Architects, developers and system administrators are guided through the threat modeling process. It is the primary security analysis task, executed during the software design stage. Threat modeling is typically performed in 4 steps:



Step 1: diagram the application

In this step, you gain a **comprehensive understanding** of the mechanics of your application. In other words: you understand what you are building. That makes it a lot easier for you to uncover more relevant and more detailed threats. This also includes the identification of clear security objectives. They help you to focus the threat modeling activity and determine how much effort to spend in the following steps. When you have documented the important characteristics of your application and actors, you can identify relevant threats during the next step more easily.

Step 2: identify threats with STRIDE

You use details from the previous step in the STRIDE phase to identify threats relevant to your application scenario and context. With STRIDE, you can flawlessly **identify what can go wrong**.

STRIDE was developed by Microsoft to educate developers how to think about computer security threats, and is an acronym for:

- **Spoofing**: can an attacker gain access using a false identity?
- **Tampering**: can an attacker modify data as it flows through the application?
- **Repudiation**: if an attacker denies doing something, can we prove he did it?
- **Information disclosure**: can an attacker gain access to private or potentially injurious data?
- **Denial of service**: can an attacker crash or reduce the availability of the system?
- **Elevation of privilege**: can an attacker assume the identity of a privileged user?

Each of these threats is the opposite of a property that you want your system to have. Spoofing – for example – is the opposite of authentication.

Steps 3: mitigate identified vulnerabilities

In this step, you review the layers of your application to identify the necessary security controls related to your threats. **Vulnerability categories** help you focus on those areas most prone to mistakes.

Steps 4: validate

The final step is to validate the whole threat model. Is each threat mitigated or not? And for unmitigated threats: are the residual risks clearly explained and tied into business risks? In the validation step, you also decide and follow-up on the **next steps** to manage the identified threats.

Gain more insight and create doomsday scenarios for better threat modeling

On the previous pages you already read about what threat modeling is, and about the **4 steps** it contains. In practice, however, threat modeling is more than just a technical analysis of your application. The threat landscape is constantly evolving, and so is your organisation. Therefore, you need to understand the technical and business context, and create doomsday scenarios. As a result, you have a broader insight of the threats to your application.

The ecosystem

Applications are not always stand-alone. On the contrary; they are mostly part of an ecosystem of applications. You need to find out how it works and how it supports your organisation. You also need to have a clear understanding of the security requirements. You should, for example, know what other applications or services the application is exchanging information with.

The business context

What business process is being performed or supported? What are the characteristics of that specific process? And how crucial is that process for your business? You also need to find out which people are using the application and identify threat actors. In most cases, they fall into one of the following categories:

- **Insider trusted**: privileged users
- **Insider untrusted**: very regular users, contractors …
- **External trusted**: suppliers, partners, service providers …
- **External untrusted**: competitors, cybercriminals …

Eventually, you need to identify risks for your business: what is the **impact** and what is the **probability** that a certain risk will occur?

The added value of threat modeling

Threat modeling is quite time-consuming and thus expensive. It is therefore only relevant for important applications: those that bring in a lot of revenue or handle important data for your organization.

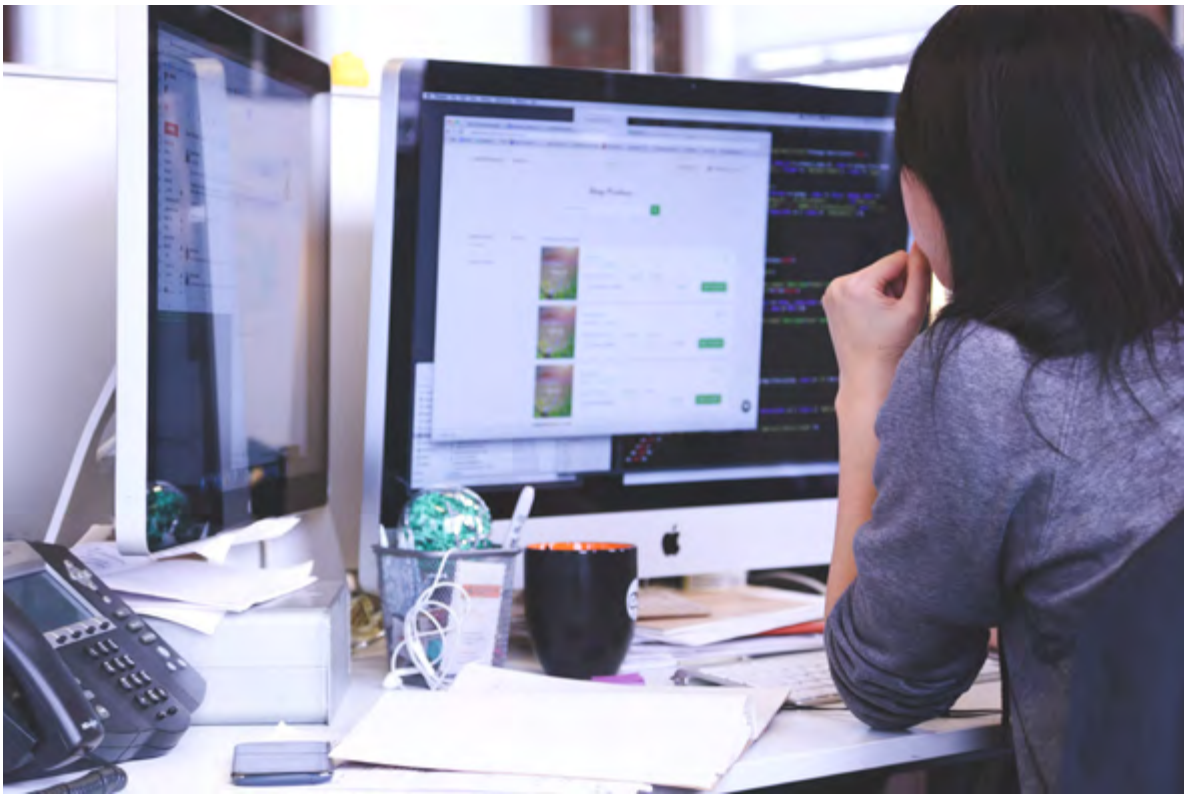
Create doomsday scenarios

Doomsday scenarios are **hypothetical** situations: the worst that could happen to an application – and for your business. Creating doomsday scenarios helps you to proactively anticipate – and even prevent – possibly catastrophic events. You need to describe the following:

- **Threat sources**: who would be interested in compromising the applications? Why would this be interesting for an attacker?
- **Impact**: what will be the impact of an attack? Some of the possibilities are theft, loss, corruption and disruption.
- **How**: how will the scenario be realized? Describe in detail how the attack would be performed.

These scenarios give feedback on your current security situation. You will discover more potential risks and steps to be taken to reduce these risks.

Use data flow diagrams for a profound understanding of your application



Now that you know more about the why and how of threat modeling, it is time to take a deeper look into the data flow diagrams. A data flow diagram gives you a **graphical representation** of the data flow through an information system. And that's quite interesting, because it provides you with a common understanding of your application. It also creates the opportunity to identify where (important) data is coming from and how it is processed and stored. Working with a data flow diagram is a focused approach to technical development, where you do more research up front, before you get to coding. It is also the perfect foundation for the STRIDE stage of threat modeling (see page 6).

The elements in a data flow diagram

A data flow diagram has a unique set of elements to represent different entities in a data flow (see also page 12):

External entity

This shape is used to represent any entity outside of the application that sends or receives data, communicating with the system. External entities are sources and destinations of information entering or leaving the system. They are typically drawn on the edges of the diagram.

Process

The process shape represents a task that handles data within the application. It might process the data, for example direct the data flow, or perform an action based on the data, such as make computations or sort the data based on logic.

Data store

This represents locations where the data are stored. They do not modify the data, but only store them.

Data flow

This symbolises the path that the data take between external entities, processes and data stores. Data flows are the interfaces between these components. An arrow represents the direction of the movement of the data.

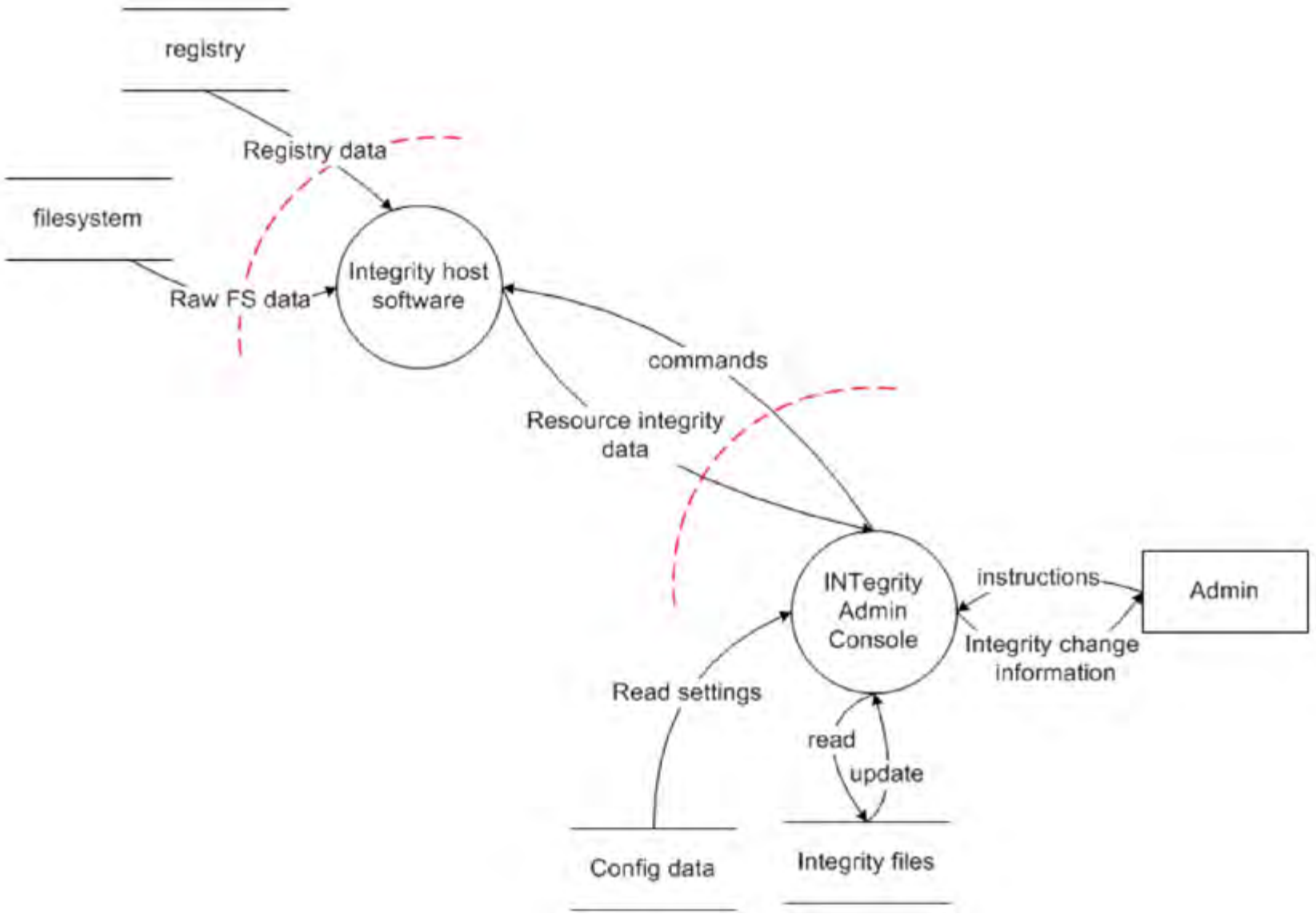
Trust boundary – an extra element for threat modeling

Trust boundaries are used as an extension of classical data flow diagrams for threat modeling, and represent the **change of trust levels** as the data flow through the application. They intersect data flows and indicate attack surfaces where an attacker can interject: machine boundaries, privilege boundaries and integrity boundaries are some examples of trust boundaries.

Trust boundaries mostly appear across processes that are **talking over a network**. There might be a secure channel, but they are still distinct entities. Encrypting the network traffic is an instinctive mitigation, but that doesn't address tampering or spoofing.

The trust boundaries in these data flow diagrams are used in the next threat identification stage.

Level 1 diagram



This high level, single-feature Level 1 diagram, uses the program integrity as an example.

DFD Basics

External Entity

The external entity shape is used to represent any entity outside the application that interacts with the application via an entry point.

Process

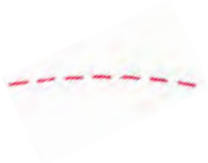
The process shape represents a task that handles data within the application. The task may process the data or perform an action based on the data.

Data Store

The data store shape is used to represent locations where the data is stored. Data stores do not modify the data, they only store data.

Data Flow

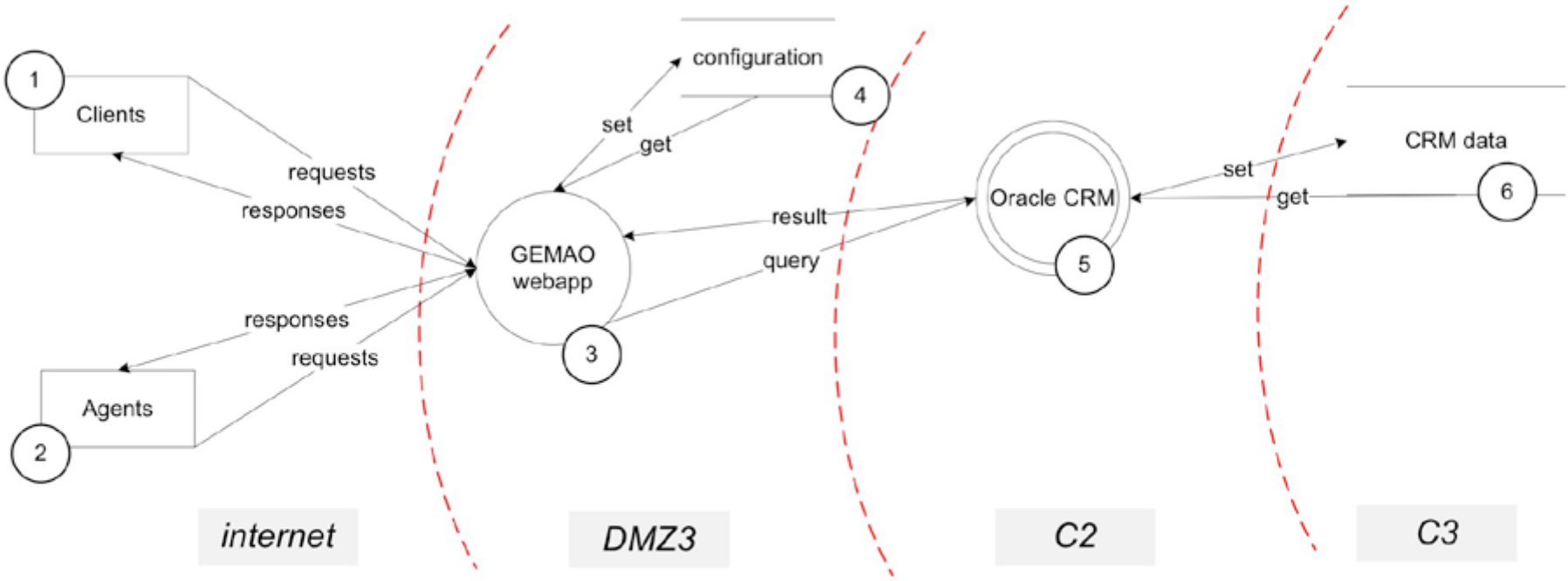
The data flow shape represents data movement within the application. The direction of the data movement is represented by the arrow.



Trust Boundary

The trust boundary shape is used to represent the change of trust levels as the data flow through the application.

Trust Boundaries



This example of a trust boundaries diagram, of the ACME Insurance GEMAO application, shows where trust boundaries intersect data flows.

Now you know the basics of threat modeling. If you want to learn more, we are happy to invite you to our 2-day Hands-on Threat Modeling Course where you will discover everything you need to know about it. And you get concrete tools to implement threat modeling in your organization.

Ready to take your application security to the next level? Take a look at our calendar and book your seat in our 2-day Hands-on Threat modeling course, or read more on our blog.

About Toreon

We believe that security is vital for people to live and work confidently and with trust in our digital society. That's why we dedicate ourselves to provide Information Security Consulting Services. What's there to know about us?

We are ICT security consultants

We help you to leverage your information technology and achieve your organisation's goals. While you run your business, we keep track of the information risks that your organisation faces and we help you to only take actions that fit your risk appetite.

We are an independent partner you can trust

We act as trusted advisors for our clients. We accompany you and help you make informed decisions about ICT security. We help to optimise your choices so that you can have peace of mind.

We are a team of experts

For every engagement, we mobilise our team of experts. This always brings solid experience and expertise to the task at hand. It benefits you to always get the right person or team for the job.

We are young, entrepreneurial and ambitious

We intend to be the go-to information security company in Belgium by 2020. We are growing steadily at more than 50% per year and currently have 20 consultants with various skills in-house.

We are all about people

We care about our employees and support their ambitions. We invest heavily in the professional education of our employees and give them the opportunities to develop their skills and the freedom to evolve as a person and as a professional.

We share our knowledge

Working in ever changing multi-skill teams fosters knowledge sharing and personal development. This leads to well-functioning project teams that better support you. On top of that, we love to share our knowledge with you as well.

Contact us:

Grotehondstraat 44/1
B-2018 Antwerpen
Belgium
+32 3 369 33 96
info@toreon.com

Creating trust for a safer digital society

TOREON