White paper

The power of Threat Modeling: a more secure digital solution

iquality

Contents

01

Threat Modeling: reduce your digital vulnerability

Identifying digital vulnerabilities at an early stage

In the ever-changing world we live in, it is very important that our personal data, trade secrets, financial transactions and other information are handled securely. Digital security is an important spearhead in the design and realization of digital solutions.

How do we ensure digital security? We do this by becoming aware of the potential threats we may face. Threat modeling is a powerful method that helps us think ahead, strengthen our defenses and prevent potential security incidents.

> “Threat Modeling is a powerful method that helps us think ahead, strengthen our defenses and prevent potential security incidents.”

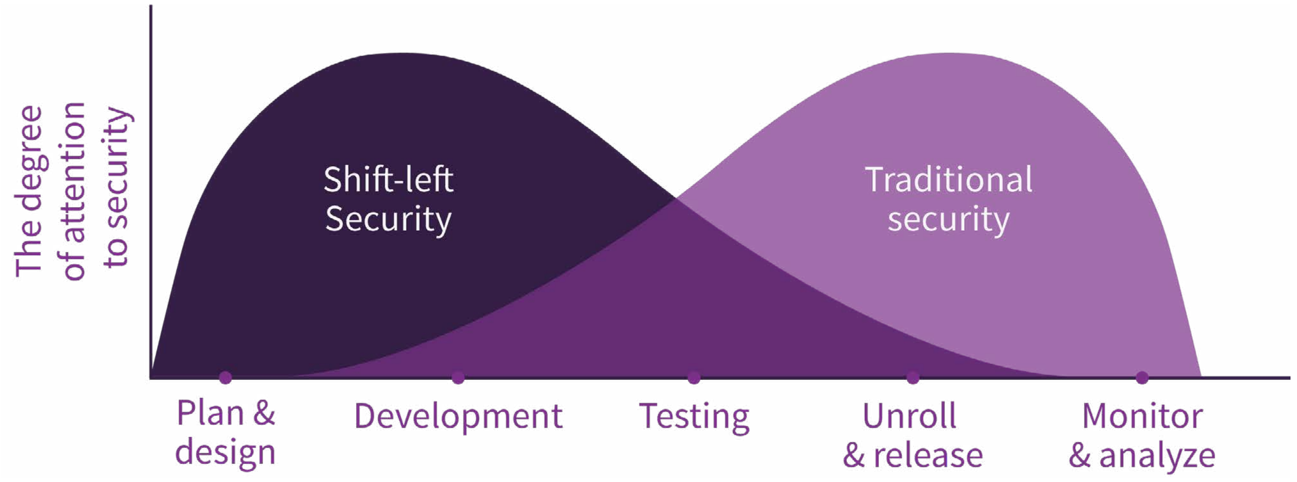
By reading this white paper, you will learn how we use threat modeling to design and build secure digital solutions. We actively look for the "open ends" to ensure that nothing is forgotten.

The result? A more robust and secure system, with effective security measures and minimized risks.

01 Shift-left security

Proactive software security

Before we introduce threat modeling, we want to introduce you to shift-left security. Shift-left security represents a proactive mindset. The idea is to already have security measures and controls in place build during the design phase and throughout the development process, instead of fixing security issues afterwards. The name 'shift-left security' says it all, security is literally going to shifted left in the development cycle.



Imagine this...

Imagine a situation where an organization is in the process of developing a new application. The organization has chosen not to conduct a security assessment until the end of the development process, just before deployment. During the assessment, several vulnerabilities are discovered.

The development team then faces a race against time to fix the security vulnerabilities, which unfortunately leads to a delay in the release of the application. Moreover, they face increased complexity because most of the code is already written and major changes must be made to resolve the security vulnerabilities (=increased cost).

This scenario could have been avoided if threat modeling was integrated into the plan and design. The development team would have had time to take appropriate action on weaknesses in the system.

Threat Modeling as an intrinsic part of software development

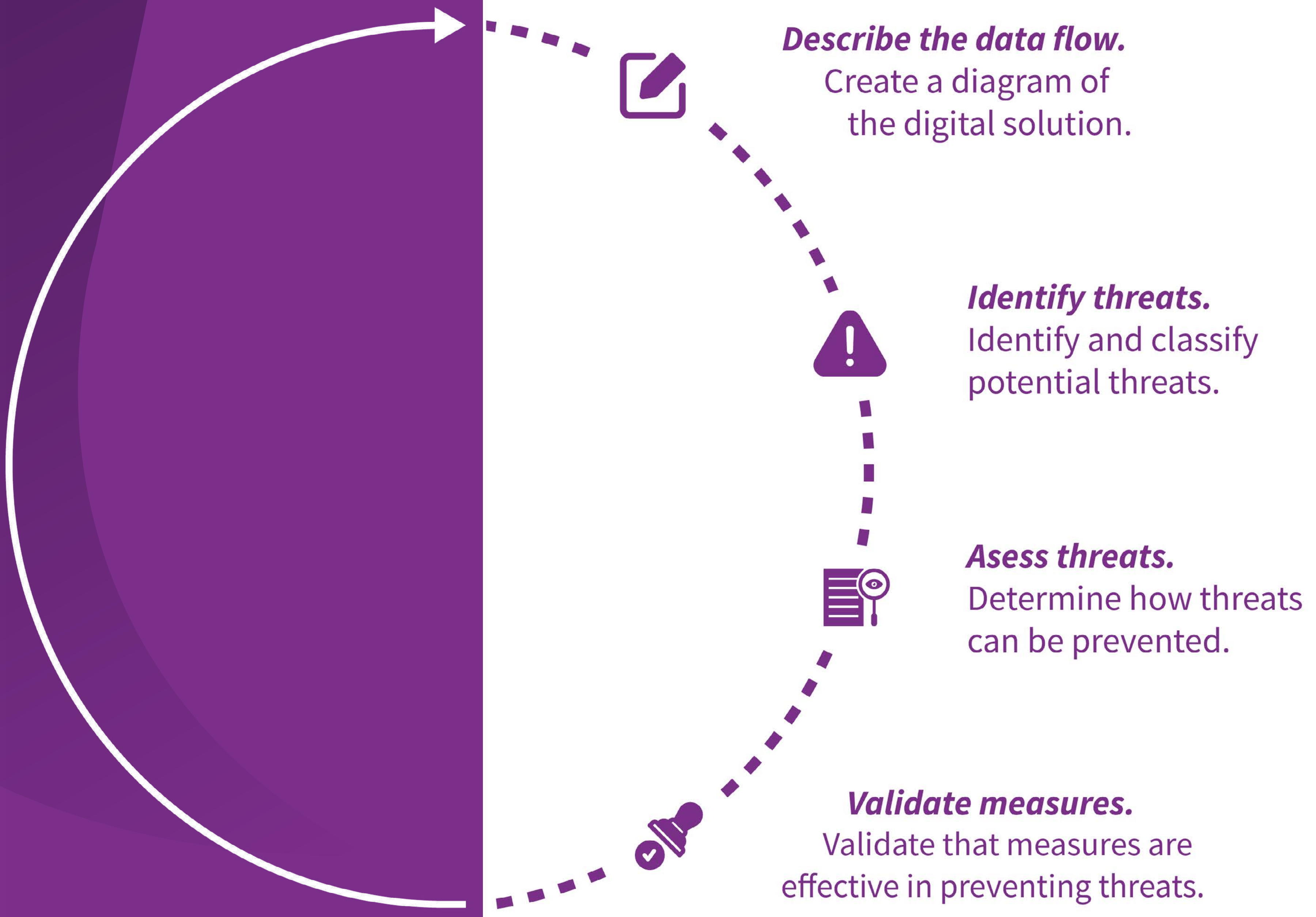
Applying threat modeling within the shift-left security mindset promotes the culture of 'security by design', becoming an intrinsic part of the development process. This ensures that security is not seen as an afterthought, but as an essential aspect that is taken into account from the very first steps. This results in higher quality software because of potential security vulnerabilities identified and addressed before they can escalate.

02

Threat Modeling in four steps

Threat Modeling step-by-step

The threat modeling process includes several steps, including defining the data flow of the digital solution, identifying potential threats and vulnerabilities, defining measures to mitigate the vulnerabilities and then validating them. It is an **iterative process** that keeps repeating itself. The software is therefore constantly assessed and evaluated so that new threats and vulnerabilities are recognized in time.



Describe the data flow.
Create a diagram of
the digital solution.

Identify threats.
Identify and classify
potential threats.

Asess threats.
Determine how threats
can be prevented.

Validate measures.
Validate that measures are
effective in preventing threats.

02

Step 1: Describe the data flow

Mapping out the digital solution

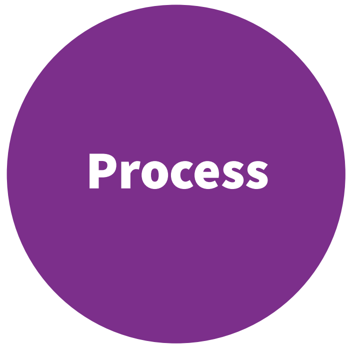
An important part of threat modeling is describing the data flow of the digital solution. Data flows in the system are analyzed to determine what data is being sent, where it is coming from and where it is going. This identifies the key assets.

Creating a diagram

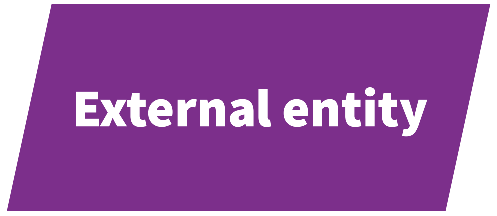
The data flow of the digital solution is sketched in a diagram, which maps the entire digital solution. Components that are more complex are highlighted and the same type of diagram is made at a deeper level.

The building blocks of the diagram

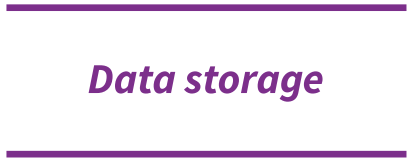
The following building blocks are used to provide a schematic insight into the structure of a digital solution.



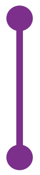
A process is a component (custom or not) that facilitates tasks.



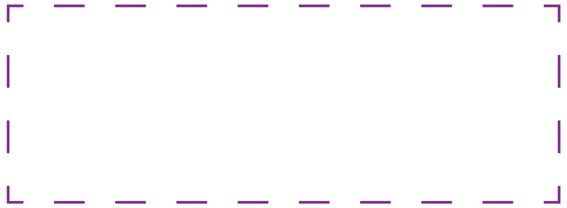
An external entity is beyond our control (for example, a user or an external service).



Data can be stored in, for example, a database, search index, file on a hard disk or cloud storage.



When communication takes place, then we indicate that with a line.



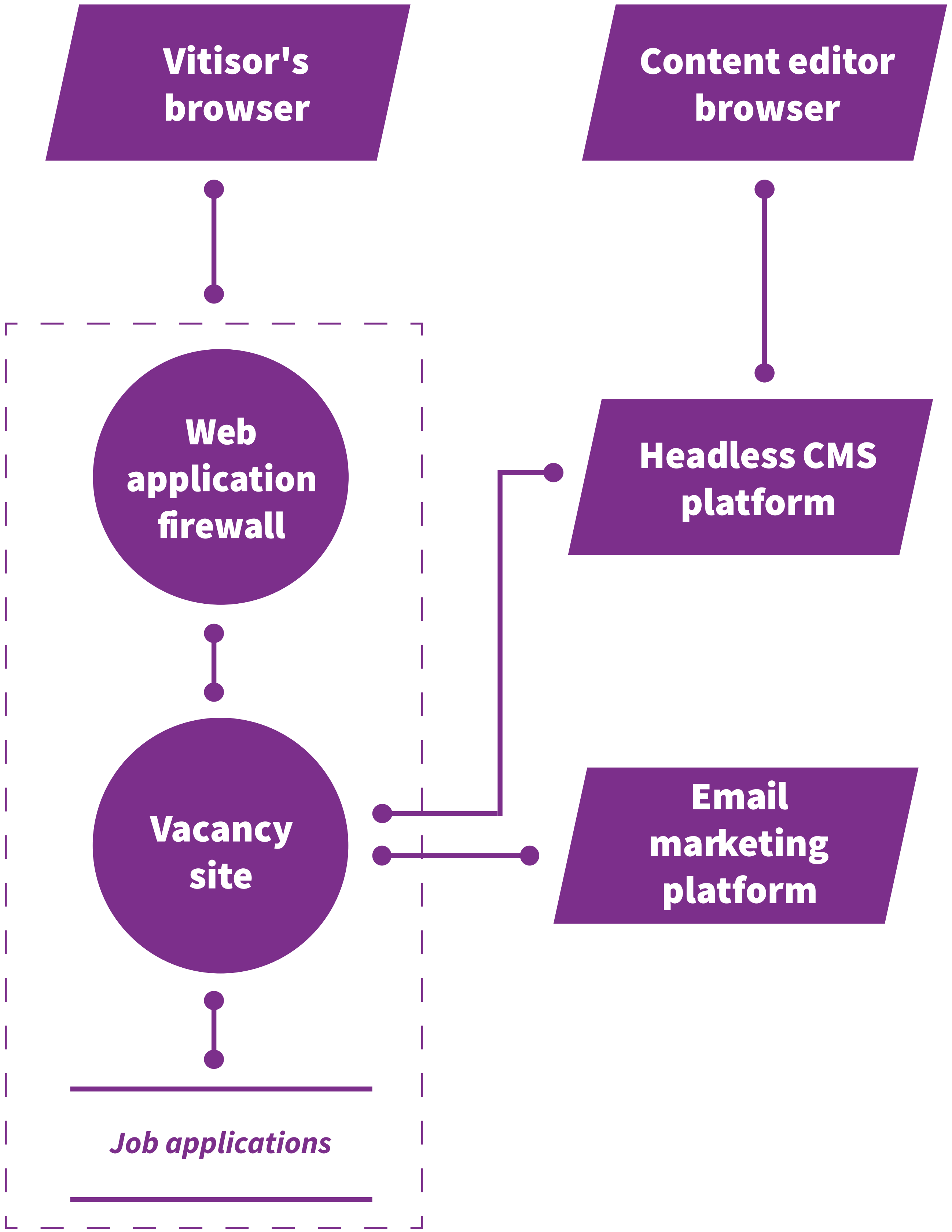
A trust boundary indicates where there is a separation between parts that we do and do not trust (for example, between a private network and the internet).

Example: job site

On the right you can see, simplified, how the different building blocks are combined into a complete data flow diagram for a job site. The first step, and thus the basis for threat modeling, has been taken!

Context for this digital solution:

- **Vacancies are managed in an external content management system.**
- **Visitors can view vacancies and apply for jobs on the website.**
- **Applications are saved and an e-mail is sent to an HR employee to point this out.**



02

Step 2: Identify threats

Move into a hackers' mindset

In the next step, the diagram is looked at and potential threats are identified. We put ourselves in the mindset of a hacker and look at how we can damage the **availability**, **integrity** and **confidentiality** of the system.

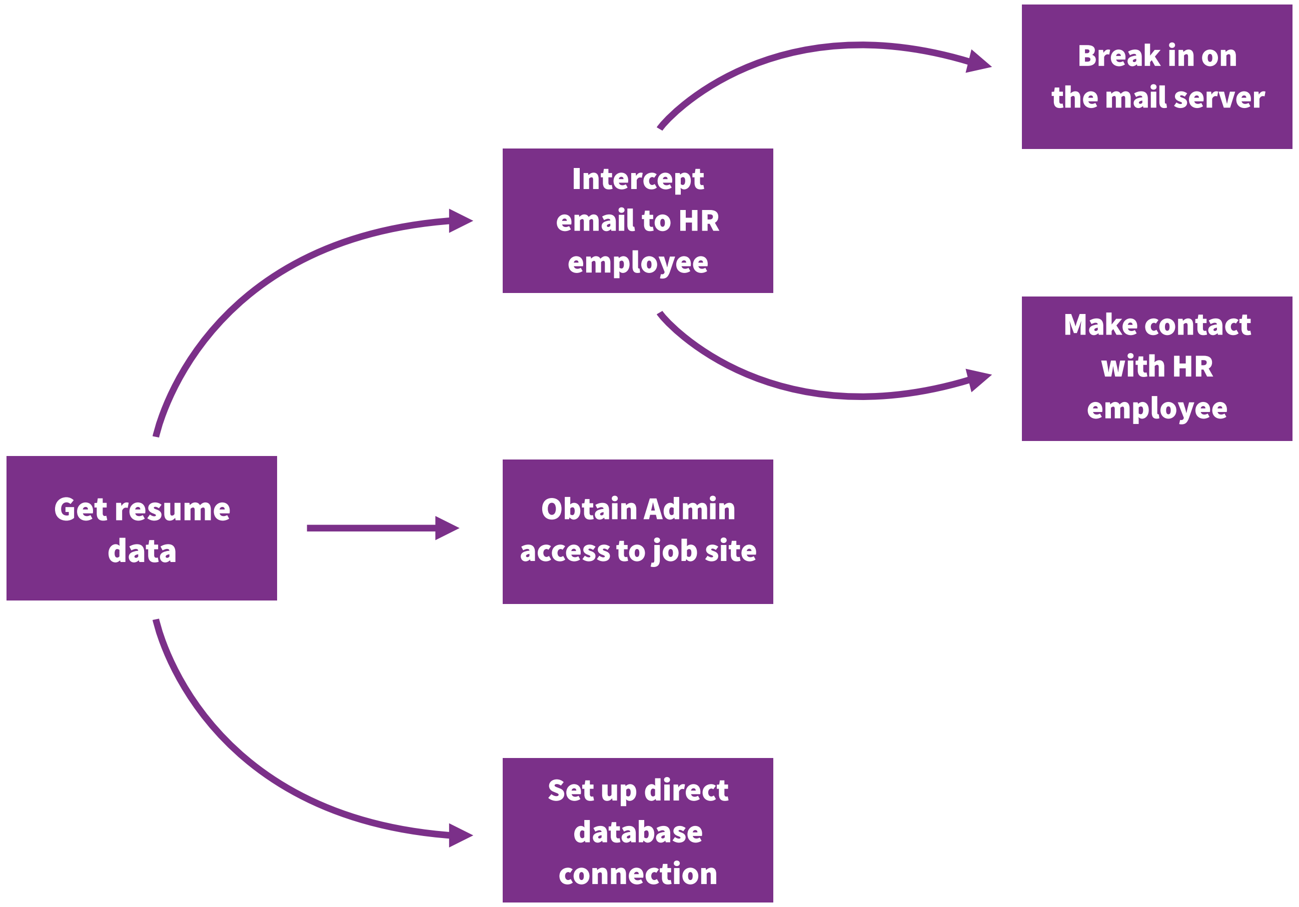
But we also look at what could happen if an incompetent or even malicious own employee were to get to work. And what could happen if an external service being used were hacked?

Attack tree

One of the ways to identify threats is by using so-called **attack trees**. It is a visual representation of the different steps a hacker can take to achieve a specific goal. An attack tree therefore starts with the goal, also known as the target, such as stealing sensitive information or gaining access to a system. We then identify the ways in which a hacker can reach the target, for example by exploiting vulnerabilities in software.

For each possibility we get more and more concrete and they are broken down into sub-steps. These sub-steps are then further divided until no further steps are possible.

This tree structure maps out possible security risks based on the job site on the previous slide.


Break in on the mail server
Intercept email to HR employee
Make contact with HR employee
Get resume data
Obtain Admin access to job site
Set up direct database connection

Step 3: Evaluate threats

Classify threats by the STRIDE model

After identifying the threats, it is important to assess them and evaluate their severity. It determines the likelihood of a threat occurring and its potential impact on the system.

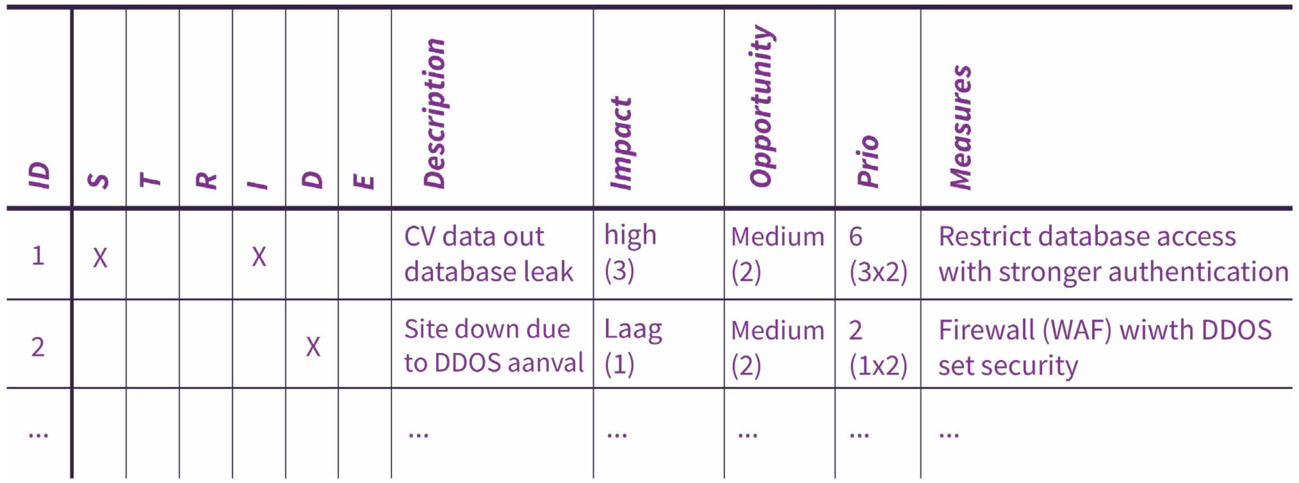
This is done by drawing up a list where threats are classified based on the STRIDE model.

STRIDE consists of six threat categories and stands for: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege. Each category describes one way in which a threat has an impact. For example, "Spoofing" means that someone is impersonating someone else and "Tampering" means that information has been altered in a harmful way.

Example: job site risks

The list is approached as is often done in risk management processes (see image). For each item on the list, we determine:

- **Which STRIDE categories apply.**
- **A description of the risk.**
- **A score indicating the size of the impact.**
- **A score that indicates how likely it is that we will be affected.**
- **A score that is derived from the above and indicates what the priority is.**
- **How we can reduce or completely prevent the risk.**



ID	S	T	R	I	D	E	Description	Impact	Opportunity	Prio	Measures
1	X			X			CV data out database leak	high (3)	Medium (2)	6 (3x2)	Restrict database access with stronger authentication
2					X		Site down due to DDOS aanval	Laag (1)	Medium (2)	2 (1x2)	Firewall (WAF) wiwth DDOS set security
...							...	...	...	...	...

02

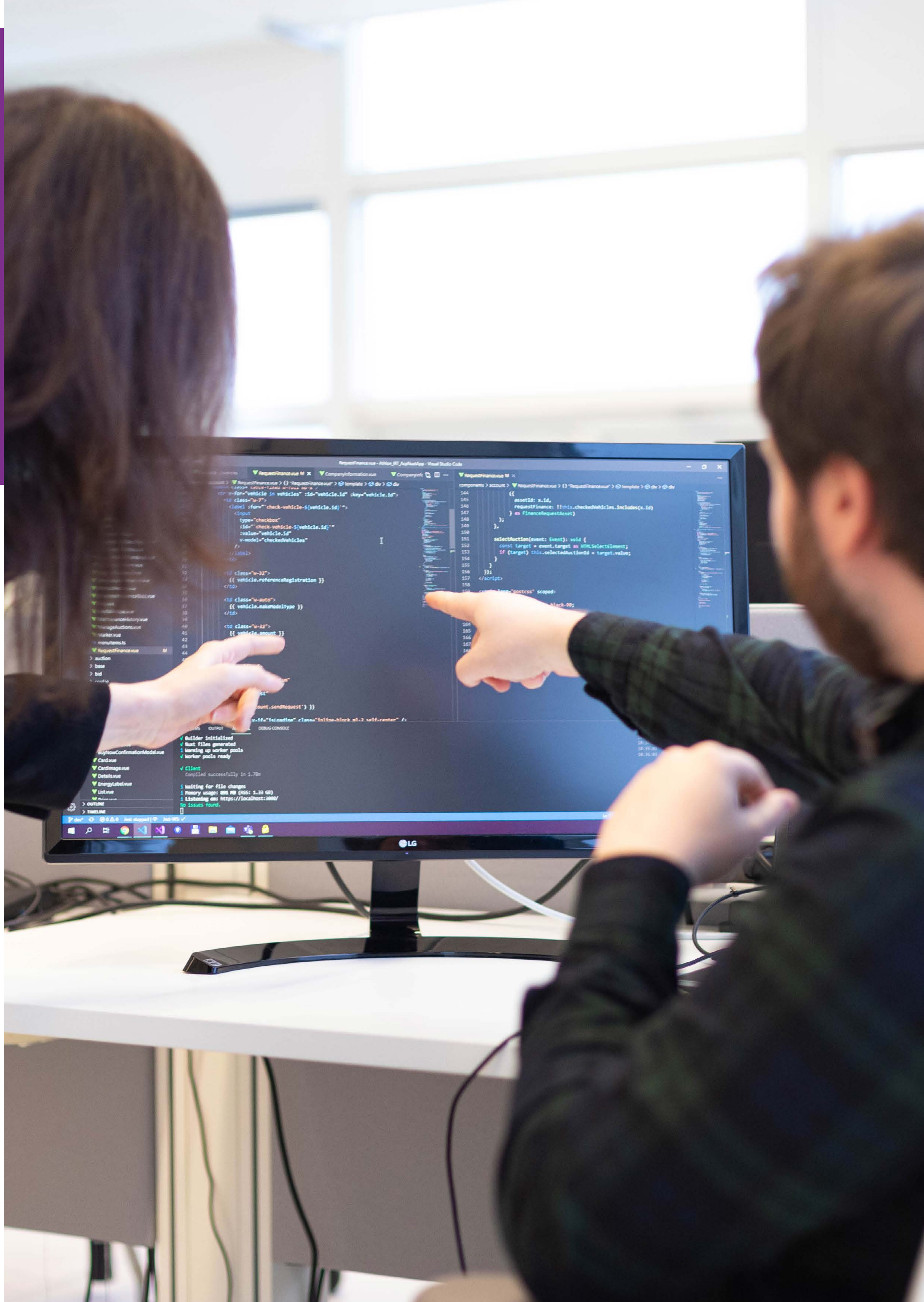
Step 4: Validate measures

Start effective activities to mitigate threats

Finally, it is important to validate the measures taken. The prepared list from step 3 is used to initiate activities to mitigate identified threats. This can be done through code reviews, penetration testing, vulnerability assessments and other techniques to test whether the measures actually work as expected.

When one of these activities is completed, the original risk can be updated in the list. It is important to check whether the changes made are effective and whether the risk is sufficiently covered. An assessment of the impact and priority is made again. If the probability and/or impact are sufficiently reduced, the risk can be removed from the list entirely.

The purpose of the validation process is to ensure that security measures are effective and to identify any shortcomings so that they can be addressed before software is released.



03

The value of applying Threat Modeling

What results do you really notice?

1. A more secure digital solution
You offer a more secure digital solution to your users. It contributes to a strong reputation as a reliable and safe organisation.

2. Obtain certifications and licenses
In many cases, threat modeling fits well with the measures that must be taken to obtain certifications and licenses. For example, it can fulfill some requirements for ISO27001.

3. Improved collaboration within teams
The joint effort to ensure security ensures a shared understanding of information security, communication between different disciplines are thus stimulated.

4. Preventing high recovery costs
Identifying and resolving security risks early prevents remediation costs later in the development process.

03

Better security of your information

Threat Modeling: a valuable part of the development process

Start improving the security of your digital solution with threat modeling! By systematically identifying and analyzing potential threats and vulnerabilities, organizations can take targeted measures to mitigate or prevent them.

When properly applied and integrated into software development and security processes, threat modeling contributes to:

1. **Safer digital solutions;**
2. **Obtain certifications and licenses;**
3. **Improved collaboration;**
4. **Avoid high repair costs.**

Would you like to be even more inspired or receive personal advice on your next digital challenge?

Contact us!

Kudos
Robin Hermanussen
(Software Architect)
Merel IJpelaar
(Online Marketer)

Get in touch with us through ***INFO@IQUALITY.NL***
or call to +31 (0)85 080 2300

iquality

Follow us @iquality