Protecto

Mission

Threat modeling is one of the main requirements for any (Agile) team. Traditional approaches provide a false sense of security, leading to products and services that attacker personas can easily exploit.

Protecto fixes the four main flaws we have in our current process, which results in a big step towards creating more secure services.

Define: Threat Modeling

Threat modeling is analyzing representations of a system to highlight concerns about security and privacy characteristics.

At the highest levels, when we threat model, we ask four key questions

- What are we working on?
- What can go wrong?
- What are we going to do about it?
- Did we do a good enough job?

Want to stop the attackers? Could you not give them something to attack?

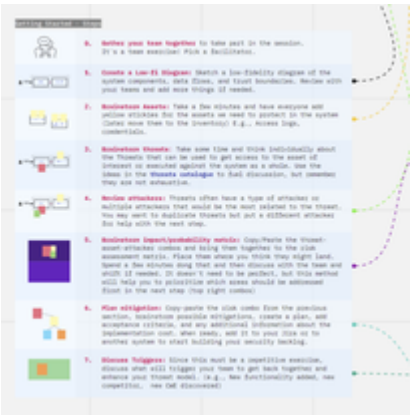
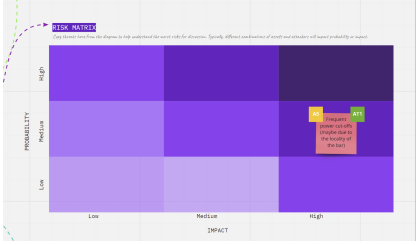
Qualities	It's a process	Who will benefit from it?
Set of tools and a workshop to start with Threat Modeling and build much more secure products! 1. A step-by-step guide to making the threat modeling together, often and with fun, for maximum efficiency. 2. A learning path that is fixing the four main flaws in our current threat modeling to build much more secure products! 3. t's a way of working through a threat model	Protecto works **across all methodologies for doing a viable Threat Model**. Our goal is to promote the following **methodology-independent** process: • Gather your team together to take part in the session • Identify objects (components) in the system under assessment by writing a low fidelity diagram at first • Recognize the flows between those objects • Create an inventory of assets of interest • Identify the attacker personas • Create a register of threats (in combination with an attacker and an asset) • Determine exploitability and risk by using a fundamental risk assessment matrix • Identify mitigations • Prepare a security roadmap based on your findings. • Identify the triggers that would require your team to enhance the model	If you want to learn why and how to do threat modeling, often using the best available tools. • If you are part of a (scrum) team but never participated in a Threat Modeling exercise. • If you are a leader who wants to explore a way to involve your team/s more in the threat modeling process so you can build better products. • If you are the only person doing the thread modeling in your group and want to explore some more ideas on involving the others.

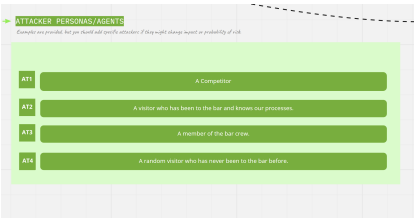
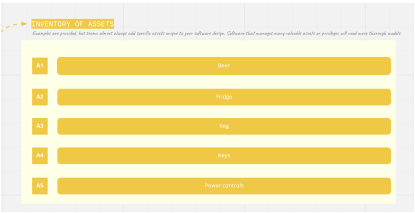
Four key problems Protecto solves

Problem	Description
Limited Exposure (Hero Threat Modeler)	Most of the time, threat modeling is made by a single user because they have the most knowledge of the system or compete with others. A dialog is a key to establishing the **common understandings** that lead to value, while documents record those understandings and enable measurement. The framework's goal is to make sure everyone **has a chance to participate in the exercise** - to raise the entire team's security posture and strengthen the product lines in general. The other benefit is that this could be adopted as an internal standard for all the team inside the company and make sure we do the threat analysis with the proper attention and using the same techniques.

Not aligned with the way we deliver software.	The current approach to Threat Modeling is close to a Waterfall model, and it's far away from the dynamicity of the modern (Agile) way of doing software. **Threat modeling must align with an organization's development practices and follow design changes in iterations that are scoped to manageable portions of the system**. The updates are made in the beginning, and no one is updating them iteratively. With Protecto, the team will be engaged regularly to repeat the exercise and focus on the most important security issues first.
The Remote is out of the picture.	The usual way of doing threat modeling is using a whiteboard. By using Protecto, you can do that from anywhere and assemble a diverse team with appropriate subject matter experts and cross-functional collaboration.
Threat Modeling as an output	Our perception I that threat modeling is an output - a file we need to create. No, threat Modeling is a process and a mindset we need to grow constantly.

Built-in concepts

Concept / Tool	Screen	Purpose
Follow the process		By following a process that works, the team can put their effort into where it will be gaining maximum efficiency.
Risk Matrix		1. Score the threat risk quickly on the probability /Impact scale and use the output to prioritize your security backlog. 2. Combine a threat with an asset and an attacker and discuss the risk. 3. The items with a higher risk go to the top of your security backlog.

Threats Catalogue		A list of the most common threats with easy-to-understand use-cases and a micro-flow. The library will cover just one use-case per threat for both online and offline infrastructure. • STRIDE (by Microsoft) • Privacy (by F-Secure) • Ethical Design Also, you are free to add your own content - Security Patterns, Kill Chains, the most common K8s attacks, or whatever you think is useful.
Risk mitigation Pane		When you identify your risks, use the pane to identify all possible mitigations and create a plan for implementing them.
Attacker Personas		A basic set of attacker personas + a way on how to visualize them.
Inventory of Assets		A basic set of the assets to protect, which you can use t build your own inventory. In the end, knowing what you need to protect is a very crucial part.
Triggers		What do you need to do and when to repeat the Threat Modeling exercise.

Workshop/Learning Path

Component	Goals	Time	Key Takeaways
Component Pilsen	Every workshop starts with a basic exercise on doing threat modeling step by step with a facilitator on protecting a **beer tap infrastructure**: • Map your offline knowledge and way of thinking to the threat modeling practices. • Get the know the tools and on working remotely with others. • Work as a team to protect the infrastructure and create a basic backlog of items to be solved. • Have fun!	35 min	The knowledge inside the workshop helps the team to remember the 3 main pieces of advice that will make our products a bit more secure: • Build a habit of doing threat modeling often and add improvements or spikes in your backlog constantly. • In 1976, a British statistician named George Box wrote the famous line, “All models are wrong, some are useful.” Explore what is currently going on in the security world. Everything is changing fast, and we need to adapt. Maybe the threat model you finished 2 months ago is not relevant anymore. • Work as a team. We cannot afford to ignore great ideas coming from a person who recently joined the team or was working on different types of stories before.
Brake/ Coffee Refill		5 min	
Component SimpleApp.io	Threat Model a simple web application: • Use the learnings from the previous component and map it to the online world • Start using the **threat catalog** individually and as a team • Focus on web-related threats. • Explore privacy and ethical design flaws as well • Build knowledge of how to use the framework for your own product • Still, have fun!	25 min	Focusing on the 4 key problems and see how they are fixed with Protecto.

Licensing