CASE STUDY

A cybersecurity company chooses IriusRisk to meet its security by design practices, and introduces self-sufficient security across teams.

Security by design, and by default

The company is a cybersecurity company specializing in developer-first security tooling, with a presence in Europe and America.

The team in charge of choosing and rolling out a threat modeling program at The company, had done so before, at another company, using IriusRisk. When the chance arose to further distill The company's security best practices, The Director of Product Security knew IriusRisk would deliver on their two main goals of:

1. Ensure all company products are secure by design
2. Enable the engineering teams to be self-sufficient for their own security consideration

> ***We needed to get security feedback and verification as soon as possible, but also shift our security left as much as we could into the design phase - for both new and existing products. We knew threat modeling would enable us to do that.***
>
> Director of Product Security

THE SITUATION

Turning manual threat modeling into a repeatable process, for timely and reliable security feedback

The security teams were already threat modeling, but this was a manual approach. Of course, the nature of doing it manually is less consistent due to relying on a security engineer to do the threat model and identifying threats themself. The company identified the need to further streamline these existing efforts, and introduce a repeatable and scalable framework that everyone could use.

Receiving feedback as early on in the SDLC as possible, is a huge benefit to take action at a point where the cost is lowest. The Product Security team recognized that this activity could drive further value if this could be enhanced further with an enterprise threat modeling tool.

> ***Threat modeling is one of the best security practices you can do as it allows you to go wide and deep for a full view of assets in scope for a product or application. Having a full picture enables you to identify the relevant threats and security controls to effectively implement and mitigate them.***
>
> Director of Product Security

THE SOLUTION AND RESULTS

Repeatable, scalable threat modeling, with crucial customizations and integrations for automated validation state testing

The Product Security Team saw three key challenges with rolling out threat modeling successfully. And knew with IriusRisk they would be able to effectively overcome these:

1. Accurate representation of the system you are threat modeling
2. Getting the quality of threat libraries
3. Validating the implementation state - of the required countermeasures

Accurate system representation

With IriusRisk, The company is able to use the diagramming function to represent things that don't exist yet, as well as the architecture that is already in place. With customization options, the team was able to get a full view of their risk architecture to identify the true security requirements. Even if they were simply threat modeling some new functionality over a whole brand new application.

> ***"It's been the difference between spending a few hours instead of a few days to create the threat models.***
>
> Director of Product Security

High-quality threat libraries

The company chose to add their own libraries into the IriusRisk solution, to give even better context to their unique threats and countermeasures. This was to further aid their second business goal of providing a repeatable self-service security process for all engineers to be able to use.

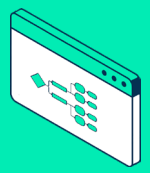
> ***We wanted to manage threat libraries the same way as code under version control, in DSL as a Git repository that we import into IriusRisk. This worked well for us to ensure consistency, scalability, accuracy, and quality.***
>
> Director of Product Security

Validating the implementation state

The Product Security Team added custom functionality to IriusRisk to achieve this, to allow them to validate and verify the security activities, after they have been implemented as a security control.

> ***The IriusRisk API has been useful to hook in automated testing for validation state testing, and to configure our own integrations and formats to enable us to move faster. It also lowers the barrier to entry when the wider teams are using the tool. All they need to do is populate Jira stories into their backlog for countermeasures that our automated testing has determined are missing, working top down based off the inherited prioritization..***
>
> Director of Product Security

Why IriusRisk Threat Modeling?



Familiarity, as used the tool before and trusted its user experience and threat outputs

Flexibility of the API - to implement their own functionality and integrate with their existing tools

Once established in the SDLC they knew they would achieve stability, reliability and better performance

Support for SSO and RBAC - fitting with the company's Identity and Access Management (IAM) requirements

The ability to meet the goals of security by design, and a repeatable self-service security process

Customization through threat libraries - to give a true reflection of their risk architecture

> *We knew what we needed to do and that we could achieve it within the time required if we chose IriusRisk. The flexibility of the API and ability to customize as we needed, made IriusRisk the clear winner.*
>
> Director of Product Security