



« Dutch Bank builds a self-service threat modeling process for DevOps and scales secure design across its organization

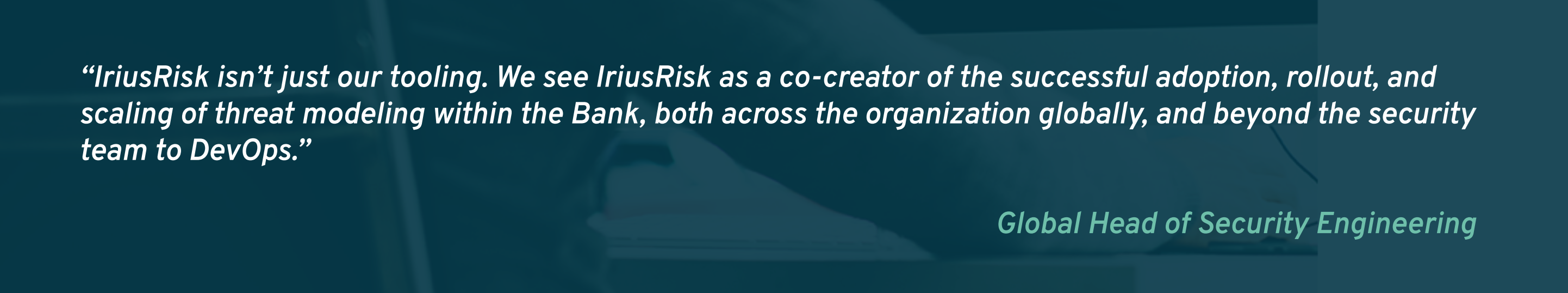
Case Study

IriusRisk«

A double chevron icon (»») is located to the left of the section header. The chevrons are dark blue and point to the left.

## Introduction

Threat modeling took center stage in planning conversations as their security engineering team embarked on the ultimate effort to 'start left' in security - by implementing a self-service secure design process for developers.

A dark blue rectangular box with rounded corners contains a quote. The text is white and italicized.

*“IriusRisk isn’t just our tooling. We see IriusRisk as a co-creator of the successful adoption, rollout, and scaling of threat modeling within the Bank, both across the organization globally, and beyond the security team to DevOps.”*

*Global Head of Security Engineering*

## « Key challenges

### Inability to scale across hundreds of teams due to a manual threat modeling approach

- Lack of a self-service threat modeling solution for DevOps
- Small number of teams using threat modeling
- Lack of centralization for security requirements and data

Prior to its digital transformation project, the Bank had already implemented ad-hoc, manual threat modeling within its software development lifecycle. It originally had no internal capability but having learned and understood the business value of threat modeling, it inspired people, and was the key activity to shift security left.

*“We weren’t looking for a solution, but when we were introduced to IriusRisk, their platform immediately validated the problems we were up against. However, getting security on the engineering agenda isn’t always straight-forward, nor is it simple to propose a new solution that will add to an already large and complex toolstack.”*

*Global Head of Security Engineering*

## « Solution

### Threat modeling becomes a mandatory requirement for development. Embedded into existing workflows

The Security Engineering team worked with IriusRisk to demonstrate value up and across the organization by highlighting automated threat modeling as the crux to the success of their migration and to cement IriusRisk as the vital tooling that enabled conversation between DevOps engineers and security teams.

*“We were using STRIDE as a methodology and drawing architecture in draw.io, managing data in spreadsheets, before uploading documentation of models to our collaboration platforms. This approach was very dependent on our security teams, but for the migration to be successful, we needed DevOps teams to threat model for themselves, which raised questions: how would we even go about integrating threat modeling into the existing DevOps way of working?”*

*Global Head of Security Engineering*

## « Results

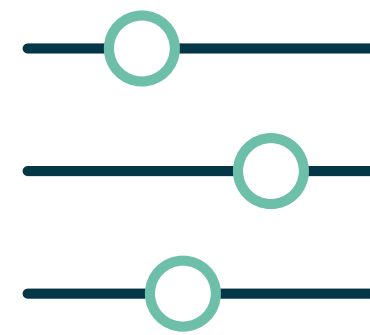
### Seamlessly integrated into DevOps and Security workflows, issue tracking, and project management

Threat modeling is now a mandatory activity. This is because the Bank has been able to demonstrate value from implementing IriusRisk. The central security team is now able to have visibility over all of the threat modeling activity across these teams. It took the Bank 1.5 years to achieve 100 teams threat modeling manually. With IriusRisk's automated threat modeling platform, the Bank has been able to add another 100 teams in just 7 months.

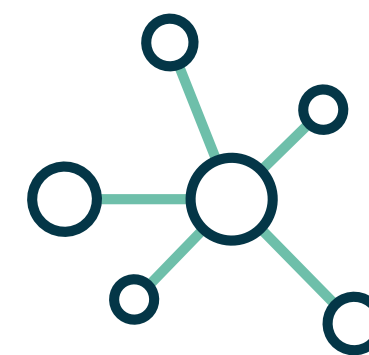
*“The largest achievement? For me, it’s that IriusRisk enables us to centralize our security requirements. Previously, we exchanged requirements through our GRC platform which was never enough.”*

*Global Head of Security Engineering*

## Key reasons for using IriusRisk



Highly configurable and centralized creation, iteration and storage of threat models



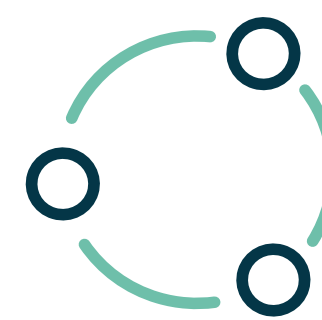
Consistent repeatable results and centralized policy definition



Reduced duplication of efforts since moving from manual to automated



Auto-generated reporting and fully auditable record of threat model creation



Seamlessly integrated into DevOps, Security workflows, issue tracking and project management



Shared threat models and security standards content libraries - centrally and instantly accessible to all

Automate Threat Modeling to fit your existing SDLC.  
Secure design right from the start.

[Request a demo](#)

IriusRisk