IriusRisk

« CASE STUDY

ABN AMRO SCALES SECURE DESIGN TO 200+ TEAMS WITH IRIUSRISK TO START LEFT WITH SECURITY

ABN·AMRO

Banking / Financial Services
Enterprise, 64000 Employees

Global, NL Headquarters

Irfaan Santoe, Global Head of Security Engineering

ABN Amro reached out to IriusRisk as they embarked on a major digital transformation program - moving from their private data centers to the cloud - which would affect 500+ teams across the organization. Threat modeling took centre 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.

IriusRisk: A Co-Creator of ABN Amro's Threat Modeling Capability

« SELF-SERVICE THREAT MODELING FOR DEVOPS

« 400+ ENGINEERS ACROSS 200 TEAMS USING IRIUSRISK

« CENTRALIZATION OF SECURITY REQUIREMENTS AND DATA

"IriusRisk isn't just our tooling. We see IriusRisk as a co-creator of the successful adoption, rollout, and scaling of threat modeling within ABN Amro, both across the organization globally, and beyond the security team to DevOps. This partnership doesn't stop there; we look forward to exploring the possibilities of enhanced reporting and integration with the other existing tooling in our value chain. Their dedicated people have a unique mindset to help make their clients successful, and without IriusRisk, our digital transformation to the cloud would not have been efficient.
We are now realizing our vision to start left with security."

~ Irfaan Santoe, Global Head of Security Engineering - **ABN Amro**

Realizing the value of threat modeling

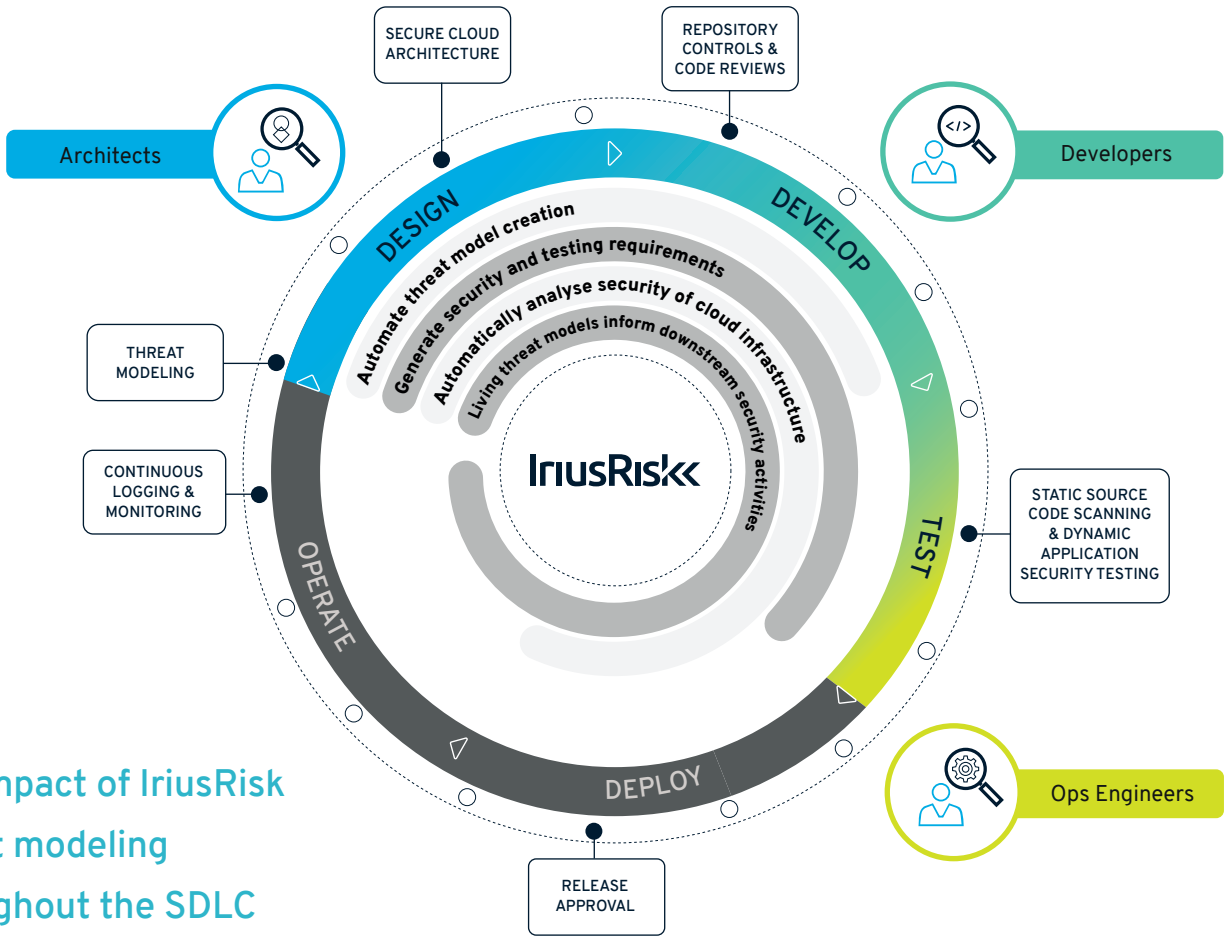
Prior to its digital transformation project, ABN Amro had already implemented ad-hoc, manual threat modeling within its software development lifecycle. It originally had no internal capability but having learned and understood the business value of threat modeling, it inspired people, and was the key activity to shift security left . A year on, they had successfully implemented manual threat modeling and achieved the first step of capability building.

Although successful, the bank was to undergo a large-scale migration from private data centers to the cloud - one affecting 500 teams - which prompted questions around how well their approach would scale. “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?” It led Irfaan Santoe, Head of Security Engineering, to wonder if there was a more agile and scalable solution.

The limitations of a manual approach: how can we threat model more effectively?

"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. 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.

The impact of IriusRisk threat modeling throughout the SDLC



« The results: moving to collaborative, scalable threat modeling

ABN Amro was supported by a cross-functional team from IriusRisk - spanning DevOps, Security, Senior Management, and Customer Success. “Within only 7 months’ of deployment we were able to not only onboard the existing 100 teams already threat modeling, but scale to an additional 100 teams. To give this context, it took us 1.5 years to build our original capability, so we were able to scale a lot faster with IriusRisk”, notes Irfaan.

“The largest achievement? For me, it’s that IriusRisk enables us to centralise our security requirements. Previously, we exchanged requirements through our GRC platform which was never enough. Some stakeholders questioned the difference between our GRC and IriusRisk. Simply put, the GRC demonstrates compliance to regulators - it’s high-level, or policy-level by nature, and shows you’re using some sort of encryption, facilitating some form of access management etc. IriusRisk goes far beyond that. It’s granular: it tells the engineer that by changing this part of an application, these are the threats you need to address and this is how to address it - something the GRC was never designed, to do. It’s a valuable toolkit for teams to use before, during, and after a build. In fact, IriusRisk has made our GRC platform more effective as both systems complement eachother.”

Time to create
a threat model from scratch

Increased the number of teams threat modeling from 100 to 200 using IriusRisk

Time taken to achieve 100 teams threat modeling manually: **1.5 years**

Time taken to achieve 100 teams using IriusRisk: **7 months**

Before: Manual threat modeling	After: Threat modeling with IriusRisk
Ad-hoc threat modeling of products. Optional activity, not a formal requirement	Threat modeling becomes a mandatory requirement for development. Embedded into existing workflows
Complex process using multiple tools. No standardisation of threat models	Highly configurable and centralised creation, iteration, and storage of threat models. Consistent, repeatable results and centralised policy definition
Time-intensive upload, edit, and reporting on progress, results and risk	Auto-generated reporting and fully auditable record of threat model creation and iteration. Reduction in duplication of efforts
Missing data due to inability to integrate with other tooling	Seamlessly integrated into DevOps and Security workflows, issue tracking, and project management
Duplication of process, efforts, and models - costing time and resource	Shared threat models and security standards content libraries - centrally and instantly accessible to all

« The Future of Threat Modeling at ABN Amro

"Never would I have imagined a scenario where developers and engineers described threat modeling as 'fun' - let alone an activity which has been very much welcomed into our workflows and processes. The future is bright for threat modeling within ABN Amro. We are not just shifting left, but starting left, and have demonstrated that this can be done within an organization like ours thanks to our co-creators, IriusRisk. IriusRisk has been a crucial element in enabling DevOps to independently gather security requirements during design, generating standardized, consistent results across all teams. I highly recommend both the platform and the people at IriusRisk - and look forward to our next task which is to further scale threat modeling across our enterprise."

- Irfaan Santoe, ABN Amro

"There are three things that have been consistent throughout ABN Amro's journey which have helped them succeed: They have an innovative team who are always looking for opportunities to push boundaries. They have incredible drive and are dedicated to making an impact with their threat modeling activities. They've actively driven change which has meant that they're now able to centralize their global security requirements using IriusRisk and it's been a pleasure to experience this change with them."

- Jonny Tennyson, Head of Customer Success, IriusRisk

To find out more about ABN Amro's threat modeling journey,
visit our website and watch an exclusive webinar featuring Irfaan Santoe,
the Threat Modeling Manifesto's Irene Michlin, and Jonny Tennyson, in
'Starting Left: How ABN Amro scaled Security to Development'

www.iriusrisk.com/abn-amro-threat-modeling

info@iriusrisk.com
www.iriusrisk.com