Global Top 10 Bank Standardizes and Scales Threat Modeling with IriusRisk

Case Study

IriusRisk

« Introduction

The objective of the global Bank was to migrate the threat modeling activity from security architects, in the central risk team, to the solution architects in the engineering teams. As a Global Systemically Important Bank (G-SIB) with over 200,000 employees and presence across the globe, the Bank needed an automated and scalable solution.

"IriusRisk has helped us achieve a level of standardization and consistency that means we can undertake threat modeling at scale across our solutions. The customer support from IriusRisk to enhance the platform and customize it to our own company processes has been outstanding. We are now exploring how we can integrate threat modeling with our other security practices to make the IriusRisk platform our consolidated view of application security."

Global Head of Cyber Controls Assessment

« Key challenges

Bank looks to threat model at scale

The Bank's Security Architects were already performing threat modeling manually but they wanted to increase the repeatability, consistency, and breadth of these models.

The Bank had identified that some components and risk patterns for its applications were being missed by this manual approach and that there were gaps in what was covered, including user journey and business logic threats.

"It was our objective to increase the number of threat modeling engagements throughout our solution portfolio but before IriusRisk we were struggling to convince solution architects to incorporate threat modeling into their design process. I recognized the need for a solution to standardize and bring in automation in order to engage solution architects and roll out threat modeling at scale,"

Global Head of Cyber Controls Assurance at the Bank

« **Solution**

Utilizing in-built intelligence and customization

The Bank evaluated IriusRisk alongside other threat modeling tools as part of a competitive procurement process. IriusRisk's SaaS approach meant that the solution integrated well with the bank's architecture and it was impressed with the platform's API and customizable content and rules, which immediately enabled the automation of threat modeling processes, making it possible to undertake more threat models at scale.
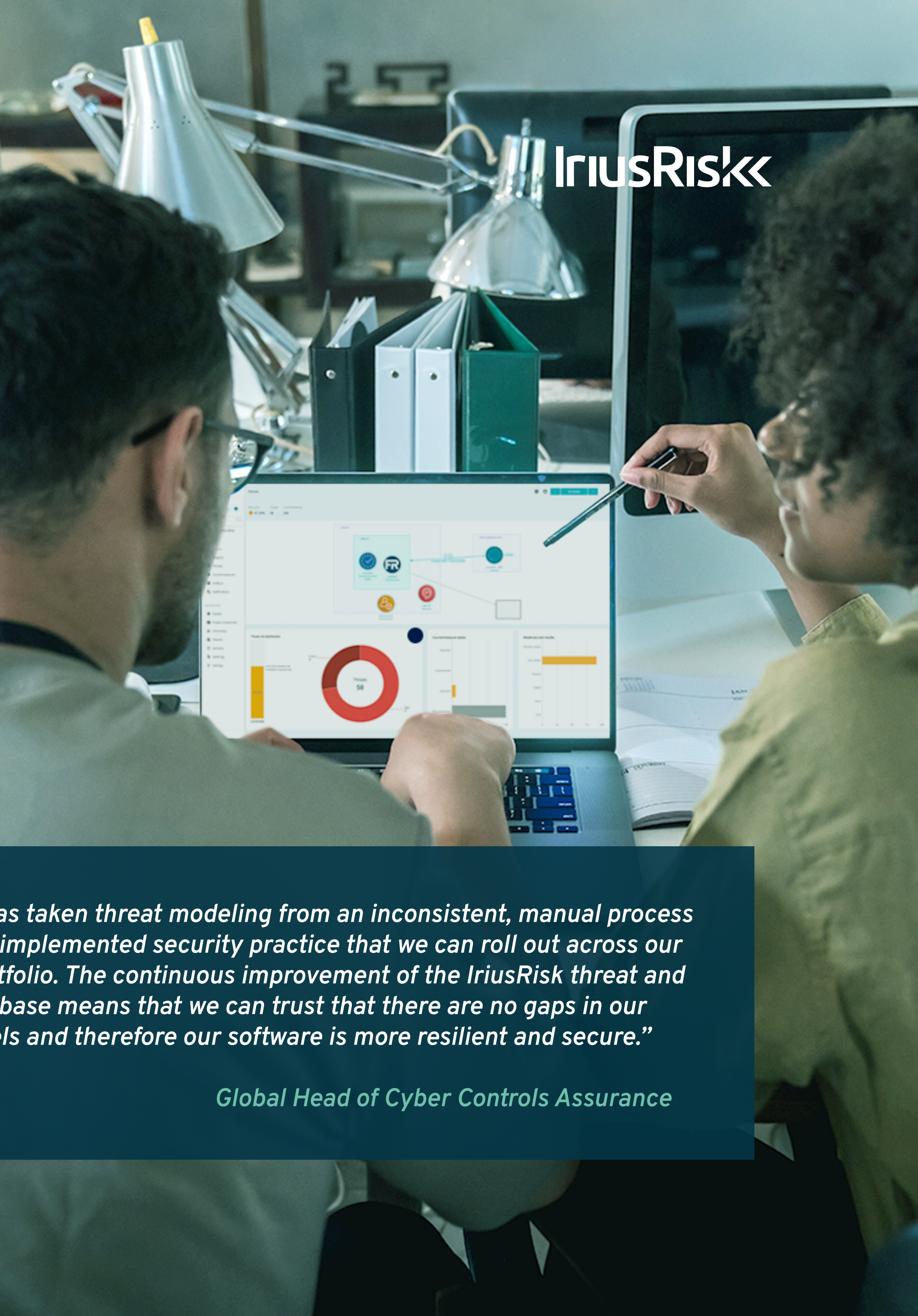
One of the stand-out features that led to the Bank choosing IriusRisk was its flexible framework which enabled teams to make use of both the comprehensive library of threat models built-in to the IriusRisk platform, and augment these with their own organization-specific threats, countermeasures and architectural security rules. This meant that the bank could customize threat models to its own solutions so that engineers implement security controls approved by the Bank and by the central security team.

« Results

New level of maturity as solution architects buy into threat modeling

With IriusRisk, the Bank has managed to make its threat modeling process more efficient, comprehensive and reliable. It has increased the number of threat models it runs across its product portfolio and removed the bottleneck of the central security team, by putting threat modeling in the hands of engineering. This is thanks to automation relieving the manual burden on security professionals and enabling the solution architects to take on a more active security role. IriusRisk's comprehensive security standards and compliance libraries have also helped to increase the consistency of threat models and ensured that key risk patterns are covered during the threat modeling process.

As a consequence, the Bank has been able to get solution architects to buy into the threat modeling process, inputting architecture details into the IriusRisk platform directly. The Bank is now looking to increase the use of "self-service" threat models by solution architects to put security into the hands of the engineering teams. With a base level of consistency in threat modeling, the bank is also exploring how it can integrate the IriusRisk platform with penetration testing, automated scanning and the configuration compliance service to create a holistic view of the security posture of its applications.

"IriusRisk has taken threat modeling from an inconsistent, manual process to an easily implemented security practice that we can roll out across our product portfolio. The continuous improvement of the IriusRisk threat and control database means that we can trust that there are no gaps in our threat models and therefore our software is more resilient and secure."

Global Head of Cyber Controls Assurance

⟪ Key reasons for using IriusRisk
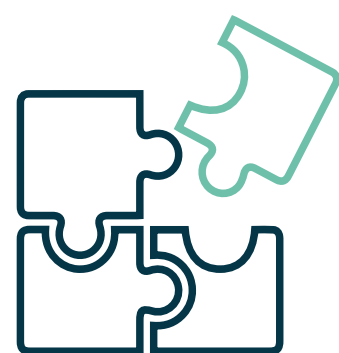
Ability to create and customize its own security content based upon their own frameworks

IriusRisk's open approach combined with a powerful API allows connectivity with the Bank's vulnerability management software and other tools
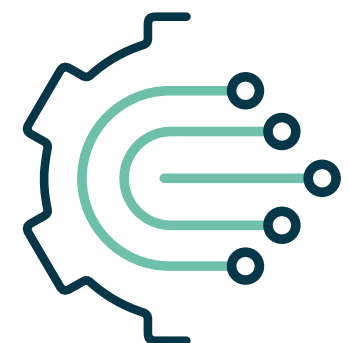
Shift left within the Bank with a focus to ensure all critical applications are threat modeled
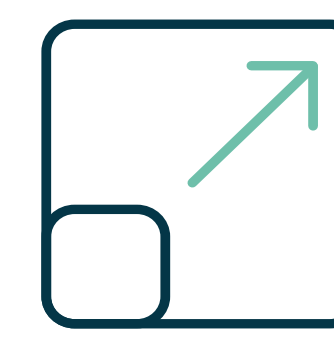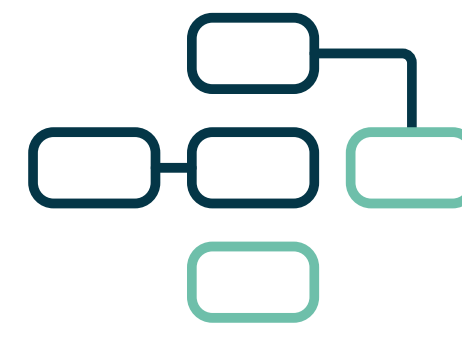
Scalability and performance with over 5,000 threat models
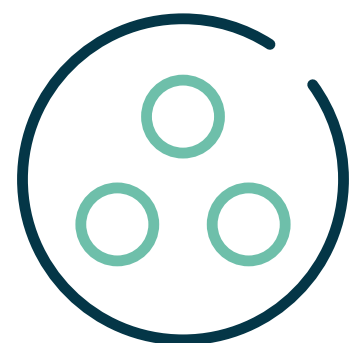
Global collaboration with teams with control over roles and permissions as well as separation of duty

Rules engine allows banks controls to be incorporated within the tool to replicate its security logic and workflows

Threat Model Templates have allowed for standardization and ease of adoption across the Bank

IriusRisk's Global Support team is available to meet the Bank's growing requirements

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

Request a demo

IriusRisk