Threat Modeling from the ground up

Hear how a multinational professional services brand began it’s threat modeling journey with IriusRisk.

Case Study

IriusRisk

IriusRisk

Company Background

Starting the threat modeling Journey

The company is a multinational professional services brand.

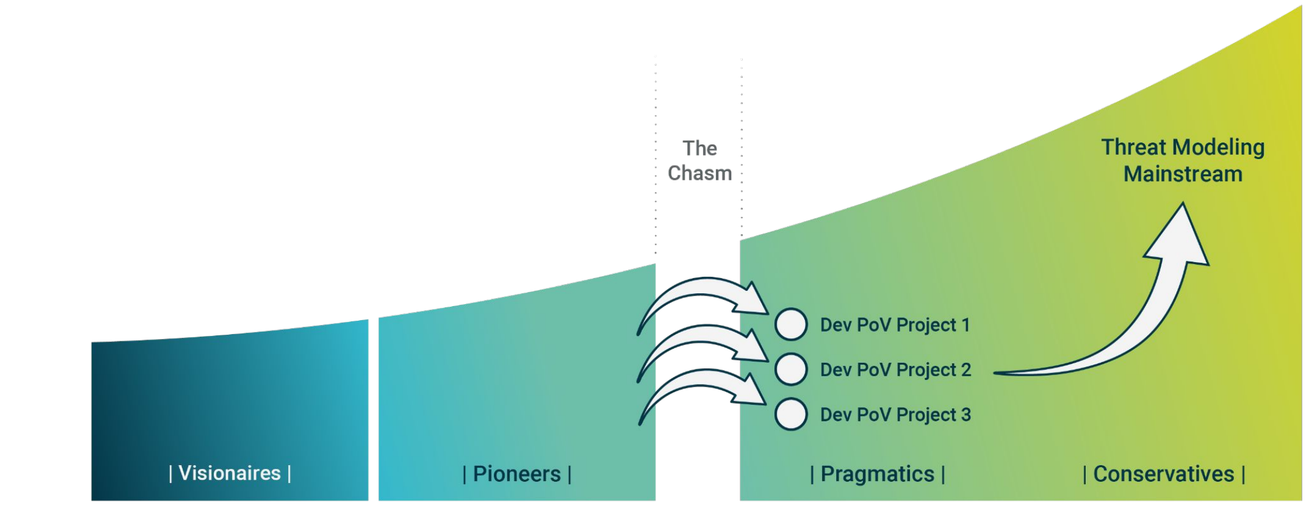
The company was not threat modeling at all before rolling out IriusRisk. However, they saw the value that threat modeling could bring, and decided to add this proactive security measure into their processes.

Key challenges

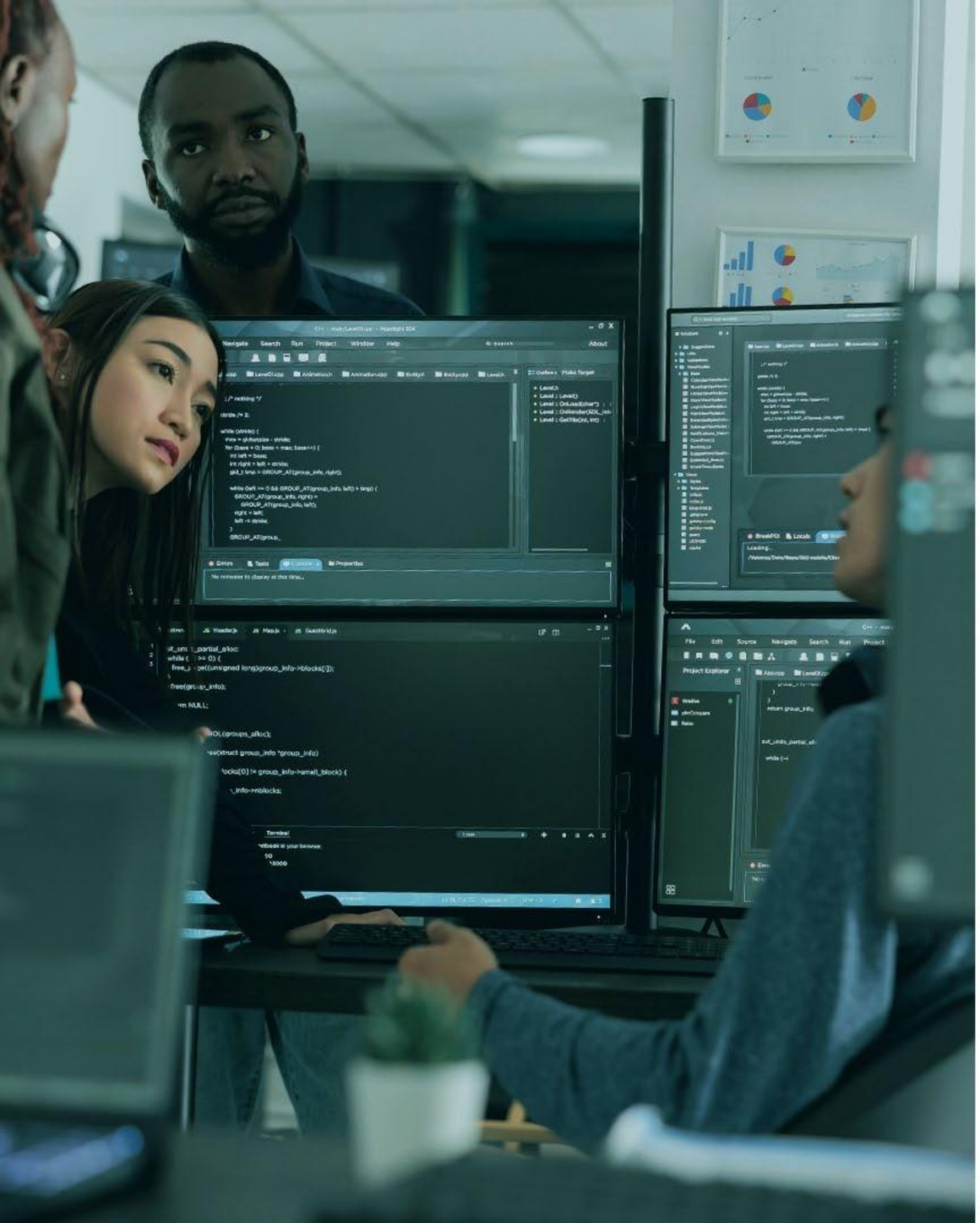
Understanding where to begin

The company was initially very focused on threat intelligence and threat analysis which then led them to look more closely at proactive security and threat modeling.

Using IriusRisk's guide to Rolling out a Threat Modeling Program, the company established that their current status was within The Chasm. This led to the establishment of a security champions program to help with the rollout, and adoption of the threat modeling process using IriusRisk as their automated tool.



	Phase I	Phase II	Phase III	Phase IV
What	**Deliver value first**	**Recruit your virtual team of Security Champions**	**Start small, gain credibility**	**Gather evidence and plan**
Who	**Security Team**	**Security Team & Security Champions**	**Developers, Security Champions, Security Team**	**Developers, Architects, Compliance**
How	• Define roles, BU's, permissions • Define integrations • Select/Define Standards and Compliance • Define Customized Risk Patterns and Components • Define Workflows • Define value, principles & KPIs • Set Risk, Dashboard & Reports • Session with Stakeholders	• Define Issue Tracker level (component, threats) integrations • Select Security Champions • Check former & architect formats • Define customized components • Select Dev Teams for PoV • Refine goals • Dashboard: Set a Tool for Governance (Analytics module) • Session with Stakeholders	• Track Security Champion progress • Refine integrations • Refine Standards • Refine customized components • Refine Workflows • Set a Communication Plan (Notifications) • Refine goals, indicators • Refine Dashboard metrics • Session with Stakeholders (internal PoV results)	• Refine the Communication Plan • Update Security Champions • Refine goals, indicators • Adopt new standards • Refine Dashboard metrics • Regular sessions with stakeholders



IriusRisk

Solution

Supporting the a Security Champions program

IriusRisk's customer success team began and continues to help the company to drive its security champions program which includes 20 teams.

They have regular check-in calls which support the company's team with the user adoption of the program, as well as using written resources and community advice to help them continue on the right path. They are now at a stage where they are trying to gain critical buy-in from higher management and wider teams.

They achieved this through an ROI study detailing the time saved by firstly threat modeling in general and then the added saving by using an automated tool such as IriusRisk.

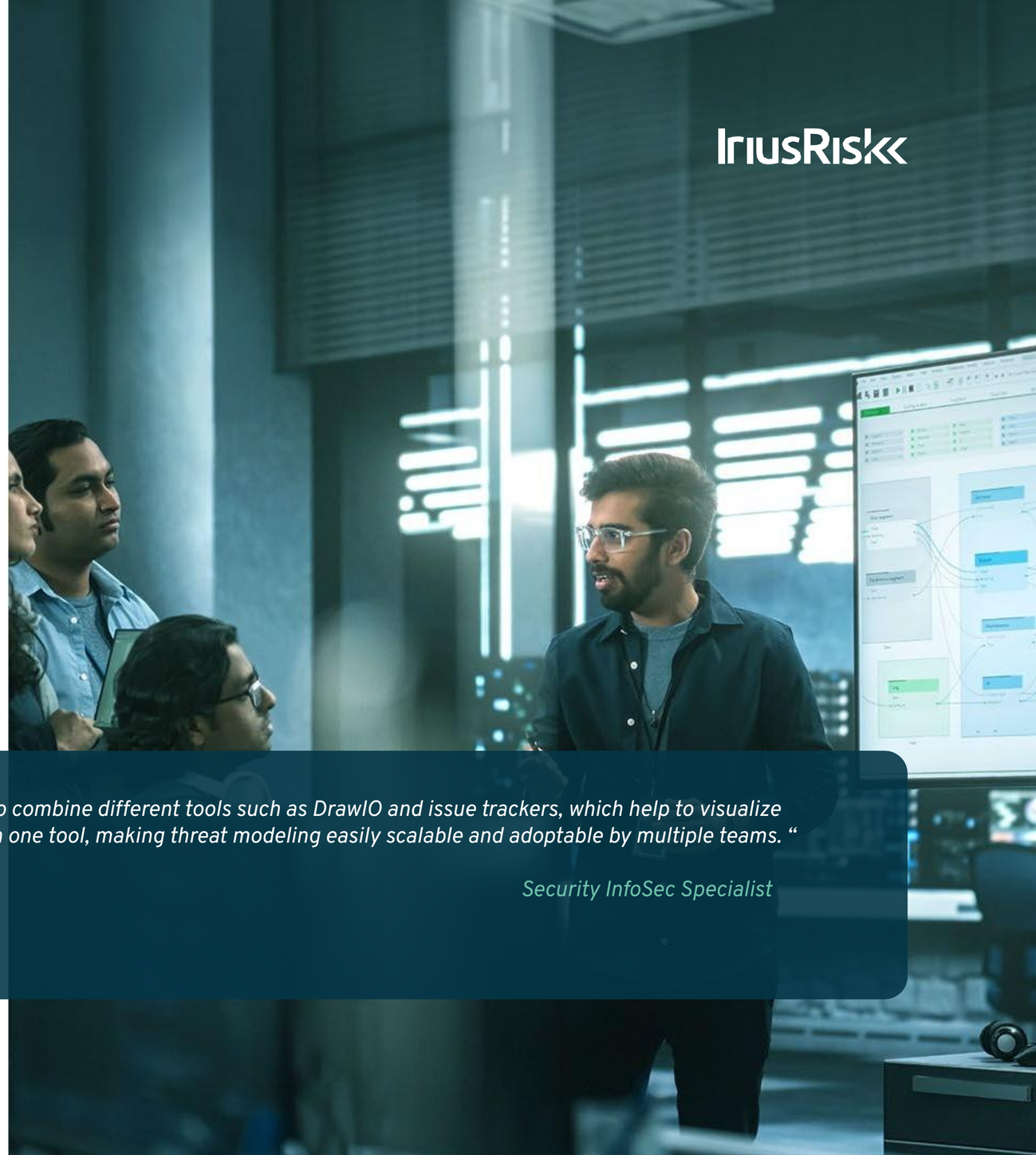
Results

Increased Collaboration Across Teams

With manual threat modeling you have to think of all the risks, IriusRisk provides that information quickly and easily saving time and effort.

On the flip side of this, the long list of threats can be seen as intimidating to new users which is why a rollout process and support from the Customer Success team can be key to initial buy-in and success. This additional support gives users the chance to better understand how these threats can be prioritized depending on the required outcome.

The speed at which this can be achieved whilst still being collaborative and fitting into existing workflows is invaluable.

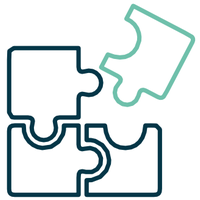


“IriusRisk also helps to combine different tools such as DrawIO and issue trackers, which help to visualize and manage threats in one tool, making threat modeling easily scalable and adoptable by multiple teams. “

Security InfoSec Specialist

IriusRisk

Key reasons for using IriusRisk



Integration

Links into existing developer workflows and existing tools

Open API

It allows risk management processes to be improved, with a holistic view of the entire risk estate

Ease of use

Speeds up adoption for non-security professionals

Simple transition

Replaces draw.io, OWASP Threat Dragon and other free or manual tools

Scalability

Seamlessly scales threat modeling efforts across teams and in line with product development

Repeatability

Results in self sufficiency and time-saving across teams, but especially for Developers

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

Request a demo

IriusRisk