

A man in a light blue sweater and glasses stands in a server room, holding a folder and gesturing towards server racks. The room is dimly lit with blue and green tones. The background features rows of server racks and a large, abstract geometric graphic on the right side of the image.

« Axway Globalizes Threat Modeling within its Leading Data Integration and Digital Experience Company.

Case Study

IriusRisk«



« Introduction

Axway is a global enterprise with 6 R&D locations across North America and Europe. In an ideal world, security teams could sit down in a conference room with engineering and product stakeholders to conduct a live threat modeling session on a whiteboard.

However, even pre-pandemic, bringing teams physically together at each R&D site, multiple times per year for threat modeling was cost prohibitive.

« Key challenges

Over 300 engineers and almost 100 security specialists meant difficulty in bringing teams together to collaborate and threat model

Axway has over 100 enterprise products and cloud services in their catalog and each engineering group and product may have different release cadences. Scheduling time with a software security expert to perform a threat model would cause delays and reduce engineering velocity due to an overwhelming number of requests and difficulty in coordinating calendars.


A dark blue double chevron icon pointing to the left, positioned to the left of the section header.

Solution

Collaborative and scalable threat modeling within their secure software development lifecycle

IriusRisk makes online, visual threat modeling with distributed teams a possibility and allows Axway to collaborate in real-time and asynchronously with its globally distributed engineering teams.

Through the implementation and use of IriusRisk, automated threat modeling is now integrated into Axway's Secure Software Development Lifecycle (SSDLC), Security Reviews, and CI/CD processes. Teams can conduct a threat model as needed for their products, and readily see the list of issues. This allows engineering teams and product owners to catch potential security risks early in the development cycle and address issues before the products are released.

A background image showing a diverse group of software developers in a modern office setting. They are gathered around computer workstations, looking at screens and discussing. The lighting is bright, suggesting a window view of a city.

“Although Threat Modeling isn’t a new process to Axway, bringing together international teams of people to carry out manual threat modeling was never an easy task. With IriusRisk, we’ve been able to carry on our threat modeling practices across our existing products with much greater ease - to the point where it is now a systematic process which alleviates any Security Champion bottlenecks that we used to have.”

Sandy Blackwell, Global Director of Software Security

« Results

Threat modeling now globally available to all teams and embedded into workflows

Axway now leverages IriusRisk to democratize and standardize the framework for threat modeling to ensure that each engineering team has proper training and tools to conduct their own threat model, on their schedule, and consult with the Software Security Group (SSG) as needed to address risks.

As their development organization and security procedures have evolved, so has the IriusRisk tool. Axway SSG has been pushing the envelope in scaling a world-class DevSecOps program and the IriusRisk Product Management and Customer Success teams have been great partners in Axway's journey.

“The integration between IriusRisk and Jira has been invaluable to our workflow. Speeding up our processes and removing the need to create lengthy documentation. Jira tickets are created seamlessly for any controls which need to be put in place making the process flow smoothly for all teams.”

Chris Ramirez, Principal Software Security Engineer

« Key reasons for using IriusRisk

Before

Manual threat modeling



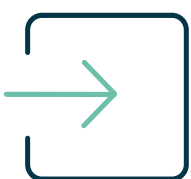
Bringing several multinational teams together is ideal, but not a scalable activity, resulting in only key products being threat modeled



Intermittent and time-intensive upload, edit, and reporting on progress, results and risk



Software Security Group (SSG) consisted of 3 people with threat modeling experience



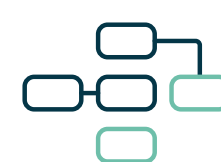
Inconsistent inputs into Continuous Integration/Continuous Delivery (CI/CD) operations



Duplication of process, efforts, and models, costing time and resources

After

Threat modeling with IriusRisk



Threat modeling becomes available to all product teams and is embedded into existing workflows



Initial threat modeling activity is now distributed to all SPOCs across the organization



Fully centralized solution allowing reporting and fully auditable record of threat model creation and iteration



Seamlessly integrated into DevOps and 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