

CASE STUDY

A global financial leader scales to 4,500 threat models with IriusRisk



Company Background

As one of the world's largest banking and financial services organizations, this financial leader is a pioneer in cybersecurity, requiring all critical applications to have a threat model as part of a top-down security initiative. Having adopted IriusRisk in 2020, the company has scaled its threat modeling efforts to manage a total of almost 4,500 active threat models across its product base, leveraging the platform to drive secure design and robust risk reduction across its global infrastructure. It also utilizes over 4,000 threat models in staging and in development.

THE CHALLENGE

The need for an industrial-strength solution:

The organization's cybersecurity team, with over a decade of threat modeling experience, had historically evolved from manual control lists to an Excel-based threat modeling approach. The primary challenge was the need for an industrial-strength solution that could:

- Standardize and scale a mature threat modeling program across thousands of applications and a large user base.
- Achieve secure design and reduce risk at scale by shifting security practices further left in the development lifecycle.
- Simplify and automate processes to enable an eventual full self-service model for IT Service Owners and developers without sacrificing visibility or control.

THE SOLUTION

Facilitate an ambitious shift-left security strategy

The company adopted IriusRisk to serve as the core platform for application-based threat modeling. The solution provided the necessary structure to drive consistency and complete baseline security controls, facilitating their ambitious shift-left security strategy.

Key aspects of the implementation include:

- **Application-Centric Modeling:** The team models application data flows and external connections directly within IriusRisk, using the platform to draw diagrams and identify open threats via the risk patterns engine.
- **Three-Environment Setup:** The client utilizes a sophisticated development, staging, and production tenant setup to manage and test their deployment and data.
- **Automated Workflow:** The financial org leverages IriusRisk to generate reports on threat levels and outstanding countermeasures, which are then reviewed and transferred to background systems and Power BI dashboards for reporting. They are also actively working on a direct integration with their JIRA ticket system to further streamline the process.

“For us, threat models have to be living, breathing documents. The ability to easily view changes—what has changed between last year’s version of Project X and today’s—is absolutely necessary for maintaining our long-term security posture.” – Cyber Security Manager

High countermeasure efficiency

IriusRisk has enabled the financial leader to achieve significant scale, efficiency, and cost savings across their security program.

1. **Unprecedented Scale:** The company plans to scale to 15,000 threat models, with 4,439 models completed to date and approximately 200 monthly active users.
2. **Significant Time and Cost Savings:**
 - **120 years** of threat modeling time saved to date.
 - **108 years** of time saved in the last year alone from the creation or updating of nearly 4,000 threat models.
 - **High Countermeasure Efficiency:** The team has implemented over 500,000 countermeasures and consistently maintains a **countermeasure efficiency of over 91%**, mitigating threats during the design phase to reduce costly downstream rebuilds.
 - **Maturity and Adoption:** The client has a mature program in place where all new and critical applications must be threat modeled, demonstrating strong, consistent utilization.

Key Reasons for Using IriusRisk



Enabling Shift-Left and Self-Service

IriusRisk provides the foundational tools necessary to encourage IT service owners to perform threat modeling themselves, moving toward a full self-service model for non-critical applications.



Driving Consistency and Baseline Controls

The platform ensures a consistent, repeatable approach to threat modeling, helping the client complete all baseline security controls across their diverse product base.



Support for a Mature, Scaled Program

With a sophisticated three-tenant setup and full API access, IriusRisk supports a high-maturity program that leverages their own custom content and reports threat data via Power BI.



“Living, Breathing” Threat Models

The tool enables easy tracking and review of changes, which is critical for maintaining iterative threat models and ensuring long-term accuracy.

“IriusRisk is a key enabler for our shift-left security strategy. The platform is crucial to encouraging our IT service owners to perform more threat modeling tasks themselves as we gradually move toward a full self-service model for all non-critical applications.” – Cyber Security Manager