CASE STUDY

How Nexi Streamlined Security at Scale with IriusRisk

INTRODUCTION

Company Background

Nexi is a European leader in the digital payments space, powering transactions for banks, merchants, and institutions across multiple countries. With security as a cornerstone of its services, Nexi must continuously evolve its software development lifecycle (SDLC) to meet regulatory requirements and protect sensitive payment data.

When facing heightened security expectations during a critical project with a Central Bank Customer, Nexi began exploring how to integrate threat modeling more consistently into their development processes. The team quickly discovered IriusRisk as a comprehensive and scalable solution that aligned with their long-term

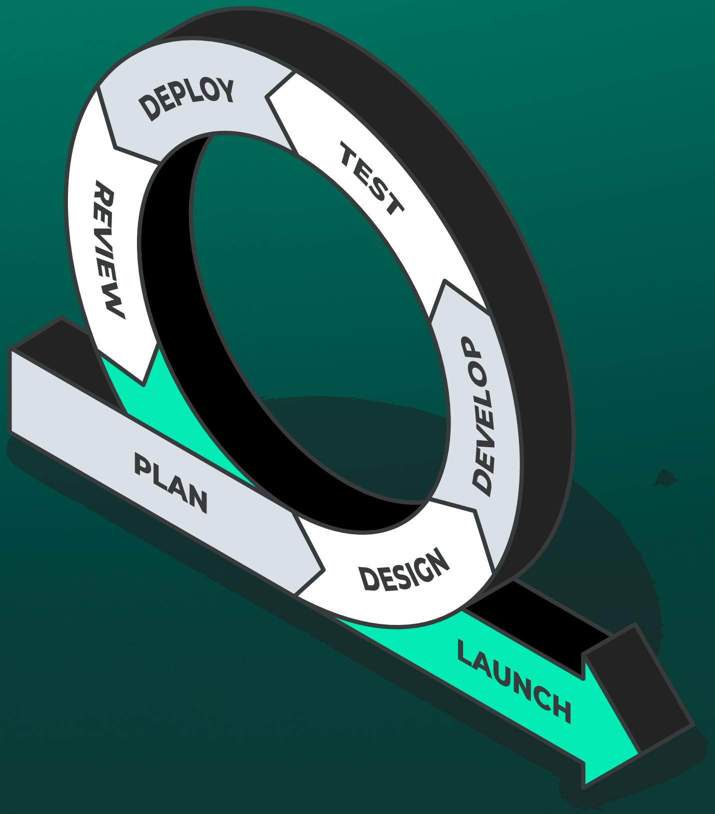
THE CHALLENGE

Lack of formalized threat modeling process

Before engaging IriusRisk, Nexi lacked a formalized threat modeling process. They needed a proactive way to identify vulnerabilities earlier in the development cycle, particularly during high security engagements without overburdening engineering teams.

Their goals included:

- Meeting regulatory compliance expectations.
- Preventing late-stage vulnerability discoveries during client penetration tests.
- Creating reusable models across their diverse customer base security goals.



THE SOLUTION

IriusRisk's secure-by-design platform

Nexi adopted IriusRisk's on-premise threat modeling platform to:

- Automate the identification and mitigation of threats.
- Generate detailed, actionable reports for internal use and client assurance.
- Reuse architecture and component models across projects for efficiency.
- Integrate with existing tools like Jira to streamline workflows.

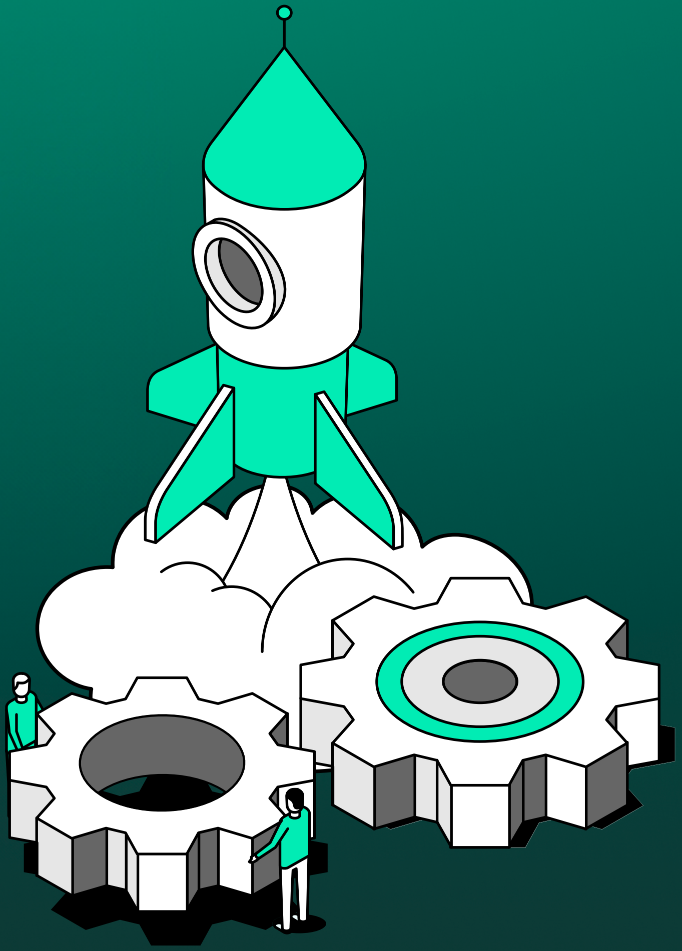
Although initially unfamiliar with the tool, the Nexi team quickly adapted. Over time, they found the learning curve manageable and the value of the platform increasingly clear, especially for projects requiringsecure-by-design development.

> “
>
> ***With IriusRisk, we've gone from reacting to security findings late in the cycle to proactively identifying and resolving them before they ever reach the client. It's fundamentally improved how we develop secure systems.***
>
> Willem Beukes, Solution Architect, Nexi

THE RESULTS

Accelerated risk mitigation

- Proactive risk mitigation: Nexi detects vulnerabilities before client security scans or penetration tests, avoiding costly rework and reputational risk.
- Full threat model utilization: All 10 licensed slots are actively used across projects, including new initiatives in the Middle East.
- Client confidence: Security discussions are more structured, supported by detailed IriusRisk reports and insights.
- Time savings: The ability to reuse components and models has accelerated delivery without compromising security.



Key Reasons for Using IriusRisk

Built-in automation that provides threat insights from architecture diagrams and custom components.

Regulatory readiness by aligning with security standards and controls early in development.

Integration with Jira, simplifying task creation and tracking for threat remediation.

Reusable templates and models, reducing duplication and ensuring consistency across projects.

Scalable licensing model that supports multiple customer architectures concurrently.

> ***When a client adds a new integration—like an XYZ system—we can quickly update the threat model. It guides us through key checks, helping us engage more effectively and ask the right, focused questions.***

Rashaad Essop, Head of Software Development, Nexi