CASE STUDY

German Transport Company shifts left by partnering with IriusRisk to automate a repeatable threat modeling rollout plan.

THE REQUIREMENT

Onboard multiple teams with an automated threat modeling tool

Threat modeling is being done in a variety of manual ways across teams, with generally a good awareness of threat modeling and its benefits for enhanced security. However, as The Transport Company is large with multiple subsidiaries, this means there are a large number of stakeholders and existing security practices in place. The Project Team wanted to introduce an automated tool to further enhance their existing efforts, while introducing a repeatable process that could be adopted more broadly within the organization.

The project is currently overseen by two Security Experts. With many products within The German Transport firm, the existing process meant that threat modeling was occuring much later on in the SDLC, usually several weeks before pentesting activity occurred. The Project Team identified that introducing threat modeling earlier in the process would provide additional benefits from both increased security, time-savings, and introducing automation will mean creation of a higher number of threat models.

THE SOLUTION

Creating a repeatable rollout plan

As the first two users of IriusRisk, the Security Specialists wanted to become competent within the IriusRisk Tool before implementing this internally, and being able to provide support to peers. They became Super Users of IriusRisk, and began rolling out two-day workshops internally to demonstrate the tool, its capabilities, and generate bespoke reports for each department. This allowed the managers of those teams to take the reports and execute any actions or mitigations identified from the countermeasures.

The training feedback was excellent with 85% positive feedback, and teams saying they enjoy using IriusRisk. With key benefits being that it enabled them to create attack scenarios that had never been thought of before to make products better. There has also been interest in using the Infrastructure as Code (IaC) descriptors and future issue tracker integration to further scale and speed up the outputs.

Shifting left with best practice and increased adoption

To date there are 25 active threat models across teams, with more training scheduled. There is an increased understanding of threat modeling processes and best practice, with technical teams in particular seeing that the tool can further support existing efforts and workflows. Next steps may include some configurable assets to better represent architecture, environment or industry aspects.

Instead of threat modeling towards the end of a product life cycle, just before pentesting, the current leading team is making progress to incorporate threat modeling earlier at the design phase. With the future plan being to threat model sooner in the SDLC. In addition, as the company adheres to ISO27001, the tool is able to assist with this due to its reporting capabilities and auditing trail.

Looking to the future

The Transport Company will make threat modeling a mandatory activity starting in 2025, the current team leading the project, are advocating the use of IriusRisk to help scale the activity in an easy, consistent way across the company.