CASE STUDY

From standard to battle-ready: How ARAG IT embedded a measurable, culture-led approach to cyber security training

Introduction

Before TryHackMe, ARAG IT's security education was mostly ad-hoc: seminars when a topic came up, workshops when teams asked for them. Helpful in the moment, but hard to scale—and even harder to measure. Managers had little visibility into skill baselines, learning was discontinuous, and practical labs were risky to run on-prem because exercises could interfere with internal defences.

ARAG IT needed a step change: a repeatable, continuous programme that could support a 270-specialist IT organisation spread across disciplines like development, infrastructure, networking, and project delivery. Just as importantly, they wanted evidence—clear milestones and records to demonstrate progress and support EU NIS-2 directive cybersecurity expectations.

Why TryHackMe?

To get there, ARAG IT chose TryHackMe for one main reason: it made realistic practice safe and easy to adopt. The team could run hands-on scenarios in browser-based, isolated labs without touching production systems. And with guided pathways—from foundations through to SOC Level 1, DevSecOps, Incident Response Exercises and more—they could align training to different roles rather than forcing a one-size-fits-all course.

The rollout began on a small scale. In a pilot phase interns and apprentices were trained using foundational learning paths, gaining cybersecurity basics through a structured, guided, and flexible approach. Progress was measured using German-language quizzes, helping participants strengthen their cybersecurity understanding both English and German. This dual-language strategy prepares future generations to understand complex cybersecurity topics in both languages.

From there, ARAG expanded the programme to core IT, developers, and infrastructure teams with role-aligned assignments. Their SOC team and interns began using SOC Level 1 labs and log-analysis scenarios to build blue-team confidence in a controlled environment.

Operationally, the model is simple but deliberate: departments are set up as learning groups, paths are created in collaboration with team leads and team experts, tested and then introduced as compulsory learning content. A split leadership structure keeps the programme grounded in both governance and real technical need. TryHackMe's analytics dashboards give managers visibility they didn't have before—showing completion against defined milestones and helping teams plan what comes next.

The challenge

The biggest change, though, wasn't the platform. It was the culture around it. ARAG IT makes full use of flexible learning offered by the platform, allowing teams to complete TryHackMe challenges in groups remotely or meet colleagues on-site in dedicated study rooms. They encourage both individual and group learning, so that cybersecurity education becomes part of the work process. In the future, they plan to additionally organize new formats such as "study-lunches", where participants can explore new rooms on TryHackMe or try out new features, discuss solutions meanwhile having a lunch.

ARAG reports faster onboarding to baseline readiness, improved inclusion thanks to optional German entry-level materials, and a measurable view of skill growth through content milestones.

Longer-term outcomes—such as incident trends, phishing metrics, SOC KPIs, and reductions in pen-test findings—are now being tracked over time as the programme matures.

> **"It helps us quantify the knowledge level on defined subjects. We assign a path; once it's completed, we know what the learner knows."**
>
> **Aleksandra Dubovik - Job Title**

Impact

ARAG reports qualitative and early quantitative benefits while deliberately avoiding over-claiming outcomes that require longer observation.

What has improved progression

- **Onboarding efficiency for new employees:** faster to baseline readiness (based on pathway completion and manager observation).
- **Planability and measurement:** ability to quantify knowledge through completion of defined content, with dashboards evidencing progress.
- **Inclusion:** German-language quizzes/materials at entry level increase accessibility and confidence for early-career staff.
- **Adoption and scale:** scalability of business license models reflects broadening use across departments.
- **Operational safety:** hands-on practice isolated from production avoids noisy tooling impacting internal defences in place.

Value provided by TryHackMe

- **Speed to competence:** structured pathways accelerate foundational knowledge for early-career talent.
- **Scalable governance:** group-based assignments and analytics for department leads and managers.
- **Production-safe realism:** genuine tools and scenarios, isolated from enterprise systems.
- **Breadth and currency:** from awareness to SOC/Threat Hunting and AI Security, with ongoing content refresh.
- **Inclusion by design:** localisation at entry level (German where needed) broadens participation.
- **Compliance readiness:** auditable records supporting EU cybersecurity expectations for ongoing training.