Try Hack Me

TryHackMe for Business

How DZ BANK AG Strengthened SOC and Incident Response Readiness with Hands-On, Role-Based Training

A success story for highly regulated organisations where traditional L&D metrics are not viable

Introduction and Executive Summary

DZ BANK AG is Germany's second-largest bank and acts as the central institution for around 800 cooperative banks. Together with local cooperative banks and specialised service providers, DZ BANK forms the Cooperative Financial Group, delivering a broad range of financial services to private and corporate customers.

Within DZ BANK, the Cyber Security department uses TryHackMe across its SOC and Incident Response functions, with CSIRT stakeholders also engaged through incident response and tabletop-style activities. TryHackMe currently supports a core group of SOC Analysts and Incident Responders, with wider adoption across the security organisation.

Operating in a highly regulated environment, DZ BANK does not track individual usage data, onboarding times, or quantitative training impact in order to remain compliant with German legislation. Instead, the organisation focuses on **operational confidence, consistency, and readiness**, using observable behaviours and structured training practices as indicators of success.

DZ BANK's objectives were to provide effective, role-relevant technical training, strengthen CSIRT capabilities, standardise onboarding, and enable realistic group-based incident response exercises without introducing additional compliance or reporting overhead.

Try Hack Me x

The Challenge

Before adopting TryHackMe, DZ BANK faced challenges common to many regulated financial institutions:

- Limited time for training alongside operational SOC workloads
- Fragmented onboarding across three to four separate tool-specific platforms
- Inconsistent participation due to shift work and incident pressure
- Gaps in emergency management, organisational processes, and hands-on incident response practice
- Limited access to realistic, technically focused tabletop-style exercises

As a result, onboarding lacked predictability, baseline knowledge varied between analysts, and coordinating meaningful group training required significant manual effort.

Impact of these challenges

While training existed, it was difficult to deliver consistently and cohesively. New hires relied on multiple disconnected sources, making it harder to establish a shared baseline of knowledge across the SOC and Incident Response teams.

Group-based learning was particularly difficult to coordinate, reducing opportunities for teams to practise collaboration and decision-making under realistic incident conditions.

The Solution

DZ BANK required a platform that could support self-paced individual learning, while also enabling structured, immersive group training that reflected real-world SOC and CSIRT workflows.

TryHackMe met these needs by combining hands-on technical content, structured Learning Paths, and scenario-driven simulations, all without requiring invasive reporting or usage tracking.

Approach

- → Enable self-paced, bite-sized learning aligned to shift work and operational pressure
- → Standardise onboarding through required Learning Paths to ensure a consistent baseline of knowledge
- → Run regular group exercises to strengthen collaboration and decision-making under pressure
- → Maintain up-to-date, threat-relevant content without increasing coordination overhead

Key features and content used

Onboarding and baseline knowledge

- Required completion of SOC Level 1 and SOC Level 2 within the first six months for new SOC Analysts
- SOC Team Internals and SOC Simulator phishing scenarios to support early role readiness

Ongoing individual development

- Walkthroughs and CTFs for continuous skills development
- Splunk-focused content assigned across SOC roles

Group and collaborative training

- Monthly use of the SOC Simulator and Threat Hunting Simulator
- Incident Response and Digital Forensics rooms, including DiskFiltration, Exfilnode, Ironshade, Loglesshunt, and Supplementalmemory
- Honeypot Collapse CTF challenges
- APT28 mini-scenarios from the SOC Simulator, broken down into modular group exercises

How this addressed their needs

TryHackMe enabled DZ BANK to move away from ad-hoc training towards a **predictable and repeatable structure**.

- New hires now follow a clearly defined onboarding path, creating consistency in baseline knowledge across analysts
- Self-paced learning reduces friction and allows individuals to train without disrupting operations, while also giving them the opportunity to upskill in various areas of cybersecurity
- Monthly group exercises improve readiness to collaborate under pressure and strengthen cross-role communication
- Consolidating training into a single platform significantly reduces coordination overhead for the security leadership team

Senior Analysts and Incident Responders retain flexibility, with no mandatory modules enforced, while still benefiting from structured group sessions and advanced technical content.

Implementation and Training Structure

DZ BANK is a long-standing TryHackMe customer, with usage evolving as the organisation's training priorities matured. As of December 2025, around 30 team members actively use the platform.

Key implementation indicators include:

- One full-day, mixed-role group training session per month
- Approximately 12 group training days per year
- Near 100 percent attendance across sessions
- Training facilitated by a dedicated internal training manager who is also a SOC Analyst
- Regular review calls with TryHackMe to align on priorities, share feedback, and plan future content

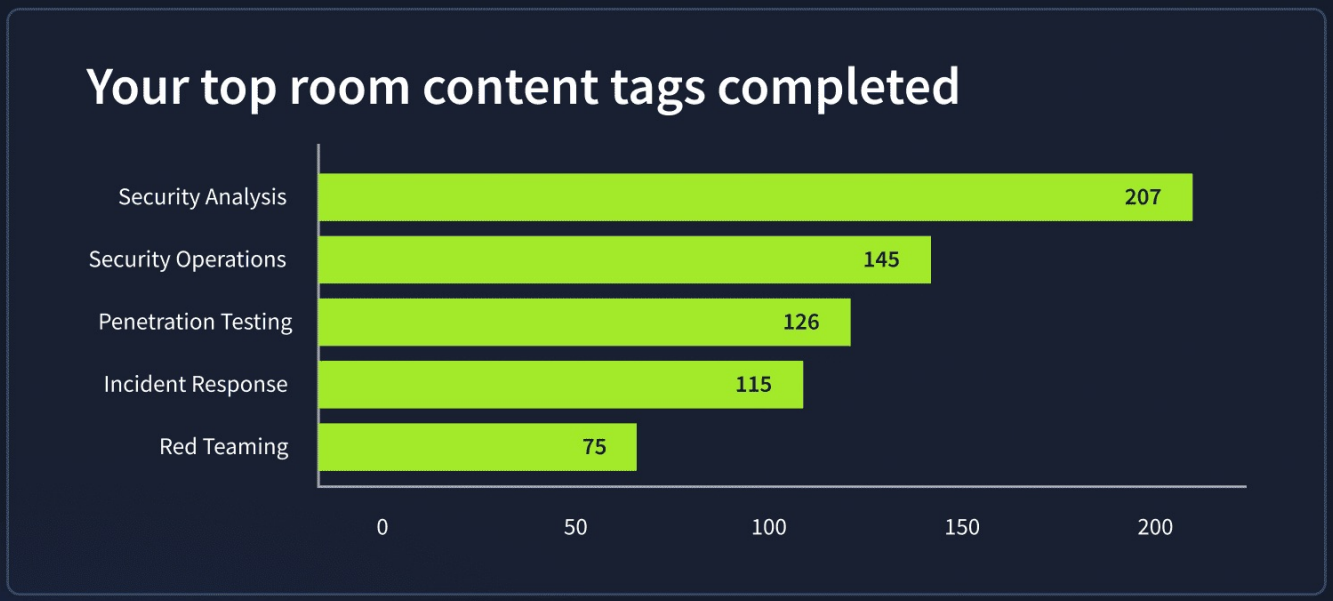
Training data is intentionally not reported internally to remain compliant with German legislation.

Results and operational outcomes

Rather than measuring success through traditional L&D metrics, DZ BANK evaluates impact through **operational confidence and observable outcomes**. Key outcomes include:

- More predictable onboarding for new SOC Analysts
- A consistent baseline of technical knowledge across SOC roles
- Lower effort required to coordinate and deliver training
- Increased readiness to collaborate during realistic incident scenarios
- Strong engagement during and after tabletop exercises, reflected in depth of discussion and follow-up actions
- Team Engagements across a variety of incident types:
  - Financial Fraud
  - Phishing

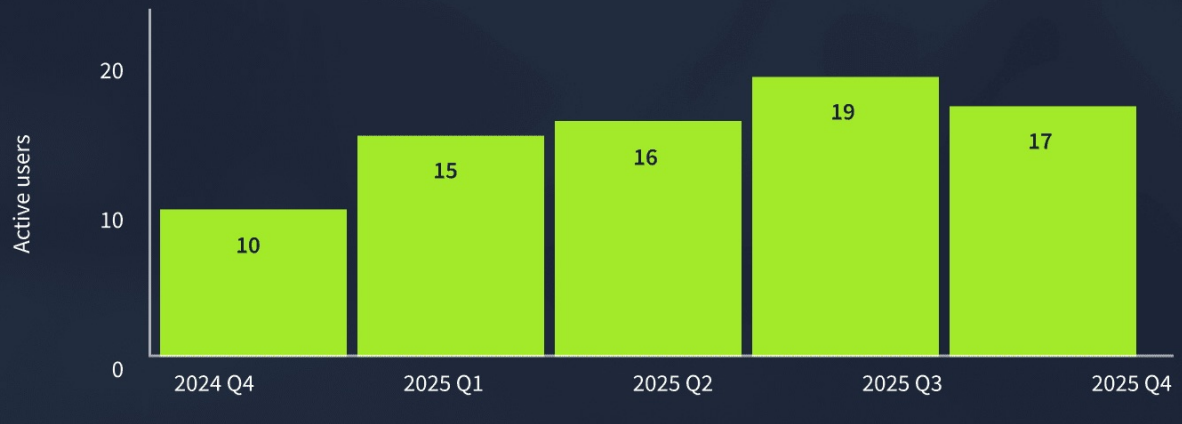
DZ BANK continues to expand its use of TryHackMe and has expressed strong interest in upcoming Incident Response content and the planned IR Simulator in 2026.



Questions answered over time

Rooms completed over time

Active users over time



Conclusion and Testimonial

DZ BANK values its partnership with TryHackMe for its flexibility, relevant content, and ability to support meaningful security training without introducing compliance risk.

This case study demonstrates how highly regulated organisations can achieve structured onboarding, consistent skill development, and improved incident readiness, even when traditional training metrics are not viable.

Tabletop Exercise Feedback

A Cyber Security Manager and Training Supervisor at DZ BANK shared:

"Overall we really enjoyed the exercise, the scenario was interesting and useful for us as it was in the finance sector as well. All in all we had a lot of fun and some really good discussions during the session and afterwards, so I am planning to run these regularly with the CSIRT."

> **TryHackMe has helped us in gaining flexibility, technical knowledge and soft skills, all while being super fun!"**

Leadership Takeaway

By standardising onboarding, reducing coordination overhead, and enabling regular, realistic team-based exercises, TryHackMe has helped DZ BANK strengthen SOC and Incident Response readiness while remaining fully compliant with regulatory constraints.