KORUR

THREAT SIMULATION · FRAMEWORK

Threat Simulation Framework

How Korur designs, runs, and debriefs a realistic incident-response exercise tailored to your organization.

Ransomware is faster, AI-powered, and targeting SMEs specifically. Plans that have never been tested will fail. We design a simulation around your threat model and deliver a written findings report.

Why Simulation Readiness Matters

Ransomware attacks are faster, AI-powered, and targeting SMEs specifically. Plans that have never been tested will fail.

€220K

Average Ransomware Payout

The average EU SME ransomware payment reached €220,000 in 2025, not counting recovery costs, downtime, or reputational damage.

21 days

Average Downtime After Attack

Most SMEs that suffer a ransomware incident are operationally disrupted for three weeks. Untested response plans are a major contributor.

68%

Majority Never Ran a Simulation

68% of organizations that suffered a major incident had never conducted a simulation or tabletop exercise beforehand.

NIS2

NIS2 Requires Tested Plans

The NIS2 directive requires organizations to have tested, not just written, incident response capabilities. Paper plans don't qualify.

What Your Organization Gains

Concrete deliverables and skills from every simulation exercise.

- A tested and calibrated incident response procedure adapted to your specific environment
- A documented gap analysis with a prioritized, actionable remediation plan
- Team coordination skills under pressure: communications, escalation chains, decision-making
- Executive briefing deck showing your security posture and resilience evidence
- NIS2-compliant documentation of tested incident response capability
- A written debrief report suitable for cyber insurance and regulatory compliance

Simulation Framework Stages

A full end-to-end exercise from scenario planning to executive debrief.

1. **Scenario Design**

   We work with your team to design a threat scenario aligned with your industry, technology stack, and the threat actors most likely to target you.

2. **Pre-Simulation Briefing**

   Participants are briefed on their roles, communication channels, and rules of engagement. We establish what's in scope and out of scope.

3. **Live Simulation Exercise**

   The controlled attack begins. Your team responds in real-time, detecting, containing, communicating, and escalating as events unfold.

4. **Debrief and Gap Analysis**

   Immediately after the exercise, we walk through what happened: what worked, what failed, and where the gaps are.

5. **Written Findings Report**

   Within 5 business days, we deliver a full written report with findings, risk scores, and a prioritized remediation roadmap.

> This document is a companion to Korur's Threat Simulation Framework. It summarizes the framework covered during the live training. The hands-on labs, role-specific breakouts, and Q&A take place during the session itself.

Ready to run this with your team?
Korur delivers this training on-site, tailored to your industry and stack. Book a session at **korur.nl/contact**.