EMERSA

KRUPIQ

Threat detection and fluid deception

Emersa Labs | August 2026

Every time you block it, you teach it something.

A refused connection tells whatever is on the other end that the route is shut, so it tries the next one. Something automated will do that thousands of times an hour and learn the shape of your defences as it goes. KRUPIQ withholds the refusal instead. Bulk traffic is turned away early, but a deliberate intrusion is allowed to succeed into a copy of your service where nothing is real. They stop hunting for another way in, and everything they do is written down, on their time rather than yours.

89%
more attacks by AI enabled adversaries in 2025 than 2024

29 min
average initial access to lateral movement. Fastest seen, 27 seconds

73.4%
of tested models used a decoy after naming it a trap in their own reasoning

CrowdStrike 2026 Global Threat Report; Prinos et al., arXiv 2606.21037, June 2026.

How it works

STEP 1
Flood
Bulk traffic is turned away before it costs you anything. The only place we refuse something.

STEP 2
Bait
Files and logins nothing legitimate ever touches. One of them being opened is all the signal we need.

STEP 3
Move
The connection succeeds, into a copy of your service. Your real systems are never on the path.

What it is built to handle

- **Something automated gets in**
  It is given a convincing success instead of a refusal.
- **Ransomware starts encrypting**
  Bait files are touched first, and that is the alarm.
- **Small devices you cannot protect**
  Watched at the gateway instead of on the device.
- **Bulk traffic floods you**
  Turned away before it costs you anything.
- **Something nobody has seen before**
  Caught after it connects, and kept away from anything real.
- **The decoy costing you money**
  Spend on each session is capped by the software, not by a promise.

What you can show afterwards

- Six parts, each with one job. Three handle traffic, one decides, one caps cost, one keeps the record.
- Eight helpers that sort, contain, investigate and write your compliance reports.
- Sits alongside what you already run. Nothing has to be torn out.
- Runs on SUSE Linux Enterprise Server 16, which already ships post quantum cryptography.
- Mapped to NIST and MITRE, and we walk your team through it so it feeds your own audit.
- Every decision recorded in order, signed, and impossible to quietly change later.
- A permanent block needs two named people, not one.
- Nothing fails quietly. If a part degrades, you are told.
- It runs on your hardware. There is no connection back to us, and you can check that on day one.
- We never see your data. Only what you choose to show us in a review.

Accreditations Certified SUSE Ready for SUSE AI. NVIDIA Inception Program partner. Independent penetration testing by Secarma. Certified by TechPassport.

TECHPASSPORT

Next step A live walkthrough, then an isolated sandbox built to mirror your environment. Nothing installed until you ask.