



TIER 4

INTELLIGENT AGENTIC SOC

Your SOC never sleeps.



TIER 4 is an **agentic SOC solution delivered as a native SIEM extension**. It extends your existing security operations center, ships with a ready-made package of pre-tuned detection rules, and runs AI agents across Tier 1–3 — triage, enrichment, and response — with human approval on every consequential action. Built by a team with 10+ years in IT security.

01 Solution Layers

SERVICE	INFRASTRUCTURE Harden	Hardening services reduce attack surface before detection is even needed.
	SOC ARCH. Foundation	Enhanced log tuning · threat hunting · configuration assessment.
	DETECTION Content	Use-case tuning + attack & breach simulation validating every rule.
PRODUCT	TIER 1 Triage	AI-agentic triage & enrichment turns alerts into analyst-ready cases.
	TIER 2 Respond	AI-agentic response with human guardrails & explicit approval. v2
SERVICE	TIER 3 Expert	Incident response and digital forensics services.

Day 1

Ready-made package of pre-tuned detection rules, live from deployment

Tier 1–3

Agentic AI, human-supervised

6 layers

Infra → Forensics

Day 1

Working detection

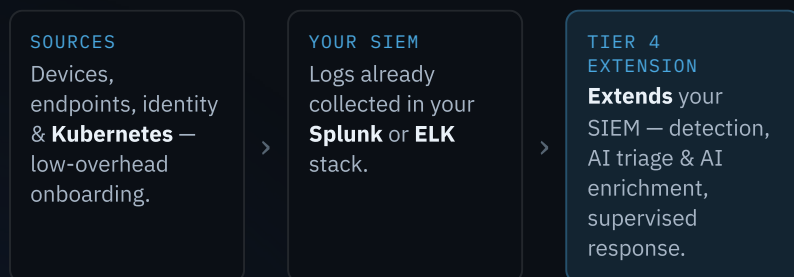
10+ yrs

Security expertise

02 Detection Engineering

- ✓ **Mapped to MITRE ATT&CK** — coverage across the tactic chain, with gap visibility in-console.
- ✓ **Low false-positive rate** — rules are pre-tuned and simulation-validated before shipping.
- ✓ **Custom content** — org-specific rules, one rule per asset, and Kubernetes-native use-cases.
- ✓ **Policy enforcement** — use-cases that detect violations of your operational policies.
- ✓ **Minimal AI token cost** — tuned alerts feed the models, never raw or untuned logs.

03 Deployment Model



04 Technical Specs

Delivery	SIEM extension
Deployment	Alongside existing SOC / SIEM
Supported SIEMs	Splunk · Elastic (ELK)
Detection library	Ready-made tuned rule package, MITRE-mapped
AI scope	Triage, enrichment, response (T1–T3)
Human control	Approval gates on all response actions
Validation	Attack & breach simulation
Log sources	Endpoint, network, K8s
Threat intel	Integrated IOC matching & enrichment
Services	Hardening, IR, forensics

05 Console

