TIER 4

INTELLIGENT AGENTIC SOC

Your SOC never sleeps.

TIER 4

INTELLIGENT AGENTIC SOC

PRODUCT DATASHEET

SIEM-native · AI-agentic detection & response

TIER 4 is an **agentic SOC solution delivered as a native SIEM add-on**. It installs inside your existing security operations center, ships with 2,000+ pre-tuned detections, 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

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.
TIER 1 **Triage**	**AI-agentic triage & enrichment**	turns alerts into analyst-ready cases.
TIER 2 **Respond**	**AI-agentic response**	with human guardrails & explicit approval.
TIER 3 **Expert**	**Incident response**	and digital forensics services.

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

SOURCES
Devices, endpoints, identity, cloud & **Kubernetes** — low-overhead onboarding.

›

YOUR SIEM
Logs already collected in your **existing SOC**.

›

TIER 4 ADD-ON
Installs inside the SIEM — detection, AI triage & supervised response.

2,000+

Pre-tuned detection rules, live from day one

Tier 1–3
Agentic AI, human-supervised

6 layers
Infra → Forensics

Day 1
Working detection

10+ yrs
Security expertise

04 Technical Specs

Delivery	Native SIEM add-on
Deployment	Inside existing SOC / SIEM
Detection library	2,000+ tuned rules, 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

`Overview & ATT&CK coverage` `Alerts` `Tickets / Cases` `Response & Approvals` `Threat Intelligence` `Detection Content` `Assets & Log Sources` `Copilot`