ANOMALI

MODERNIZE YOUR SIEM

WHY LEADING SOC TEAMS CHOOSE TO AUGMENT THEIR SIEM

THE PROBLEM

Why Leading SOC Teams Choose to Augment Their SIEM

- Exploding Ingestion Costs
- Limited Data Retention
- Slow Search & Correlation
- Missing Threat Context
- Legacy Licensing Lock-In

THE SOLUTION

Layer Anomali's Agentic SOC Platform on top of your existing SIEM — no rip-and-replace required.

OPTION 1: SIT ON TOP: Enhance your analytics and intelligence layer

Anomali manages the analytics and intelligence layer. All advanced analytics, IOC correlation, and AI-driven response run through Anomali.

Your SIEM manages compliance and log aggregation. Zero disruption, immediate uplift.

Best for: Organizations that want advanced analytics without touching existing SIEM workflows.

OPTION 2: SELECTIVE OFFLOAD: Reduce cost of managing non-standard SIEM data

Route high-volume, high-cost telemetry — cloud logs, endpoint telemetry, and threat intelligence data for correlation — to Anomali's flat-rate data lake. Your SIEM manages legacy log data at significantly reduced cost.

Best for: Organizations facing SIEM cost pressure or nearing capacity limits.

SIX CAPABILITIES

IOC CORRELATION AT SCALE

Correlates against billions of indicators with zero performance impact.

RETROSPECTIVE THREAT HUNTING

Search billions of logs in seconds — Reduce threat investigation time by up to 96%.

RICH, CONTEXTUAL ALERTS

Every alert includes threat actor, campaign, confidence score, and recommended next actions.

SIEM COST REDUCTION

Route high-volume telemetry to a flat-rate data lake. Customers achieve up to 60% TCO reduction.

AI-DRIVEN ANALYST TRIAGE

Agentic AI handles enrichment, prioritization, and initial investigation reasoning before alerts reach analysts.

VULNERABILITY PRIORITIZATION

Correlate CVEs against live telemetry to focus remediation on what's actually exploitable in your environment.

JUST THE STATS

300X	Faster threat hunting vs. traditional SIEMs
UP TO 60%	TCO reduction vs. legacy SIEM
96%	Reduction in threat investigation time
7+ YEARS	Always-hot, fully searchable data retention

FOUR-STEP PROCESS

1. ASSESS → **2. DEFINE** → **3. IMPLEMENT** → **4. OPTIMIZE**

1. Evaluate current data sources, blind spots, and ingestion costs.
2. Set KPIs: mean time to investigate, data coverage %, and alert fidelity.
3. Start with one high-impact data source. Prove value fast. Scale iteratively.
4. Track time-to-detect and time-to-contain. Let Agentic AI surface correlations automatically.

READY TO MODERNIZE YOUR SIEM?

START REALIZING VALUE IN 30–60 DAYS WITHOUT DISRUPTING CURRENT WORKFLOWS OR COMPLIANCE REQUIREMENTS.

Request a Demo

ANOMALI