# SIEM Optimization for the Modern SOC

Modern SOCs don't need to start over — they need to get more from what they already have. Traditional SIEMs remain central to detection and alerting, but they were never designed for the AI-era with exploding data volumes and automated attacking from adversaries.

Traditional SIEMs create trade-offs between cost, scale, and search speed that leave analysts struggling to keep up. Replacing them can feel daunting, disruptive, and expensive, especially when detection logic, workflows, and compliance controls are built around them.

Modernize your SIEM without migrating. With Anomali, you can keep your current SIEM and processes intact while unlocking faster investigations, broader visibility, and richer context. By adding a high-speed data lake built for intelligence and scale, Anomali extends your existing SIEM's reach and performance without changing the way a security operations center (SOC) works.

## Scale, Speed, and Visibility

Today's threat landscape demands that security teams fight AI with AI. Adversaries use advanced automation, synthetic identities, and generative tools to execute multi-stage attacks in seconds. Yet most SOCs are constrained by slow queries, siloed data, and ingestion models that penalize visibility.

Common challenges for today's SOC teams include:

- **Exploding data volumes** overwhelm ingestion budgets
- **Limited retention** restricts visibility for threat investigations, hunting, and compliance
- **Slow searches and manual correlation** delay incident response
- **Limited context** slows investigations and increases dwell time
- **Legacy licensing costs** force trade-offs between visibility and insight

Modernization does not have to cost operational burden. Optimizing your SIEM delivers faster ROI and prepares your SOC for the AI-driven future.

# The Anomali Advantage: Optimize Without Disruption

Anomali enhances and accelerates a SIEM by pairing it with a scalable, open data lake that feeds intelligence, speed, and automation, while maintaining existing workflows, dashboards, and alerting logic.

**No Retraining. No Re-Architecture. No Disruption. Just Optimization.**

## Seamless Coexistence

Works alongside your current SIEM — alerts, dashboards, and playbooks stay intact

## Full and Centralized Visibility

Consolidates all security and IT telemetry — logs, identities, cloud events, and threat feeds — into one accessible platform, with the ability to retain 7+ years of searchable, hot data at storage level economics

## Flexible Architecture with Cost-Efficient Scale

Built on open standards that integrate with any analytics engine, AI technology, or SIEM vendor, giving organizations the flexibility to evolve, adapt, and scale as the security ecosystem grows

## Fast Search and Analytics

Sub-second queries at petabyte scale across all telemetry enable faster investigation and response

## Native Threat Intelligence Enrichment

Automatically enriches all data with threat intel to strengthen triage and prioritization

## Governance and Control

Ensures compliance and audit readiness by retaining 7+ years of hot, fully searchable data, meeting regulatory mandates without relying on costly SIEM storage or archived cold data

# Built-In Intelligence, When You Need It

While optimization starts with data and speed, it's amplified by intelligence. With Anomali Copilot, SOC analysts can use natural-language queries to explore data, surface patterns, and automatically correlate related events across systems. Copilot doesn't just retrieve information — it thinks and reasons across data sets, connecting users, assets, alerts, and threat intelligence to build a clear investigative storyline. It's an added layer of agentic AI that helps analysts work smarter, not differently.

# How Anomali Works with Your Existing SIEM

Anomali acts as a power source for your SIEM, fueling it with accessible, enriched data and AI-ready insights.

| Category | Current SIEM | With Anomali |
|---|---|---|
| **Data Integration** | Structured, costly to scale | All data types, storage-level economics |
| **Visibility** | Limited by license | Complete telemetry coverage |
| **Search & Correlation** | Manual, slow | Sub-second search and automated correlation |
| **Intelligence** | Minimal context | ThreatStream enrichment and AI-assisted analysis and reasoning |
| **Workflows** | Existing dashboards and alerts | No change; just faster insight across 7+ years of retained data |

# Use Cases

## Full Visibility Without Rework

Many SOCs can't afford to expand SIEM ingestion but still need access to complete telemetry for threat hunting, investigations, and compliance. The Anomali Security and IT Operations Platform solves this by mirroring and extending the SIEM's view, centralizing all security and IT telemetry in an open data lake that feeds enriched insights back into existing workflows. The result is full visibility across all data sources without the need to reconfigure tools, rebuild workflows, or retrain teams.

## Faster Incident Investigation

Analysts often wait minutes or even hours for search results during incident response, delaying containment, and increasing dwell time. Anomali eliminates these delays with searches done in seconds across petabytes of historical and live data. Analysts can investigate, correlate, and act in real-time while maintaining the same workflows. With AI support, analysts achieve outcomes dramatically faster as the platform reasons through complex investigations and surfaces connections that might otherwise be missed.

## Threat Intelligence Everywhere

SOC analysts often lack adversary context when triaging alerts, potentially wasting time on low-value signals. Anomali ThreatStream enrichment automatically adds relevant campaign data, risk scores, and related indicators to every alert and dataset — enabling smarter prioritization, reducing alert fatigue, and accelerating decision-making.

## Continuous Compliance and Retention

Meeting long-term log retention and audit requirements is a growing burden as SIEM storage costs rise. Anomali stores and indexes years of telemetry affordably while keeping it instantly searchable and audit-ready, helping security teams meet compliance mandates without the trade-offs of traditional storage limits.

# Results

- 300× faster search performance
- >50% faster investigations
- 30 TB ingested in hours
- Petabyte-scale retention at a fraction of SIEM cost
- Zero workflow disruption

# The Four Steps to Modern SIEM Optimization

SIEM modernization doesn't have to be a massive overhaul or a risky rip-and-replace project. In fact, as outlined in Anomali's **4 Steps to Modernize your SIEM for the AI Era**, organizations see the biggest gains when they take a structured, phased approach. Instead of trying to migrate everything at once, security teams can progressively expand visibility, intelligence, and efficiency. Meanwhile, your current SIEM continues to run as the system of record.

## Assess: Understand Your Data and Gaps

The first step is evaluating your current SIEM environment: data sources, blind spots, and ingestion costs. Many SOCs find that valuable telemetry (cloud, endpoint, identity) isn't captured because of license limits or siloed tools. Anomali helps unify and enrich that data, building a foundation for true visibility without costly ingestion trade-offs.

## Define: Set Clear, Measurable Goals

Modernization is more than a technology upgrade — it's aligning capabilities with organizational risk tolerance and maturity goals. Anomali works with teams to define KPIs, such as mean time to investigate, data coverage percentage, and alert fidelity. Then builds towards a "system of action" model that blends intelligence, automation, and human decision-making.

## Implement: Modernize in Phases

A full rip-and-replace introduces risk; a phased rollout ensures continuity. Anomali's modular architecture allows SOCs to start small, integrating one high-impact data source, proving value quickly, and scaling iteratively. This approach delivers early wins, gains stakeholder confidence, and avoids operational gaps.

## Optimize: Measure, Improve, Automate

Once visibility and enrichment are in place, the final phase focuses on continuous improvement. With Anomali Copilot and agentic AI, teams can track time-to-detect, time-to-contain, and investigation accuracy, while AI models automatically surface correlations and context. This keeps your SOC's efficiency above the industry's average "breakout time" and ensures the platform continuously learns and adapts.

# Ready to Optimize?

Anomali gives organizations a way to modernize without the disruption, risk, or cost of ripping and replacing a SIEM. Instead of forcing analysts to learn new tools or rebuild playbooks, Anomali amplifies the investments already made — adding speed, intelligence, and scale where legacy SIEMs fall short. The result is a future-ready SOC that can operate at machine speed, keep every dataset searchable, and apply AI where it matters most: reducing investigation time and improving outcomes.

Modernization doesn't require starting from scratch. It requires a platform that delivers full visibility, rapid response, and intelligence action.

Request a Demo →

# Security and IT Operations Done Differently.

Anomali delivers the leading AI-Powered Security and IT Operations Platform. Only Anomali integrates ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP into one powerful platform. At the center is the Anomali Copilot that navigates a proprietary cloud-native security and IT data lake to drive first-in-market speed, scale, and performance at a fraction of the cost. Modernize security and IT operations to protect and accelerate your organization with better analytics, visibility, productivity, and talent retention.

Be Different. Be the Anomali. **Request a demo** to learn more.





ANOMALI