ANOMALI

GUIDE

4 Steps to Modernize Your SIEM for the AI Era

4 Steps to Modernize Your SIEM for the AI Era

Today's threat actors are highly organized, well-funded organizations. They leverage the same advanced AI and automation tools as legitimate companies, flooding organizations with attacks. SOCs relying on legacy SIEMs are falling behind. Data volumes have exploded making analysis more difficult and costly, all while the speed and complexity of attacks ratchets up.

CISOs and security leaders know they need to change. Leveraging AI to counter threats equipped with the same technology is priority number one in many organizations. But the prospect of SIEM modernization can seem daunting and expensive.

Anomali simplifies SIEM modernization with a clear strategy and practical four-step process. The approach drives quick wins, delivers lasting improvements, strengthens cyber resilience, and reduces costs.

4 Steps to Modernize Your SIEM for the AI Era

1. **Assess the State of the SIEM**
   Take inventory of current capabilities and gaps.
2. **Define Your Goals**
   Set clear objectives for modernization success.
3. **Implement a Phased Approach**
   Roll out of improvements in manageable stages.
4. **Measure and Optimize**
   Track progress and continuously refine.

STEP 1

Assess the State of the SIEM

To know where you're going, you have to know where you're starting from. In SIEM modernization, that means carefully evaluating your data sources. By examining the security tools providing inputs to the SIEM and the processes in place to collect and refresh the data, you can begin to identify where security gaps exist.

Often, organizations have maturity goals for their security posture. But experienced CISOs and SOC teams know goals aren't reality. To begin SIEM modernization, you need to take an objective look at the data foundation your SIEM is truly built on. If the holes are too big, the endeavor could fall apart.

To assess the state of your SIEM, it's important to ask:

- What are the data sources?
- Are there any blind spots?
- What pain points exist around data (e.g., silos, latency)?
- How effective are my tools and team at synthesizing all data sources?

Budget constraints can also cause blind spots. Legacy SIEMs with consumption-based pricing models set before the advent of AI can skyrocket costs of using your own data. If your SIEM architecture isn't built to handle today's data flood in a cost-effective way, you'll continue to struggle with visiblity—and overpay for it.

Unified Data Architecture: The Foundation of AI-Powered SIEMs

Threat actors rely on obfuscation to carry out their attacks. They are able to hide amongst the complicated landscape of security information, spreading their attacks across multiple systems. This makes it difficult to understand how details that seem innocuous in isolation actually point to an adversarial attack in context.

Siloed data gives an incomplete view of an organization's attack surface. And the time it takes to piece data together is a boon to threat actors.

A unified data architecture breaks down silos between tools, integrating data from endpoints, network traffic, identity information, entitlement usage, threat intelligence platforms, etc. It creates a high-fidelity data lake of all observable cyber data that can feed SOC analysts and Agentic AI alike.

STEP 2

Define Your Goals

Once you've assessed the state of your current SIEM, you need to clearly define the goals of your modernization journey.

Every organization has a level of risk tolerance. And every information security group contributes to their organization's residual risk due to actions taken, technology deployed, etc. At its most basic, the end goal of SIEM modernization should be that SOC's residual risk is at or below their organization's risk tolerance.

More detailed goals around must-have capabilities can also be defined in this stage. For example:

- **AI-Powered Detection and Response:** Your new platform must be able to detect sophisticated, AI-generated threats like AI phishing, deepfakes, and synthetic identity attacks by analyzing behavioral anomalies across systems.
- **Data Provenance and Integrity:** You need to be certain that the data feeding your models hasn't been tampered with. This requires robust controls like cryptographic watermarking or hashing to ensure the data is trustworthy.
- **Securing the Architecture:** A modern SIEM is a critical part of your defense, so it must be hardened against poisoning, adversarial attacks, and vulnerabilities. This is where a Zero Trust architecture becomes paramount.
- **Active Identity and Access Management (IAM):** Continuous authentication and risk-based access decisions are essential to protect the system from credential stuffing and social engineering.

Evolving the SIEM to a "System of Action"

SIEMs have undergone many changes over the years in response to shifts in the threat landscape. They've moved from passive ledgers to intelligent alert systems, and now, to proactive command centers.

Where does your SIEM fit now? Which kind of SIEM are you aiming for?

- **System of Record:** This "era" of SIEM is a passive platform that collects and stores logs, documenting events for audit and compliance requirements. Security teams manually sift through log data to identify threats and suspicious activity
- **System of Intelligence:** This type of SIEM analyzes logs from different sources, identifies patterns, and raises alerts. Security teams sift through alerts deciding which ones to resolve and how.
- **System of Action:** The latest class of SIEM ingests and enriches data, prioritizes alerts by risk and relevance, and automates response. Agentic AI speeds investigations by automatically gathering context and presenting analysts with the insights they need to act quickly.

STEP 3

Implement a Phased Approach

The thought of a full-scale SIEM replacement can be daunting, but a phased implementation is key to avoiding disruption. Organizations will not accept any gap in their risk tolerance or residual risk protection.

Think of SIEM modernization as a pit crew changing a tire on a race car—fixes are made quickly where they're needed most, with no interruption to the race. The main difference is communication. Be transparent with stakeholders on why you're undertaking this project and what's in it for them (e.g., increased cyber resilience, cost savings). Rinse and repeat as you work your way through different organizational segments.

Keep these three things in mind when executing SIEM modernization projects:

- **Start Small:** Begin with a high-value, high-impact use case to demonstrate success and build confidence within the organization.
- **Secure Buy-In:** Be transparent with all stakeholders. Explain why you are making the change and what the benefits are for them (e.g., improved protection, increased efficiency, cost savings).
- **Migrate Methodically:** Follow a consistent and agreed-upon plan. The process should be transparent, so everyone knows what is being done and when.

This approach ensures a smooth transition, building momentum and proving value along the way without creating gaps in your cyber defenses.

Did You Know...?

In 2025, the average breakout time of an attack is less than an hour and shrinking constantly. How does your mitigation time compare?

STEP 4

Measure and Optimize

You've implemented an ultra-modern SIEM platform—congratulations! Now it's time to ensure it's working as you intended and continually making improvements.

To measure the value of your new SIEM platform, metrics need to go beyond just detection counts and focus on the impact to security posture. Two metrics can give you critical insight:

- **Reduction in Critical Incidents:** The primary measure of success is a decrease in the number of critical incidents or breaches. This proves that the new SIEM is effectively predicting and preventing attacks before they can be successful.
- **Mitigation Time:** Track the time it takes to contain a potential threat once it's detected. A key goal is to keep your mitigation time consistently below the average "breakout time" of an attack.

Tracking these metrics will help you to continuously refine AI models to be more efficient, the alerts more confident, and actions more successful. Through optimization and maturity processes, you can ensure your "system of action" SIEM is significantly lowering your risk exposure.

Let's Begin

SIEM modernization doesn't have to be painful. With a strategic, systematic approach, you'll come out with superior capabilities, improved cyber resilience, and lower costs. Start your journey by building a strong data foundation, set clear project goals, phase implementation for quick and repeatable wins, measure success, and continuously optimize.

Take on AI-powered threats with an AI-powered SIEM. To talk with the experts at Anomali on the benefits of an ultra modern SIEM, schedule a demo.

Be Different. Be the Anomali.

It's all in the name

Anomali defies convention and delivers the unexpected, because legacy cybersecurity tools weren't built for the speed, scale, and complexity of today's AI-enabled adversaries.

In a market flooded with point solutions, siloed tools, bloated platforms, and outdated mindsets, we are the Anomali: a purpose-built, full-stack security platform. With AI woven throughout, Anomali is built for the future to drive meaningful outcomes and measurable productivity gains.

Let your data defend you

Data is your greatest untapped advantage. It holds the truth, reveals hidden threats, and uncovers opportunities — but only if you can harness it all, in real time, with relevant, actionable context.

From fragmentation to clarity: see the whole picture

The future of cybersecurity is unity, not division. Anomali dismantles silos, streamlines your stack, and transforms overwhelming data into decisive action. This isn't just about detection or response — it's confident, proactive control in a world where speed, precision, and clarity are non-negotiable.

A system of action, without compromise

No more choosing between speed and scale. Forget bolt-ons, blind spots, and tradeoffs. Powered by an integrated, high-speed data lake, Anomali unifies your intelligence, telemetry, and AI to deliver what others can't: total visibility, real-time response, lasting context, and operational productivity.

From GenAI to Agentic AI, Anomali applies intelligence across the entire security workflow and delivers clarity through contextual reasoning, intuitive interaction, and automation you control.

Forget legacy acronyms. Whether you're augmenting or replacing your stack, unlock the power of big data — and do more with less.

Radically smarter, faster, and cheaper

Anomali helps you uncover what others overlook, outpace evolving threats, and lead with confidence in the AI era.

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.

© Copyright 2025 Anomali Incorporated®. All rights reserved. ThreatStream® is a registered trademark of Anomali Inc. Anomali Match™ ("Match"), Anomali Lens™ ("Lens"), and Anomali Copilot are trademarks of Anomali Inc.

ANOMALI