USE CASE

ANOMALI

Time to upgrade your SIEM

CHALLENGE WITH LEGACY SIEMS

- **Complexity**
  Installing, configuring, and updating traditional SIEMs requires significant specialized expertise. This drives up operating costs substantially.
- **Scalability**
  Most legacy SIEMs can't handle massive data ingestion and queries efficiently. This requires constant tuning and trade-offs.
- **Limited retention**
  90 days is typically the maximum affordable data retention period. But attackers dwell for months or years.
- **Blind spots**
  Storage limits force rolling deletions, creating visibility gaps. Critical security context gets lost.
- **Slow hunt times**
  Batch-based indexing hampers hunting agility, with queries taking hours or days.
- **Rising costs**
  Legacy SIEMs require perpetual upgrades, additional storage, and more personnel to manage complexity.

The High Costs of Legacy SIEMs

Legacy SIEM (security information and event management) solutions are struggling to keep pace with modern threats and data volumes. Deploying and managing traditional SIEMs has become hugely complex, while high costs limit retention periods to 90 days in most cases. This constrains the security teams' ability to hunt threats and understand full attack timelines. Many organizations are starting to replace legacy SIEMs to boost detection, accelerate response, and reduce TCO.

Coping with Limits of Legacy SIEMs

Many security teams compensate through complex workarounds. Some deploy multiple SIEMs for retention tiering. Others manually backup event data to external sources. But these band-aids add cost and management burden while failing to deliver the underlying capabilities modern security programs need.

The lack of historical visibility means most threats are detected via outside alerts from the FBI or other external parties long after compromise. Limited scalability leads to unpredictable performance issues as data volumes grow. And the infrastructure sprawl creates data silos that prevent unified visibility and control.

Modern SIEM Alternatives

Fortunately, purpose-built replacements are now available that meet today's use cases. Modern SIEM platforms deliver:

- Cloud-native and on-prem support
- Unlimited, long-term data retention
- Rapid search across petabytes of data

- Advanced ML/AI threat detection
- Tight integrations and automation
- Intuitive interfaces aligned to workflows
- Affordable tiered pricing that scales up

For resource constrained teams, replacing rigid and costly legacy SIEMs can significantly improve threat visibility, hunt times, TCO, and user experience. The limitations of traditional SIEMs necessitate a new approach.

Personas Goals

Practitioner Goals

As a SOC Manager, my concern is the effectiveness of my security infrastructure and the ability of those controls to capture threat information in a timely manner. Keeping up with continuous threats is a real challenge, mapping that in an actionable way to my internal attack surface is a fundamental challenge, and ensuring that my organization is aware of and able to respond to threats in a way that is timely and relevant is an area I often struggle against.

CISO Goals

As the CISO, I am ultimately responsible for the success of my organization's security investments. I need to persuade executive management and our board of directors of the importance of investing in rapid-response solutions that are adaptable enough to manage a highly dynamic threat environment and provide an immediate and actionable perspective on how this affects our internal potential attack surface. And everything I describe needs to be done in business terms.

ANOMALI CAPABILITIES

ThreatStream
As a high-performance threat intelligence management platform, ThreatStrream curates and enriches raw data from hundreds of diverse sources of threat intelligence, including Anomali Labs curated feeds, open-source OSINT feeds, specialized premium feeds, and information sharing and analysis (ISAC) centers.

Lens
Anomali Lens includes a powerful Natural Language Processing engine that helps operationalize threat intelligence by automatically scanning digital content to identify relevant threats and streamline the lifecycle of researching and reporting.

Match
Anomali Match gathers security telemetry from various security controls such as endpoints, firewalls, cloud platforms, proxies, and DNS. This data is stored in a scalable cloud-native data lake, ensuring efficient storage.

Attack Surface Management
Anomali ASM provides comprehensive visibility into all IT assets, including shadow IT, to fuel actionable Match security analytics

Digital Risk Protection
Anomali DRP combines expert human analysis with AI and ML insights to indicate which assets are most at risk, which threat poses the greatest danger, and how to prevent an attack before it happens. DRP also monitors for fake domains, social media accounts, brand impersonation, stolen PII, fraud campaigns, or stolen IP.

Anomali Contribution

The Anomali Security Operations Platform is the core of an ecosystem of technologies that can accelerate an organization's ability to detect and respond to threats within minutes of their appearance. This includes the world's largest threat repository (ThreatStream), a security analytics-driven correlation engine (Match), and an NLP solution (Lens) that provides actionable context to a wide range of threats mapped to the organization's attack surface. All of this is driven by a curated GPT solution that has made speed and accuracy the cornerstone of our solution to cybersecurity concerns.

Use Case Outcomes

Immediate response is driven by GPT-enabled security analytics. Process terabytes of information in seconds, tracked against telemetry data going back years.

Ease of deployment allows you to make changes and additions to your security environment measured in hours, not weeks, and at a significantly lower price point.

Correlated information tracks telemetry across business lines that work from the same technology infrastructure, preventing lateral movement of attacks and driving collaboration across functional groups.

Workflow Automation through accelerated detection and prioritization of threats, enabling SOC analysts to focus on more complex and strategic challenges and avoiding the day-to-day grind of high-speed transactional processing.

ANOMALI