

ANOMALI

GUIDE

Top 2025 SIEM Demands for Finserv Security Teams



Top 2025 SIEM Demands for Finserv Security Teams

In an era when digital transactions outpace cash, cybercriminals are training their crosshairs on financial services. Attacks are sophisticated and unrelenting, evolving faster than FinServ's traditional security information and event management (SIEM) platforms can keep up.

Financial Services Needs a New Approach — Now.

As a highly regulated industry sector, banks, accounting firms, insurance companies, and investment groups need a security operations (SecOps) platform tailored to their unique challenges — detecting fraud and compliance issues, responding to potential breaches in real time, and predicting future attacks.

The ideal solution would provide comprehensive visibility across the extended network ecosystem, including third-party integrations. It would query and analyze vast numbers of financial transactions faster than attacks could unfold. It would use AI to empower security analysts of all experience levels to become masterful threat hunters. And it would do it all while keeping budgets in check and maintaining customer trust.

The good news? You can have it all.

Read on to learn how an AI-powered modern SIEM can transform your organization's cybersecurity posture, alleviate the burden on your overworked SecOps teams by simplifying and paring down the technology stack while bolstering your defenses against the world's most onerous cyber threats.

1. You Need to See it All

Fueled by digital transformation, financial data is proliferating faster than viral dance trends on TikTok. The industry is hungry for the insights contained within these massive datasets. AI and machine learning are insatiable consumers, greedily gobbling unprecedented amounts of data in their quest to help us create new lines of business and opportunities. Even regulators are demanding more granular, traceable data.



While it's exciting, it also spells trouble for security teams, who cannot defend what they cannot see.

If your SIEM doesn't give you visibility into every data source in your environment — every endpoint, server, network, website, cloud application, and device — your organization is exposed and vulnerable.

Most traditional SIEMs provide only partial coverage, leaving you to bolt on extra tools to get comprehensive visibility. Anomali, on the other hand, provides visibility into every data source in your environment, right out of the box.

2. You need retrospective data

Lookback data is critical for comprehensive security. It helps you identify and understand long-term patterns, uncover dormant threats, and investigate breaches that may have originated months or even years ago.

However, traditional SIEMs are designed for near real-time analysis of log data. They usually only provide immediate access to data from the last three to six months of activity. Older data is held in cold storage, making deep retrospective analysis time-consuming and impractical.

When you're investigating a suspected attack, time is of the essence. Querying cold data becomes a hindrance when the details of the recently announced breach you're investigating happened many months ago, or even as far back as a year.

The bottom line is that these old-school SIEM platforms are incapable of deep retrospective analysis. You'll never know if a malware time bomb was injected three years ago, lurking in the shadows, waiting to deploy.

In contrast, Anomali is purpose-built to collect and store a record of all internally logged activity dating back more than seven years. It doesn't matter whether an event was logged five days or five years ago. Anomali's groundbreaking Security Data Lake keeps all data at your fingertips.

Anomali's modern approach to SecOps completely eliminates these issues: all data, regardless of age, is hot and readily accessible for rapid searching — no extra cost.

You've Got a Need for Speed

Achieving comprehensive visibility is critical. But it's only the first step. You need to be able to extract meaningful insights from vast datasets faster than attacks can unfold. Speed and performance are paramount.

Anomali is purpose-built to collect, store, and rapidly retrieve a record of all internally logged activity. This allows analysts to pinpoint activity by known bad entities in the blink of an eye, searching a billion records in just 10 seconds!

A customer who recently replaced Splunk with Anomali reported that the switch reduced the company's average query time from 48 minutes to 44 seconds.

What's in the secret sauce?

Here are the ingredients for Anomali's unparalleled speed:

Cloud-native architecture – Anomali's agentless, cloud-native design makes it scalable enough to handle petabytes of data without compromising performance. It leverages lossless compression algorithms to reduce data storage requirements. It efficiently ingests logs to ensure rapid data availability.

Serverless – Anomali's serverless architecture enables SOC's to scale resources on demand. This efficiency significantly improves response times and overall performance.

Agentless – Deploy faster and more efficiently with no-installation-required agentless deployment. The simplified architecture makes it easier to manage and scale and, with no agents to update or patch, reduces ongoing maintenance and operational risk. Additionally, agentless deployment reduces your attack surface, decreases endpoint load as there is no consumption of endpoint resources such as CPU or memory, and eases compliance headaches.

Integrated Security Data Lake – At the heart of Anomali's revolutionary approach is its integrated IT and Security Data Lake. This powerful feature efficiently manages the exponential growth of security data, providing high-speed collection, processing, and analysis at scale — all while maintaining cost efficiency and ensuring your data is safe. Anomali's Security Data Lake puts you in control, keeping your corporate data hot and accessible without ever storing client data.



What's more, Anomali is the only security analytics solution that doesn't rely on another big data provider, allowing it to deliver more capabilities faster and pass the savings back to customers. With the ability to store high-fidelity indicators of attack (IOAs) and its seven-plus years of lookback, it takes security analytics to a whole new level.

3. You Don't Need to Fly Solo When You've Got a Smart Copilot

Traditional SIEMs require analysts to master a proprietary query language — an advanced skill set. Given the dearth of analyst talent, this presents a major obstacle for a growing organization. Constructing queries can also be complex and time-consuming, even for senior analysts. But it doesn't have to be that way.

Eliminating complexity

Anomali's safe and intelligent AI-Powered Copilot helps you overcome these obstacles. Copilot's advanced AI and natural language processing (NLP) enables users

of all skill levels to conduct sophisticated threat-hunting tasks simply by asking questions in plain language (it supports over 80 languages!). This capability reduces threat research time from hours to seconds, slashing the time required to investigate newly reported global threats by half and empowering junior analysts to perform at the level of far more experienced team members.

Machine learning (ML) integration

The sheer volume of security incidents today far exceeds human capacity. To rise to the challenge, modern

SIEMs must leverage ML models in real time. While effective AI is not a given with traditional SIEMs, it is the underpinning of Anomali Copilot, enabling its extended visibility, lightning-fast detection, and comprehensive response.

Putting threats in context

Imagine investigating a newly released IoC and receiving real-time alerts that match the intel to internal telemetry. Anomali Copilot makes this possible by integrating

ML models that enable real-time anomaly detection and threat scoring across hundreds of thousands of incidents. No other SIEM compares.

Building a bridge to management

At the end of the day, your company's leadership needs the answer to one simple question: "Are we at risk?" Anomali Copilot helps you demystify complex security concepts and provide clear situation reports in easy-to-understand language.

4. You Need a Higher Threat IQ

Cybersecurity isn't a collection of disparate activities. Rather, it's a holistic integration of threat detection, investigation, and response (TDIR). Even so, traditional SIEM vendors treat threat intelligence as a separate capability.

Anomali ThreatStream, the leading threat intelligence platform (TIP), provides curated access to more than 80 threat intelligence feeds from a wide range of sources, including open-source intelligence (OSINT), commercial feeds, dark web monitoring, and proprietary research. Users can also add threat intel feeds (often with free trials) via the Anomali App Marketplace. This diverse, customizable library covers a large spectrum of potential threats and attack vectors mapped to the MITRE ATT&CK framework.

However, with Anomali, threat intelligence doesn't live in a silo. Instead, Anomali's Security and IT Operations Platform infuses it into all alerts and incidents. This

integration ensures seamless data analysis and better contextualization of threats, leading to more efficient detection and response.



Intel in action

ThreatStream empowers analysts with the AI-enriched threat intelligence they need to understand their threat landscape, security posture, and in-progress attacks.

The solution filters and prioritizes data by relevance to help security teams focus on what's essential and optimize decision-making at scale.

Its features include:

- Automated unstructured intelligence ingestion with NLP
- Machine-readable intelligence integrated with existing security controls
- Simplified intelligence licensing with the Anomali App Marketplace
- The ability to share intelligence with ISAC peers
- Security alerts enriched with actors, campaigns, TTPs, and more

What does it look like to integrate threat intelligence, AI, and world-class security analytics? Imagine investigating a suspicious IP address and seeing relevant high-fidelity threat intel alongside your internal log data in real time, immediately drawing your attention to the connection.

This holistic view allows analysts to make faster, more informed decisions, reducing the time from detection to resolution.

Anomali also integrates data from vulnerability assessment tools like Qualys, allowing for risk prioritization based on real-world activity. By leveraging the MITRE ATT&CK framework, Anomali provides deep context across strategic intelligence, enabling analysts to assess and respond with great efficiency. Also, various sources can be directed to Anomali without increasing SIEM storage, licensing, processing power, or overall budget.

5. You (Literally) Don't Want to Break the Bank

Scaling analyst efforts, optimizing compute, and consolidating your security operations tech stack all contribute to cost savings across your entire security and IT operations infrastructure.

Jump the skills gap

Anomali Copilot's conversational AI empowers junior analysts to perform at the level of senior analysts by eliminating the need to master a proprietary query language. This helps you avoid the need to hire highly skilled (and expensive) team members.

Use resources more efficiently

Anomali's integrated Security Data Lake lets you store only the data you need (saving money on storage costs). Its serverless architecture lets you optimize your use of computing resources by scaling in response to workload demand.

Consolidate your tech stack

Anomali lets you do more with less and relieve tool fatigue by combining ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP into one streamlined, efficient platform. It empowers you to bind threat hunting and security operations into one discrete workflow, eliminating the need for multiple tools.

Vanquish unnecessary storage costs

Anomali's Security Data Lake doesn't sit on top of another big data provider. Bonus: Anomali passes the savings on to its customers.



Anomali: the evolution of SIEM

Anomali is a revolutionary AI-Powered Security and IT Operations Platform that gives you comprehensive visibility, speed, AI, and world-class threat intelligence in one, easy-to-use integrated platform. It provides first-in-market speed, scale, and performance, consolidates your tech stack, and empowers your team to do more with less.

It is the only platform capable of meeting FinServ's unique challenges, keeping you compliant while scaling effortlessly and affordably.

Innovative, effective technology. Cybersecurity solutions for organizations of all sizes. AI-Powered intelligence-driven solutions for a more secure world. That's Anomali.

Discover how Anomali can help you create a robust, highly adaptive security solution. [Schedule a demo](#) of Anomali's Security and IT Operations Platform to see why it's different and how it can transform your organization's cybersecurity.

Security and IT Operations Done Differently.

Anomali is the leading AI-Powered Security and IT Operations Platform that delivers mind-blowing speed, scale, and performance at a fraction of the cost. Our cloud-native approach modernizes the delivery of legacy systems, combining ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR and TIP to deliver security analytics that enable our customers to detect, investigate, respond, and remediate threats in one integrated platform.

[Request a demo](#) to learn more about the Anomali AI-Powered Security and IT Operations Platform.