BLOG

Inside Anomali's Disruptive Advantage

Security leaders shouldn't have to choose between power and usability, or between flexibility and speed. With Anomali, they don't.

SHERRY LOWE | APRIL 16, 2025

Share:

TABLE OF CONTENTS

When cybersecurity researcher and independent analyst Francis Odum published his latest piece about Anomali, it resonated across our team, not just because it was accurate (thank you, Francis!), but because it captured the shift already underway in security analytics and the security information and event management (SIEM) market with both clarity and conviction.

In his piece, Francis acknowledges what Anomali customers know to be true: legacy SIEM tools and conventional cloud-based data lakes often come with high costs, slow queries, and disconnected workflows. For years, the industry has seemingly just accepted these pitfalls as the cost of doing business. But as he noted, organizations are beginning to demand more.

Francis surfaced several themes that reflect the challenges we hear from customers every day. A few stood out because they highlight not just where the market is headed, but what's already working — and why Anomali is built for this moment.

1. From 74 Hours to Two Minutes (and Why It Matters)

The story Francis shared about an Anomali customer who reduced detection query time from 74 hours to just two minutes is powerful. But the real impact goes far beyond speed. It's about unlocking true real-time threat detection — and finally eliminating the operational bottlenecks that have plagued security teams for years.

For many SOCs, this kind of leap forward is transformational. Analysts, threat hunters, and incident responders no longer waste hours or days waiting to test a theory or validate a lead. They can move at the speed of threats.

Faster queries lead to faster decisions. And faster decisions lead to quicker containment, reduced dwell time, and fewer missed threats. That's not just a performance upgrade — it's a major morale boost for teams constantly battling alert fatigue and tool sprawl.

2. Accelerating Migrations Without Breaking What Works

Let's be honest — no one wants to spend a year migrating a SIEM. That's why Francis's point hits home. The very notion of SIEM migration strikes fear into the hearts of security leaders, and for good reason. It's a resource-intensive process that stalls momentum and disrupts daily operations.

At Anomali, we knew that had to change. Our AI-powered migration is fast, painless, and low-risk. At the heart of this acceleration is Anomali Query Language (AQL), our purpose-built syntax, designed to flexibly search, correlate, and analyze threat intelligence and security telemetry across a unified architecture. It's powerful, flexible, and intuitive — giving analysts the ability to move fast without having to learn a whole new way of thinking.

We fully stand behind our ability to migrate your SIEM in 90 days to maximize performance and cost savings. Or optimize your existing SIEM to boost visibility, speed, and efficiency from day one.

3. The Architecture Advantage

While Francis rightly highlights the integration of TIP, SIEM, and data lake functionality, we also believe the real advantage lies in the architecture itself.

Anomali embeds threat intelligence and security telemetry directly within the integrated data lake. There's no need to move data across systems or storage layers to get insights. In any analytics

platform, reducing data movement is critical: it improves performance, lowers costs, and simplifies operations.

This isn't just about operational efficiency — it's about setting a new standard for what analytics platforms need to be. As detection engineering evolves to incorporate broader telemetry — from IT and cloud environments to supply chain and third-party risk — the flexibility of the underlying platform becomes the difference between reactive and proactive defense.

We Are The Anomali

As Francis put it, Anomali isn't just a new type of solution. It's not a SIEM. It's the future.

In a market crowded with conventional point solutions, bloated platforms, and outdated thinking, **we are the Anomali** — purpose-built as a full-stack security platform, designed for what's next.

Security leaders shouldn't have to choose between power and usability, or between flexibility and speed. With Anomali, they don't.

We appreciate Francis for recognizing the shift and for spotlighting what makes it work. We look forward to other analysts following his lead.

If you're evaluating SIEM replacements, or an optimization of your current SIEM, request a demo . Watch us get it done — in 90 days.

Sherry Lowe

Sherry Lowe is the Chief Marketing Officer at Anomali. Lowe is a 25-year veteran of high growth technology companies in Silicon Valley. Prior to Anomali, Lowe served in marketing leadership roles at Exabeam, Expanse, and Splunk. Lowe is also an award-winning print and broadcast journalist. She holds a bachelor's degree in journalism from Arizona State University and a master's degree in English from Indiana State University.

Discover More About Anomali

Get the latest news about cybersecurity, threat intelligence, and Anomali's Security and IT Operations platform.

SEE ALL RESOURCES

BLOG

Elevating Threat Intelligence and Security Operations With Anomali's Latest Innovations

LEARN MORE

BLOG

Anomali Named Most Innovative Cybersecurity AI by Cyber Defense Magazine's 2024 Top InfoSec Innovator Awards

LEARN MORE

BLOG

Anomali Outpaces Modern Threats with Quantum-Quick Security Analytics

LEARN MORE

Propel your mission with amplified visibility, analytics, and AI.

Learn how Anomali can help you cost-effectively improve your security posture.

SCHEDULE A DEMO

ANOMALI

808 Winslow Street,
Redwood City, CA,
94063, United States

+1 844 4 THREATS (847328)
+44 8000 148096 (International Toll-Free)

Platform and Products

- Anomali Platform
- Anomali Copilot
- Anomali Security Analytics
- Anomali ThreatStream

Marketplace

- Anomali Marketplace
- Threat Intelligence Feeds
- Threat Analysis Tools and Enrichments
- Security System Partners
- Marketplace for Partners

Partners

- Partners Overview
- Join the Technology Partner Program
- Anomali SDKs
- Threat Intel Sharing
- Partner Portal Login

Resources

- Resource Library
- Blog
- Events
- Support
- Glossary

Company

- About Anomali
- Careers
- Contact Us
- Leadership
- Press Room
- Schedule Demo