ANOMALI

GUIDE

2025 SIEM Essentials: A Banking Industry Guide for Saudi Arabia

2025 SIEM Essentials: A Banking Industry Guide for Saudi Arabia

In the Kingdom of Saudi Arabia (KSA), the financial services sector is undergoing a profound digital transformation, driven by Vision 2030 and the rapid adoption of financial technologies. As financial institutions across KSA adopt advanced technologies to drive innovation and customer experience, they face increasingly sophisticated cyberthreats that demand intelligent, comprehensive security solutions. The unique challenges of protecting digital transactions, maintaining regulatory compliance, and safeguarding critical financial infrastructure require a transformative approach to security information and event management (SIEM).

In addition to PCI DSS, ISO 27001, and other international standards, KSA's financial institutions must comply with regulations governed by Saudi Arabian Monetary Authority (SAMA), the country's central banking organization. The SAMA regulations outline strict requirements for governance, threat intelligence, incident management, third-party risk management, regulatory compliance, and authentication security. Their goal is to strengthen the resilience of KSA's financial sector against cyberthreats by ensuring proactive threat detection, continuous monitoring, and robust incident response measures.

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, and bolster your defenses against the world's most onerous cyberthreats.

1. You Need to See it All

Fueled by digital transformation, financial data is proliferating at an unprecedented rate, challenging traditional security paradigms. The industry is hungry for the insights contained within these massive datasets. AI and machine learning (ML) 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.

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!

Organizations implementing advanced SIEM solutions have reported dramatic improvements in query performance, reducing complex search times from hours to 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 SOCs 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 Data Lake: At the heart of Anomali's revolutionary approach is its integrated Data Lake. This powerful feature efficiently manages the exponential growth of security data, providing high-speed collection, processing, and analysis at scale — all while keeping costs low. Anomali's Data Lake keeps all your data hot.

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.

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 indicator of compromise (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 200 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 globally recognized threat modeling frameworks like MITRE ATT&CK.®

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.

ThreatStream's 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 SecOps 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 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 by combining ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP into one 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.

SAMA Cyber Security Framework: Compliance Made Simple with Anomali

SAMA Cyberthreat Intelligence (CTI) Requirements

1. **Core CTI Principles**
   a. Establish processes for intelligence collection and analysis
   b. Deliver actionable threat intelligence
2. **Strategic CTI Principles**
   a. Identify the cyberthreat landscape
   b. Assess threat actor objectives, motivations, and intentions
   c. Develop tailored threat assessments
3. **Operational CTI Principles**
   a. Analyze attack chains and threat actor tactics
   b. Understand techniques, tactics, and procedures (TTPs)
   c. Monitor tools and malware used in cyber attacks
4. **Technical and Tactical CTI Principles**
   a. Collect IoCs
   b. Monitor vulnerabilities and cyber incidents
   c. Provide timely intelligence for security operations

SAMA's Approach to Threat Detection

1. **Operational CTI Principles**
   a. Identify cyberthreats based on real-world attack chains.
   b. Analyze adversary TTPs.
   c. Monitor cybercriminal and nation-state actors to predict potential attacks.
2. **Technical and Tactical CTI Principles**
   a. Track IoCs, such as malicious IPs, domains, and hashes.
   b. Continuously scan and analyze emerging vulnerabilities in critical systems.
   c. Use threat intelligence feeds to detect and respond to cyberthreats proactively.
3. **Incident Monitoring and Threat Intelligence Integration**
   a. Implement SIEM for real-time threat detection.
   b. Enable TIPs to correlate internal data with global threat intelligence.
   c. Share intelligence within financial institutions to mitigate sector-wide cyber risks.

Anomali: The Evolution of SIEM

For Saudi financial institutions, cybersecurity is a critical national priority that underpins economic resilience and digital transformation. As the Kingdom continues to develop its financial technology ecosystem, protecting critical infrastructure and maintaining customer trust becomes paramount. Anomali offers a cutting-edge solution that empowers Saudi financial organizations to stay ahead of evolving cyberthreats, meet rigorous regulatory requirements, and build a secure digital future.

Anomali's groundbreaking AI-Powered Security and IT Operations Platform 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 the finance industry'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 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