ANOMALI

GUIDE

# Elevating SOC Efficiency: A 2025 Guide for Banking Leaders in Saudi Arabia

GUIDE

# Elevating SOC Efficiency: A 2025 Guide for Banking Leaders in Saudi Arabia

Running a security operations center (SOC) can be complex and hectic under the best of circumstances. Analysts are overwhelmed by alerts and juggling dozens of tools. They're struggling with a shortage of skilled analysts while contending with leadership increasing pressure to reduce mean time to detect (MTTD), mean time to respond (MTTR), potential dwell time, and budget.

In financial services (FinServ), the problem is compounded by unique challenges and heavy regulations, such as the SAMA Cyber Security Framework. These regulations significantly impact staffing requirements, increase the need for robust documentation and reporting, mandate specific technology tools, and impose process constraints to ensure compliance and resilience against emerging cyber threats

These factors are all obstacles to efficient operations. Once you complete your workflow documentation, processes, escalation paths, standardize responses, and get past all the bureaucracy, there is still a question of visibility, as well as manual processes.

In May 2024, SANS released their annual SOC Survey, highlighting the top challenges in security operations, as reported by the survey respondents. In addition to the challenges above, survey respondents cited departmental silos, compliance issues, and alert fatigue as obstacles to efficient operations.

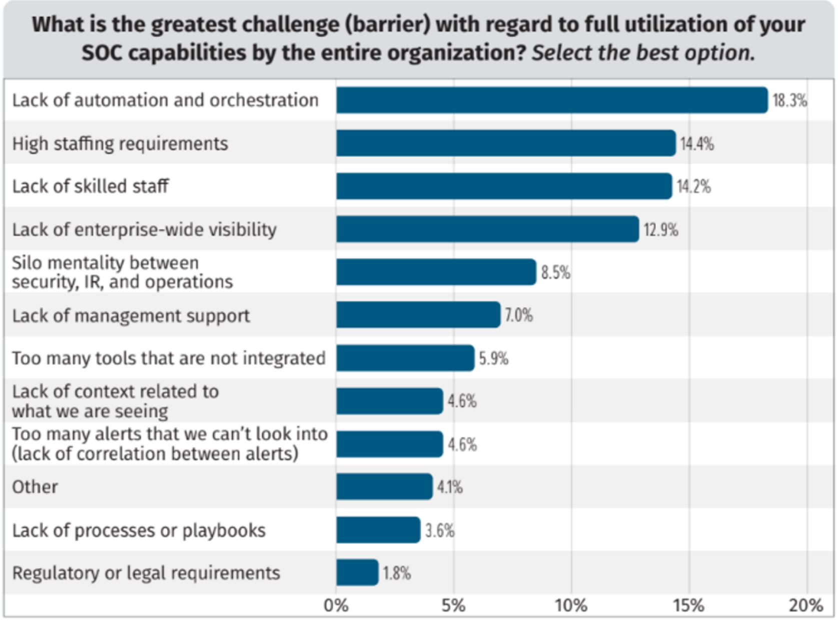

**Figure 1.** SANS 2024 SOC Survey: Facing Top Challenges in Security Operations

**There has to be a better way.**

And there is. The key is to understand where you can drive efficiency in your current people, tools, and processes while building out a foundation that makes it easier and faster for analysts to identify threats. It may be a little cliché, but yes, your SOC can be better, faster, and stronger.

This guide highlights the top hurdles impacting SOC efficiency in FinServ. It offers practical solutions for overcoming them, focusing on automation, enhanced visibility, and unified platforms that align security with IT operations to simplify the investigation steps.

By tackling key solution and automation issues head-on, FinServ security teams can streamline their workflows, reduce alert fatigue by focusing on real events of interest, and ultimately strengthen their defenses against sophisticated cyber threats.

You may still need to rejigger your staff to ensure a balance of desktop support, network operations, IT architecture, and engineering personnel. However, having the right solutions in place will put you on the path to greater SOC efficiency.

## 1. Embrace a Platform Approach and Automation

Over the last decade, the modern SOC is bringing in more logs from the extended security stack, from CASB and NGFW to NDR, EDR, and more. Furthermore, SOC analysts now review multiple sources of intelligence that have the same observables (IP addresses, file hashes, etc.) but with contradictory assessments of severity. Feeds can be out of date, overlap, and end up siloed.

This doesn't even address incorporating an ever-growing and changing quantity of threat intelligence. Vendors may have built-in threat feeds, some of which could be months out of date. How do you know what the right feeds are? And do your feeds go back far enough? With so many external threat intelligence sources, it can be challenging to know where to start.

### How Can We Reduce the Signal-to-Noise Ratio?

This is where platform choice and automation become critical. A modern SOC needs a central platform that can integrate and normalize logs and events from the network and security stacks into a common format and deliver them to the analyst. Many security information and event management (SIEM) systems perform these functions at a basic level by allowing the SOC analyst to write queries to sort logs by criticality. However, it is far more efficient for the SIEM itself to do the sorting, using automation to determine potential scope and whether an event is worthy of further investigation.

For example – let's say your SOC analyst sees a flood of events from a known malicious source (thanks, threat intelligence!) throwing events that test the vulnerabilities of a system in your environment. Without context or more information, a SOC analyst might escalate this, only to be told by network ops that the attack assumes an IIS web server and your main web server runs on Apache. In other words, while noisy, the activity does not present an actual threat. This is where automation, context, and integration across your stack truly shine.

If your analysts must respond to every event that your NGFW or EDR marks as critical, they'll have no time to investigate legitimate threats. Your SIEM platform should automatically sort the wheat from the chaff and prioritize events so your team knows what to focus on.

Automation can also play a central role in improving how SOCs analyze and disseminate threat intelligence by consolidating dense or duplicative data, prioritizing threats, and ensuring that it's delivered to the right place at the right time.

## 2. Ensure Timely Network-wide Visibility and Context

By design, some threats lay dormant for months. Adversaries know that most SIEMs default to keeping data hot for only 30-90 days. Beyond that point, the volume of data becomes excessive, and keeping it hot is prohibitively expensive. Even cloud-native SIEMs require you to open a ticket and reload data older than your contracted limit, and that's if you contracted for archived storage to begin with. As such, "low and slow" attacks are more likely to evade detection. How can security teams track these advanced, persistent threats?

### Unlock Full Visibility to See the Big Picture

Comprehensive visibility and context require a different approach. If your SIEM can only analyze one gigabyte of data before timing out, you'll never see the whole picture. The good news is that modern platforms have evolved to the point where you no longer need to be constrained by the technical limitations of traditional and next-gen SIEMs.

You may need to ingest terabytes and search petabytes of structured and unstructured data to find persistent threats. Answering the question "Are we impacted?" should take seconds or minutes, not hours or days.

## 3. Transform Threat Detection into Action

Every SOC must start by determining whether there is a threat and if the organization is impacted. However, the answers often prompt further questions, such as

- "Is the threat known or unknown?"
- "Is the threat actor familiar?"
- "What is the attack vector?"
- "Is my infrastructure at risk?"

Comprehensive, contextualized, real-time external threat data can help. Having a better understanding of what is happening in the wild helps analysts identify and stop attacks when they happen.

## 4. Invest in a Comprehensive Platform

Most SOC stacks are a collection of single-purpose security tools acquired over time. Because of their single function, these tools become siloed and ineffective, rendering this approach unmanageable and expensive.

### The End of Franken-SOC

The answer lies in a unified, integrated platform that provides a holistic view of your extended ecosystem, including all of your tools, applications, and associated workflows. Silos are the enemy of efficiency. Bringing threat intelligence together with telemetry creates a more seamless workflow, surfacing issues sooner and reducing the time between detection and response.

Additionally, a platform approach eliminates the work and hassle involved with developing and maintaining third-party integrations.

Better visibility, quicker threat detection, and lower maintenance make a platform approach a triple win.

## 5. Use AI to Address SOC Staffing Shortages

The security industry is suffering from a staffing shortage, making it difficult to find and hire qualified personnel. Part of the challenge is that analysts need advanced skills, including mastering proprietary query languages. Further, analysts are drowning in alerts, unable to process all the issues on their daily task lists. It's a high-stakes job, and the conditions are stressful.

Natural language processing (NLP) is changing all that. Allowing analysts to ask questions in natural language instead of authoring complicated detections means that a Tier 3 analyst can do the work of a Tier 1 analyst, closing the skills gap without the ramp-up time.

AI can also help reduce alert fatigue. A best-in-class platform that enriches internal telemetry in real time with high-quality threat intel can replace analysts' initial triage, prioritizing and escalating only the issues that truly need attention. This reduces analyst workload and makes the job much less onerous.

Leading AI tools can also help analysts write clear, business-level summaries of incidents and threats, saving them time and upleveling the quality of SOC communications.

### Security and IT Operations Done Differently.

Anomali's Security and IT Operations Platform is the only solution that integrates ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP for visibility, analytics, and actions like you've never seen before.

### Visibility and Context

Anomali delivers real-time security insights — along with historical context — and correlates them with up-to-the-minute threat intelligence so SOC teams can take immediate action before an attack gains traction. Anomali's AI-Powered Security and IT Operations Platform pinpoints critical threats in a vast amount of data (seven-plus years of lookback!) at unprecedented speed. In fact, one Anomali customer reports reducing its complex query time from 48 minutes to 44 seconds.

### Integrated Threat Intel

Anomali ThreatStream, the leading 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. By correlating this external threat data with internal telemetry, analysts can better understand their security posture and in-progress attacks.

### Comprehensive Platform

Anomali provides seamless data analysis and better contextualization of threats, ultimately leading to more efficient detection and response. An integrated approach ensures that SOCs move beyond disparate tools and activities (and all the overhead that entails), and towards an approach that enables analysts to assess and respond with greater efficiency.

### Talent Enablement and Retention

At the center of the Anomali platform and core to its suite of solutions is the best-in-class intelligent Anomali Copilot — a powerful, security-optimized AI assistant that automates important tasks so your SOC team can work more productively. Empower your talent and leaders, be more efficient, and safeguard your organizations from cyber threats. In fact, Anomali platform automation frees up 50% (or more!) of your SOC team's days, which means reports, dashboards, and results in seconds, not hours.

Further, NLP empowers even the most inexperienced threat analyst to do sophisticated threat hunting and analysis quickly and inexpensively.

## Bonus: It Won't Break the Bank

Traditional SIEM tools and their associated storage costs can be significant cost drivers in the SOC. The cost of storing massive amounts of data (with limited visibility) over time is not trivial.

Since many SIEMs rely on expensive tools to provide logs and other data for analysis, the costs can quickly become overwhelming.

Anomali's Data Lake doesn't sit on another big data provider, so customers get to reap the savings. By only storing the data you need and using a modern, serverless architecture, Anomali's Data Lake can operate at scale without the cost.

## SAMA Cyber Security Framework: Compliance Made Simple with Anomali

### SAMA Cyber Threat 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 indicators of compromise (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 TTPs of cyber adversaries.
    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.

## Be Different.
## Be the Anomali.

As Saudi Arabia continues to position itself as a leading financial hub, cybersecurity is fundamental to maintaining competitive advantage and national economic resilience. Financial institutions must move beyond traditional security models to embrace intelligent, integrated platforms that can anticipate and neutralize emerging threats. Anomali stands ready to support UAE financial organizations in building secure, compliant, and future-ready security operations that protect critical national infrastructure.

Explore how Anomali can transform your cybersecurity approach and help you stay ahead of evolving digital risks — schedule a personalized demonstration.

## 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