

CASE STUDY

Turbocharged security resilience and control for an East African bank via MDR

Overview

- Private sector
- Banking
- 10,000 Employees
- East Africa

SharkStriker

www.sharkstriker.com

About

Our client was an East Africa based bank that offers a range of commercial banking services and products. It is reputed for its private banking, investment management, wealth management, asset management, and commercial and personal loan products.

Service Delivered

MDR as a Service

Metric	Before	After	Improvement
Mean Time to Detect (MTTD)	Hours-long detection cycle	Minutes	96.7% reduction
Mean Time to Respond (MTTR)	Hours-long response cycle	Minutes	>95% reduction
Alerts Generated	~700	~60	~91% reduction

What we integrated?

Category	Integrated Sources
Network and Perimeater	Fortinet Firewall
Endpoint	Cortex XDR
SIEM	IBM Qradar

The Problem

- An approaching audit
- Need to integrate SIEM into central bank SOC as per mandate
- No value from existing SOC service provider
- Alignment of existing stack with regulatory requirements

The Challenges

- A stack that was not operationalized despite having a SOC
- Fragmented visibility across SIEM and other solutions
- High volume of alerts
- Lack of timely security insights
- Identifying and addressing security and compliance gaps

The Solution

- Integrated, designed, configured and operationalized security stack
- Built a whole set of customizations for IBM QRadar - Detection engineering, alert optimization, and automation.
- Proactive threat hunting – for threats like the FortiBleed vulnerability
- Continuous threat intelligence & security advisory
- End-to-end compliance management to Rwanda's data protection and security regulations

The Outcome

- A unified stack with centralized visibility, control, and timely security insights, across IBM QRadar and other solutions.
- Enabled continuous threat hunting and improved detection through customized detection engineering, alert correlation, and ongoing rule optimization.
- Significant reduction in false positives, enabling analysts to focus on genuine security incidents and improving the overall detection accuracy.
- Timely security reporting - including dashboards with real-time insights, and regular advisories on emerging threats and vulnerabilities.
- Continuous improvement - through continuous security assessments, simulations, and awareness training and end-to-end support.

Challenges

- A stack that was not operationalized despite having a SOC.
- Fragmented visibility across SIEM and other solutions.
- High volume of alerts.
- Lack of timely security insights.
- Identifying and addressing security and compliance gaps.

A security stack that was not operationalized

One of the most financially costly challenges was that, despite having invested heavily in a security stack made up of top solutions like IBM QRadar for SIEM, Cortex XDR for endpoint, and a Fortinet firewall, they were not getting the enterprise-grade security they expected. The reason was that the existing SOC provider had not operationalized the stack with the appropriate configurations, optimized alerts, rules, or customized playbooks. With an audit approaching and a recent mandate by the Central Bank requiring their SIEM to be integrated with the central bank's SOC, they were in a dire situation that couldn't be solved just by adding more tools.

Fragmented visibility across security stack

The client struggled with fragmented visibility across SIEM, endpoint security, and network security tools. Despite having a SOC provider, their solutions were still operating in their own silo, holding their own slice of telemetry. Even though the client had a picture of their security posture health, it was not complete enough to improve resilience or deteremine the full path of an attack (if one happened). For a bank preparing for an audit, having top-notch security solutions in place without the full visibility meant a huge security gap that was unaddressed.

High volume of security alerts

Our client was receiving close to 700 alerts a month without a reliable way to separate genuine threats from noise. This was a direct consequence of a stack that was never tuned or optimized after deployment despite having hired a SOC provider. Due to this, analysts had to go through a flood of alerts manually instead of focusing on alerts that are real incidents. For an organization that had made a significant investment in IBM QRadar SIEM, this lack of accurate and actionable visibility was frustrating. The client was struggling to find a way to reduce alert noise, improve detection accuracy, and focus on real threats.

Lack of timely security insights

Without any shared context across their stack and a lack of timely insights reaching the right people at the right time, our client struggled with reactive as opposed to proactive security disabling them to act on time.

For an organization facing an approaching audit and a mandate for centralized oversight, this reporting lag made it challenging to demonstrate continuous monitoring and timely response that regulators expect.

Unaddressed security and compliance gaps

Aligning the existing security stack with regulatory requirements was a challenge without clear visibility of current gaps across the security posture.

It meant assessing the infrastructure from both a security and compliance perspective, which was challenging with a SOC provider that only had expertise in security. They were in need of a partner that offered them both technical and regulatory expertise without having to build one in-house.

Solution

- Integrated, designed, configured and operationalized security stack
- Built a whole set of customizations for IBM QRadar - Detection engineering, alert optimization, and automation.
- Proactive threat hunting – for threats like the FortiBleed vulnerability
- Continuous threat intelligence & security advisory
- End-to-end compliance management to Rwanda's data protection and security regulations

Solution

Operationalized security stack

Unified Microsoft's and third-party security tools into one integrated, operationalized, and managed platform.

Fully tuned and optimized SIEM

Fully configured and managed IBM QRadar with a full set of customizations that brought alert volume from ~700 alerts to ~70 alerts a month.

Proactive threat hunting and intelligence

Proactively investigated emerging campaigns like FortiBleed through dark web recon, credential exposure searches, and infrastructure mapping.

Continuous security improvement

Delivered ongoing threat intelligence and customized advisories to strengthen detection accuracy, risk mitigation, and response readiness.

End-to-end compliance management

Bridged compliance gaps and realigned detection, alert handling, and reporting to compliance requirements.

Operationalized security stack

Our client's security stack was made up of some of the top cybersecurity solutions being managed by an external SOC provider. These solutions included IBM QRadar for SIEM, Cortex XDR for endpoint security, and a Fortinet firewall for network and perimeter security. However, despite having a SOC provider, their stack was never fully operationalized, leaving the client with fragmented visibility, incomplete context, and limited control.

Through our MDR service, we integrated, configured, and managed their stack on our vendor-agnostic, open-architecture STRIEGO platform. We configured it based on the identification of misconfigurations and managed it using industry best practices. With centralized visibility, control, and a fully managed & integrated security stack, our client was ready with the unified stack that regulators expected to see.

Built a whole set of customizations for IBM Qradar

Despite having one of the top SIEM solutions in place, our client was struggling with staggering alert volume (close to 700 alerts a month) that was exhausting their team's bandwidth. Without any effective way to separate real threats from false positives, they were increasing their exposure to risk.

Through our MDR service, they got a team that offered them the dedicated vendor and domain expertise they needed to configure and operationalize their SIEM, which was integrated with STRIEGO.

We built a comprehensive set of customizations for IBM QRadar, from alert optimization and correlation to automated response playbooks. This helped not only bring down the alert volume from ~700 to ~60 but also improve their MTTD by 96.7% and MTTR by over 95% without any replacement or upgrade.

Proactive threat hunting – for threats like the FortiBleed vulnerability

Since our client was handling sensitive customer and financial data, any disruption from a cyber threat carried a significant operational and reputational risk.

Therefore, instead of waiting and reacting to suspicious activity, our threat hunting team proactively investigated emerging global campaigns across our client's environment, including the FortiBleed campaign that was unfolding at that time.

Through dark web reconnaissance, credential exposure searches, and infrastructure mapping, our team proactively assessed and monitored the environment for exposure. As a precautionary measure, we also recommended hardening measures for their Fortinet environment. By providing our client with timely global threat intelligence and threat indicators, we helped them stay ahead of threats.

Continuous security improvement

As a bank that was preparing for an audit, timely intelligence was critical to demonstrating ongoing, proactive monitoring that regulators expected to see.

We provided continuous threat intelligence and customized security advisories on emerging threats and vulnerabilities relevant to their environment. This helped them improve their detection accuracy, risk mitigation, threat prevention, and response.

End-to-end compliance management

Our client needed more than a technically sound security posture. They needed it to be aligned with Rwanda's data protection expectations. Without any dedicated expertise internally, our client faced a challenge identifying the hidden compliance gaps to be addressed. Through our team, they were able to address this challenge. They got the dedicated security and compliance expertise to realign their security posture with their compliance expectations. Our detection engineering, alert handling, and reporting practices were shaped with compliance in mind from the start instead of aligning them one-by-one to a checklist. This helped them become audit-ready in less time.

SharkStriker Action	Law N° 058/2021 requirement area addressed
Integrated IBM QRadar, Cortex XDR, and Fortinet firewall into one operationalized stack.	**Article 47** Measures to ensure security of personal data. Adopt appropriate, reasonable technical measures to prevent loss, damage, or destruction of personal data, and establish and maintain safeguards against identified risks.
Identified and addressed gaps in information security.	**Article 38** Duties of the data controller and the data processor **1°** - Implement appropriate technical and organizational measures as a duty of the data controller and data processor
Detection engineering, alert correlation, and rule optimization on Qradar.	**Article 47, 2°** Regularly verify whether personal data security safeguards are effectively implemented.

SharkStriker Action	Law N° 058/2021 requirement area addressed
Proactive threat hunting, including the FortiBleed campaign.	**Article 47, 1°** Identify foreseeable risks to personal data and establish and maintain appropriate safeguards against those risks
Continuous security improvement through threat intelligence and security advisory.	**Article 47, 3°** Ensure personal data security safeguards are continually updated in response to new risks or identified deficiencies
End-to-end compliance management, including pre-audit support.	**Article 43** Notify the supervisory authority of a personal data breach within 48 hours of becoming aware of it, supporting demonstrable, ongoing compliance oversight ahead of audit

Outcome

- A unified stack with centralized visibility, control, and timely security insights across IBM QRadar and other solutions.
- Enabled continuous threat hunting and improved detection through customized detection engineering, alert correlation, and ongoing rule optimization.
- Significant reduction in false positives, enabling analysts to focus on genuine security incidents and improving the overall detection accuracy.
- Timely security reporting - including dashboards with real-time insights and regular advisories on emerging threats and vulnerabilities.
- Continuous improvement - through continuous security assessments, simulations, awareness training, and end-to-end support.

Before		After
Fragmented visibility and limited control across security stack	→	**3+** vendors unified into one security stack with centralized visibility & control and timely insights.
High alert volume - ~700 alerts	→	**~91%** reduction in alert noise
Slow detection despite having one of the industry leading SIEM solutions	→	**96.7%** reduction in Mean Time to Detect
Security tuned as per annual security assessments	→	Continuous security improvement based on threat intelligence and advisories
Compliance status with Law N° 058/2021 unknown	→	Detection, response, and reporting aligned with **Law N° 058/2021**

“Despite having an industry-leading SIEM and a SOC provider overseeing it, we were struggling with hour-long detection, delayed response, and a weak compliance posture.

By becoming our single partner for security and compliance, SharkStriker has helped us go from fragmented to unified, operationalizing our security stack to be resilient and compliant with East Africa's regulatory expectations.”

- President

Phone: +1 925 5321900
Email: sales@sharkstriker.com
Website: www.sharkstriker.com

©2026 ©SharkStriker Inc. All rights reserved.

Visit SharkStriker