

CASE STUDY

Helped a public sector bank in South Africa modernize its cybersecurity with Microsoft

Overview

- Public Sector
- Housing Finance
- 200-300 Employees
- South Africa

SharkStriker

www.sharkstriker.com

About

Our client was a South African financial institution that was reputed for its digital and accessible financial services. Over the years, they have been one of the key drivers of economic growth in the region through its network of partners who help individuals and businesses grow sustainably.

Service Delivered

MDR for Microsoft

Metric	Before	After	Improvement
Mean Time to Detect (MTTD)	Hours-long detection cycle	Minutes	96.7% faster
Mean Time to Respond (MTTR)	Hours-long response cycle	Minutes	95% faster
Alerts Generated	~500	~100	~80% reduction

What we integrated?

Category	Integrated Sources
Network and Perimeater	Fortinet Firewall, Perimeter Firewalls, Network Switches
Endpoint	Microsoft Defender, Check Point Endpoint Security
Identity & Access	Microsoft Sentinel (Identity Monitoring)
Email	Mimecast, Checkpoint Email Security

The Problem

- An approaching audit
- Need for a modernized Microsoft-security-powered-SOC
- Alignment of existing stack with regulatory requirements (POPIA)
- Improve security maturity without expanding internal security

The Challenges

- No harmony between Microsoft stack and 3rd party tools
- Fragmented visibility
- High volume of alerts
- Limited expertise for establishing modernized Microsoft-powered SOC
- Lack of timely security insights

The Solution

- Integrated, designed, configured and operationalized Microsoft security stack
- Third party security integration
- Detection engineering, alert optimization, and automation
- Proactive threat hunting
- Continuous threat intelligence & security advisory

The Outcome

- A unified Microsoft-powered Security Operations Center (SOC) with centralized visibility, control, and timely security insights, across Microsoft and third-party security 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

- No harmony between Microsoft and Third-party tools
- Fragmented visibility and delayed insights that affected response times
- High alert volume that was affecting focus on what is important
- Limited expertise for a compliant and modernized Microsoft-powered SOC

No harmony between Microsoft and Third-party tools

Our client's security stack was made up of different solutions from different vendors: Defender & Sentinel from Microsoft, firewall from Fortinet, and endpoint & email security from Check Point. However, none of the tools operated in harmony to give a complete picture of the security.

Each tool operated in its own silo, generating alerts without any correlation or shared context between Microsoft and third-party tools. Since the client had already invested a lot in security, this disharmony was a primary gap between them and a resilient and compliant security posture.

Fragmented visibility and delayed insights when it matters the most

The team had security data, but it was fragmented and in isolation. And this was for all the telemetry across the infrastructure, including endpoint, network, and email layers. So, they had little to no context of the full attack path of an incident.

It didn't just make the context unclear but also affected how quickly a useful piece of information reached the right person at the right time. For an organization approaching audit, this was a big obstacle while trying to demonstrate the timely oversight that regulators expect.

High alert volume affecting focus on what is important

Their team was receiving close to 500 alerts a month, and the team was unable to distinguish whether they were a genuine threat or noise. High alert volume without correlation was slowing analysts down and increasing the probability of missing incidents.

The client wanted to address the challenge of alert volume without having to replace or upgrade anything.

Limited expertise for a compliant and modernized Microsoft-powered SOC

Our client needed both the vendor (Microsoft) and domain expertise (like endpoint, firewall, email, identity security) to establish a resilient and compliant Microsoft-powered security posture. As they were approaching an audit, they needed POPIA-specific dedicated compliance experts who could also help them align their security posture with POPIA's requirements.

Building domain, vendor, and compliance expertise from scratch wouldn't just be highly expensive, but also demand time that the client's audit timeline didn't allow. They needed a partner who could provide them all instead of relying on a tool that the internal team would take years to master.

Solution

Unified security stack

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

Detection engineering

Correlated & optimized alert rules with customized playbooks for automated response.

Proactive threat hunting

Ongoing hunting for attack paths and exploitable risks.

Threat intelligence & security advisory

Continuous threat intelligence and advisories on emerging threats and vulnerabilities.

POPIA compliance support

Dedicated experts offering end-to-end support for POPIA compliance.

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

Our client's security stack was made up of Microsoft Defender and Sentinel along with third party tools like Fortinet firewall, Check Point endpoint and email security. Through our MDR for Microsoft service, we integrated their stack on our vendor agnostic, open-architecture security platform, STRIEGO that unified telemetry across their stack.

This allowed them to correlate better with shared context that was missing before with Microsoft and third-party tools working in unison instead of isolation. They had a clear picture of their security posture across every layer without having to work on siloed tools.

Detection engineering, alert optimization, and automation

Our client's team was receiving close to 500 alerts a month with the team unable to tell whether an alert is about a genuine threat or noise. Through our team, they got the dedicated domain (SIEM, endpoint, and firewall security) and vendor expertise (Microsoft, Fortinet, CheckPoint) to configure, manage, and operationalize their stack. Once their stack was integrated on STRIEGO, we helped them bring the volume down through customized detection engineering, alert correlation, and rule optimization. This helped them reduce alerts from 500 to 150 in a month while improving their MTTD by 96.7% and MTTR by 95%. All this without having to replace or upgrade anything in their existing security stack.

Proactive threat hunting

Since our client was handling sensitive housing finance, customer, and financial data in a public-sector environment, any disruption from a cyber threat wouldn't just impact operations but also cause financial and reputational damage. Our threat experts conducted ongoing, proactive threat hunting across their environment.

Through early discovery of potential attack paths, exploitable risks, and exposed environments, rather than just relying on alerts to surface issues. Through early discovery of potential attack paths, risks, and exposed environments, the client gained a complete picture of what was happening across their infrastructure.

Continuous threat intelligence & security advisory

In the world of threats where attackers keep evolving their techniques, not being able to adapt can cost years of hard work. With continuous threat intelligence and regular advisories on emerging threats and vulnerabilities relevant to their environment, we helped the client add accuracy to their risk mitigation, threat prevention, and response.

For an organization approaching audit, timely intelligence wasn't just useful in establishing resilient security but also demonstrating ongoing oversight that regulators expect to see.

Dedicated support for POPIA compliance

We offered both the Microsoft domain specialists and the dedicated POPIA compliance experts to our client offering them a single partner for both technical buildout and regulatory alignment they needed ahead of audit.

POPIA compliance was where the unified correlated Microsoft powered SOC mattered the most.

Rather than treating compliance as a checklist or documentation exercise, our detection engineering, alert handling, and reporting practices were shaped with compliance in mind from the start. This enabled the client to walk into their audit with a security posture that was demonstrably aligned

SharkStriker Action	POPIA requirement area addressed
Integrated Microsoft and 3rd party tools into one operationalized stack	**Section 19(1)** Prevent loss damage, or unauthorized access to personal information through appropriate technical and organizational measures. **Section 19(2)(b)** Establish and maintain appropriate safeguards against identified risks.
Identified and addressed the gaps in data protection controls	**Section 19(1)** Prevent loss damage, or unauthorized access to personal information through appropriate technical and organizational measures.
Enabled File integrity monitoring via STRIEGO for round-the-clock security of data.	**Section 19(1)** Prevent loss damage, or unauthorized access to personal information through appropriate technical and organizational measures. **Section 19(2)(b)** Establish and maintain appropriate safeguards against identified risks.
CIS-based security posture assessments (STRIEGO)	**Section 19(2)(a)** Identify all the reasonably foreseeable internal and external risks to personal information. **Section 19(2)(C)** Regularly verify that safeguards are effectively implemented.
Detection engineering, alert optimization and automation	**Section 19(2)(b)** Establish and maintain appropriate safeguards against identified risks. **Section 19(2) (C)** Regularly verify that safeguards are effectively implemented. **Section 19(2) (d)** Ensure safeguards are continually updated in response to new risks or deficiencies.
Proactive threat hunting	**Section 19(2)(a)** Identify all the reasonably foreseeable internal and external risks to personal information. **Section 19(2) (c)** Regularly verify that safeguards are effectively implemented
Continuous threat intelligence & security advisory	**Section 19(2)(a)** Identify all the reasonably foreseeable internal and external risks to personal information. **Section 19(2) (c)** Regularly verify that safeguards are effectively implemented. **Section 19(2) (d)** Ensure safeguards are continually updated in response to new risks or deficiencies
Continuous security assessments, simulations, and awareness training	**Section 19(2) (C)** Regularly verify that safeguards are effectively implemented. **Section 19(2) (d)** Ensure safeguards are continually updated in response to new risks or deficiencies

Outcome

- A unified Microsoft-powered Security Operations Center (SOC) with centralized visibility, control, and timely security insights, across Microsoft and third-party security solutions.
- 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.
- A compliant security posture – with a Microsoft-powered stack and security controls that are aligned with POPIA requirements.

Before		After
Security tools operating in siloes with no correlation between Microsoft and third-party solutions.	→	Unified Microsoft-powered SOC with centralized visibility and control
Hours-long detection cycle	→	Mins mean time to detect
Hours-long response cycle	→	Mins mean time to respond
~500 alerts per month, mostly noise	→	~150 alerts per month, high signal
Static detection rules, no continuous improvement	→	Continuous threat hunting, detection engineering, and rule optimization
Delayed insights reaching decision-makers after issues escalated	→	Real-time dashboards, threat intelligence, and regular advisories on emerging threats
No demonstrable path to compliance ahead of audit	→	Microsoft-powered security stack with security controls aligned to POPIA

"We have brought our alert volume down by 70% and cut our mean time to detect from hours to minutes.

That alone was a big win for us, coming from fragmented visibility and little context. And you couldn't expect any less from a global cybersecurity company that means business.

Partnering with SharkStriker gave us the confidence we needed to walk into the POPIA audit that was just months away."

- President

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

Visit SharkStriker

©2026 ©SharkStriker Inc. All rights reserved.