



CASE STUDY

A Malaysian Oil & Gas company strengthened its security & compliance with MDR

Overview

- 📌 Private sector
- 📌 Oil & Gas
- 📌 51-250 employees
- 📌 Malaysia

About

Our client was a Malaysian Oil and Gas company that had been operating for more than 10 years. They were known for their Oil & Gas products and services, from production, fuel retailing, and lubricants to the supply of industrial & commercial fuels in Southeast Asia.

Service Delivered

MDR as a Service

Metric	Before	After	Improvement
Alert volume	~3000 alerts monthly	~100 alerts monthly	97% reduction
Mean Time to Detect (MTTD)	Hours-long detection cycle	Minutes-long detection cycle	94% reduction
Mean Time to Respond (MTTR)	Hour-long response cycle	Minutes-long response cycle	95% reduction

What we integrated?

Category	Integrated Sources
Firewall	Perimeter firewall
Endpoint	Microsoft Defender for Endpoint
Network	Network Detection and Response

The problem (their objective)

- 🔑 Securing a multi-branch OT environment without affecting production uptime.
- 🔑 Strengthen existing SOC capabilities.
- 🔑 Extend Network Detection & Response coverage.
- 🔑 Meeting Malaysian data protection obligations.

The Challenges

- 🔑 A complex multi-branch infrastructure with critical OT software.
- 🔑 Enforcing strong endpoint security without impacting production-critical software.
- 🔑 High volume of alerts (~3000 alerts) with false positives.
- 🔑 Limited visibility of hidden security risks like dormant former employee accounts.
- 🔑 No dedicated expertise to identify and bridge compliance gaps.

The Solution

- 🔑 Unified security across OT and IT with centralized visibility and control.
- 🔑 Security hardening and automation.
- 🔑 Strong endpoint security enforced without affecting uptime.
- 🔑 Identity & Access hygiene.
- 🔑 Alignment with regulatory expectations.

The Outcome

- 🔑 Fully unified and operationalized security stack with centralized visibility, control, and timely insights without disrupting production uptime.
- 🔑 Significant improvement in detection accuracy and improved focus on critical security risks and threats through the elimination of false positives.
- 🔑 Security response tuned to industry best practices for improved response accuracy and speed.
- 🔑 Continuous improvement of security with round-the-clock monitoring, continuous security advisories, and threat intelligence.
- 🔑 Enhanced readiness for Malaysia's Personal Data Protection Act requirements with dedicated compliance support.

Challenges

- 🔑 A complex multi-branch environment with critical OT software.
- 🔑 Endpoint security that wasn't configured to whitelist production applications.
- 🔑 High alert volume with false positives.
- 🔑 Limited visibility of hidden risks.
- 🔑 No dedicated expertise to identify and bridge compliance gaps.

A complex multi-branch environment with critical OT software

Our client operated business-critical OT software across multiple branch locations, with an estate that included servers, endpoints, firewalls, switches, and wireless LAN controllers. In such a complex setup, ensuring centralized visibility through a unison of telemetry across the infrastructure was a complex deployment, with many device types each needing its own log source configuration. Our client already had a network vendor, but they weren't supporting the deployment. They were looking for a partner who could take over for a successful rollout.

An unconfigured endpoint security solution that didn't whitelist production applications

One of the primary challenges for our client was that several of their business-critical OT applications behaved in ways that could be flagged by endpoint security tools as suspicious. Their EDR solution risked blocking legitimate software, and that too in a production environment.

If legitimate production-related software was blocked, it could cause disruption of operations. The client needed security expertise that helps them establish a balance between endpoint security and operational uptime without leaving any blind spots that can be exploited by attackers.

High alert volume with false positives

The client's team was struggling with a high volume of alerts, with many of them being false positives or redundant alerts. This made the team lose focus on real threats, as they had to check each alert before acting on it. Triaging was not just time-consuming but also caused inaccuracies in detection due to high noise. It multiplied their workload, with much of their effort going towards reviewing routine events rather than investigating new threats.

Limited visibility of hidden risks

Our client had little visibility into risks inside their own environment due to complexly connected systems and fragmented telemetry. They were unaware of red flags like active accounts belonging to former employees that generated repeated login failures because of the low coverage of monitoring that didn't extend to Microsoft 365. The endpoint-only monitoring was failing to offer visibility of east-west traffic across the OT environment. Coupled with limited network-level coverage and weaknesses in identity management, it made proactive and continuous security a challenge.

No dedicated expertise to identify and bridge compliance gaps

As a renowned Oil & Gas company operating for more than a decade, our client was handling massive amounts of data, including employee and customer information. However, without dedicated expertise on the team for compliance, it was challenging for them to identify the hidden security and compliance risks across their environment, which was highly complex, with interconnected systems and OT systems. Malaysia's Personal Data Protection Act (PDPA) required them to have certain safeguards in place for protection against loss, misuse, and unauthorized access to data. Any kind of security gap posed direct exposure to regulatory risk. They needed a partner who could help them proactively identify and bridge the gap.

Solution

- Unified security across OT and IT with centralized visibility and control.
- Security hardening and automation.
- Strong endpoint security enforced without affecting uptime.
- Identity and access hygiene.
- Alignment of security with regulatory expectations.



Unified security across OT and IT with centralized visibility and control

Integrated endpoint security, firewall, and NDR telemetry on the vendor-agnostic STRIEGO platform.



Security hardening and automation

Tuned detections to cut alert volume to fewer than 100 alerts from ~3,000 alerts.



Strong endpoint security enforced without affecting uptime

Fine-tuned EDR to exclude production-critical OT software.



Identity and access hygiene

Created a playbook for automated detection and disabling dormant accounts.



Alignment of security with regulatory expectations

Identified and bridged compliance gaps and realigned security with PDPA

Unified security across OT and IT with centralized visibility and control

We unified the client's security stack on our vendor-agnostic, open-architecture STRIEGO platform, including their perimeter firewall and Microsoft Defender for Endpoint. This gave their security team centralized security visibility and control of a complexly connected OT-IT network.

Our in-house firewall and networking specialists helped our client extend their visibility and NDR coverage, covering east-west traffic, correlating OT and IT telemetry, and onboarding log sources across every branch. This gave their security team unified visibility into security across production and corporate networks.

Security hardening and automation

By tuning the alert rules, our team helped bring the alert volume down from ~3,000 alerts monthly to fewer than 100 actionable alerts. Through automated playbooks, we streamlined the routine triage and response, hardening configurations against industry-benchmarked baselines. This resulted in higher alert fidelity and a significant improvement in detection (MTTD - 94% improvement) and response cycles (MTTR - 95% improvement), going from hours to minutes. It also shifted the team's focus from routine to deeper investigation and high-severity threats, helping them improve productivity overall.

Strong endpoint security enforced without affecting production uptime

The client needed strong endpoint security without affecting production uptime. So, we tuned the exclusion policies of Microsoft Defender for Endpoint. This way, production-critical OT software was no longer at risk of being blocked, and strong endpoint security against genuine threats was still preserved. Rather than applying a broad set of exceptions, we scoped each exclusion to the specific OT application, mitigating the protection gap. We continuously tuned/configured the stack from time to time instead of a one-time activity. This ensured that the client's environment remained resilient in an evolving threat landscape.

Identity and access hygiene

While integrating telemetry from Microsoft 365, we discovered multiple former employees' accounts were still active and generating repeated logins. This posed a significant risk to the security of the organization. Therefore, we disabled the accounts immediately and customized a playbook that flags/disables a dormant/former employee account based on login-failure analysis. This ensured that inactive accounts are automatically flagged and disabled without needing manual intervention.

This shifted the client's security from discovery by chance to proactively averting risks by managing access, automatically flagging/disabling dormant/former employee accounts through an established process.

Alignment of security with regulations

The client didn't have the dedicated in-house expertise to identify and address security and compliance gaps. We solved this by offering a team with dual expertise in cybersecurity and compliance and assessing their environment against PDPA's security requirements. We offered them the end-to-end support they needed to bridge the identified compliance gaps, develop policies for data protection and monitoring, and ensure documentation.

Instead of being a one-time activity that was carried out later, compliance was built into security from the start. Through continuous monitoring, proactive threat hunting, and continuous security improvement (through security advisories), we helped the client stay compliant with the evolving PDPA compliance expectations.

SharkStriker Action	PDPA requirement area addressed
Integrated security solutions into one unified and operationalized stack.	Section 9(1) Security Principle Take practical steps to protect personal data from loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.
Detection engineering and alert optimization	Section 9 (1)(a) Security Principle Security measures must be appropriate as per the nature of the personal data and the risk of loss, misuse, modification, unauthorized or accidental access or disclosure, alteration/destruction.
Production-critical OT software excluded from EDR.	Section 9 (1)(a) Security Principle Appropriate endpoint-level safeguards as per the risk without affecting production.oversight ahead of audit.
Proactive threat hunting, global threat intelligence, and security advisories	Section 9 (1)(a) Security Principle Ongoing safeguards against all the emerging risks to personal data.
Streamlined reporting and security policy development	Section 12 (B)(1) Data breach notification When a personal data breach has occurred, the data controller shall notify the Commissioner as soon as practicable and in the form determined by the Commissioner.

Outcome

- A fully unified and operationalized security stack with centralized visibility, control, and timely insights without disrupting production uptime.
- Significant improvement in detection accuracy and focus on critical security risks and threats through the elimination of false positives.
- Retuned security response against industry- trusted baselines for improved response accuracy and speed.
- Continuous improvement of security with round-the-clock monitoring and continuous security advisories & threat intelligence.
- Enhanced readiness for Malaysia's Personal Data Protection Act requirements with dedicated compliance support.

Before		After
Fragmented visibility across a multi-branch OT/IT environment.	→	3 sources (Microsoft Defender for Endpoint, NDR, and perimeter firewall) unified on STRIEGO platform for centralized visibility and control.
High alert volume - ~3000 alerts a month	→	97% reduction in alert volume with fewer than 100 actionable alerts.
Hour long detection cycle	→	94% reduction in MTTD
Hour long response cycle	→	95% reduction in MTTR
Compliance status to PDPA unknown	→	Detection, response, and reporting aligned with PDPA requirements

“ Ensuring a balance of resilient security and undisruptive operation was our biggest concern. SharkStriker took the time to understand how our OT and IT environments were connected and helped us secure our infrastructure across branches, unlocking the visibility we needed to maintain our productivity without worrying about risk or disruption. “

- CEO

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

Visit SharkStriker

