

CASE STUDY

Helped a Malaysian critical infrastructure organization uncover a hidden compromise with SOC-as-a-service

Overview

- Public sector
- Water supply services/utilities
- 200-400 employees
- Malaysia

SharkStriker

www.sharkstriker.com

About

Our client was a Malaysian water utility provider known for its massive and longest distribution network. It is one of the oldest providers in the country, offering an uninterrupted supply of water across 10 states, making it an essential part of the critical infrastructure.

Service Delivered

SOC-as-a-service, Incident Response

Metric	Before	After	Improvement
Mean Time to Detect (MTTD)	Months undetected	Same day detection	>97%
Incidents detected	Two undetected for months	>5 Critical escalations flagged on the same day	99% alert noise removed
Cost of damages	300+ endpoints at risk	Complete infrastructure secured, including 300+ endpoints	> RM 1 million Saved (from the cost of data breach)

What we integrated?

Category	Integrated Sources
Firewall	Perimeter Firewalls
Endpoint	Sangfor EDR (deployed across 300+ endpoints)

The problem (Their Objective)

- Sanitizing an infected/exposed environment from two consecutive cyber attacks.
- Securing critical systems and data.
- Operationalizing security stack without expanding internal team.
- Aligning security posture with regulatory and compliance needs.

The Challenges

- No systematic IR in place to identify, contain, and remediate.
- Limited/no visibility across critical systems and wider environment.
- Unconfigured tooling with high alert volume and false positives.
- Limited expertise to operationalize existing stack.
- No mechanism or expertise in place for meeting compliance expectations.

The Solution

- Comprehensive threat hunting and investigation.
- Threat containment and environment sanitization.
- Integrated, configured, and operationalized security stack including third-party EDR solutions.
- Comprehensive security and compliance guidance.

The Outcome

- Secured and sanitized infrastructure, including the most sensitive systems like the production billing database and the GIS infrastructure from exposure.
- A fully operationalized security stack with centralized visibility, control, and timely insights and 24/7 security support.
- Improved detection accuracy and focus of security team on critical security alerts due to a massive reduction in false positives.
- A systematic IR mechanism in place with the required processes, procedures, and clarity of roles and responsibilities.
- Enhanced readiness for regulatory requirements with multiple compliance-friendly formal IR and EDR analysis reports.

Challenges

- Limited/no visibility across critical systems and wider environment.
- Unconfigured tooling with high alert volume and false positives.
- Limited expertise to operationalize existing stack.
- No systematic IR in place to identify, contain, and remediate.
- No expertise in place for meeting compliance expectations.

Limited/no visibility across critical systems and wider environment

Our client's existing monitoring only covered 32 designated servers. There was no telemetry emitted from the wider environment, including workstations, branch offices, and several hundred additional endpoints across their complex IT infrastructure. Their most sensitive systems, including their billing database and GIS infrastructure, were invisible to their detection tools. This limited visibility gave an added advantage to the threat that was already inside the network.

The adversary had domain-level access, had weaponized Active Directory infrastructure, adapted to defensive maneuvers, and was targeting the client's billing systems, preparing for a ransomware attack.

Unconfigured tooling with high alert volume and false positives

The client's existing security stack comprised a perimeter firewall and a third-party solution, Sangfor EDR, that was deployed across 300+ endpoints.

It was operating primarily in alert mode with a high volume of false positives, limited coverage, and inconsistent policy enforcement. With a team already struggling with limited visibility, getting alerts that can't be trusted or acted upon with confidence only worsened the situation. It gave more opportunity to an active adversary that was actively working on defense evasion.

Limited expertise to operationalize existing stack

Due to limited expertise, our client was finding it challenging to identify configuration gaps across their stack, operationalize it, and interpret the telemetry it produced.

Undiscovered misconfigurations, unaddressed security gaps, and limited visibility all created more entry points for attackers.

The increased exposure to security risks made our client more susceptible to financial damages from non-compliance and cyber incidents.

The global widening of the cybersecurity skills gap, rising cost of security solutions, and increased pressure to meet regulatory obligations made it a real challenge for them to address security gaps and operationalize the existing stack without retooling or expanding the internal team.

No systematic IR in place to identify, contain, and remediate

Our client's environment had no clean baseline from day one of our engagement. They had already experienced two security incidents with no professional incident response ever conducted. There was no systematic mechanism in place for incident response.

No documented playbooks, established escalation paths, or shared understanding between the SOC and IT team on how to coordinate during an active incident.

For our SOC team, it meant expecting high risk exposure and a starting point that had a pre-existing attacker foothold as opposed to a clean environment.

No expertise in place for meeting compliance expectations.

As a national critical infrastructure organization, it was expected of our client to timely address risks across its infrastructure and demonstrate that its environment was secured through active security monitoring. However, they didn't have any expertise on the team to timely address risks and meet the changing regulatory expectations.

Without any mechanism in place for evidence like formal incident documentation, auditable evidence of remediation activity, and a structured reporting mechanism. This exposed them to operational and compliance risks, especially in a compliance environment where regulators keep changing their expectations of organizations.

Solution

- Comprehensive threat hunting and investigation
- Threat containment and environment sanitization
- Integrated, configured, and operationalized security stack
- Comprehensive security and compliance guidance

Comprehensive threat hunting and investigation

Investigated and tracked an active domain-level threat actor and pre-ransomware activity before execution.

Threat containment and environment sanitization

Same-day escalation of critical findings, with immediate isolation guidance and continuous remediation roadmap.

Integrated, configured, and operationalized security stack.

Integrated security stack including Sangfor EDR on vendor-agnostic security platform STRIEGO for unified visibility & control.

Continuous incident reporting and advisory support

Delivered 25 detailed reports mapping attacker TTPs to MITRE ATT&CK and offered timely advisories.

Security and compliance guidance

Offered end-to-end guidance to align detection, response, reporting, and other security practices with Malaysia's regulatory obligations.

Comprehensive threat hunting and investigation

Since our client experienced two cyber incidents before approaching us without having engaged in formal incident response, we discovered that our client's environment was far from a clean slate. Rather than waiting for symptoms to surface, we began our threat hunting and investigation. Our SOC team raised multiple critical security tickets and documented the first two IR reports in the first week of commencement.

Over the course of 72 days, we investigated and tracked a skilled, adaptive threat actor operating with domain-level privileges across the client's infrastructure. We identified the core propagation mechanism, named the specific accounts and scripts involved, and documented the attacker's anti-forensic techniques. Our team documented every pivot as the attacker tried to evade every defensive maneuver, moving between scripting interpreters, staging infrastructure, credential techniques, and persistence methods. Our investigation uncovered an active threat targeting the production billing database with proof of pre-ransomware staging activity, including credential dumping, exfiltration, and lateral movement tooling before the encryption was executed.

Threat containment and environment sanitization

We shifted our focus to containment and sanitization once we detected compromise. We immediately escalated the detected pre-ransomware staging activity to the client on the same day it was identified. We gave immediate isolation recommendations, with hosts flagged for forensic preservation, and highlighted the urgency of a domain-level credential reset.

Throughout the IR activity, we identified and closed gaps that can let attackers go undetected for months. We offered a prioritized remediation roadmap with our first IR report, continuously improving it as the attacker adapted. It ensured that containment kept pace with the actively evolving threat, as opposed to a one-time fix.

Integrated, configured, and operationalized security stack

Our client's existing security stack, including their perimeter firewall and Sangfor EDR, was integrated into our vendor-agnostic security platform STRIEGO. This allowed them to extend monitoring and visibility from a fraction of the attack surface (32 servers) to a tenfold increase (300+ endpoints).

Our team configured their existing Sangfor EDR with industry best practices, addressing gaps like excessive alert generation, inconsistent policy enforcement, and high false positives.

Rather than just flagging the gaps, our team enabled active prevention mode, built whitelist recommendations, resolved policy inconsistencies, and realigned detection categories, going beyond standard monitoring to fully operationalize the stack.

Continuous incident response and advisory support

Over 72 days of incident response, our SOC team delivered 25 detailed EDR and telemetry reports, each an improved version from the last.

These were more than just alert summaries, offering a complete, real-time picture of the threat with quantitative event analysis, MITRE ATT&CK TTP mapping, period-over-period comparisons, false-positive triage, and prioritized recommendations.

It was reinforced with continuous advisory support from scoping discussions, compromise methodology walkthroughs, and joint troubleshooting calls with the Sangfor team. All this was backed up with structured documentation offering the client an auditable record of oversight.

End-to-end compliance support

As a reputed state-owned water utility services provider and a part of the nation's critical infrastructure, our client was obligated to comply with multiple data security regulations. These included Malaysia's Personal Data Protection Act 2010, CNII obligations under the National Cyber Security Policy, and broader operational expectations placed on state-owned utilities.

Rather than treating compliance as a separate checklist bolted on afterward, we aligned our client's detection, response, and reporting practices with the compliance requirements from the start.

SharkStriker Action	Regulatory area addressed
Integrated security stack including Sangfor EDR and firewall into one platform for a unified operationalized stack.	PDPA 2010 - Security Principle (Section 9) - practical steps to protect personal data from loss, misuse, or unauthorized access
Identified and addressed existing data exposure risks	PDPA 2010, Security Principle(Section 9) - prevention of unauthorized access to personal data. CNII obligations - protection of critical infrastructure systems from compromise.
Enabled round-the-clock visibility	CNII obligations - continuous monitoring and protection of systems designated as critical national infrastructure.
Detection engineering, alert optimization, and stack configuration	CNII obligations - Incident detection and response for critical infrastructure safeguarding of billing and customer data integrity
Remediation guidance with formal written follow-up and advisories	PDPA 2010, Security Principle (Section 9) Maintaining and updating safeguards Governance evidence for regulators and oversight bodies

Outcome

- Secured and sanitized infrastructure, including the most sensitive systems like production billing database and GIS infrastructure, from exposure
- A fully operationalized security stack with centralized visibility, control, and timely insights and 24/7 security support
- Improved detection accuracy and focus of security team on critical security alerts due to a massive reduction in false positives
- A systematic IR mechanism in place with the required processes, procedures, and clarity of roles and responsibilities
- Enhanced readiness for regulatory requirements with multiple compliance friendly formal IR and EDR analysis reports.

Before		After
Already compromised environment with unknown exposures and footholds.	→	Complete attack campaign involving **308+** host coordinated attack campaign uncovered. Domain-level actor identified, contained, and remediated before ransomware execution.
Monitoring limited to a fraction of attack surface - 32 designated servers.	→	**10X** expansion of monitoring – covering **300+** endpoints, servers, and infrastructure.
EDR running in alert-only mode with high false positives.	→	EDR shifted to active prevention mode with **99%** elimination of false positives.
Reactive reporting with an incomplete picture of active threat.	→	**25** detailed reports delivered over **72** days with TTPs mapped to MITRE ATT&CK.
Compliance status with Malaysian regulations unknown.	→	Detection, response, and reporting aligned with PDPA and CNII obligations.

"Thanks to SharkStriker, we went from exposed to resilient! They helped us not just find an active threat targeting our critical assets but also address gaps we didn't know existed. With their expertise, we were able to expand our monitoring by 10x, eliminate noise, and become compliance confident."

- President

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

©2026 ©SharkStriker Inc. All rights reserved.

Visit SharkStriker