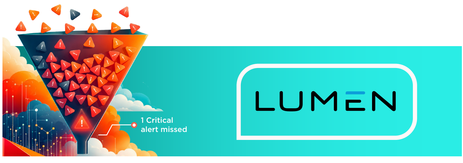

From Alert Overload to Automation-First: Your SOC Transformation Journey

Your SOC generated signals but did not effectively identify or act on them.

In various breach investigations, alerts were present. They were just buried — lost in a sea of noise, false positives, and disconnected tools.

86%↑

of organisations experienced more cyberattacks compared to the previous year[1]

AI has compressed ransomware build time from 12 hours (2021)- 3 hours (today)-projected 15 minutes (2026+)[2]

92%

of respondents indicated that the cost of cyberattacks increased by more than 10% year over year[3]

The Cost of Inaction

Making the wrong processes faster just gives you more of the same — more blind spots, more waste, and more burnout. Here's what APAC security leaders are struggling with right now:

Detection Gap

42% struggle with real time threat detection[1]

Talent Shortage

37% face cybersecurity talent shortages[1]

Visibility/Blind Spots

34% lack visibility across expanding attack surfaces[1]

Tool Sprawl

60% are not confident they properly manage their security tools[1]

Where are you on the Journey?

SOC optimisation and transformation arent a single leap — it's a structured progression. Most APAC enterprises sit somewhere on this path. The key is knowing where you are today so you can plan what comes next.

SOC Optimisation | **SOC Transformation**

01 Fragmented

Best-of-breed tools, low integration. Siloed visibility leads to duplication and alert fatigue.

What can you do?

Take a SOC Readiness Assessment – Am I ready for a SOC?

02 Coordinated

Moderate integration with shared workflows. Improved response efficiency but still manual-heavy.

What can I do?

Take a SOC Maturity Assessment – How effective is my SOC?

03 Unified

Single platform, centralised policies, common controls. Simplified management and lower risk.

What can I do?

Take a SOC Transformation Assessment – How do I modernise at scale?

04 Intelligent Platform

Enhanced visibility and orchestration via AI. AI-assisted detection, predictive analytics, and resilience-focused operations.

What can I do?

Consider Co-Managed SOC – Operate at scale, 24x7

83% **of Asia/Pacific enterprises are looking to partner with service providers to deliver their top security investment priorities.[3]**

What happens when you transform (or What Good Looks Like)

Organisations that embrace an automation-first, AI-driven SOC model may experience improvements in operational efficiency, response workflows, and resource utilisation.

Faster Response

98% reduction in MTTR* [2]

Certain reported deployments have achieved reductions from days to minutes in specific use cases.

Fewer Incidents

75% reduction in incident volume* [2]

AI-driven stitching and correlation dramatically cuts noise.

Automated Resolution

86% of incidents resolved automatically* [2]

Analysts freed to focus on strategic, high-value work.

*Based on Palo Alto Cortex XSIAM customer case studies and reported results. Actual outcomes will vary depending on customer environment, configuration, data quality, operating model, and implementation.

Supporting Benefits

- Independent identification of automation and AI-enabled opportunities
- Reduction of manual L1 effort through workflow modernisation
- Stronger alignment with regulatory and operational expectations
- A defensible roadmap and business case to support strategic investment

Work with a Partner who's been in the Trenches — not just on the Sidelines.

Lumen doesn't just advise on SOC transformation. We run SOCs. Every day. Across the region.

- Global SOCs across 4 continents – including 4 in APAC (Tokyo, Singapore, Melbourne, Bangalore)
- Black Lotus Labs - Monitors ~46,000 C2 servers, and 200+ billion NetFlows sessions daily
- ~2,500 Clients subscribing to Lumen Security Services Globally
- Aligned to relevant frameworks such as NIST CSF, MITRE ATT&CK®, ASD Essential 8, APRA CPS 234, ISO27001, where applicable

The maps provided are for visual guidance only and are not drawn to scale. They should not be considered as an accurate portrayal of official, geographic, political, or administrative divisions. These maps are a simplified depiction and may not reflect precise boundaries. They are meant for basic reference purposes only. The map information should not be taken as legal or professional advice, and no guarantees or warranties are made regarding the precision or completeness of the data shown.

"Lumen's wide threat coverage extends beyond endpoints and network into areas such as cloud, identity, email, IoT, and OT environments, providing customers with broader visibility and protection across hybrid environments."[4]

Not sure where you sit on the journey? Lets find out!

Lumen's **complimentary SOC Scoping Assessment** is security specialist led session to evaluate your organisation's objectives to provide immediate clarity on the scope and expected outcomes. Thereafter, you may wish to proceed for a structured, two weeks detailed assessment that evaluates your organisation's readiness across people, process, and technology.

Whether you're evaluating whether to build, buy, or co-manage a SOC — this assessment gives you the clarity and confidence to take the right next step with executive, boards, or external partners.

Book Your Complimentary SOC Scoping Call Now

Find out more at Lumen Technologies or contact us at apac.mail@lumen.com to kickstart a conversation.

Source:
1. IDC Infobrief, The new cybersecurity equation: Risk, Response, and Business Outcomes, Feb 2025, IDC #US53083025
2. Palo Alto, Cortex XSIAM Next Generation SOC Platform, 2025
3. IDC, The AI Security Shift_Fuelling the Next Stage of Cybermodernisation, Dec 2025, #AP24254510
4. IDC MarketScape: Asia/Pacific (Excluding Japan) Managed Detection and Response Services 2025 Vendor Assessment, Sep 2025, IDC #AP52998725

LUMEN