LOGICALIS
Architects of Change

Clarity at Machine Scale with MXDR

Escape the black hole of security spending

Contents

It's time to get a clearer view

Despite increased spending in cybersecurity across the Asia-Pacific (APAC) region, many organisations are still losing ground to attackers. These companies are also realising that simply throwing more money at the problem isn't making it go away. A more in-depth understanding and strategic approach is needed.

The APAC results of the 2025 Logicalis Global CIO Report revealed the depth of the challenges facing CIOs when it comes to cybersecurity. Let's review some of the data.

- Over 81% of organisations in APAC said the number of cyberattacks had increased or remained the same compared to the year before.
- More than half of all CIOs in APAC found security patch systems too complex, potentially leading to vulnerabilities.
- While two-thirds of CIOs say their current spend fully meets their organisation's needs, 45% say they have overinvested in security solutions they haven't needed.
- Only 63% say they are confident they can pinpoint any security gaps.
- AI-driven attacks and compromises are now one of the top three most reported incidents. Nearly three out of every four CIOs are aware of rising credential leak risks.

In its latest State of AI Security report , Cisco outlined several emerging AI security risks and attack vectors, including direct compromise of AI assets and supply chain. Emerging attack vectors were found to be targeting large language models and AI systems, using jailbreaking, indirect prompt injection attacks, data poisoning and data extraction attacks.

In brief: the attacks are rising in number, becoming more sophisticated and are pervasive, while the product solutions are often complex, overprovisioned and not fully understood. Meeting the security challenge requires a strategic mindset and a set of skills which are increasingly in short supply.

See the whole picture with holistic visibility

Logicalis believes the key to escaping the security spending black hole is clarity through **holistic visibility** - a unified view of the entire environment on one intuitive platform. This holistic view transforms raw data into actionable intelligence, closing the confidence gap for Security Operations (SecOps). CISOs and leaders at Security Operations Centres (SOCs) often struggle with overwhelming volumes of data, not a lack of it. They need smarter systems that can help by reducing 'alert fatigue', validating threats, automating investigations and guiding their responses.

True security confidence no longer comes from how fast you can detect attacks or the breadth of coverage. It comes from having clearer verdicts and knowing the precise next steps. Elite security teams empower its analysts to validate alerts, dismiss false positives, explain attacks to executives, and act decisively on weak signals.

Logicalis global partnership with Cisco, focuses on closing the cognitive gap by building solutions that bring disparate security intel together, providing context and intelligent automation to deliver trusted and explainable decisions. Without this form of overarching visibility, security investments will continue to feel like a black hole.

> We've seen a "tidal wave" of demand for cybersecurity services amidst a growing skills gap, emphasising the need for advanced visibility and clear security metrics for organisations.

Lee Chong-Win, CEO, Logicalis Asia Pacific

Get clarity at machine scale using AI-driven Managed XDR

Secure your path to confidence with MXDR

Quickly identifying an attack is just the beginning. What's more critical is knowing what comes next and having confidence in the steps to take.

This is where managed extended threat detection and response (MXDR) comes into play, specifically Cisco XDR as a managed service. It offers a transformative and holistic solution that can supercharge a team's ability to adapt and react. This unparalleled visibility into cyberattack chains leans on AI-powered automation and global threat intelligence for 24/7 detection, analysis, and response. Combine this with Logicalis's managed SOC capabilities, and it can deliver next-level security coverage and a faster route to actionable answers. CIOs can quickly go from a position of uncertainty to clarity and confidence.

Cisco XDR doesn't require a skilled or experienced analyst to access new capabilities and take confident action. It augments decision-making with Agentic AI to investigate and understand security signals, and provide all the supporting evidence needed. Once instant attack verification is automatically activated, Agentic AI is alerted across multiple vectors. It then kicks into gear to determine real threats, reduce false positives and speed up investigations.

Thanks to these AI-led investigations, analysts can begin to understand attacks in less than 30 seconds using the Cisco XDR Attack Storyboard. It's how holistic visibility becomes possible, providing a dynamic attack graph (mapped against MITRE ATT&CK tactics) and plain-language summaries for all stakeholders. Meanwhile, XDR Forensics automatically collects deep evidence across endpoints, letting analysts determine the root cause with a high degree of confidence. Threat detection and zero-trust enforcement can also be integrated in real-time, with instant cut-off for compromised users and devices.

Security leaders are often judged by their response capabilities. With Cisco XDR, leaders gain clear verdicts, confident decisions and accelerated detection and response, without requiring any additional skills. Both versatility and accuracy are what make XDR a suitable and elastic solution for small teams right up to global SOCs. It delivers expert-grade and AI-driven capabilities to chart a scalable path to SecOps confidence.

Unlocking next-gen security capabilities across APAC

According to the latest Logicalis CIO report, the incidence of cyberattacks in APAC is very high. In the past year, 91% of organisations reported having an incident, while more than half (53%) experienced multiple breaches - 10% above the global average. In response Logicalis has partnered with Cisco to reshape the security narrative in APAC.

The holistic visibility and capabilities provided by MXDR seamlessly integrates current security toolsets giving customers an advanced and effective cybersecurity solution while optimising security spending. In APAC, the managed service is delivered via Logicalis's 24/7 SOC in Malaysia, and backed by its global SOC network.

Logicalis's global SOC framework combines local expertise with global threat intelligence, to provide high levels of threat visibility and compliance, proactively anticipating and neutralising threats.

With the surge in demand for cybersecurity skills, and the pressures of a global skills gap, Logicalis continues to strategically invest in regional SOCs around the world. The company was the first partner in APAC to launch Cisco XDR as a global managed service (MXDR), giving customers across the region access to AI-driven Security protection. In addition, Logicalis recently announced they were first to achieve the 'Cisco Powered' specialisation for Managed XDR, meaning they've passed a rigorous audit process on their XDR solution and the Managed Services they provide to customers.

Understand your readiness and take control

The focus of cybersecurity in future is going to shift towards being more proactive than reactive. Solutions like MXDR empower CIOs with security that thinks, learns, and acts quickly, providing clear insights, precise actions, and intelligent automation.

To determine if MXDR could benefit your business, Logicalis offers a free and vendor-neutral MXDR readiness assessment. It takes less than 10 minutes to complete, and identifies your current security posture highlighting where MXDR can make a tangible difference.

These areas include:

- **Process and People:** Readiness of your security team and workflows.
- **Remediation and Recovery:** Your organisation's resilience and recovery ability.
- **SecOps Efficiency:** How effectively your security team responds to threats.
- **Visibility:** Extent of security activity insight across your IT environment.
- **Threat Detection:** Your ability to accurately detect, validate, and prioritise threats.

Based on your assessment, Logicalis provides a personalised report identifying strengths and opportunities to strengthen your security posture with actionable recommendations.

Logicalis MXDR Readiness Assessment

Optimising your security operations, so you can focus on what matters - driving business forward.

Take the assessment now