LOGICALIS
Architects of Change

Closing the Security Maturity Gap

Benchmarking best practice security operations

Contents

About the report

Logicalis' latest cyber security report draws on 357 responses from IT and security professionals across EMEA and Asia Pacific. It benchmarks maturity across the capabilities that define effective security operations — ownership, 24x7 response, visibility, detection, incident readiness and access to external expertise — and identifies the practices that can help organisations close the gap.

Executive summary

Cyber security is entering a new operating era. AI is increasing the speed, scale and adaptability of both attack and defence, while expanding digital estates make complete visibility harder to achieve. In this environment, awareness and investment are no longer enough. Organisations need the readiness to detect and respond continuously, the maturity to coordinate people, processes and technology, and the resilience to recover and adapt when compromise occurs.

Across 357 survey responses from key markets in EMEA and Asia Pacific, Logicalis' data shows meaningful progress, but also a persistent gap between ambition and operational capability:

41% of organisations now have a separate security function from IT

40% use real-time automated threat intelligence

33% have centralised SIEM or XDR with automated correlation

34% say they are fully resourced and proactive

64% do not have a fully mature 24x7 security operation

74% are not extensively using security automation

The findings describe a market in transition to maturity rather than one defined only by underinvestment. Organisations are building the components of modern cyber defence, but many have not yet connected them into a continuous, intelligence-led operating model.

Together, the findings reveal a clear maturity journey: establish ownership and capacity; extend response beyond business hours; connect asset, telemetry and threat intelligence; test and automate incident response; and use external expertise to accelerate progress where internal capability is constrained. The organisations closing the gap are not simply adding more tools. They are building adaptive security functions that can anticipate, act, recover and learn.

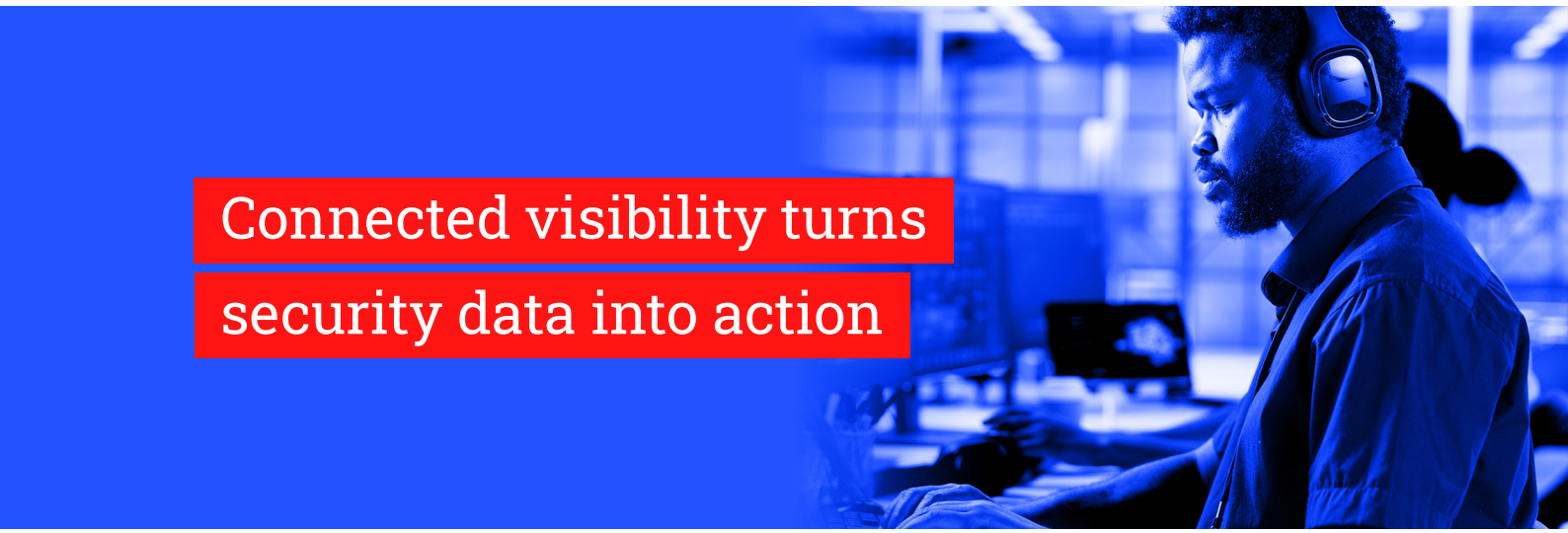
Clear ownership is the foundation of security maturity

The first signal of maturity is ownership. The survey highlighted that many organisations are establishing clearer accountability for cyber security with 41% of respondents operating with a clearly separate security function and ownership model, while 24% have dedicated security leadership with some overlap with IT. Together, that means that nearly two-thirds of organisations have started to distinguish security from general IT operations. The value is not simply organisational separation, but clearer accountability, stronger governance and faster decision-making when priorities compete or incidents demand a rapid response.

However, 36% of organisations still manage security primarily through IT teams. This can create challenges as threats evolve. In fact, 39% say they manage day-to-day security tasks well but struggle to keep pace with emerging threats, while only 34% say they are fully resourced and proactive across both routine operations and new risks.

> **39%** of organisations say they manage day-to-day security tasks well but struggle to keep pace with emerging threats.

Team size further highlights the gap. 28% of organisations have ten or more dedicated security professionals, but 26% have no dedicated security team and rely on IT resources instead. Mature organisations address this by clearly defining security ownership, protecting specialist capacity and bringing in external expertise when needed. The goal is not a standalone security team for its own sake, but a security operating model with clear accountability, sufficient expertise and the authority to respond as threats evolve.



Connected visibility turns security data into action

Visibility is the foundation of effective security. Yet 45% of organisations still maintain asset inventories manually, while only 1% have comprehensive automated inventories. A further 14% have only partial visibility and 8% do not maintain an inventory at all. As a result, almost 70% of organisations lack either complete visibility or automated asset management, making it harder to understand risk, prioritise vulnerabilities and respond quickly.

> **70%** of organisations lack either complete visibility or automated asset management.

Asset visibility is about more than keeping records up to date. Without a clear view of assets across cloud, SaaS, remote endpoints and third-party environments, organisations cannot accurately assess exposure or ensure security controls are working. Mature organisations treat asset inventory as a continuously updated source of security intelligence, linking assets to ownership, business importance and risk.

The same challenge exists with security monitoring. While 33% of organisations use centralised SIEM or XDR platforms with automated correlation, the majority still face visibility gaps. 27% have SIEM or XDR tools but with limited visibility, 24% collect logs but cannot correlate them effectively, and 14% still rely on locally stored logs. In other words, 65% of organisations lack fully integrated and automated security telemetry, limiting their ability to detect and respond to threats quickly.

Mature organisations go beyond collecting data. They connect telemetry across the environment, enrich it with asset and threat intelligence, and use automation to turn signals into prioritised action.

Continuous response capability defines security maturity

The ability to respond continuously remains a challenge for many organisations. While 36% of respondents report fully operational 24x7 security operations with dedicated staff, 64% do not yet have that capability. Among them, 17% rely on rotating on-call teams, 31% can monitor activity outside business hours but have limited response capability, and 16% do not actively monitor or respond after hours.

31% of organisations can monitor activity outside business hours but have limited response capability.

The data highlights a clear and important distinction between visibility and operational readiness. Monitoring activity outside business hours is valuable, but without the ability to investigate and respond quickly, organisations remain exposed to evolving threats. The 31% that can monitor but have limited response capability illustrate this challenge. They may detect potential incidents, but lack the resources, processes or coverage required to act consistently when risk emerges.

Threat activity never stops, and security maturity is increasingly defined by the ability to respond as well as detect. Organisations with mature security operations combine continuous monitoring with clearly defined response processes, skilled resources and the capacity to act at any time. With nearly two-thirds of respondents lacking fully mature 24x7 operations, the data suggests that extending response capability beyond traditional business hours remains a critical step in closing the security maturity gap.

Intelligence-led detection improves confidence and prioritisation

Threat intelligence adoption is gaining momentum. 40% of organisations now use real-time automated threat intelligence feeds, while 30% rely on periodic intelligence reports, 18% gather intelligence on an ad-hoc basis, and only 12% have no threat intelligence capability. The next step is to embed intelligence into everyday security decisions, investigations and response activities.

40% of organisations now use real-time automated threat intelligence feeds.

Detection capabilities are also improving. 28% use AI-driven behavioural detection, while 45% combine signature-based and anomaly detection, meaning 73% have moved beyond traditional signature-only approaches. However, 14% still rely mainly on signatures and another 14% have no dedicated threat detection capability.

The biggest challenge is confidence. Just 28% are highly confident in distinguishing real threats from false positives, while 43% are only moderately confident and 29% struggle with false positives or are unsure how to identify genuine threats. Mature organisations address this by combining threat intelligence, behavioural analytics and automation to reduce noise and focus human judgement on the risks that matter most.

AI is accelerating the maturity imperative

The survey captures organisations at a pivotal moment. The wider significance of AI is strategic: agentic systems can perform sequences of tasks, analyse code and adapt workflows at a pace that compresses the time between vulnerability discovery and exploitation. Security readiness must therefore be judged against a new question: can the organisation understand and interrupt an attack moving at machine speed?

AI can assist with investigation, correlation, vulnerability discovery and routine response, while people provide oversight, judgement and accountability.

This does not remove the need for human expertise. It changes where that expertise creates most value. AI can assist with investigation, correlation, vulnerability discovery and routine response, while people provide oversight, judgement and accountability. The organisations best placed for the next phase will combine broad telemetry, intelligent automation, governed orchestration and skilled analysts into a security function that learns and adapts continuously.

Tested and automated response turns readiness into resilience

Detection only delivers value if organisations can respond effectively. 40% have a regularly tested incident response plan, but 60% do not have a fully tested response capability. Of these, 27% have a plan that is not tested regularly, 16% have outdated plans, and 17% have no formal plan at all. Regular testing is what turns a plan into real resilience.

40% of organisations have a regularly tested incident response plan.

The gap is just as clear in response processes. Only 33% have comprehensive incident response playbooks, while 35% have partial documentation and 32% rely on ad-hoc or no playbooks.

Automation is another challenge. Just 26% of organisations use extensive automation in security response, meaning 74% are not extensively automating response activities. Specifically, 35% use limited automation and 39% remain largely manual.

As attacks become faster and more complex, mature organisations rely on tested plans, well-defined playbooks and governed automation to respond quickly, consistently and at scale.

Ransomware exposes the gap between readiness and resilience

Ransomware provides the clearest test of resilience. Only 36% of respondents consider themselves fully prepared for ransomware. 38% say they are moderately prepared but acknowledge gaps, and 26% report limited or no preparedness. That means nearly two-thirds are not fully confident in their ransomware readiness. Good practice extends beyond prevention and detection to tested containment, trusted backups, recovery priorities and clear business decisions about how operations will continue.

> Nearly **two-thirds** are not fully confident in their ransomware readiness.

> **41%** either lack insurance or are still evaluating options.

Cyber insurance cannot substitute for those capabilities. 32% have comprehensive cyber insurance coverage, 27% have limited coverage, and 41% either lack insurance or are still evaluating options. Insurance can help transfer part of the financial impact, but it cannot restore systems, maintain customer trust or make critical decisions during an incident. Operational resilience must therefore be built before a claim is needed.

Closing the maturity gap through adaptive security operations

Demand for managed security services is strong. 34% of organisations believe MXDR would improve response times and effectiveness, while 28% see it as a valuable extension of their security team. A further 25% see value but have concerns about visibility and responsiveness. Overall, 87% see a positive or potentially positive role for Managed SOC or MXDR services, with only 13% believing managed services would reduce control or slow them down.

87% see a positive or potentially positive role for Managed SOC or MXDR services.

This reflects a growing need for support that goes beyond monitoring and alert management. Organisations are looking for providers that can combine 24x7 coverage, specialist expertise, threat intelligence, automation and rapid response.

For security services providers such as Logicalis, the opportunity is not simply to outsource security, but to help customers strengthen their capabilities. The most effective partners act as an extension of the customer's team, improving visibility, response and resilience while maintaining transparency and control. With 87% of respondents seeing a positive or potentially positive role for Managed SOC or MXDR services, the market is ready for an adaptive model that can operate at machine speed while keeping people firmly in control.

We are Architects of Change™.
We help organisations succeed in a digital-first world.

At Logicalis, we harness our collective technology expertise to help our clients build a blueprint for success, so they can deliver sustainable outcomes that matter.

www.logicalis.com

LOGICALIS
Architects of Change