ncc group

A Guide to Assessing your Managed Security Strategy in 2025

In today’s rapidly evolving threat landscape, traditional managed security approaches are no longer sufficient. CISOs and IT Directors must reassess their strategies to ensure they are equipped not only to detect and respond to cyber threats, but also to recover and maintain operations when disruptions occur.

This guide provides a structured approach to evaluating your current managed security posture and introduces Intelligent MXDR (Managed Extended Detection and Response) as a modern, proactive solution that enhances both security and organisational resilience.

The Current State of Managed Security

Many organisations rely on legacy systems or traditional MSSPs that struggle to keep pace with modern threats.

Common challenges include:

- **Alert fatigue**: Security teams are overwhelmed by high volumes of alerts, many of which are false positives.
- **Skills shortages**: There's a global shortage of cyber security talent, making it difficult to maintain effective in-house operations.
- **Siloed tools and data**: Disconnected systems hinder visibility and slow down response times.
- **Inadequate threat detection**: Legacy tools often miss advanced threats or detect them too late.
- **Limited response capabilities**: Traditional MSSPs may lack the agility or automation needed for rapid incident response.

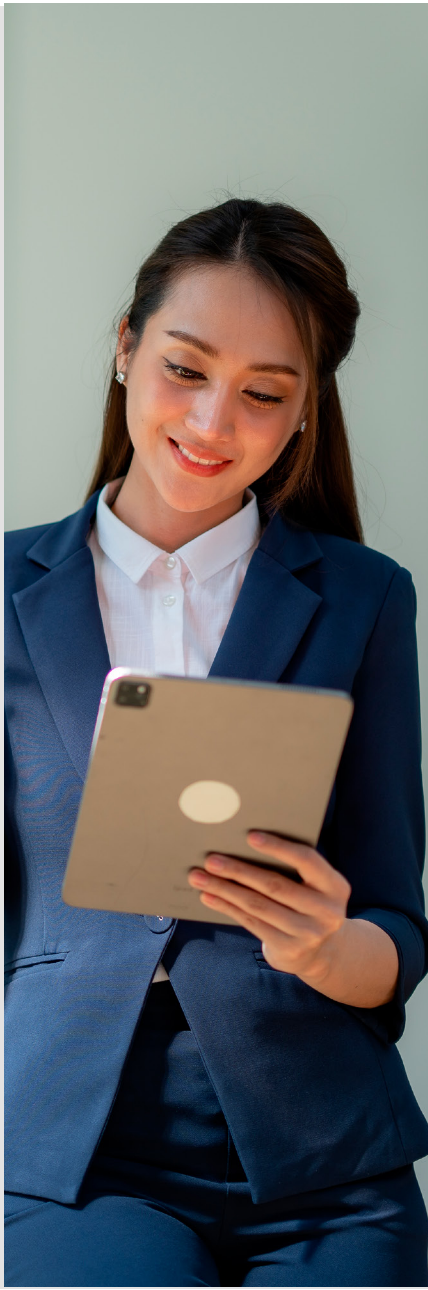
These challenges don't just create security gaps, they also undermine organisational resilience, leaving operations vulnerable to extended downtime, financial loss, and reputational damage.

Key Indicators Your Strategy Needs Reassessment

Ask yourself the following questions to determine if your current strategy is still effective:

1. Are you detecting threats in real-time, or only after the damage is done?
2. Is your team overwhelmed by false positives and manual investigations?
3. Do you have full visibility across endpoints, cloud, network, and identity?
4. Are your tools integrated and providing actionable insights?
5. Can you respond to incidents quickly and minimise disruption?
6. Are you meeting compliance and regulatory requirements with confidence?

If you answered "no" to any of these, it's time to reassess. A resilient strategy ensures your organisation can detect, respond, and recover with minimal impact on operations.



The Rise of MXDR

MXDR represents the next evolution in managed security. Unlike traditional MDR, it combines:

AI-driven threat detection: Identifies anomalies and threats faster and more accurately.

Automated response: Reduces dwell time and limits damage through rapid containment.

24/7 expert monitoring: Security analysts provide continuous oversight and threat hunting.

Unified visibility: Integrates across cloud, endpoint, network, and identity for holistic protection.

This approach doesn't just improve security, it builds resilience into your operations, enabling your organisation to maintain continuity, recover quickly from incidents, and adapt to evolving threats.

Evaluating Your Current Security Posture

Use established frameworks like NIST Cybersecurity Framework or MITRE ATT&CK to assess:

- ✓ **Visibility:** Do you have real-time insights across your environment?
- ✓ **Detection and response speed**: How quickly can you identify and contain threats?
- ✓ **Threat intelligence:** Are you leveraging up-to-date, contextual threat data?
- ✓ **Compliance:** Are you audit-ready and aligned with industry regulations?
- ✓ **Operational resilience:** How effectively can you recover from incidents and maintain business continuity?

A structured evaluation helps identify gaps, prioritise improvements, and strengthen your organisation's ability to withstand and adapt to cyber disruption.

Building a Future-Ready Security Strategy

To future-proof your security posture:

- **Align with business goals**: Security should support innovation, growth and uninterrupted operations.
- **Embrace automation and AI:** Reduce manual workloads, improve accuracy and accelerate response to threats.
- **Foster collaboration:** Break down silos between IT, security, and business units to enable coordinated recovery.
- **Plan for scalability**: Ensure your strategy can grow with your organisation without compromising resilience.
- **Invest in continuous improvement:** Regularly reassess and adapt to new threats to maintain long-term operational strength.

Case Study: Transforming Security with Intelligent MXDR

A global manufacturing firm faced increasing ransomware threats and alert fatigue. After implementing an NCC Group's Intelligent MXDR solution, they achieved:

60 %

reduction in false positives

75 %

faster incident response time

- Full visibility across hybrid cloud and on-prem environments
- Improved compliance with ISO 27001 and GDPR

Crucially, they enhanced business resilience - minimising downtime, protecting production schedules, and enabling the organisation to recover swiftly from incidents. The CISO was able to shift from reactive firefighting to strategic risk management, with security and resilience built hand-in-hand.

Introducing NCC Group’s Intelligent MXDR

Powered by the Unified Cyber Platform

NCC Group’s Intelligent Managed Extended Detection and Response (MXDR) exemplifies the power of a people powered, tech-flexible, and insight enriched approach.

Built on our Unified Cyber Platform (UCP) and underpinned by decades of offensive security expertise, Intelligent MXDR combines adaptive technology with NCC Group’s unparalleled human insight and proprietary intelligence to deliver industry-leading threat detection and response.

The UCP integrates seamlessly with existing and future tools, reducing the complexity of managing diverse tech stacks while preserving the flexibility and resilience of a best-of-breed approach. By harnessing AI, machine learning, and advanced automation, it filters out noise and enables analysts to focus on high-value tasks, ensuring faster, more accurate threat resolution.

Adaptable by design, Intelligent MXDR aligns with each client’s operating model and scales as needs evolve. Whether meeting compliance in highly regulated industries or addressing the resource challenges of growing organisations, it provides tailored, proactive protection that simplifies complexity and strengthens resilience.

What makes NCC Groups MXDR Intelligent?

People powered:

Our Intelligent MXDR service is powered by the expertise of our pioneering global cyber team, renowned for their strong heritage in offensive security.

We’re on hand to listen, understand your challenges, and deliver trusted, transparent guidance while helping you to prioritise which threats matter most. No chatbots. No call centres. No menus. Just a great team behind you.

Tech-flexible:

Our Unified Cyber Platform (UCP) brings together NCC Group’s unique technology and methodology to seamlessly integrate MXDR with your existing and future tech stack - without vendor lock-in - reducing complexity, maximising your security investments and future proofing your strategy.

Insight enriched:

Stay ahead of emerging threats with the combined strength of NCC Group’s industry leading threat intelligence, worldwide proprietary research and aggregated data taken from real time testing and incident response.

40% of threats detected come directly from our own intelligence, helping you stay one step ahead.

Born to hack.
Built to defend.

Intelligent MXDR from the experts in offensive security.

Adaptive, innovative, Intelligent MXDR for complex tech stacks and hybrid environments.

Future-proof your cyber security today

UK & Europe | +44 331 630 0690

Disclaimer: This content is for general purposes only and should not be used as a substitute for consultation with professional advisors