Solution brief

NCC Group Intelligent MXDR

People powered | Tech-flexible | Insight enriched

The Challenge – Why Organisations Struggle to Keep Pace

Every organisation, from fast-growing businesses to global enterprises, faces the same reality: threats are more persistent, sophisticated, and adaptive than ever. As digital estates expand across on-premise, cloud, SaaS, OT, and hybrid environments, the volume and complexity of security data grows exponentially.

This creates several critical challenges:

- **Tool sprawl** – Multiple, disconnected solutions create fragmented visibility, wasted investment, and integration headaches.
- **Complexity overload** – Highly diverse tech stacks generate vast amounts of data that security teams struggle to interpret quickly.
- **Regulatory pressure** – Compliance and audit frameworks (NIS2, DORA, HIPAA, PCI, SOC2 and more) demand not only effective controls but also the ability to evidence them.
- **Analyst fatigue** – In-house teams face burnout dealing with high false positives, repetitive triage, and slow incident resolution.
- **Evolving attacker tactics** – Traditional perimeter and endpoint-led approaches miss subtle activities, leaving blind spots for emerging threats or that threat actors could exploit.

The impact? Longer dwell times, higher remediation costs, operational disruption, and reputational damage that can be hard to recover from.

The Market's Response – (and limitations)

MDR/MXDR solutions typically take one of two forms:

- **Tool-led** - A platform-centric approach that scales well but limits flexibility. Often integrates poorly with existing investments, and human analysis can be minimal, reducing contextual accuracy.
- **People-heavy** - Analyst-first delivery but fixed to a narrow set of technologies, making integration with diverse stacks slow and costly.

While each approach has merits, both can:

- Create **vendor lock-in** and dependency.
- Deliver **generic detection logic** not tailored to the organisation's environment.
- Fail to fully **simplify complex estates,** forcing clients to adapt to the service rather than the other way around.

NCC Group's Response – Intelligent MXDR

Intelligent MXDR from NCC Group delivers the best of both worlds - the precision of human-led detection engineering and threat hunting, amplified by a highly adaptive technology platform.

People powered

- Delivered by a pioneering global cyber team with deep offensive security heritage.
- Every client is assigned a **dedicated Technical Account Manager** - your strategic security partner and extension of your internal team.
- CREST-accredited analysts, CHECK and OSCP-certified consultants, and testers cleared to SC and DV levels.
- Continuous SOC tuning, baselining, and behavioural analytics tailored to your organisation's context.

Tech-flexible

- Powered by our proprietary **Unified Cyber Platform (UCP)**, an integration and analytics layer that unifies data from multiple EDR, NDR, SIEM, cloud, identity, and deception technologies.
- Works with your existing and future stack, avoiding costly rip-and-replace.
- Pre-built integrations for leading vendors like Microsoft, Splunk, SentinelOne, CrowdStrike, Dragos, Thinkst Canary, Searchlight, and CyCognito for faster onboarding.
- Future-proofs your strategy by adapting as threats, technology, and regulatory needs evolve.

Insight enriched

- 40% of true threats detected come directly from **NCC Group's own detection logic.**
- Offensive security heritage means we think like attackers, spotting subtle indicators before they escalate.
- Proactive threat hunting using our HITS framework: Hypothesis-led, Intelligence-driven, Targeted hunting at Scale.
- Behaviour-led detection uncovers evasive techniques such as, living-off-the-land activity, C2 channels and memory-only attacks.

We don't just monitor complex environments, we make sense of them, transforming fragmented data into clear, actionable decisions that enable faster, more confident responses.

Why Organisations Choose NCC Group

- **Faster detection & response:** 58 seconds to pick up critical alerts.
- **Automation at scale:** 99% of alerts processed automatically, enabling analysts to focus on genuine threats.
- **Maximised ROI:** Leverage and optimise your existing security investments.
- **Reduced noise:** Advanced SOC tuning, machine learning, and context-driven triage slash false positives.
- **End-to-end resilience:** Integrated access to incident response, digital forensics, identity threat assessment, and attack surface management.
- **Global reach, local presence:** Over 420 cyber experts worldwide, with in-region delivery and strict data sovereignty controls.

Use Cases & Outcomes

- **Proactive ransomware disruption** – Threat hunting revealed stealth activity in a manufacturing environment before encryption began, preventing millions in potential losses.
- **Identity risk mitigation** – Assessment for a global operator identified active accounts for former employees, 20% of which had been accessed post-departure.
- **Seamless integration** – Full-stack visibility for a healthcare provider without replacing existing EDR/SIEM tooling, improving detection coverage by 30%.

Recognised Expertise

- CREST Member Company, NCSC accredited, CHECK & OSCP certified experts.
- Verified Microsoft Managed XDR Solution Provider.
- Elite Global Partner for Managed Services with Splunk.
- Microsoft Security Researcher Leaderboard recognition for vulnerability discovery.
- Leader in the IDC MarketScape European Managed Detection and Response.
- Strong Performer in The Forrester Wave: Managed Detection and Response. Shape

Ready to Elevate Your Security?

Focus on the events that matter. Simplify complexity. Strengthen resilience. Get in touch to explore how NCC Group's Intelligent MXDR can protect your business, your reputation, and your future.

Get in touch