NCC Group Managed Extended Detection and Response (MXDR)

A managed security solution aligned to your business's unique risk

Implementing and optimizing a security monitoring solution isn't easy. Your environment, threat landscape, and risk appetite are unique to your organization — Your solution should be unique too.

NCC Group Managed Extended Detection and Response (MXDR) solution provides security expertise, systems, and processes that optimizes and correlates your threat landscape from a broad range of sources natively, including vulnerability information, phishing awareness, data governance, classification and data loss prevention. We maximize the depth of your current security tooling and your business environments. The result? Robust awareness and defenses that are targeted at your risks, allowing you to focus on what matters — your business.

Our MXDR solution at a glance.
We developed a security monitoring service that allows clients to focus on growing their business instead of pulling their attention to security needs. With NCC Group, security enables your business, not hold it back. Our industry leading MXDR solution is combined with NCC Group's unique global capability, leveraging our research, incident response, threat intelligence and research practices, giving you the highest quality of threat detection and response management.

NCC Group MXDR changes the narrative on security monitoring. We provide a holistic approach to security, taking enrichment and correlation from all available sources to increase the speed and quality of defenses — giving you a benchmarked view of your defensive posture.
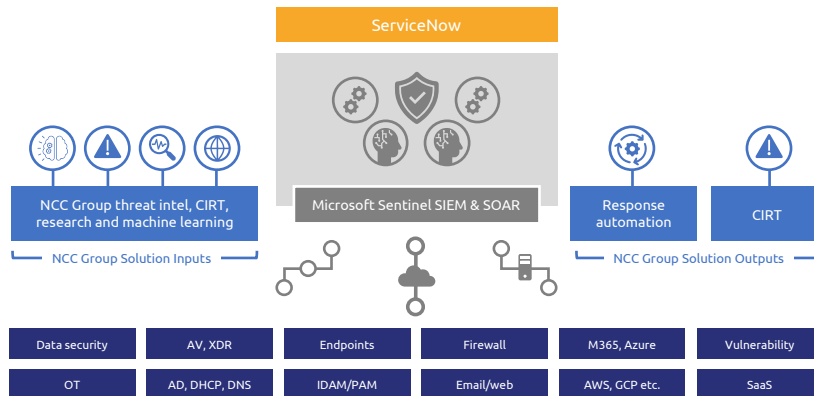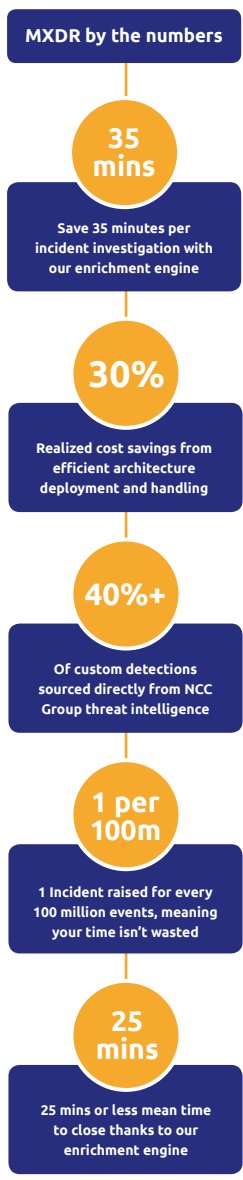

Clients receive an individual security benchmark to assess their cyber monitoring posture.
We threat model every customer to ensure that the most efficient and appropriate sources, detections, and responses are aligned to your organization. We'll continue to iterate and evolve defenses efficiently and effectively. With regular reviews, you'll have industry benchmarks to measure and improve your defensive posture, keeping your organization ahead of your attackers.

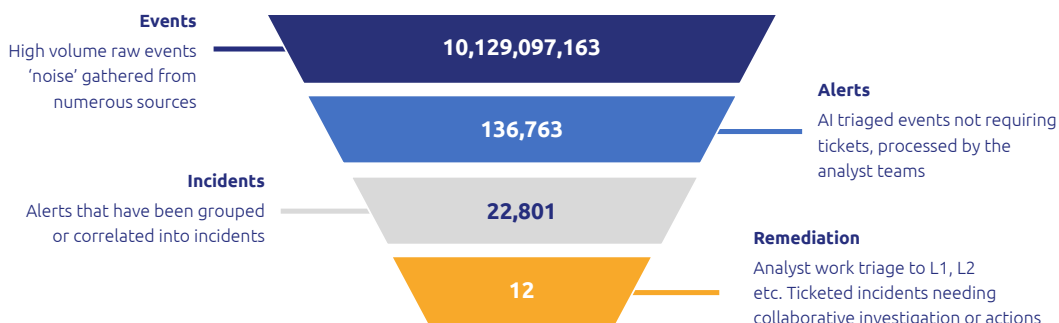Illustrative client benchmark report
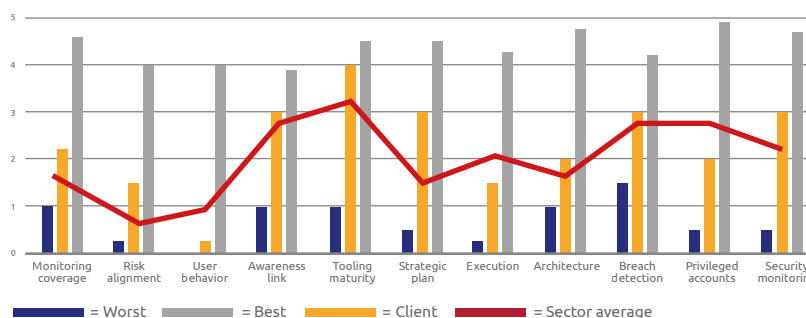
nccgroup

All our unique capabilities are delivered through a dedicated technical account manager — an extension of your team with broad cyber expertise and the reach of NCC Group specialized experts who can improve not just your security monitoring, but your whole defensive posture.

MXDR by the numbers

35 mins

Save 35 minutes per incident investigation with our enrichment engine

30%

Realized cost savings from efficient architecture deployment and handling

40%+

Of custom detections sourced directly from NCC Group threat intelligence

1 per 100m

1 Incident raised for every 100 million events, meaning your time isn't wasted

25 mins

25 mins or less mean time to close thanks to our enrichment engine

Experience the NCC Group difference and...

- **Save time with NCC Group's machine learning enrichment engine.** We've taken our top analysts and automated their investigation tactics into our enrichment engine, saving you on average 35 minutes per incident investigation. Receive an instant timeline view in your SIEM of incident contextual data instead of spending valuable time researching it.

- **Work with experienced security experts in a dedicated Microsoft XDR SOC.** Optimize your security investments to leverage maximum security benefits including, data governance, multicloud and operational technology (OT).

- **Achieve efficient time to value** with NCC Group's unique infrastructure as code (IaC) approach that provides immediate security value with defenses being active in weeks — not months.

- **Get the appropriate amount of security** by leveraging your current security subscriptions (Microsoft or any other technologies) existing devices and environments. We deliver the right level of security that meets your business objectives.

- **Defend against the latest IOCs and attacker techniques by aligning 60 unique data feeds.** Leverage NCC Group advanced threat intelligence — it feeds directly into our custom threat detections. We're constantly assessing, investigating, and aggregating threat intelligence from the dark web, research, and our learned insights from customer engagements. Our intel provides defenses for the latest IoC's and attacker techniques, identifying and discovering things that others don't, with more than 40% of detections from our custom rules and queries.

- **Control your estate through our shared delivery model.** You'll remain in total control and ownership of your data, and access to it. You'll see not only what we're doing, but why, and be able to contribute to and consume it in real time.

- **Comprehensive threat management and response.** Managing threats in real time including incident response through our embedded IR Team. When it's required, we'll engage our dedicated Incident Response team, working seamlessly to rapidly defend and recover from complex incidents.

Focus on the events that matter. Save time remediating them.

Events
High volume raw events 'noise' gathered from numerous sources

10,129,097,163

136,763

Alerts
AI triaged events not requiring tickets, processed by the analyst teams

Incidents
Alerts that have been grouped or correlated into incidents

22,801

Remediation
Analyst work triage to L1, L2 etc. Ticketed incidents needing collaborative investigation or actions

12

nccgroup

About us

NCC Group is a global cyber and software resilience business, operating across multiple sectors and technologies.

As society's dependence on the connected environment and associated technologies increases, we use our global expertise to enable organizations to assess, develop and manage their cyber resilience posture to confidently take advantage of the opportunities that sustain their business growth.

With over 2,400 colleagues, we have a significant market presence in the UK, Europe and North America, and a growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contact Us:
1 (800) 813 3523
uscons-info@nccgroup.com
www.nccgroup.com