NCC Group MDR for Microsoft Sentinel

Best-of-breed Cloud XDR technology from Microsoft meets best-in-class service from NCC Group

Gold Microsoft Partner

Microsoft

To have an effective defence against advanced threat actors, your organisation needs the ability to analyse vast datasets in order to surface the activity that indicates something nefarious could be in play. On top of this, you then need the skills to understand how serious the activity might be, how to contain it and what to do to prevent it from happening in the future.

Your investment in Cyber Security should be focused on the highest risk and highest impact areas of return. The Microsoft Sentinel Cloud Native SIEM provides simple deployment, automatic scaling and intelligent threat detection to reduce infrastructure management costs by up to 48% compared to on-premise SIEM solutions. NCC Group augments this capability with robust SOC operations, human-driven threat hunting powered by our Advanced Threat Analytics pipeline and Global CIRT readiness.

The Challenge

Threat actors are relentless in their attempts to find and exploit vulnerabilities which will give them a foothold into a business' IT environment. With the ever-increasing amount and complexity of data that modern businesses generate, it can be daunting to build, maintain and update the systems necessary to give Cyber Security Analysts visibility of data and traffic patterns which they rely on to identify potential threat actor activity.

In order to maintain a high level of threat detection, it is vital to create and deploy new threat detection logic, whilst also ensuring that playbooks are kept updated to advise SOC analysts of the steps to take when threat activity is suspected, as well as how to contain and remediate confirmed threats.

Creating a highly effective yet cost efficient Threat Detection & Response operation requires the prudent allocation of tools, skills and processes in the right place at the right time.

The Solution

Microsoft Sentinel takes full advantage of Cloud economics, integration and automation to remove a significant proportion of the engineering and administrative overheads associated with running an enterprise-wide cyber security platform. It is a key component of Microsoft's Extended Detection & Response (XDR) technology stack and provides the foundation for end-to-end visibility and detection of threats across users and infrastructure.

NCC Group offers the full spectrum of Cyber Security services including Security Operations Centers for Managed Detection & Response, Ethical Hacking, Incident Response and Risk & Compliance auditing. Alongside all of this, we undertake research projects together with the leading cyber security and academic organisations to ensure we are always at the top of our game.

The NCC Group Managed Detection & Response offering for Microsoft Sentinel ensures that you have experts undertaking analysis of the alerts and notifications generated by threat detection logic and intelligence embedded in the Microsoft Sentinel technology stack. We provide robust and stringent Service Level Guarantees against Triage & Investigation of the Microsoft Sentinel output to ensure any required manual response activities are executed in a timely fashion.

Additional to this, NCC Group deploys a mature Advanced Analytics pipeline and Machine Learning-based threat detection solution.

Recognised in The Forrester Wave™ - Managed Detection & Response, Q1 2021 report, the solution translates the output of the findings from our Threat Intelligence operations, consultants in the field, Incident Response engagements and research projects into automated threat detection logic.

As a final layer of protection should the worst happen, we have Incident Response consultants across multiple global locations that can be assigned to be on standby as part of your MDR contract with us.

Why MDR for Microsoft Sentinel by NCC Group?

Defenders who think like attackers
Offering the full spectrum of Cyber Security at scale, provides NCC Group a unique perspective of the motivations and modes of operation of the various threat actor communities. We leverage this knowledge to protect our clients and strive to out-innovate the criminal underworld.

24/7/365 service excellence
Threat actors never rest and neither do we, any suspicious activity in your environment will be investigated according to Service Level targets regardless of time of day.

Integrated Threat Analytics pipeline
NCC Group deploys and updates our advanced threat analytics using Continuous Integration and Continuous Delivery pipelines to automate roll-out and remove human error potential.

Recognised leader in Machine Learning-based threat detection
NCC Group's capabilities for Data Science-based analytics scored the highest possible marks in The Forrester Wave™ - Managed Detection and Response, Q1 2021.

How do I activate Microsoft Sentinel and how much does it cost?

The Microsoft Sentinel SIEM is available to all businesses with an Azure Active Directory license and tenant plus the appropriate Azure Enterprise/Customer subscription.

Microsoft Sentinel is billed on a consumption model based on the following three components:

- Azure Sentinel
- Log Analytics
- Data Retention

Actual charges incurred will depend on how much data you ingest and whether you opt for 'Pay as you go' or data 'Commitment tiers'.

About NCC Group

NCC Group is a global cyber and software resilience business operating across multiple sectors, geographies and technologies. We assess, develop and manage cyber threats across our increasingly connected society.

We advise global technology, manufacturers, financial institutions, critical national infrastructure providers, retailers and governments on the best way to keep businesses, software and personal data safe.

Arrange a call with one of our MDR experts today and learn more about Microsoft Sentinel and NCC Group.

uscons-info@nccgroup.com +1-800-813-3523 www.nccgroup.com