XDR Consulting

XDR Consulting

XDR Consulting provides structured support for organisations implementing Microsoft's security technologies across three key areas: Microsoft Defender XDR, Microsoft Sentinel, and Microsoft Purview.

The service is designed to help organisations establish a coherent security architecture, configure core capabilities correctly, and align operational processes with the functions of the Microsoft Security stack.

The engagement can be delivered as a single integrated programme or as individual modules depending on the organisation's requirements.

NCC Group's role within the service is to provide specialist technical expertise in deployment, configuration, and optimisation.

Our teams have extensive experience delivering Microsoft Security solutions in a range of environments. NCC Group is recognised by Microsoft as a Managed Security Solutions Provider (MSSP) and is a member of the Microsoft Intelligent Security Association (MISA), which reflects established capability in implementing Microsoft security technologies.

Microsoft Purview

This module focuses on establishing data governance and protection capabilities within Microsoft 365.

Activities typically include analysis of the organisation's data landscape, configuration of data classification and labelling structures, and deployment of Data Loss Prevention and Insider Risk Management controls.

Work carried out in this module ensures that sensitive information is identified, handled consistently, and governed in line with organisational policies and regulatory requirements.

Outputs commonly include defined labelling taxonomies, retention schedules, DLP policies, and supporting operational processes for monitoring and review.

Microsoft Defender

The Defender module covers deployment and configuration of Microsoft Defender XDR components across endpoints, identities, email, and cloud applications. This work may include onboarding devices, configuring identity protection, enabling threat analytics capabilities, and establishing automated investigation and remediation actions.

Where organisations are transitioning from existing XDR or endpoint protection platforms, the module also includes planning and execution of the migration, ensuring continuity of coverage and alignment with operational expectations. The outcome is a functioning Defender XDR environment that reflects the organisation's requirements and integrates with other components of its security tooling.

Key benefits

- Creates a unified security approach across data, detection, and response.
- Improves detection quality through tuned analytics and aligned controls.
- Reduces ongoing SIEM and security tooling costs.
- Maximises value from existing Microsoft Security licences and capabilities.
- Supports continuous maturity and adaptation as risks and requirements change.

Microsoft Sentinel

This module covers the design, deployment, and configuration of Microsoft Sentinel as the organisation's SIEM and SOAR platform. Typical activities include onboarding of log sources, creation of analytics rules aligned to relevant use cases, configuration of workbooks and dashboards, and development of automation playbooks.

A significant part of the module involves establishing a cost-appropriate ingestion and retention strategy. This may include use of Sentinel Data Lake, data filtering, or other measures to align running costs with operational needs. Where required, the service can also support migration from legacy SIEM platforms by mapping existing use cases and data sources into Sentinel.

The outcome is an operational Sentinel environment with defined detections, dashboards, automation workflows, and governance structures to support ongoing operations.

Delivery Methodology

XDR Consulting is delivered as a structured service that supports organisations in deploying, improving, and maturing their Microsoft Security technologies.

The approach is designed to ensure that Sentinel, Defender XDR, and Purview operate effectively from initial implementation through to long-term optimisation and cost-efficient ongoing use.

Baseline Review
We begin by assessing the organisation's current configuration, data flows, detection coverage, and operational practices. This establishes a clear starting point and identifies immediate gaps or inefficiencies.

Target State Definition
Using the baseline, we define how the Microsoft Security stack should operate within the environment. This includes architectural considerations, policy structures, detection requirements, and operational alignment.

Implementation and Configuration
Core capabilities across Purview, Defender XDR, and Sentinel are deployed or reconfigured to meet the defined target state. This may include onboarding data sources, enabling policies, refining analytics, and completing any required migration work.

Optimisation and Tuning
Once the technologies are in place, configurations are adjusted to improve accuracy, efficiency, and cost control. This may involve tuning detections, refining automation, improving DLP and retention settings, or adjusting SIEM ingestion patterns.

Ongoing Evolution
The final step focuses on continuous improvement. As organisational needs, threats, and Microsoft capabilities change, we assist in updating policies, enhancing detections, maturing processes, and maintaining a consistent return on investment.

About NCC Group

NCC Group is a global expert in cyber security and risk mitigation, working with organisations to protect their brand, value and reputation against the ever-evolving threat landscape.

With our knowledge, experience and global footprint, we are well placed to help organisations identify, assess, mitigate and respond to the risks they face.

We are passionate about making the Internet safer and revolutionising the way in which organisations think about cyber security.

For more information from NCC Group on our G-Cloud 15 service, please contact:

+44 (0)161 209 5200

bidteam@nccgroup.com