Microsoft Engagements

LEVERAGE MICROSOFT SECURITY PRODUCTS AND FEATURES

Business problem

Optimizing the use of Microsoft products and features is challenging. Without proper guidance, organizations may struggle to fully leverage the capabilities of tools such as Microsoft 365, Azure, or Microsoft's security solutions.

The risks of not fully leveraging Microsoft's capabilities leads to:

Underutilization of Technology
Organizations may not be using Microsoft products to their full potential, leading to inefficiencies and missed benefits that could help drive productivity and innovation.

Increased Security Vulnerabilities:
Without proper training on the latest security features, organizations may become vulnerable to cyber threats, leaving critical data and systems exposed to risks.

Slow Adoption of New Features:
If an organization isn't up to date with new features and capabilities, it may fall behind on leveraging the latest advancements, hindering growth and competitive advantage.

Wasted Investment:
If an organization is not trained to use Microsoft tools effectively, the initial investment may not provide the expected returns.

Solution

Microsoft Engagements offer a comprehensive and hands-on approach to allow organizations to gain the skills needed to maximize the value of Microsoft products and features. These by Microsoft funded engagements are designed to equip teams with the knowledge and skills necessary to understand and implement advanced security features within Microsoft's ecosystem, such as Microsoft 365, Azure, and other critical tools.

Engagements we offer

Managed XDR Engagement:

The MXDR Engagement is designed for managed XDR services, based on Microsoft Security technology, including Microsoft Sentinel, Microsoft 365 Defender, and Microsoft Defender for Cloud. The MXDR Engagement is delivered in a customer's production environment with real security threats or, as a secondary choice, in a organization's staging environment with either real security threats or an attack orchestrated by a red team.

Modern SecOps Engagement:

Modern Security Operations Engagement (formerly Microsoft Sentinel Engagement) is designed to demonstrate how Modern SecOps helps organizations use intelligent security analytics and threat intelligence to detect and quickly stop active threats and create customer intent for deploying and adopting Modern SecOps.

Threat Protection Engagement:

The Threat Protection Engagement is designed for deploying advanced Microsoft Security products, including Microsoft Defender XDR and Microsoft Sentinel. The Threat Protection Engagement is delivered in a organization's production environment by detecting real security threats and vulnerabilities.

Data Security Engagement:

The Data Security Engagement is designed for adopting Microsoft Purview solutions. By providing real world examples of data security and regulatory risks in their own environments combined with collaborative workshop sessions, the engagement helps create compelling ways for organizations to remediate and prevent data security risks using Microsoft Purview (E5 Compliance) technologies.

Funding by Microsoft

The Microsoft Engagements are part of the Microsoft Cybersecurity Investment (CSI). To participate in the by Microsoft funded engagements organizations must fit the following criteria:

- 500+ Paid Available Units (PAU) for Microsoft Entra ID Premium P1 PAU.

- 250+ Monthly Active Users (MAU) for Exchange Online, SharePoint Online or Teams.

- Organizations may not have previously attended an eligible Engagement in the prior 9-month period.

For Managed XDR Engagement the first two criteria are replaced by the criteria that customers must have 500+ Paid Available Units (PAU) for Microsoft Defender for Endpoint (MDE), Microsoft Defender for Office 365 (MDO) and Microsoft Entra ID Premium Plan 2.

Microsoft Engagement phases and activities

On a high level, the four Microsoft Engagements adhere to the following phases and activities:

01   Pre-engagement call to gather customer information and set-up planning.

02   Kick-off session to gather organizational needs.

03   Workshop and Product demonstration.

04   Configuration of Product in line with organizational needs.

05   Collect results gathered by the product.

06   Present results and recommended actions.

Benefits

- Review your security goals and objectives

- Assess your environment against industry standards and learn about digital risks

- Learn about features and benefits of Microsoft toots that can help mitigate risks

- Get the information required for you to build a business case for a deployment of Microsoft tools

- Receive an analysis and report on findings and associated risks

- Explore recommendations and next steps

Why choose Nedscaper

Pragmatic, Accessible

By focusing on Microsoft's comprehensive security tools, we build on the software that many organizations already trust and rely on to run their operations. This alignment allows us to seamlessly integrate security into existing systems and processes, making cybersecurity a natural extension of their daily workflows.

A Human Approach

With Nedscaper, organizations gain a service that genuinely enhances their security. Our consultants are an integral part of our managed service: guiding clients, strengthening preventive measures, and providing them with a sense of safety and security.

More Value through Microsoft Specialisation

Nedscaper maximizes value by standardizing on a core of Microsoft technology. With our deep specialization, we understand how to secure our clients' environment effectively, and our close partnership with Microsoft not only leverages current capabilities but also allows Nedscaper to capitalize on future advancements.

Unique combination of Prevention and Detection

Our 'best of suite' strategy enables seamless integration of Microsoft's comprehensive security tools, allowing us to maximize the benefits of both preventive and reactive measures for our clients. While we acknowledge the critical role of detection in ensuring swift action when breaches occur, we are equally committed to elevating prevention measures beyond industry standards, significantly reducing the likelihood of incidents.

Making a Positive Impact

By partnering with Nedscaper, clients contribute to a better world while benefiting from high-quality talent at a reasonable cost. We are dedicated to nurturing young talent, particularly in South Africa, providing them with opportunities to develop into skilled cybersecurity experts.

About Nedscaper

Nedscaper delivers pragmatic, accessible cybersecurity services across Europe and Africa. Its Managed XDR platform provides real-time threat detection, rapid response, and expert consulting, ensuring 24/7 protection for organizations, and SMBs are supported through a partner network. Built around Microsoft's security tools, Nedscaper leverages software many organizations already trust, seamlessly integrating security into existing systems. This approach makes cybersecurity a natural extension of daily operations. With offices in Amsterdam, Cape Town, and Johannesburg, and a growing global partner network, Nedscaper continues to expand, building trust in the digital world.

hello@nedscaper.com
www.nedscaper.com

kiwa kiwa

Member of
Microsoft Intelligent
Security Association

Microsoft Security   Microsoft Verified
Managed XDR Solution