Managed Microsoft Sentinel Security

Fully outsource your Sentinel set up and ongoing management to optimize security across your organization with limitless speed and scale.

1-HOUR BRIEFING

In this 1-hour briefing we will discuss MNP's fully managed approach to onboarding and maximizing your ongoing investment in Azure Sentinel security information event management (SIEM). Once up and running, your environment will be monitored 7x24x365 by MNP's Canadian staffed Security Operations Centres (SOCs).

Our SOC can help you detect and respond to advanced threats in your cloud, SaaS applications, and data centres. With immediate visibility, our teams gain confidence and automate responses more quickly and decisively using Azure Sentinel. More than just an alert – MNP's SOC provides an integrated approach combining manual alarm investigation, contextual awareness, and threat intelligence.

Key Benefits

MNP's Managed Microsoft Sentinel SIEM program delivers:

- ✓ A fully Managed SIEM Solution
- ✓ Fulfill many of the NIST Detect & Respond Requirements
- ✓ 7x24x365 Canadian staffed and security cleared Security Operations Centre
- ✓ Get more value out of your existing security investments with built-in orchestration and automation.

Gold Microsoft Partner

Microsoft

MNP's Managed Sentinel Overview

To be tailored to your organization's needs.

	1. Discover / Deploy	2. Tune	3. Detect & Respond
Objectives	• Capture business requirements and understand network topology and data flows.	• Conduct reviews security team and ensure regular events and reports are developed • Ensure alerts, call escalation scripts are completed	• Prepare documentation and training materials • Recommend tools & services to extend security visibility • Orchestration & Automation
Activities	• Validate the state of the existing environment • Deploy virtual log collectors on-prem and built-in connectors for cloud-based applications	• Ensure customized dashboard views are established. • Integration of additional 3rd party systems and applications with Sentinel • Ensure accurate event ingestion • Complete any cloud or SaaS based application connectors.	• Optional - Finalize and formalize your response plan with MNP's Incident Response Team. • Optional – Perform tabletop exercises with executives • Document and implement security automation workflows
Deliverables	• Proof of value • Review critical and high detections over the two-week deployment period.	• Review & Triage any critical or high-risk findings • Complete log tuning and filtering as appropriate. • Provide final "as-built" documentation workbooks	• Finalize dashboard and reporting functionality • Implementation of security orchestration activities. • Establish External Vulnerability scanning and Virtual CISO cadence
Timing	• Week 1	• Weeks 2-4	• Ongoing

MNP | TECHNOLOGY SOLUTIONS

MNP Technology Solutions applies a collaborative, modern, and measured approach to help organizations thrive in a digital economy. With locations across Canada, our experienced professionals bring the industry and technical know-how needed to accelerate cloud transformation through the adoption of Power Platform, Dynamics 365, and a full array of Azure services and solutions.

For more information, visit mnptechnology.ca

Ready to Get Started?

Mike Alexander
Director, Strategic Partnerships
800.399.5370 x2002
mike.alexander@mnp.ca