NuHarbor SECURITY

www.nuharborsecurity.com

SERVICE OVERVIEW

Sentinel MXDR

Managed extended detection and response on Microsoft's proven Sentinel and Defender XDR platforms

Security beyond the endpoints

Sentinel MXDR from NuHarbor Security is a fully managed cybersecurity service that protects beyond your endpoints. The solution equips your team with comprehensive detection and response capabilities across multiple security domains—helping safeguard identities, Office 365, cloud services, and applications. With the powerful combination of Microsoft's integrated Defender XDR and Sentinel SIEM platforms and deep expert support from NuHarbor Security, you can feel more confident in securing your organization.

How XDR + SIEM + MXDR work together

Defender XDR

Microsoft Defender XDR collects, correlates, and analyzes threat signals and alerts from across the Microsoft 365 environment including endpoint devices, email, applications, and identities.

Sentinel SIEM

Microsoft Sentinel then correlates alerts provided by Defender XDR with a vast amount of external intelligence to detect and assess new threats.

NuHarbor MXDR

NuHarbor's expert-led detection, response, and prevention then uses telemetry provided by both Defender XDR and Sentinel SIEM.

"Microsoft Sentinel is a powerful platform that can be adapted to the specific needs of each organization. NuHarbor has demonstrated their expertise in customizing and managing Sentinel solutions for optimal results."

Jeffrey Asis, Team Lead Principal Security Architect at Microsoft

How Sentinel MXDR can help

The combination of Microsoft's industry-leading machine learning and NuHarbor's deep expertise enables our team to deliver comprehensive support—giving your team the time and peace of mind to focus on other priorities.

- ✓ **Near real-time threat detection and analysis**
  Improve threat detection and response with decreased false positives and thorough investigations of critical alerts.
- ✓ **Expert remediation response strategies**
  Depend on our 24/7 team of trained defenders armed with rapid detection and advanced analytics.
- ✓ **Recognize new attacks and techniques before they cause harm**
  Our analysts leverage the latest threat intelligence and experience across hundreds of clients to identify vulnerabilities and embed automations to disrupt future threats.

Sentinel MXDR service details

With Sentinel MXDR, our award-winning security experts become an extension of your team to manage detection and response 24/7.

Health Check

- Assessment of your desired security outcomes, gaps, and optimal Sentinel data ingestion strategy.
- Actionable recommendations within Sentinel that align with your organization's security.

Consistent Tuning

- Security reviews for improvement of alerts, workbooks, and playbooks.
- A cycle that ensures security alerts and incidents become continually more efficiently manageable.

Daily Environment Reviews

- Daily expert review of the Sentinel workspace, including the identification of anomalies.
- Filtering of false positives, identification of possible threats, and escalations of valid incidents.

Rapid Investigation and Remediation Strategies

- Contextual expert analysis of threats for improved protection and effective remediation strategies.
- Management of threats that goes beyond alerts not prioritized as critical by your Sentinel workspace.
- Ability to operate independently and alongside your security operations center.

Learn more about Sentinel MXDR