Netwoven

Microsoft Security

Four ways Microsoft Sentinel transforms your security operations center (SOC)

Transform your SOC with a trusted security information and event management (SIEM) system built on leading AI, automation, and threat intelligence to secure your multi-cloud, multi-platform environment.

1 Protect everything with a comprehensive SIEM solution

Monitor for and respond to threats across your entire digital attack surface.

- **Normalize data** across a variety of log sources for insight on how attackers move across vectors.
- **Easily augment data** with customizable out-of-the-box content, connectors, automation playbooks, workbooks and more.
- **Store data for up to 12 years** to meet compliance requirements.

2 Drive efficiency with automation

Every minute matters in your investigation. Microsoft Sentinel gives your security operations center (SOC) enhanced tools to ensure rapid incident response.

- **Automate workflows and streamline processes** with built-in security orchestration, automation, and response (SOAR) and curated and fully customizable playbooks.
- **Enrich incidents automatically** with threat intelligence.
- **Reduce time to act** with machine learning that automatically correlates alerts into prioritized incidents.

3 Find threats lurking in your organization

Security analysts want to be more proactive about looking for security threats. Microsoft Sentinel can help.

- **Boost threat hunting** with powerful search and query tools.
- **Search across all your data sources** quickly and easily, with unified hunting across SIEM and XDR/
- **Benefit from Microsoft Threat research's robust insights** to identify threats sooner.

4 Catch emergent threats sooner with AI and Threat Intelligence

Your organization needs to have the latest threat intelligence information to help prevent and detect threats and attacks. Microsoft security is embedded into Sentinel.

- **Take advantage of the more than 65 trillion signals** processed by Microsoft Threat Research every day.
- **Benefit from AI** built for security.
- **Detect threats sooner** with machine learning enriched features.

Let's modernize your SOC with Sentinel

Netwoven can help you accelerate your security operations modernization project through our unique service offering Security Operations Center (SOC). As a Microsoft Solution Partner, we have deep experience providing customers with assessment, migration, hunting expertise, and incident response services to ensure a smooth transition to a modern cloud-based security operations center.

Contact us today

info@netwoven.com

www.netwoven.com

877 638 9683