PROSOC MANAGED DETECTION AND RESPONSE SERVICES FOR MICROSOFT SENTINEL

Extend your IT team by partnering with Proficio for monitoring and management of your Microsoft Sentinel environment. Proficio's ProSOC MDR for Sentinel helps you detect actionable threats, eliminate the noise of false alerts, and enable response orchestration and management of your networks. The addition of Proficio's services allows you to to reduce risk and protect your enterprise, and frees up your team to concentrate on other priorities.

PROFICIO™

Microsoft

SECURITY EVENT MONITORING & ALERTING

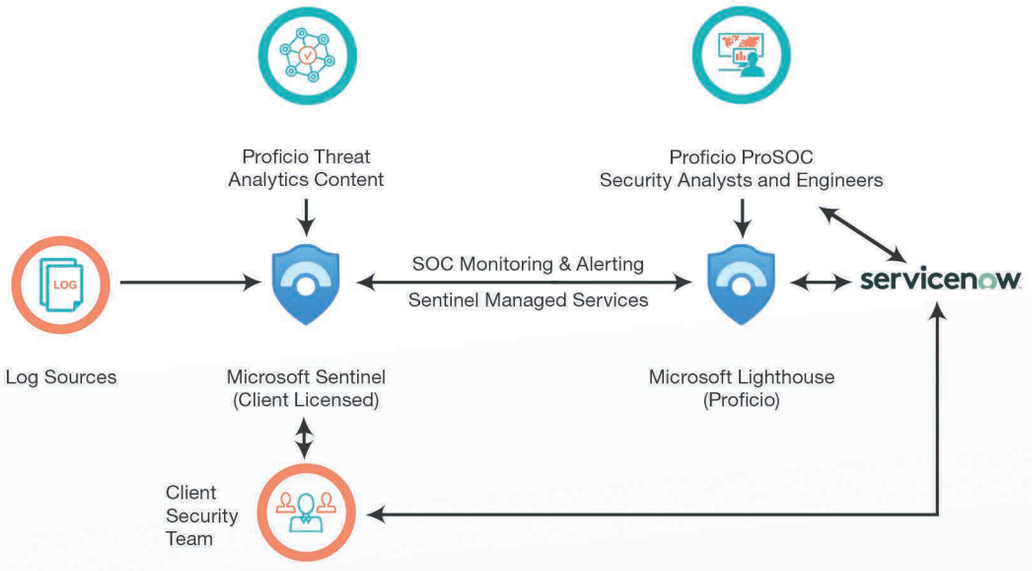
- 24/7 security monitoring, investigation, and alerting
- Rapid threat detection and response triage
- Accurate alerts with data enrichment and guided response
- Detection analytics enabled, added and managed in your MS Sentinel
- Threat Intelligence Data added and integrated
- Manage and report on security compliance and posture
- Detections mapped to MITRE ATT&CK

MANAGED SERVICES FOR MICROSOFT SENTINEL

- Team of Sentinel experts for administration, updates and change management
- Sentinel infrastructure availability monitoring, automation, and notification
- Continuous monitoring of log collection and forwarders
- Extended troubleshooting and resolution of any problems or parsing issues
- Expert-on-call for extended services and content creation
- Support for User and Entity Behavior Analytics (UEBA), Health Monitoring, and Automation Controlled by Resource Group.

Logs and Data Collected

- Azure Cloud
- MS 365 Defender
- MS 365
- Security & Network
- Identity & Access Management
- Endpoint Protection
- Infrastructure
- SaaS Applications
- Threat Intelligence



SUPPORTED PLATFORMS INCLUDE

- Microsoft 365
- Azure Active Directory
- Microsoft Defender for Endpoints
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Cloud
- 3rd Party Security Products for Azure

Recognized in Gartner's Market Guide for MDR Services and Managed SIEM

PROFICIO®

PROFICIO ADVANTAGES

IMPROVED THREAT VISIBILITY

Proficio has built a large library of threat discovery use cases for identity threat detection, leveraging events from Microsoft 365, SharePoint, VPNs, Windows, Active Directory, and security tools like Microsoft Cloud App Security (MCAS). Machine learning models help improve threat detection by identifying anomalies and unusual user activities. Identity-related events are further enriched with threat intelligence data, with correlation rules used to increase the fidelity of alerts. For example, the combination of impossible travel, IP traffic from a known source of malware, and mass downloads is an indicator of an identity compromise. Through Proficio's ProView portal, clients can view dashboards of suspicious user activity and their ThreatInsight® risk score, which includes threat identity in the threat coverage algorithm.

AUTOMATED ACTIVE DEFENSE RESPONSE

Active Defense, Proficio's proprietary automated-response technology allows you to quickly respond to specific security alerts or incidents at the endpoint, perimeter, cloud, or identity layer. When an Active Defense use case is triggered, our solution initiates an automated or semi-automated remediation action in alignment with your change-management process. Actions include blocking abusive IP traffic at a firewall, isolating infected endpoints, and suspending compromised users.

ENHANCED ACCURACY FOR THREAT DISCOVERY

With Proficio's Managed Services for Sentinel, you can get the most out of your investment. Our team continuously adds and tunes analytics and can auto-verify malicious anomalies to reduce false positives. We provide custom dashboards for insight into your Sentinel blade and custom watchlists to help tune use cases and further reduce false positives. We also offer whitelist automation, for greater control of your Sentinel environment, and SOAR playbooks for response and remediation orchestration.

PROFICIO'S MICROSOFT SENTINEL CAPABILITIES VS. OTHER PROVIDERS

Capability	Proficio ProSOC MDR	Other MSSP/ MDR Providers
24/7 SOC monitoring	✓	✓
Azure and Microsoft 365 resources	✓	✓
Multi-cloud resources (AWS, GCP)	✓	✓
Security, network, user, and SaaS resources	✓	✓
Expert threat analytics content	✓	Limited
Tuned to your environment	✓	Limited
Added directly to your MS Sentinel instance	✓	Limited
Active Defense response for automated threat containment for firewalls, endpoints, and identities	✓	Limited
Creation of SOAR playbook	✓	Limited
24x7 Managed Services for MS Sentinel by Certified MS Experts	✓	Limited

Contact us at: Proficio.com | info@proficio.com | 800.779.5042