PROFICIO®

DATASHEET

Seamlessly integrating with your Microsoft Sentinel SIEM, ProSOC® MDR for Microsoft, delivers 24/7 security monitoring, advanced threat detection, automated threat response, expertly managed SIEM services, and implementation support for your Microsoft Sentinel SIEM.

Microsoft Solutions Partner
Security

ProSOC® Managed Detection and Response Services for Microsoft Sentinel

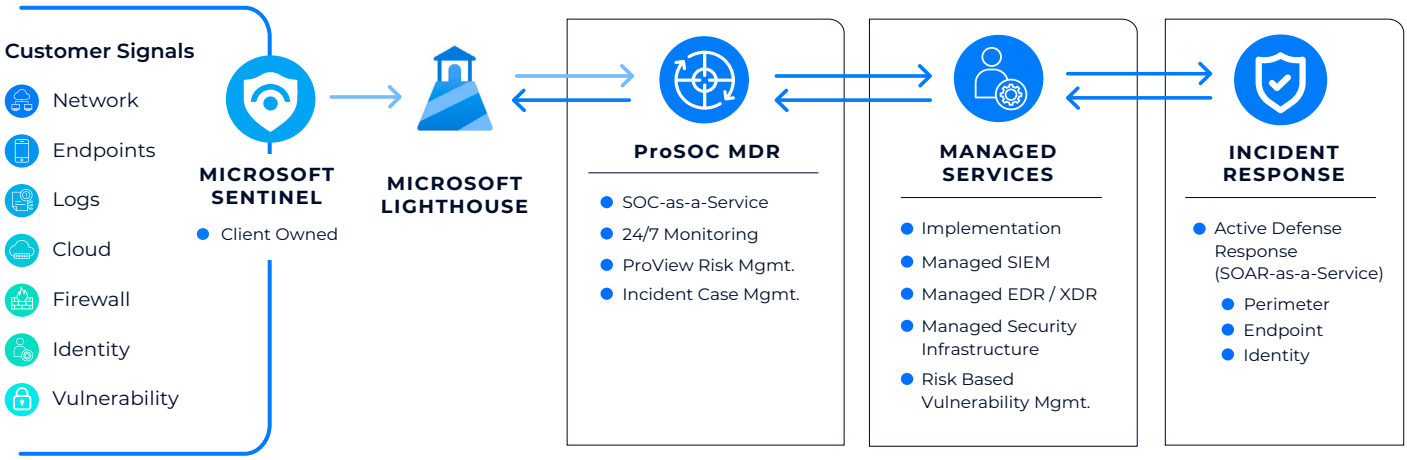
Platform Management and 24/7 SOC-as-a Service

Security Event Monitoring, Alerting, and Response

- Advanced threat detection, investigation, and response alerting
- Leverages your Microsoft Sentinel SIEM, lowering TCO
- SOAR alert enrichment
- Automated and semi-automated response actions to prevent threats and contain compromises across the perimeter, endpoint, cloud, and identity
- Proactive threat hunting to identify and mitigate potential security threats before they can cause harm
- Proficio content and use case tuning

Managed SIEM Service

- Expert management and administration of your Microsoft Sentinel platform, ensuring optimal performance and security
- Continuously updated and enriched threat detection content
- Continuously tuned detection rules to your environment, ensuring relevance and efficacy in identifying threats
- Continuous integration of the latest threat intelligence data, providing deeper insights and improved detection capabilities



PROFICIO®

Proficio Advantages

SOC Monitoring, Investigation, and Alerting

Our expert SOC team leverages Proficio content and SOAR alert enrichment for advanced threat detection, investigation, and response. Additionally, we integrate the Proficio Threat Intelligence Profiler for enhanced threat intelligence. Valid threats are promptly communicated to you with guided remediation steps. Alerts are managed through our ServiceNow®-powered ticketing system, with notifications via email and our ProView Portal. Optional bi-directional integration between our ticketing system and your ITSM tool is also available.

Automated Active Defense Response

Active Defense, Profico's proprietary automated response technology contains and neutralizes threats across networks, endpoints, identities, and cloud environments in less than 3 minutes on average, with actions such as automatic IP blocking, user account suspension, and endpoint quarantine.

Enhanced Accuracy for Threat Discovery

MDR for Microsoft Sentinel ensures robust security through continuously updated threat detection content, keeping your defenses current against evolving threats. Additionally, detection rules are finely tuned to your specific environment, maximizing the relevance and effectiveness of threat identification. This dual approach enhances your overall security posture, providing proactive and customized protection.

Supported Platforms

- 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

Key Differentiators

- 24x7 SOC Monitoring
- Log volume budget alerting
- Multi-cloud resources (AWS, GCP)
- Proficio threat intelligence profiler integration
- Use case tuning
- Automated and semi-automated threat response
- SOAR alert enrichment
- Certified Microsoft experts support
- Proficio content

Available on Microsoft Azure Marketplace

PROFICIO®
ADVANCING THE MISSION OF MDR

Proficio is an award-winning managed detection and response (MDR) service provider that helps prevent cybersecurity breaches by performing and enabling responses to cyber-attacks, compromises, and policy violations. Recognized in Gartner's Market Guide for MDR services annually since 2017, Proficio's experts provide 24/7 security monitoring and alerting from global security operations centers (SOCs) in San Diego, Barcelona and Singapore.

Ready To Get Started?
Request a Demo

GET STARTED

proficio.com | info@proficio.com | +1 800.779.5042