PROFICIO®

DATASHEET

Proficio's ProSOC® Managed Detection and Response (MDR) service provides you with around-the-clock protection from today's advanced cyberthreats. We combine advanced analytics, machine learning, and business context modeling with human-led threat hunting and expert investigations to quickly and accurately identify indicators of attack or compromise.

PROSOC MDR

1. Log Management
2. Use Case Library
3. Machine Learning
4. Threat Intelligence
5. Threat Analyst Investigation
6. Actionable Incident Alerting
7. Case Management
8. Active Defense Response
9. Security Management Portals

Recognized in Gartner's Market Guide for MDR Services annually since 2017

Managed Detection and Response

Comprehensive Cybersecurity Protection

Proficio's ProSOC MDR solution supports cloud or hybrid environments, works with your existing infrastructure, and does not require proprietary sensors or agents. Our security experts act as an extension of your team, monitoring your environment and providing proactive recommendations.

- **24/7 Security Monitoring** from our global Security Operations Centers (SOCs) includes investigation, validation, and triaging of threats and provides actionable alerts.
- **Machine Learning Threat Hunting Models,** combined with analyst threat hunting, help to identify suspicious behavior and targeted attacks.
- **Automated Response** through Proficio's Active Defense reduces the risk of a breach by instantly containing serious threats.
- **Threat Intelligence and Advanced Analytics** help enrich log data for better detection of high priority threats on your network.
- **Managed Endpoint Detection and Response (EDR)** secures endpoints through device monitoring and management at a critical entry point to your network.
- **Proficio's ThreatInsight®** identifies blind spots in your security controls and quantifies cyber risk compared to your peers.
- **Risk-Based Vulnerability Management (RBVM)** prioritizes vulnerabilities based on the risk of exploitation and business context, to ensure patching and remediation efforts have the greatest impact on reducing your business risk.
- **Managed Infrastructure Services** provide expert management of your critical infrastructure, so your security devices operate at maximum effectiveness.
- **Flexible Deployment** allows you to use ProSOC MDR as a fully managed cloud-based platform or work with your own SIEM.

PROFICIO®

Proficio Advantages

A Full Suite of Services

Whether you only need 24/7 monitoring and threat detection or want a fully managed solution, our expert team will help you reduce risk. You can utilize Proficio's cloud SIEM and SOC or use your own SIEM, paired with Proficio's SOC. Our patented ThreatInsight algorithm helps you prioritize your investment in security tools and your assigned senior security advisor regularly reviews your threat coverage in order to make recommendations on how to reduce risk and improve your security posture.

Automated Remediation for Faster Containment

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.

In-Depth Investigations

Proficio's service uses the MITRE ATT&CK® framework to analyze attacks as a set of behaviors that help us to respond faster and stay ahead of adversaries. Our investigations are further enhanced by Proficio's Threat Intelligence Platform (TIP), which adds contextual information and enriches log data for more accurate event detection and alerting.

Identity Threat Protection

In ransomware and other cyberattacks, adversaries are looking for ways to steal credentials, escalate privileges, and move laterally across an organization's infrastructure. Proficio's ProSOC Identity Threat Detection and Response service detects identity-based attacks and compromises to Identity and Access Management (IAM) platforms and can quickly contain a high-fidelity threat by automating the suspension of a user account.

Service Highlights

24/7 SOC Operations

- Global SOCs
- Threat Analysts Investigation
- Proficio Threat Management Platform
- Security Event Management
- MITRE ATT&CK®
- Log Management
- Governance and Compliance Monitoring
- Threat Hunting

Threat Response

- Security Event Notification
- Security Incident Response
- Active Defense

Managed Infrastructure Services

ProView Portal

Threat Investigator Portal

Expert on Call

PROFICIO®
ADVANCING THE MISSION OF MDR

Proficio is an award-winning managed security services provider (MSSP) delivering 24/7 security monitoring and managed detection and response (MDR) services. Proficio has Security Operations Centers (SOCs) in San Diego, Singapore, and Barcelona where our security teams monitor security events, investigate suspicious behavior, and hunt for targeted attacks.

US | Headquarters
San Diego, CA

APAC
Singapore

EMEA
Barcelona, Spain

Ready To Get Started?
Request a Demo

GET STARTED

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