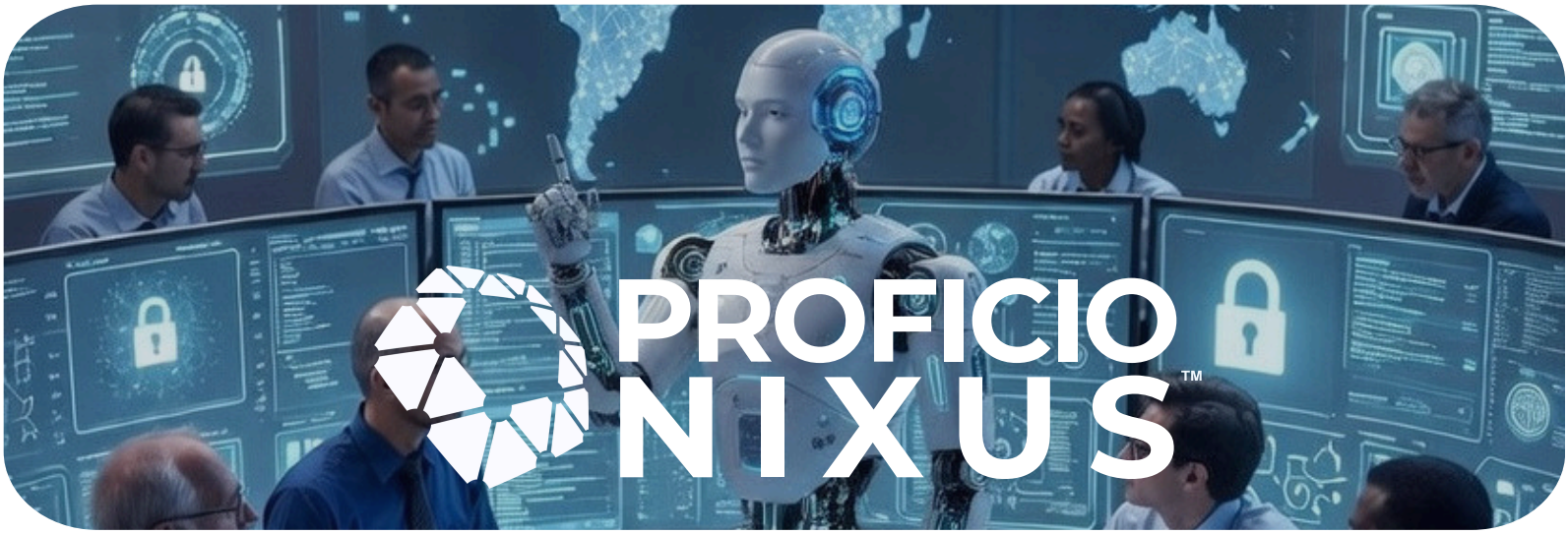


NIXUS AGENTIC AI SOC PLATFORM

Now powering The Next Generation of ProSOC MDR

Continuous Cyber Resilience

<10min

MTTD (Mean Time to Detect)

10x faster than industry avg.

<5min

MTTC (Mean Time to Contain)

20x faster than industry avg.

15+

Autonomous containment actions per week on average

preventing ransomware, lateral propagation, data exfiltration, and business disruption.

WHY NIXUS AI:
Solving What CISOs Need Most

PROTECT ME

Never miss a meaningful attack. Nixus learns your environment, assets, users, and behavior patterns to improve detection accuracy.

REDUCE MY WORKLOAD

AI enhances investigation, enrichment, and triage — your team focuses on what matters, not alert noise.

RESPOND FOR ME

Autonomous and manual containment across Identity, Endpoint, Cloud, and Perimeter with minimal business disruption.

SHOW ME THE VALUE

Executive-level Dashboards, Risk Assessments, MITRE ATT&CK mapping on attacks, KPIs, ODMs, trends, peer benchmarking, and quantified cost savings from your MDR investment.

GROW WITH ME

Supports your current, emerging, and future security and technology stack — including MDR for authorized and Shadow AI.

PROFICIO NIXUS™

WHAT NIXUS AI DELIVERS

AGENTIC AI ALERT ANALYSIS AND TRIAGE

Accurate Investigation and Triage: Nixus reviews every SIEM and security platform alert with layered agents gathering evidence, threat intelligence, historical activity, asset criticality, user behavior, and business context to determine risk, prioritize incidents, and recommend response actions.

Concise Findings: Every incident notification includes a clear summary of what was found, evidence supporting the conclusion, what was involved, what techniques were used, and what should be done immediately to respond and over time to prevent.

INTEGRATED SOC EXPERIENCE

Nixus ISOC Operational Portal: Centralized SOC operational management portal for all services including threat detection and response, managed EDR, managed Firewall, and Continuous Threat Exposure Management. Includes Analyst and AI alert analysis, investigations, triage, and response orchestration with full operational visibility.

Nixus ISOC Security Dashboards: Security gap scores, Risk Assessments, MITRE ATT&CK mapping, threat trends, posture benchmarking, and customizable executive/board reports.

Full Transparency: See what analysts see — detection rules, incident determinations, confidence scoring, and every SOC action taken on your behalf.

THREAT RESPONSE COVERAGE

Identity, Endpoint, Cloud & Perimeter: Autonomous or manual response across your full attack surface.

Prevents: Initial compromises, lateral propagation, ransomware, data exfiltration, fraud, and business disruption.

Measurable Reduction of Incidents Over Time: As autonomous prevention learns and preempts recurring attack patterns.

FLEXIBLE TECHNOLOGY SUPPORT

MDR and XDR using Proficio's hosted SIEM & response platform or your existing SIEM.

Autonomous response via your EDR, Firewall, IAM, SASE, Remote Access Gateway, and Phishing Gateway.

Managed Services for EDR, Firewalls, and Vulnerability Detection & Patching.

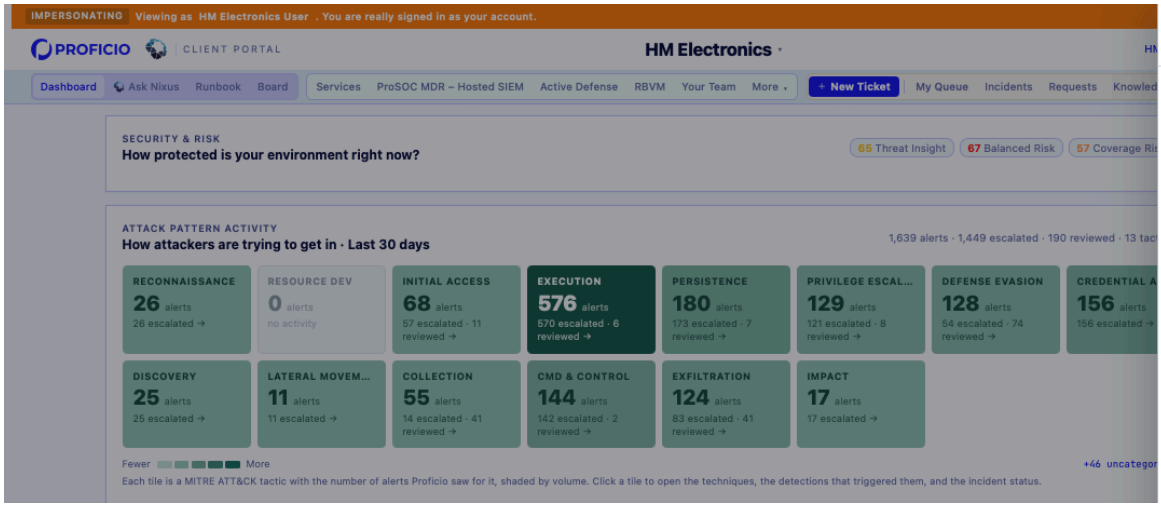
MDR for AI — coverage for both authorized AI and Shadow AI environments.

HOW NIXUS AI WORKS: THE AGENTIC AI CHAIN

1	**Event Categorization**	Classifies the use case at ingest; routes to abbreviated auto-notify or full investigation chain.
2	**Event Analyzer**	Reads the raw SIEM alert and extracts entities: IPs, users, hosts, processes, file hashes.
3	**Historical Correlation**	Deterministic lookup of prior matching events per client/entity; scores recurrence patterns.
4	**OSINT Enrichment**	Queries live public reputation services on extracted indicators; produces a client-safe evidence summary.
5	**Analyst Narrative Agent**	The analytical core — reasons over event + OSINT + history to produce a verdict (benign / suspicious / malicious), confidence score, severity, and an analyst-style write-up.
6	**Routing Decision**	Based on confidence + disposition: silent close, auto-notify client, or escalate to human analyst.
7	**Active Defense Agent**	Generates recommended response actions (isolate host, disable account, block IP) triggering Proficio Active Defense or XDR.
8	**Closure / Escalation Write-Up**	Generates the client-facing summary — branded, complete, and sanitized.

PROFICIO NIXUS™

ATTACK CHAIN VISIBILITY WITH MITRE ATT&CK



MITRE ATT&CK Mappings provide visibility into attack chains, techniques, and tactics, helping security teams understand attacker behavior and **Prioritize Response Actions.**

TRUST & TRANSPARENCY BY DESIGN

100% Auditable

Every agent decision in the chain is logged and reviewable — full traceability from raw alert to response action.

Confidence Scoring

AI determinations include confidence scores and justification — so your team can verify, challenge, or escalate with full context.

Human-Governed

AI operates at speed; humans govern at scale. Analysts review, override, and learn from every agent determination.

MEASURABLE IMPACT

10x
Faster Detection
MTTD <10 min

90%
Alert Reduction

20x
Faster Containment
MTTC <5 min

PROFICIO NIXUS™
AGENTIC AI SOC PLATFORM

Proficio® is an award-winning Next-Generation MDR provider delivering Continuous Cyber Resilience through ProSOC MDR powered by the Nixus Agentic AI Platform. Combining AI-driven threat detection and autonomous response with 24/7 global SOC expertise, Proficio helps organizations find threats faster, reduce security team workload, and stop attacks before they become breaches. Recognized in Gartner's Market Guide for MDR services annually since 2017.

Ready to see Nixus AI in action? Request a Demo

GET STARTED

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