AIRMDR

AirMDR AI SOC Platform for Enterprises

Enterprise-grade investigations and transparency deliver faster outcomes and scalable SOC capabilities using your existing security stack and team.

October 2025

THE CHALLENGE

Staffing an enterprise Security Operations Center (SOC) is costly and hard to sustain. Analysts are stretched across alerts, and workflow complexity means slow responses are the norm. Legacy automation – often static playbooks and Security Orchestration, Automation, and Response (SOAR) – has delivered limited payoff. Enterprises need speed, consistency, and audit-ready proof without relying on specialized automation teams.

THE SOLUTION

AI SOC Platform for Enterprises

AirMDR delivers an agentic AI SOC platform that automates triage and writes consistent high-fidelity cases – so your SOC analysts can focus on security judgment and action. The platform triages 90%+ of alerts in under 5 minutes, automates 80%+ of routine tasks, and produces transparent, audit-ready cases that show their work. Playbooks are written automatically, and adapt via natural language feedback.

Key Outcomes

Scale

Agentic AI triages 90%+ of alerts and automates 80%+ of routine tasks – expand capabilities using your existing security stack and team

Coverage

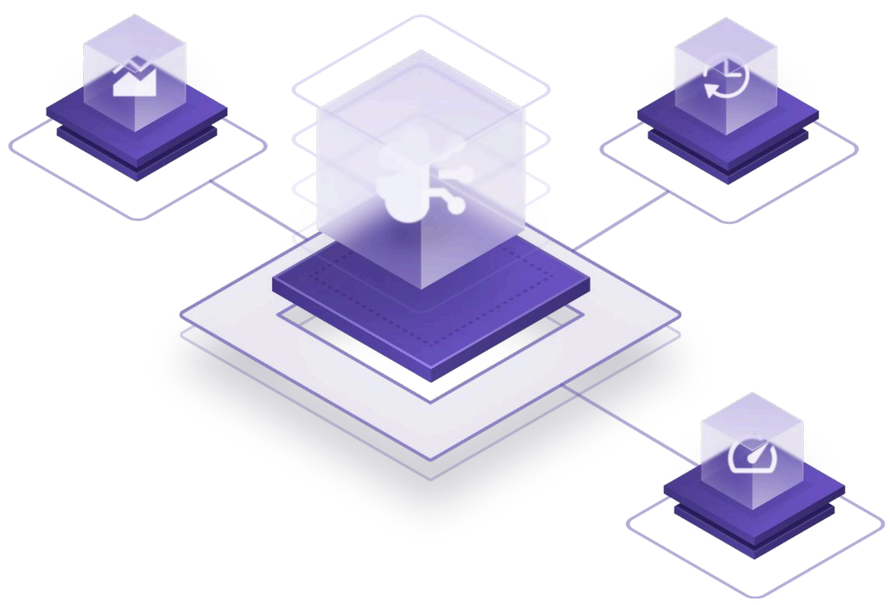
Consistent, 24x7 investigations across SIEM, EDR/NDR, identity, cloud/SaaS, and email

Speed

High-fidelity cases in <5 minutes with transparent, audit-ready evidence

Accessible automation

Every analyst benefits – no coding or scripting required.



How it Works

Ingest

Connect SIEM, EDR/NDR, identity, cloud/SaaS, email, and threat intel via 200+ prebuilt integrations

AI Triage & Prioritization

Reduce noise; rank alerts by risk, impact, and business context

Agentic Investigation

The AI Analyst enriches, correlates, and writes the case with clear rationale; escalate to your SOC experts when needed

Respond

Receive transparent, auditable cases with recommended next steps

Learn & Improve

Incorporates natural-language feedback to refine investigations—governed and auditable

Capabilities & Use Cases

Automation without SOAR headache

daptive investigations instead of static rules and playbooks.

Tier-1 alert offload

Triage every alert without rule sprawl; reduce noise and burnout

Phishing & identity

Consistent investigations with clear, auditable evidence

Cloud & SaaS threats

Faster root-cause analysis and guided response

Resilient workflows

Adapt as tools and schemas evolve without rework; 200+ integrations and growing

Get Started

Connect sources today – minutes to AI-written, audit-ready cases; scale using existing resources.

Contact AirMDR now to see a demo and discuss how it fits into your environment.