InfoSight
www.infosightinc.com

AI-Enabled Purple Team SOCaaS

Powered by AI. Fueled by Experts.

305-828-1003
info@infosightinc.com

A security team, running at machine speed.

AI accelerates telemetry processing, correlation, and threat discovery at machine speed and scale. Human experts validate findings, govern response actions, and make the business-risk decisions.

1 Program

Red + Blue + SOC

Offense, defense, and monitoring operate as one continuous validation engine.

24/7

Continous execution

AI-driven adversary simulation and detection engineering run without fatigue.

Lower Cost

Less waste

Replaces costly point-in-time assessments with a compounding defense program.

Traditional SOC vs. SOCaaS

InfoSight SOCaaS	Other SOC
AI pre-correlates events into investigation-ready context.	Alert queues pile up faster than analysts can investigate.
Continuous Purple Team validation runs as an always-on program.	Periodic testing creates point-in-time assurance only.
Human experts focus on decisions, escalation, and risk governance.	Analysts spend time de-duplicating noise and chasing raw alerts.
Gaps are identified, ranked, and improved in near real-time.	Detection gaps are often discovered after incidents or audts.
Reporting shows outcomes: coverage, exposure reduction, MTTD, and MTTR.	Reporting often measures activity: alerts, tickets, and tool output.

EXECUTIVE VALUE

- Detect faster by compressing analysis cycles from hours to seconds.
- Contain earlier by surfacing live attack paths before blast radius expands.
- Prove controls work with continuous validation and executive-ready evidence.

AI

Human-in-the-lead control

AI executes the high-volume work: telemetry processing, correlation, and gap discovery. Human experts validate outcomes, govern actions, and make every business-risk decision.

Can you prove your security controls *actually work*?

Most organizations can't. InfoSight gives you continuous, AI-driven validation — so you can answer that question in any boardroom, any audit, any incident.

What is cyber risk actually costing the business?

AI closes detection gaps in real time — reducing attacker dwell time, limiting operational and financial impact, and shrinking overall exposure across critical systems and identities.

How do we continuously validate controls and compliance readiness?

Continuous validation replaces static point-in-time assessments with measurable control testing, ongoing exposure reduction, and defensible evidence for compliance and audit requirements.

What do insurers, regulators, and auditors expect to see?

Verified control effectiveness, documented remediation activity, measurable risk reduction, and continuous visibility into coverage gaps and business exposure.

How do we justify security investment to leadership and the board?

Quantifiable MTTD and MTTR trends, risk reduction tied to business operations, continuous control validation, and executive-ready reporting that supports governance, audit, and financial oversight.

THE AI OPERATING MODEL

AI operates as the execution layer of the SOC—processing telemetry, correlating attack paths, and identifying detection gaps at machine speed.

AI processes at machine speed

Correlates telemetry across identity, cloud, and endpoints. Surfaces attack paths and detection gaps instantly — work that used to take analysts hours.

AI continuously tests your defenses

Emulates real adversary behavior 24/7. Validates whether your SIEM, EDR, and response tools actually catch what they claim to.

Humans govern every risk decision

Your experts validate outcomes, control escalation, and make every call that carries business or legal weight. AI works for them — not around them.

Defense compounds over time

Each cycle closes gaps, improves coverage, and reduces exposure. Security becomes a measurable, reportable business asset — not a sunk cost.

30-60 day launch | Continuous validation cycle | Purple SOC component

Turn testing from a compliance checkbox into a continuous source of defensive advantage.

REQUEST THE PURPLE SOC EXECUTIVE OVERVIEW