InfoSight®
www.infosightinc.com



Yesterday's Security Operations Can't Defend Today's Threats

Purple Team SOCaaS

Organizations face machine-speed adversaries while many security operations still rely on manual investigations, periodic testing, and reactive alert queues. The result is increasing operational risk, alert fatigue, and limited confidence that critical controls will perform when needed.

www.infosightinc.com info@infosightinc.com 305-828-1003

Beyond monitoring. Beyond MDR. Beyond annual penetration testing. Continuous cyber defense — powered by AI, expert-validated by InfoSight.

InfoSight's Purple Team SOCaaS

- ✓ Continuous cyber defense
- ✓ Always-on Purple Team validation
- ✓ Risk-centric
- ✓ AI-accelerated investigation
- ✓ Continuously improving detections
- ✓ Reports business outcomes

Traditional Security Operations

- ✗ Reactive monitoring
- ✗ Periodic point-in-time testing
- ✗ Alert-centric
- ✗ Manual investigation
- ✗ Static detections
- ✗ Reports activity

Purple Team SOCaaS: The AI-Native Operating Model

Within Purple Team SOCaaS, AI — powered by InfoSight's proprietary iSIGHT Security platform — becomes the execution layer of security operations.

- AI-driven correlation and behavioral analytics, expert-validated before any action is taken.
- Continuous telemetry collection across identities, endpoints, cloud, network, OT/IoT, and applications.
- Threat intelligence enrichment.
- Threat hunting and detection engineering.
- Continuous Purple Team validation — the always-on core of the program, not a periodic add-on.
- Incident response and executive risk intelligence.

InfoSight's answer is Purple Team SOCaaS: a single program that fuses offense, defense, and monitoring — red team, blue team, and SOC — into one continuous validation engine, rather than three disconnected services.

Purple Team SOCaaS in Action: Continuous Cyber Defense

Continuous Threat Detection: Identify malicious activity earlier.

Threat Hunting: Search proactively for hidden adversaries.

Detection Engineering: Continuously improve detections based on real gaps, not guesswork.

Purple Team Validation: AI-driven adversary emulation runs 24/7, validating whether your SIEM, EDR, and response tools actually catch what they claim to.

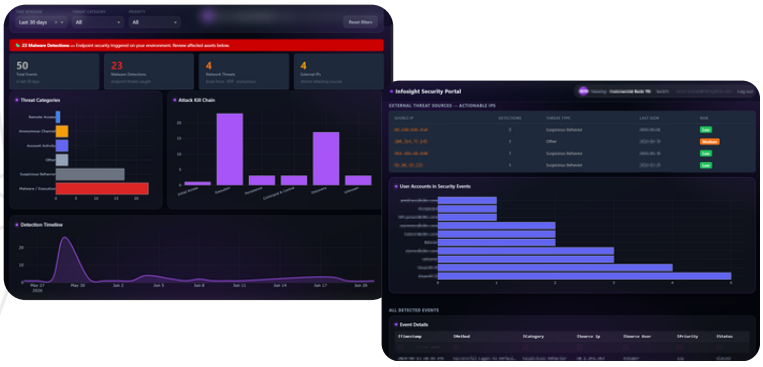
Exposure Management: Prioritize the risks that matter most.

Executive Risk Reporting: Translate technical events into business risk.

Executive Outcomes

- Detect faster by compressing analysis cycles from hours to seconds.
- Contain earlier by surfacing live attack paths before blast radius expands.
- Reduced attacker dwell time and improved cyber resilience.
- Continuous, expert-validated evidence that controls actually work — in any boardroom, any audit, any incident.
- Board-ready reporting tied to measurable risk reduction.
- Improved cyber insurance readiness and greater regulatory/audit confidence.

Security operations should become more effective every day — not simply process more alerts. That's the compounding advantage Purple Team SOCaaS is built to deliver.



Executive Visibility

A Purple Team SOCaaS executive dashboard should answer:

1. Are we reducing cyber risk month over month?
2. Which controls are improving or degrading?
3. Where are our greatest exposure concentrations?
4. How quickly are we detecting and responding?
5. What trends should the board know?

The organizations that will outperform tomorrow are not those with the most security tools — they are those whose security operations, powered by AI and validated by InfoSight's experts, learn, adapt, validate, and improve continuously through Purple Team SOCaaS.