

Managed Services

Managed Security Operations

THE CHALLENGE

Organizations are facing an increasingly complex threat landscape, where the volume, speed, and sophistication of cyberattacks are outpacing traditional security operations and internal team capacity. At the same time, a shortage of skilled cybersecurity talent and fragmented tooling makes it difficult to achieve consistent, 24x7 monitoring, rapid response, and effective risk reduction.

THE SOLUTION

Presidio Managed Security Operations (Managed SecOps) delivers 24x7 monitoring, detection, investigation, and response across endpoint, network, identity, cloud, and log telemetry — helping organizations reduce operational burden, improve visibility, and accelerate response to modern threats.

The platform is designed around flexible operating models, allowing customers to engage through customer-owned, co-managed, or fully managed delivery depending on their current security maturity and operational goals.

Together, the Managed SecOps framework aligns operational maturity, service flexibility, and measurable business outcomes into a scalable security operations model.

THE APPROACH

The architecture is a four-layer operating model with one cross-cutting overlay. Each layer is read top-down: outcomes drive capability requirements, capabilities define what the service model must operate, and the service model determines which technologies belong in the stack. Technology is the bottom layer — it supports the others, it does not lead them.

KEY BENEFITS

- ◆ Round-the-clock protection, zero gaps: 24x7 monitoring, detection, investigation, and response across endpoint, network, identity, cloud, and log telemetry, so nothing waits for business hours.
- ◆ Faster threat containment at the Accelerate tier: Response commitments as fast as P1 ≤ 10 minutes and P2 ≤ 30 minutes, so incidents are contained before they escalate.
- ◆ Flexibility to match your maturity: Customer-owned, co-managed, or fully managed delivery, scaling across three tiers (Essential, Optimize, Accelerate) as your program grows.
- ◆ Reduced operational burden: Helps reduce operational burden at a time when skilled cybersecurity talent is scarce and tooling is fragmented across the industry.
- ◆ AI-accelerated, human-verified response: Detection AI, Response AI, Operations AI, and Outcomes AI accelerate signal and containment, while analyst checkpoints keep human judgment in every consequential action.
- ◆ Consistent, predictable quality: Same playbooks and same SLAs run for every customer, at every tier.
- ◆ Continuous improvement, not a static service: A closed-loop lifecycle (Design, Deploy, Integrate, Operate, Improve) means the architecture compounds value over time.
- ◆ Audit and compliance support: Evidence, reporting, and audit trail built in by design; executive briefings and board-ready reporting at the Accelerate tier.
- ◆ Proven impact: early ransomware detection, and an \$829K TCV gain at Harford County.

Managed Security Operations

WHY PRESIDIO

Presidio is the bridge between where you've been (foundational IT) and where you're going (ultra-modern AI and cloud services), and we measure success in your terms. We strive to build lifetime relationships with those that give us their business, and we do so by being fearless, fast, flexible, and compassionate. It's our mission to earn your trust and deliver innovative, high-quality results at the speed your business needs to succeed.

We are a full lifecycle managed services provider. Soup to nuts. We help you procure the right technology, then we implement it, manage the environment, fill resource gaps and monitor 24/7/365. Our deep discovery process allows us to understand the full picture of your current and future tech needs, skill and process gaps, and the inner workings of your specific culture. The result is repeatable, reliable, effective IT co-management.

FROM ALERT TO ACTION, EVERY TIME

Presidio Managed SecOps delivers 24x7 monitoring, detection, investigation, and response across your endpoint, network, identity, cloud, and log telemetry, addressing rising attack volume alongside a shortage of skilled security talent and fragmented tooling. The result: containment as fast as P1 ≤ 10 minutes at the Accelerate tier, consistent SOC-grade coverage at every tier, and a posture that compounds value over time.

**Ready to close the gap between alert and action?
Let's build your Managed SecOps roadmap.**

Contact Presidio today:
www.presidio.com/contact-us
