



AI-Flex | Full-Stack MDR

Powered by **AiStrike** Preemptive AI SOC

The Future of Security Operations

Traditional Managed Detection and Response (MDR) has reached its structural limits, relying on human-led triage that is inconsistent, expensive, and slow.

ProCern AI-Flex Full-Stack MDR breaks this cycle by unifying **AiStrike's** preemptive AI SOC platform with ProCern's expert **Human-In-The-Loop (HITL)** workflows. This joint offering shifts your defense from reactive alert handling to proactive threat prevention, delivering a modern SOC operating model without replacing your existing security investments.

THE TECHNOLOGY

AiStrike Multi-Agent Architecture

The engine behind AI-Flex is an agentic AI architecture designed to correlate signals across tools, users, and time, built on Retrieval-Augmented Generation (RAG) and Knowledge-Graph Augmented Generation (KGAG). Unlike legacy automation, AI-Flex utilizes specialized AI agents designed for specific SOC tasks:

Detection Agents

Identify detection gaps and improve coverage by recommending new detections and tuning existing rules.

Triage & Grouping Agents

Group related signals to identify "toxic combinations" based on MITRE modeling and filter out 90% of noise.

Investigation Agents

Decompose complex alerts into logical steps, gathering evidence in a few minutes.

Response Agents

Coordinate automated containment and remediation actions from across the stack.

What Makes This Different

AiStrike investigates every alert — because that's where real threats often hide.

Traditional MDR providers prioritize alerts based on severity and volume, meaning low-severity alerts are often ignored or quickly closed. AI-Flex instead correlates signals across time, systems, and identities to identify patterns and trace activity to a single root cause.



The ProCern Advantage: Advanced HITL Integration

ProCern's Managed SOC provides the critical oversight and governance layer that AI alone cannot achieve.

Human-in-the-loop workflows ensure AI-driven decisions align with business context, combining machine speed with analyst judgment.

Our specific HITL workflows are mapped directly to the AiStrike architecture to ensure safety and business alignment:

AiStrike Agent Activity	ProCern HITL Workflow Alignment
Autonomous Triage	Governance & Audit ProCern analysts periodically review suppressed alerts to validate AI logic and ensure no false negatives.
Agentic Investigation	Contextual Enrichment Analysts inject internal business context (e.g., approved maintenance windows) into the AI's reasoning loop.
Recommended Response	Strategic Approval For high-impact actions, ProCern acts as the mandatory safety gate, approving containment in complex production environments.
Continuous Learning	Detection Tuning ProCern Tier 3 analysts use natural language to "teach" the platform, refining detections based on forensic outcomes.

Core Features of AI-Flex Full-Stack MDR

1. Self-Improving Detection Engineering

AI-Flex doesn't just sit on top of your tools; it improves them. The platform **evaluates existing rules in your SIEM, TDIR, UEBA or EDR**, identifies blind spots, and generates "detection as code" to close gaps at the source. This ensures patterns identified during investigation are converted into new detections, continuously improving coverage.

ProCern can also implement the detection engineering changes to your security stack.

2. Included Native Threat Intelligence

The service provides a continuously active control loop of emerging TTPs (Tactics, Techniques, and Procedures) and IOCs (Indicators of Compromise). This intelligence is included out-of-the-box, assessing your exposure in real-time **without requiring third-party subscriptions**.

3. Support for Decentralized & Federated Environments

Designed for the modern cloud era, AI-Flex supports federated detection architectures. It can deploy detections directly onto decentralized data stores, such as data lakes, ensuring comprehensive visibility across hybrid and multi-cloud footprints without massive data egress costs.

4. Superior Automation & SOAR

AI-Flex includes built-in automation and case management. This model allows for deterministic execution of playbooks in minutes, reducing the need for expensive, brittle legacy SOAR engineering.



Measured Outcomes & ROI

Based on global deployments, organizations transitioning to this AI-driven model report significant operational gains:

- **90% Noise Reduction:**
Drastic decrease in false positives reaching human analysts.
- **90% Faster Investigations:**
MTTI (Mean Time to Investigate) dropped from 4 hours to less than 5 minutes.
- **40% Broader Coverage:**
Continuous gap analysis and automated rule creation.
- **50% Cost Reduction:**
Achieving higher security outcomes with half the traditional SOC operating budget.

It's Time to Modernize
Your Cyber Defense!

info@procern.com
1 (833) - PROCERN (776-2376)