AiStrike✦

Preemptive AI SOC Platform for MSSPs

Scale Security Operations. Deliver Better Outcomes.

MSSPs are under constant pressure to support more customers and increasingly complex environments while maintaining consistent response, coverage, and service quality. Traditional MDR models rely heavily on manual investigation, detection tuning, and analyst-driven workflows, making it difficult to scale operations and deliver proactive outcomes across tenants.

AiStrike delivers a preemptive AI SOC platform purpose-built for MSSPs.

By unifying threat intelligence, detection engineering, investigation, and response in a single system, AiStrike enables providers to automate investigations, improve detection coverage across customers, and deliver proactive security outcomes at scale.

Built for Multi-Tenant Security Operations

AiStrike enables MSSPs to deliver consistent, high-quality security operations across customers while simplifying day-to-day SOC workflows.

With AiStrike, MSSPs can:

- Support more customers without increasing analyst workload
- Standardize and accelerate investigation speed and consistency across tenants
- Strengthen detection coverage across diverse environments
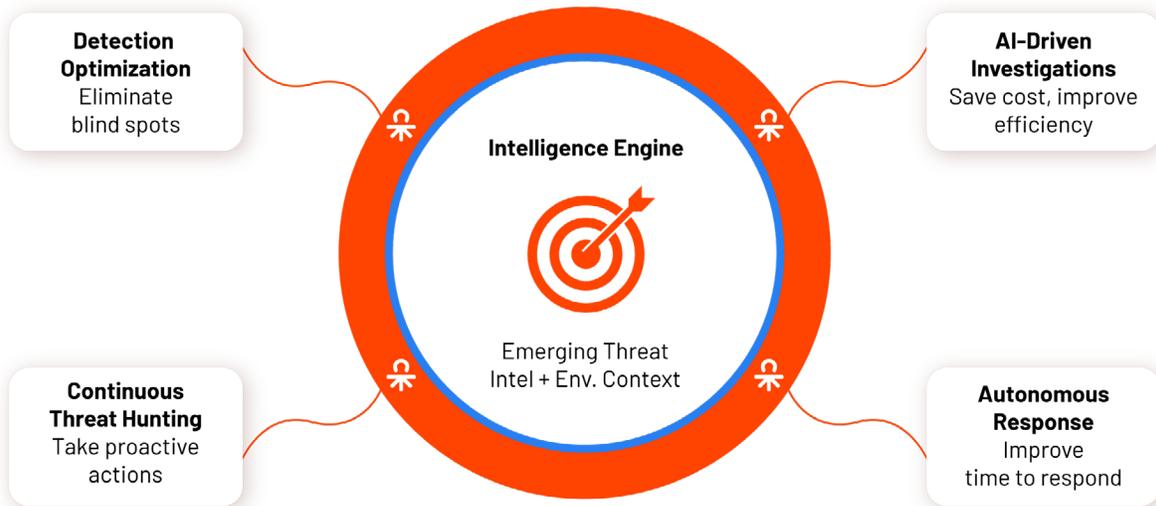- Expand beyond traditional MDR offerings

The platform integrates with each customer's existing SIEM, XDR, cloud, and identity stack, allowing MSSPs to deploy a unified AI-driven SOC model across environments.

The AiStrike Platform:

Powered by agentic AI, AiStrike improves an organization's security posture by unifying threat intelligence, detection engineering, investigation, and response in a single system. AiStrike enhances existing tools rather than replacing them, allowing MSSPs to modernize service delivery while preserving customer investments.

Shift from Reactive Alert Handling to Preemptive Threat Defense
Shift from reactive alert handling topreemptive threat defense.

Detection Optimization
Eliminate blind spots

AI-Driven Investigations
Save cost, improve efficiency

Intelligence Engine

Emerging Threat Intel + Env. Context

Continuous Threat Hunting
Take proactive actions

Autonomous Response
Improve time to respond

Proven Across MSSP and MDR Environments:

AiStrike is deployed across global MSSP and MDRs providers, helping scale existing MDR models with AI-driven operations.

> "We partnered with AiStrike to bring advanced, AI-based cybersecurity to organizations whose needs and budgets don't align with large, complex enterprise platforms. AiStrike's approach leverages AI to significantly reduce alert noise, shorten time to detection, and improve overall SOC efficiency, helping us deliver a more proactive security experience for our clients."
>
> **Carlos Alanis, CEO and Co-Founder, Banyax**

Customer Profile: Public Company, 10,000+ employees
Challenge: High-cost MDR, limited ROI

Weekly Metric	Before	With AiStrike	Impact
Tickets/Week	150	15	90% noise reduction
MTTI	4 hrs.	<5 mins	90% faster investigations
New Detection Rules/Week	0	12	Blind spots closed
Cost	$X	$0.5X	50% reduction

Key Differentiators:

End-to-End SOC Augmentation	AiStrike enhances the entire security lifecycle, not just alert triage. By connecting threat intelligence, detection engineering, investigation, and response in one system, the platform continuously improves detections and operational efficiency across the SOC.
Preemptive Risk-Driven Defense	Most tools react to alerts. AiStrike focuses on preventing incidents. By combining threat intel, alerts, vulnerabilities, and environment context, the platform identifies real exposure, closes detection gaps, and reduces risk before threats materialize.
Delivered As a Service	AiStrike delivers a modern AI-driven SOC operating model without replacing existing tools. Organizations can transition from traditional MDR and reactive workflows to a transparent, scalable AI SOC with expert oversight and continuous optimization.

Measured Outcomes: Across more than 5 million investigations in the past year, customers report

Operational Benefit	Impact
Lower operating costs	Reduce cost by 50%+ without replacing tools
Less noise, more actionability	90% fewer false positives reaching analysts
Stronger detection coverage	40% broader coverage, continuous gap analysis
Faster investigations	Over 90% of investigations completed in under 5 minutes