AISTRIKE

Use Cases

From Reactive SOC to Preemptive Security Operations

Overview

Most security teams aren't struggling because of too many alerts.
They're struggling because detection quality, coverage, and response speed haven't kept up.

AiStrike is an AI-native cyber defense platform built on a Domain-Specific Language Model (DSLM) for security operations. It makes existing SIEM, EDR, SOAR, and MDR investments measurably more effective, without requiring a rip-and-replace.

The seven use cases below cover the operational surface of modern security operations: detection engineering, triage and investigation, security analytics, threat intelligence-driven exposure assessment, threat hunting, response orchestration, and custom automation.

AiStrike Use Cases

USE CASE 01

Detection Engineering

Continuously build, validate, and optimize detections

The challenge

Detection libraries decay. In a typical enterprise SIEM, most rules never fire, a small subset generates majority of the alerts, and coverage gaps remain invisible until an incident exposes them. Quarterly content engineering cycles cannot keep pace with the evolving adversary techniques.

What AiStrike does

- Auto-creates and tunes detection content using DSLM
- Maps detections to real-world threats and behaviors and helps address gaps
- Identifies and tunes noisy, redundant, and dormant rules
- Continuously validates detection efficacy against real telemetry and environment context

Operational outcome

- Up to 90% reduction in alert noise

- Continuous expansion of detection coverage
- Higher fidelity alerts with no increase in engineering headcount

USE CASE 02

Alert Triage and Investigation

Automate investigations and surface what truly matters

The challenge

Tier-1 analyst capacity is a bottleneck in most SOCs. Alert volume and investigation complexity grows faster than headcount, dwell time grows whenever queues back up, and analyst burnout drives the attrition that compounds the problem.

What AiStrike does

- Automates triage and investigation at machine speed
- Correlates signals across identity, endpoint, cloud, and network
- Reconstructs full attack narratives
- Surfaces only high-confidence, actionable incidents

Operational outcome

- <4-minute investigations
- Up to 98% of alerts handled without human intervention
- Analysts focus on decisions—not data gathering

USE CASE 03

Security Analytics (Insider Risk, AppSec Monitoring)

Detect high-impact risks across applications

The challenge

Security analytics use cases — insider risk, application security monitoring, fraud signal correlation — typically require seperate detection and investigation tooling and dedicated analyst teams. They are first to lose attention when the SOC is under load, and first to be exploited when adversaries chain subtle signals across domains.

What AiStrike does

- Applies DSLM-driven behavioral and semantic analysis
- Detects:

- Privilege misuse/compromise
- Unauthorized data access and exfiltration patterns
- Application-layer exposure risks

- Correlates entity behavior, host and network activities, and application telemetry

Operational outcome

- Continuous visibility into insider and AppSec risk
- No need for separate tools or dedicated analyst pods
- Detection of threats that rules-based systems miss

USE CASE 04

Autonomous Threat Hunts

Continuously hunt against evolving threats without adding analyst overhead

The challenge

Threat hunting is one of the highest-leverage SOC activities and one of the first sacrificed under operational pressure. Most enterprises run hunts infrequently (quarterly at best), against threat intelligence that is already days or weeks old by the time hunts execute.

What AiStrike does

- Executes continuous, hypothesis-driven threat hunts
- Leverages real-time threat intelligence to drive threat patterns for hunt
- Automates investigation paths and eliminates false positives
- Surfaces only validated findings.

Operational outcome

- Threat hunting becomes continuous, not periodic
- Findings delivered as actionable insights—not reports
- Increased detection of unknown and emerging threats

USE CASE 05

Threat Intel Triggered Exposure Assessment

Know what matters before it's exploited

The challenge

When new threat intelligence drops - a CVE, a TTP, a campaign indicator, most security teams cannot answer “are we exposed, and where?” within the window that matters. By the time exposure is mapped manually, prioritization is already stale.

What AiStrike does

- Correlates threat intelligence with:
  - Asset inventory
  - Raw security events and alerts
  - Current state detections
  - Vulnerability state
- Identifies exploitable and exposed assets in real time
- Prioritizes remediation based on actual risk

Operational outcome

- Exposure identified **in minutes, not days**
- Risk prioritization based on exploitability
- Faster and more effective remediation

USE CASE 06

Response Automation and Case Management

Disrupt attacks while they are still in motion

The challenge

Response delays are rarely caused by ignorance of what to do. They are caused by handoffs — between tools, between teams, between shifts — and by case management overhead that consumes analyst time after the decision is already made.

What AiStrike does

- Orchestrates automated and analyst-in-the-loop controls
- Dynamic AI-generated playbooks based on the threat investigation
- Automated response across endpoint, network, cloud, and identity systems
- Built-in case management to auto-generate and maintains case records

Operational outcome

- Faster containment and reduced dwell time
- Consistent, repeatable response actions
- Case documentation generated automatically

USE CASE 07

Build Your Own Agent

Automate mundane tasks and workflows to improve efficiency

The challenge

Every SOC has workflows shaped by its own stack, regulatory posture, and operational quirks. Vendor-defined automations rarely fit cleanly, and bespoke automation traditionally requires a dedicated engineering investment most security teams cannot sustain.

What AiStrike does

- Provides a composable, agent-based framework
- Enables teams to build custom workflows using:
  - DSLM intelligence
  - Existing integrations
  - Pre-built orchestration primitives
- Operates in a federated, model-agnostic architecture

Operational outcome

- Custom workflows without engineering burden
- Platform adapts to your operating model
- Consistent automation across all use cases

How these use cases work together

The seven use cases are not independent products. They are facets of a single agentic platform built on a Domain-Specific Language Model for security operations, integrating across the existing security stack.

- Detection Engineering keeps content current
- Triage & Analytics process signals at machine speed
- Threat Hunting and Exposure Assessment close gaps proactively
- Response Automation disrupts attacks in real time
- Custom Automation extends the platform to your environment

Together, they create a continuous, preemptive security operating model.

Deployment & Architecture

- Integrates with existing SIEM, EDR, SOAR, cloud, and edge telemetry.
- Federated, model-agnostic architecture — no data centralization required, no single-AI-vendor dependency.
- SOC 2 Type II certified.

