Agentic Security Operations

Strike48 enables security operations at machine speed. Break through rigid, deterministic workflows across your entire security operations to triage faster, identify and close risks, and cover your entire log infrastructure.

Challenge: Teams have hit terminal velocity.

Alert volumes, attack surfaces, and threat vectors were already outpacing teams—and AI-accelerated threats are bending the curve steeper. Headcount stays flat. Budgets stay tight. The widening gap is existential business risk. The current model can't close it.

- Alert overload
- Rigid playbooks
- Slow response

Solution: Redefine security operations with Strike48.

Strike48 detects, investigates, and responds across your entire environment with AI agents that work like a fully-staffed SOC, 24/7. Parse-at-query architecture makes complete log coverage affordable to eliminate blind spots. Our agents don't assist investigations—they run them. Threats move at machine speed—now your team can too.

- **Pre-Built Agent Packages**
- **No-Code Agent Builder**
- **Log Intelligence Layer**
- **Test Detection Engineering Rules**
- **Non-Deterministic SOAR**

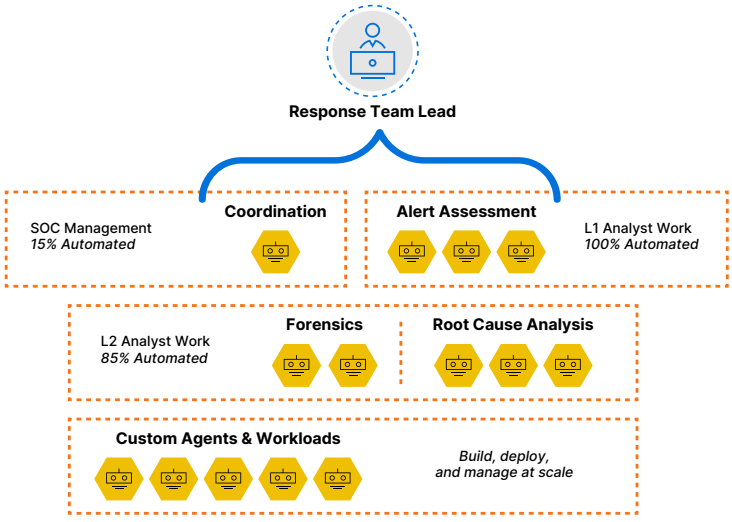
Use Cases Across Security Operations

Alert Triage	Phishing Detection	Detection Engineering	SOC Agentification
Increase Team Capability	Cross-Tool Integration	Threat Hunting	Threat Simulation
Workflow Automation	Log Store Consolidation	Universal Data Language	+ Any Log-Focused Use

Your security operations team, multiplied

Strike48 combines pre-built agent packages that can be deployed and proven quickly, and the ability to build your own agents that support workflows throughout your organization.

Narrow task scoping and multi-agent handoffs eliminate hallucinations, and every action and outcome is auditable. You set the permissions. You stay in control.



Agentic security with zero blind spots

Complete visibility, autonomous investigation, machine-speed response.

Strike48: The Agentic Log Intelligence Platform

COMPLETE LOG COVERAGE

See everything, everywhere

Gain full visibility with 100% log coverage—no more blind spots or hidden risks. Bring your logs or query them in place, never paying to store the same log twice. Monitor every system cost-effectively, and never miss a critical event.

AI AGENTS THAT WORK

Automate, investigate, respond

Deploy purpose-built agents for security, IT, and compliance that handle real tasks—without hallucinations—or build your own. Agents combine cognitive and deterministic steps, work 24/7/365, and always keep a human in the loop.

CONNECTED

Works with your stack

Get insight from your logs where they live. Use Bedrock LLMs, MCP connectors, external DNS, and your existing SIEM/observability tools. Strike48 unifies query language, so there's no rip-and-replace or learning curve required.

Strike48 Agentic Security Works at Machine Speed

	Today: Human	Strike48: Agentic
Advisory hits	hours	immediate
Rules written	days	minutes
Rules tested	never	automated simulation
Alerts triaged	hours	<8 minutes
Patient zero found	hours	minutes
Leadership briefed	end of day	live

Enterprise-ready

- Deployed in Fortune 500
- 10+ years foundation hardening
- Petabyte-scale storage
- Billions of events/day ingestion
- Cloud, on-prem, or hybrid deployments
- LLM agnostic; swap models any time
- Your data never trains our models
- RBAC, tenant isolation, SOC 2-ready

Strike48 Closes the Risk Gap Across Your Organization

Eliminate Risk Blind Spots

Access 100% of your logs—ingest, or in-place, no forced trade-offs on coverage.

90% Faster Investigations

AI autonomously handles Tier 1 triage and Tier 2 investigations around the clock.

60-80% Lower Cost

Eliminate redundant log storage, retire expensive legacy platforms, and improve efficiency.

Headcount Efficiency

Expand coverage with agentic teams while re-deploying human analysts to higher-value work.