Three-Agent Security Team

Strike48 detects, investigates, and responds to threats across your environment with three core AI agents that work like a fully-staffed SOC team, 24/7. Complete visibility, autonomous investigation, and machine-speed response.

Agentic Security With Zero Blind Spots

Strike48's agentic three-agent security team delivers enterprise-grade security operations through specialized agents that work together seamlessly to detect, investigate, and manage security incidents. This solution augments your existing security team with 24/7 automated capabilities while keeping humans in control of critical decisions.

Three Powerful Agents

The SOC Level 1 Agent triages initial alerts and enriches context before handing off complex threats to the SOC Level 2 Agent for deeper investigation and remediation planning. The SOC Manager Agent oversees this workflow by prioritizing incidents, allocating resources, and delivering insights.

By dividing each agent's work into deterministic and cognitive steps, every agent handles only the specialized tasks it's built for, minimizing hallucinations and false positives. Built-in safeguards ensure sensitive decisions are not made without human authorization, analysts can maintain oversight at every handoff, and every workflow is auditable.

Level 1 Analyst Agent	Level 2 Analyst Agent	SOC Manager Agent
• Alert monitoring and triage • Evidence collection • Confidence-based classification • Automated escalation • Lookup management	• Advanced incident investigation • Proactive threat hunting • Incident response coordination • Digital forensics • Documentation and reporting	• Case management • Alert handling • Task Management • Security automation • Data analysis & querying • Information gathering
Automates up to 100% of L1 Analyst Work	***Automates up to 85% of L2 Analyst Work***	***Automates up to 15% of SOC Management Work***

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 redeploying human analysts to higher value work.

FAQs

How does this integrate with our existing security stack without disruption?	Our three-agent security team connects via standard APIs and MCPs to your existing SIEM, EDR, and security tools with minimal configuration. The platform operates alongside your current processes without forcing workflow changes, allowing for phased adoption starting with monitoring-only mode before expanding to active response capabilities.
What safeguards ensure these agents don't make critical security mistakes?	All agent actions follow configurable approval workflows with mandatory human authorization for sensitive operations. The system includes confidence thresholds that automatically escalate uncertain scenarios to human analysts. Every recommendation includes a clear evidence trail showing exact data sources and reasoning, ensuring full transparency and auditability.
How do we measure concrete ROI and security improvements?	The platform provides comprehensive metrics showing alert handling time reductions, false positive elimination rates, and incident response acceleration. Customers typically see 90% reduction in time spent on routine investigations, 65% improvement in accurate threat classification, and quantifiable analyst time savings within the first 30 days of implementation.
How do agents handle our unique security requirements and sensitive data?	Our agents adapt to your specific security policies and can be trained on your organization's unique environment. All data processing occurs within your security perimeter with no sensitive information leaving your control. Custom playbooks ensure alignment with your industry regulations and specific compliance requirements while maintaining full data sovereignty.
Can I add additional agents?	Yes: you can add pre-built agent packages to your existing deployment at any time and start using them right away, or use Prospector Studio to build custom agents without dedicated AI expertise. Either way, there's no technical limitation on how many agents you can run in your environment.