Flocks - SecOps Agents

Free & Open Source · Locally Deployed · Self-Operating · Self-Evolving

ThreatBook

Why your SecOps team needs a digital workforce, not another AI assistant

Alert Overload

80% of SecOps effort goes to triaging alerts, querying devices, and chasing context.

Capability Gaps

Workflow orchestration and complex tasks demand specialized security expertise teams can't scale.

Fragmented Stacks

Legacy and modern tools don't talk to each other. Investigation and response stay manual.

Knowledge Loss

SecOps know-how walks out the door every time an analyst changes role.

Flocks delivers more than efficiency

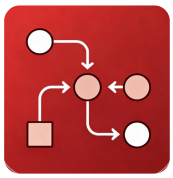
Flocks is a free, open-source, locally deployed Agentic SecOps platform. Multi-agent collaboration gives it the autonomous initiative of a real SecOps analyst, and it keeps evolving as it works.

- Investigates and responds autonomously
- Operates devices like a human
- Orchestrates workflows intelligently
- Self-evolves over time

CORE CAPABILITIES

Agentic SecOps

- Native multi-agent architecture with 7 built-in specialist agents. The Main Agent, Rex, plans and dispatches specialist agents to handle complex tasks.
- 150+ integrated cybersecurity and coding tools.

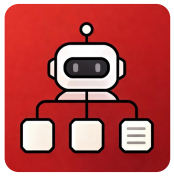


"One-Sentence" Device Onboarding

- Connect any mainstream security device via API using natural language.
- Rex can simulate a human logging into web portals to retrieve device data when an API isn't available.

Self-Evolving Capability Accumulation

- Generate Agents, Skills, Workflows, and tools in natural language, lowering the barrier to entry and adapting dynamically to operational needs.
- Distils lessons from real-world operations and self-corrects, building SecOps capabilities tailored to your enterprise.



Proactive Closed-Loop Operations

- Doesn't wait for prompts. Continuously monitors alerts, tasks, and progress, correlating events across time zones and accumulating institutional knowledge.
- Fully autonomous closed loop from data ingestion and triage to investigation and response.

ThreatBook

Move AI from co-pilot to autonomous SecOps

Scenario 1
Closed-Loop Alert Response

Triage decisions sit unactioned across scattered tools. Flocks chains the platforms together to execute response and ticket routing — so every alert reaches a verified outcome, not just a verdict.

Scenario 2
Cross-Device Correlated Investigation

Stop logging into the same five tools to answer one question. Flocks pulls and correlates data from legacy and modern devices in one pass — cutting investigation time from minutes to seconds.

Scenario 3
Security Device Health Checks

Manual device inspection leaves failures undetected for days. Flocks polls device status on a schedule and summarises findings — fully automating routine device operations.

Scenario 4
Host Compromise Forensics

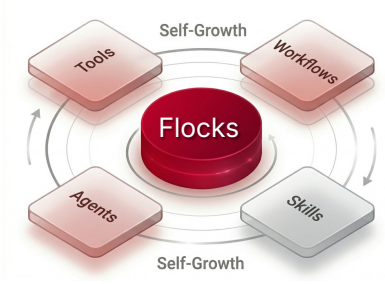
Emergency triage, compromise analysis, and forensic collection in one workflow — reconstructing the full attack chain at machine speed before lateral movement spreads.

Scenario 5
Intelligent Device Integration

Skip the complex onboarding configs. Use natural language to integrate mainstream security devices via API — cutting integration cost dramatically.

Scenario 6
Build Your Own Agents

Off-the-shelf tools rarely fit unique enterprise workflows. Modular composition, low-code customisation, and self-learning let you build proprietary agents that understand your business.



Explore more use cases. Unleash expert intelligence. Build a self-evolving digital security team.

10 million free tokens per day, for the first 30 days after onboarding

Ultra-lightweight: No heavyweight platform deployment. One-click launch on Windows, Mac, or Ubuntu — live in seconds.

Unlimited integration: Embed Flocks into your existing scripts, toolchains, security devices, or in-house platforms with a single instruction.

Agile response: Full open-source codebase and API. Define your own SecOps workflows like building with blocks.

Scan to download Flocks on GitHub