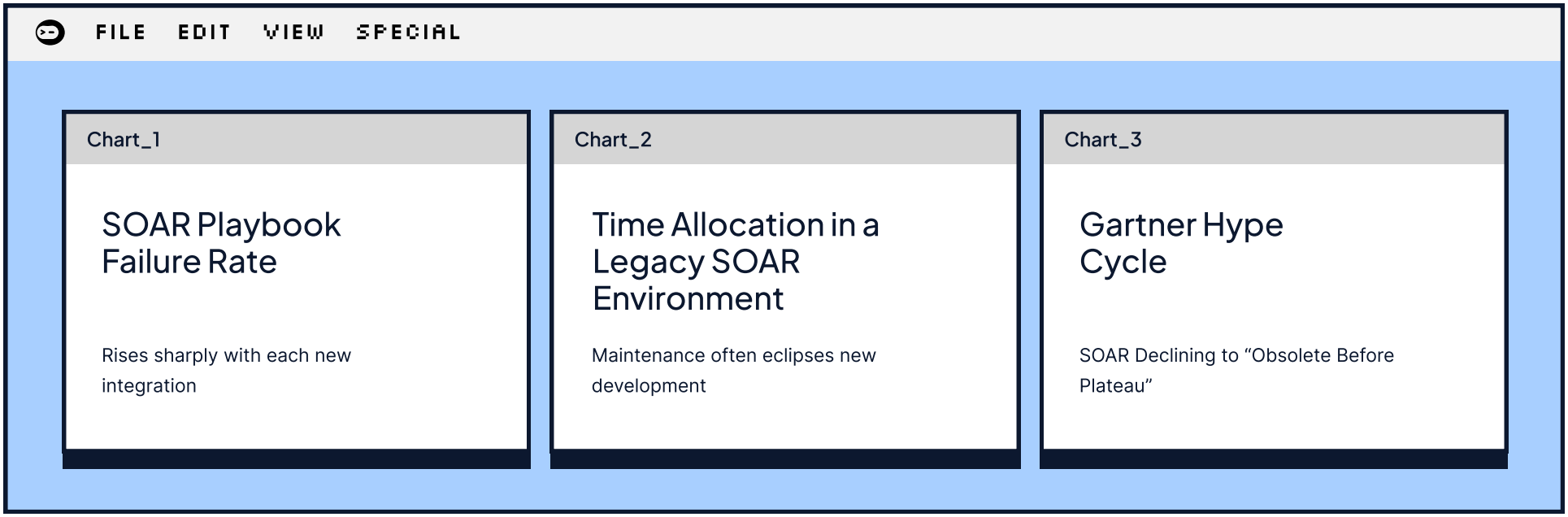
blinkops

BEYOND PLAYBOOKS

A Practical Guide To Replacing Legacy SOAR With AI Agents

The SOAR Problem In 3 Charts

Legacy SOAR was supposed to streamline operations and reduce alert fatigue. But in many environments, it has become the very thing it was meant to fix, a manual, brittle, high-maintenance platform. Here's why that happened:



Security teams bought into the promise of automation, but many were handed a platform that required constant care. Instead of reducing toil, it shifted the burden into scripting, integration repair, and governance firefighting.

Why Playbooks Break And Why That's Inevitable

The fundamental unit of automation in SOAR platforms is the playbook. A playbook is a fixed chain of actions that responds to a known alert. Sounds good on paper, but it breaks under real-world conditions.

Every security tool updates its API at its own pace. Field names shift, authentication methods change, JSON structures evolve. Each of these changes has the potential to break a deterministic playbook.

A Real-World Example

Imagine a playbook designed to extract an IP address from the field alert.source.ip. It performs enrichment via VirusTotal and tags the case.

One day, the EDR vendor updates their schema. The field is now alert.source.ip_address. That single change breaks your playbook. It silently fails, the enrichment is skipped, and the alert remains unanalyzed.

This brittleness scales linearly with the number of integrations and playbooks. Large security teams often spend the majority of their time maintaining old logic instead of building new capabilities.

The Maintenance Tax

Source of Change	Impact on SOAR	Cost to Team
API field renamed	Breaks parsing logic	Hours of rework + testing
Auth method changed	Stops data ingestion	Escalations, vendor calls
Alert format updated	Invalid assumptions	Update parsing and routing

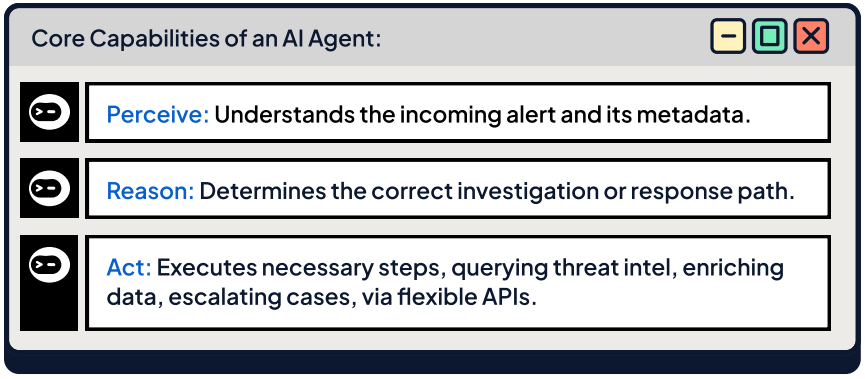
The more automations you build, the more you owe in maintenance debt. That debt compounds until SOAR becomes a bottleneck, not a force multiplier.

Enter Agentic Security:
A New Automation Model

Agentic Security shifts away from fixed playbooks and toward goal-oriented, AI-driven agents. Rather than scripting each step, you define the intent:

"INVESTIGATE THIS ALERT."

The agent then uses a reasoning engine, typically based on a Large Language Model (LLM), to dynamically interpret the context, make decisions, and execute actions.



Agents aren't tied to brittle JSON paths or fixed integrations. They understand context. If **source_ip** becomes **src_ip_address**, they adapt using language understanding.

Use Case: IOC Enrichment – Playbook Vs. Agent

IOC Enrichment_Playbook vs. Agent

Scenario	Legacy SOAR Playbook	Agentic Security Workflow
IOC Enrichment	Requires a hardcoded sequence	Dynamically selects enrichment tools
API Change	Breaks playbook, requires rework	Agent adapts using reasoning
Contextual Output	Limited to pre-configured logic	Agent can explain decisions

This flexibility reduces maintenance, accelerates response, and builds trust. Instead of being a source of toil, automation becomes a reliable teammate.

What Agentic Security Means For The SOC

This shift is not just technical, it transforms roles, workflows, and outcomes.

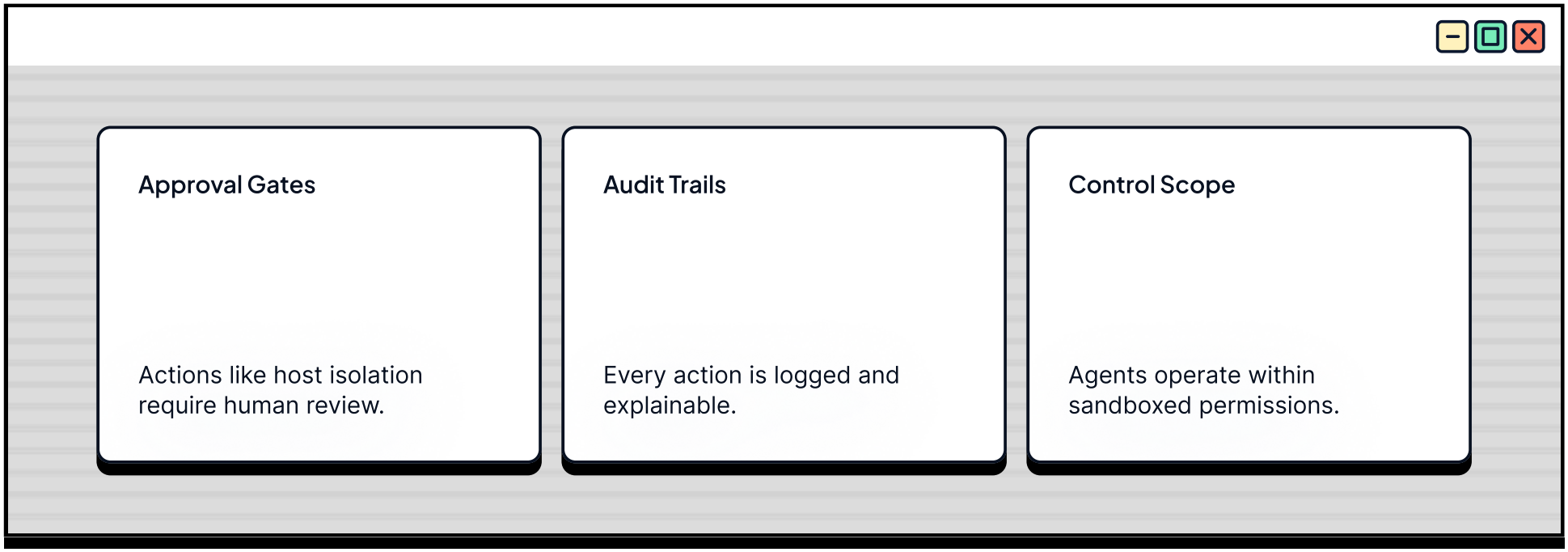
Analyst Evolution

Role	Legacy SOAR	Agentic Security
Tier 1 Analyst	Alert triage, IOC enrichment	Oversees agent, escalates novel cases
Detection Engineer	Writes YAML, tests playbooks	Defines goals, tunes agent feedback
SOC Manager	Tracks MTTR, playbook coverage	Tracks automation % + risk reduction

By reclaiming time from repetitive tasks, agentic security enables strategic work: threat hunting, hypothesis testing, tuning detections.

The Human-in-the-Loop Model

Autonomous agents don't replace humans, they operate with oversight.



This builds confidence and avoids AI-induced chaos.

How To Migrate Without Breaking Your SOC

STEP 1

Identify Pain Points

Start with repetitive workflows that are prone to failure, cloud IAM triage, phishing alerts, endpoint detections.

STEP 2

Deploy in Shadow Mode

Run agentic workflows in parallel. Log their actions. Compare their outcomes with human analysts.

STEP 3

Replace Brittle Steps

Start by replacing enrichment and data gathering steps. Avoid touching response actions until trust is built.

STEP 4

Train Your Analysts

Hold internal workshops. Let analysts inspect and provide feedback on agent output. Gradually increase trust.

STEP 5

Expand and Measure

Once shadow mode proves reliable, shift agents into active workflows. Begin measuring:

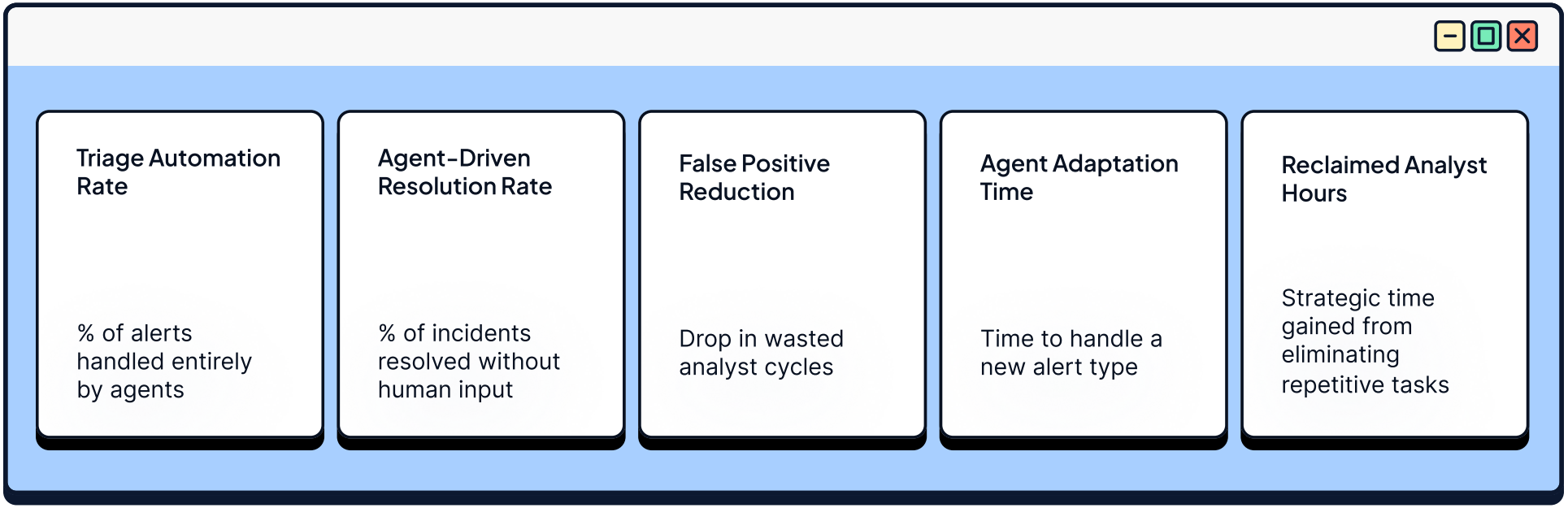
- Alert automation %
- Analyst hours saved
- False positive reductions

Metrics That Prove It's Working

Legacy SOAR was often measured by MTTR. But that doesn't capture the full story of modern security automation.

New KPIs for Agentic Automation

These metrics speak to both operational impact and strategic efficiency.



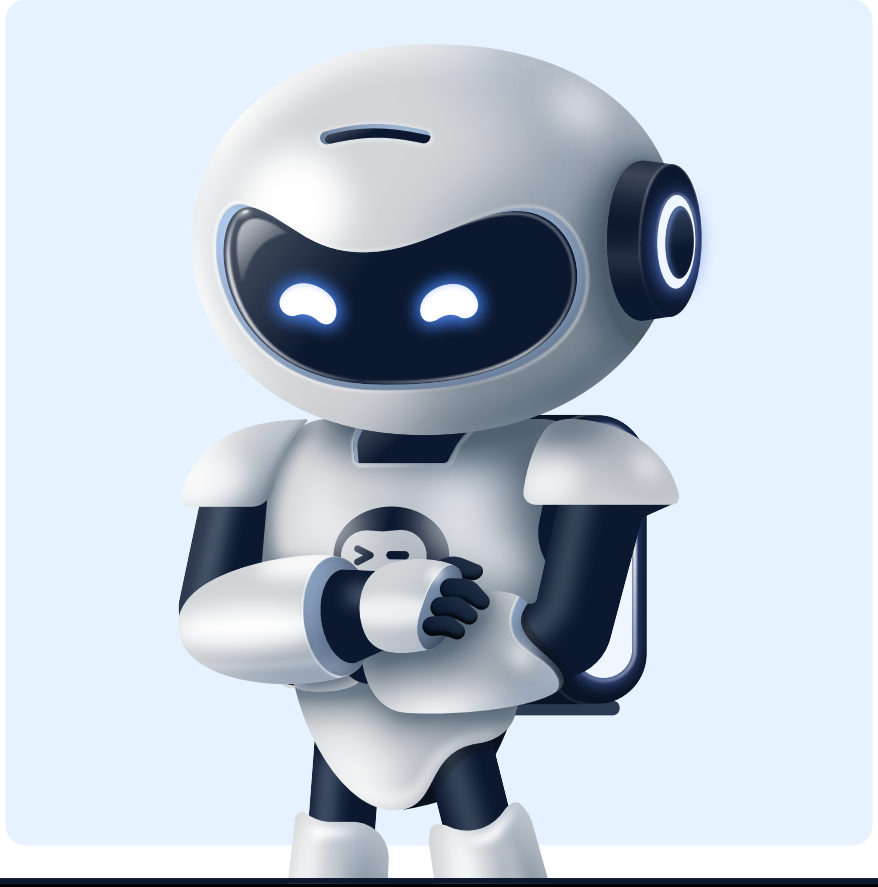
BlinkOps: Agentic Automation In Action

BlinkOps is the first platform built specifically for the agentic security paradigm. It combines no-code agent creation, seamless integrations, and human-in-the-loop governance into a powerful automation engine.

What Makes BlinkOps Different:

- **No-Code Agent Builder:** Launch agents in minutes, without writing a single line of code.
- **Prebuilt Actions + Custom Logic:** Hundreds of integrations plus BYOI support.
- **Shadow Mode:** Safely test agents before live deployment.
- **Approval Workflows:** Grant agents autonomy where it's safe, gate where it's risky.
- **Fast Time-to-Value:** Go live in days, not quarters.

BlinkOps reduces toil, increases resilience, and enables you to scale your security operations without scaling headcount.



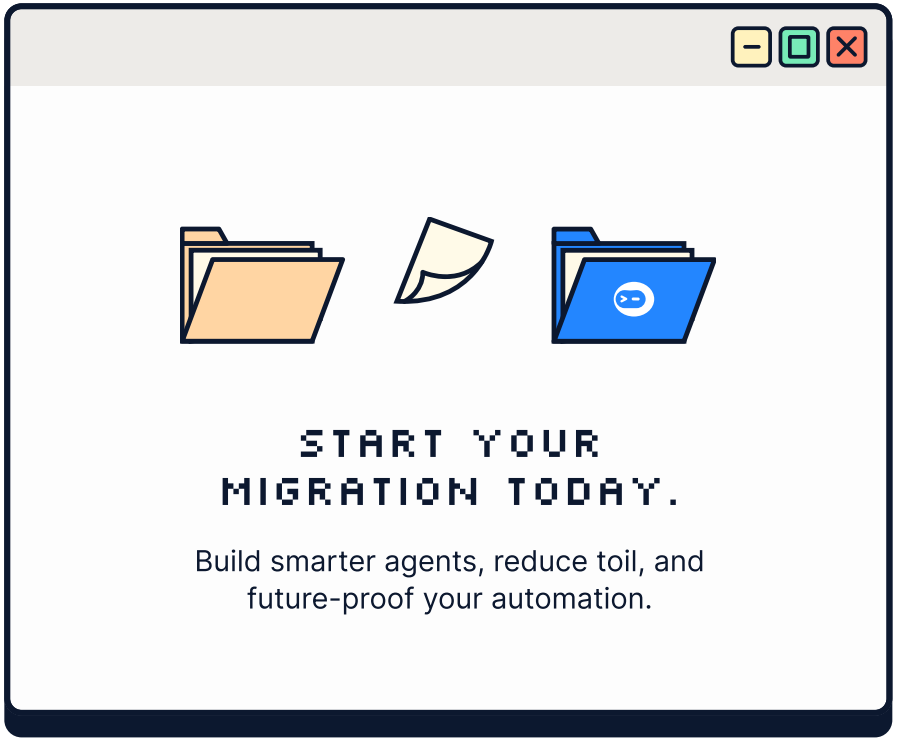
Start Building The Future Of Your SOC

Legacy SOAR is dying, not because automation isn't valuable, but because the method was flawed.

Agentic security changes the model:

- From static to adaptive
- From brittle to resilient
- From scripts to intelligence

Security teams need tooling that grows with them. BlinkOps offers that pathway.



Visit blinkops.com and see what agentic security really looks like.



blinkops

blinkops.com