Strike48™

# How Tronox Uses Strike48 Agents to Autonomously Close 75%+ of SOC Cases

Company: TRONOX | Industry: MINING & CHEMICALS MANUFACTURING

**75%+**
of cases closed autonomously by AI in one month

**670+ hrs**
of analyst time returned in one month

**80%**
decrease in overall MTTR (mean time to resolution)

"Strike48 doesn't just feel faster. It proves it with data. In one month, over 75% of security cases were closed by AI alone, saving roughly 670 hours of analyst time."



Adam Chapman
Director of Cybersecurity

TRONOX

**ABOUT TRONOX**

With approximately 5,700 employees across six continents, Tronox is one of the world's leading producers of high-quality titanium products.

## THE CHALLENGE

## A powerful SIEM, running at human speed

Tronox had an endless backlog of alerts from **identity platforms, EDR, firewalls, and threat logs**, causing many to go uninvestigated. Like most SOCs, Tronox faced the structural problem of balancing competing priorities and the constant awareness that the next serious incident could arrive unexpectedly.

The team was running **Devo** as its SIEM, which gave analysts deep, fast access to security data. The work of understanding that data and making decisions on it still **fell entirely on people**. Analysts memorized complex queries and hand-built each investigation from scratch. Every alert started as a raw signal for a human to interpret, enrich, and resolve.

While that model worked, it **wasn't scalable**.

Adam Chapman, Director of Cybersecurity, who leads the SOC at Tronox, needed a way to do more without adding to the team. Instead of another tool to produce more data, he needed a tool that could do the initial triage and deeper investigations automatically.

**Alert backlog**
FROM MULTIPLE SOURCES

**Complex queries**
MEMORIZED FOR MANUAL INVESTIGATIONS

**100%**
OF ANALYSIS DONE BY HUMANS

THE SOLUTION

## A unified agentic layer on top of the stack

**Data Visibility** | **Alert Triage** | **Case Enrichment** | **Reporting**

Strike48 gave Tronox an AI engine that runs on top of the existing security stack. Strike48 orchestrates the complex workflows that analysts used to run by hand: pulling alerts, running triage, building behavioral baselines, and producing reports. The shift was from a SIEM the team drove manually to an agentic SOC that acts on data autonomously with **investigations, enrichment, false positive detection and automated case closure** – only escalating to the SOC team when an alert needs human attention.

Many of the tools in a mature SOC weren't built with AI. For those tools that add it, the bolted on AI only works within that specific tool, not across the stack. Strike48 enables Tronox to take data from a wide variety of sources like vulnerability scanners, XDR, identity and access management tools, cloud platforms and firewalls to apply a **unified autonomous analysis** on top of the existing systems. This automatically prioritizes what matters to the team right now instead of needing a human to sort through a static list.

Vulnerabilities, suspicious downloads, mailbox rule changes, and threat logs from various sources are all continuously analyzed by autonomous agents, correlated against each other rather than reviewed in isolation.

**"Strike48's secret weapon is allowing previously siloed systems to become a single intelligent fabric."**



**Adam Chapman**
Director of Cybersecurity | TRONOX

THE JOURNEY

## From AI skepticism to closing cases autonomously

Adam's team did not begin as full believers in AI agents closing cases. Strike48 agents gained trust as the Tronox team trained them with its unique playbooks into prompts and workflows. Strike48 agents learned to ground decisions in evidence, baselines, and confidence scores. Once the team started treating the agents as apprentices who they could hand the manual to, they saw that agents could apply the right actions consistently at machine speed.

The team started small, allowing agents to handle a small set of L1 cases, and gradually expanded to more cases after seeing success. Within months, that skepticism gave way to **fully autonomous Level 1 operations**.

For more complex cases, Strike48 does the pre-investigation, building baselines, correlating user and device behavior, and surfacing anomalies. When the analyst opens a case, they find a rich, evidence-based report rather than a raw alert. The humans still make the decisions, but no longer have to spend hours assembling the evidence first.

To validate agent work, the Tronox team was initially checking the work themselves but realized they could have L2 agents verify the L1 agent case closures. For quality assurance, the team created a workflow that applies **25% random sampling** and re-analysis of closed cases, giving the team ongoing verification that autonomous closures are accurate.

**L1**
SMALL SET HANDLED FIRST, THEN EXPANDED

**Autonomous**
L1 OPERATIONS WITHIN MONTHS

**25%**
RANDOM SAMPLING FOR QA CHECKS

**Scalable**
DESIGNED TO GROW WITH USER DEMAND

**"At first, we were thrilled when we got agents to autonomously close 42% of cases in a week, but after we saw we could fully trust their work, we decided to let them do more. We had Strike48 agents close over 75% of cases autonomously in one month, saving roughly 670 hoursof analyst time."**



**Adam Chapman**
Director of Cybersecurity | TRONOX

THE RESULTS

# Moving at machine speed: hundreds of analyst hours saved each week

**75%+**
CASES CLOSED BY AI

**670+**
HOURS SAVED IN ONE MONTH

**<5 min**
PER CASE ANALYZED

**80%**
REDUCTION IN MTTR

**Strike48's value showed up in the numbers.**

In a one month period, Strike48 closed **over 75% of security cases** on its own, resolving them without a human analyst and returning over **670 hours of analyst time.** Those 670 hours equate to more than four analysts working 40+ hour weeks.

While the team was previously prioritizing cases for human attention based on severity, it was inevitable that some low priority cases would wait longer to be addressed. Strike48 **agents now analyze every case within five minutes** enabling the team to have a more manageable workload.
AI filters out false positives and takes care of repetitive triage and enrichment and only escalates to the SOC when necessary.

## This brought down Tronox's overall MTTR by 80%.

"By automating repetitive triage and enrichment and eliminating rubbish, Strike48 frees our analyst resources to focus on higher-impact work that requires a human."



Adam Chapman
Director of Cybersecurity

TRONOX

Strike48 now delivers autonomous case closures, rich investigations, and AI analysis across tools that had none. Beyond these use cases that save hundreds of analyst hours weekly, the Tronox team is planning to expand Strike48 usage across other areas of security and drive SOC innovation to the next level.

## Learn how Strike48 can help you automate investigation and save hundreds of hours of analyst time a week

Request a Demo

strike48.com/demo

Strike48™

The Agentic Orchestration Platform for IT and Security