



How One Security Team Built a Self-Reviewing AI Agent Factory on Strike48

Industry: STAFFING & PROFESSIONAL SERVICES

75%

less analyst time on account-compromise investigations

95%

automated threat hunting, after being fully manual

30 hrs

saved on password spray investigation

5 min

email header analysis, down from an hour

"Anything manual related to the SIEM, we can automate with Strike48. And it's not just reporting. It can take action and give me the analysis."

Security Operations Leader, national staffing and professional services firm

ABOUT THE CUSTOMER

A national staffing and professional services firm with 1,500+ employees and 16,000+ consultants placed with clients.

THE CHALLENGE

A reactive SOC with no time to hunt threats

The firm's security team had alerting and incident response under control. What it lacked was time. Every threat hunt started with hand-written SIEM queries and thousands of log lines that **took days to work through**, so hunts happened only when an incident forced one. That left **low-and-slow attacks**, like password sprays that hit once per IP and never crossed an alerting threshold, unexamined while the team fielded **thousands of alerts a week**.

THE SOLUTION

An agent factory that reviews its own work

Strike48 gave the team an agentic layer over its existing stack, and the team built on it. Within months, the SOC team had **20 custom agents running in production**, each created through an agent builder and checked by an **adversarial build reviewer** before it ships. The reviewer challenges every change across eight dimensions and returns a verdict: approved, approved with changes, or blocked.

IN PRACTICE

A **findings challenger** applies the same pressure to investigation results. When a hunt flagged a user who failed several logins and then registered a new MFA device, the challenger asked for alternative explanations such as the employee getting a new phone. Flagging the activity was correct, but looking at the nuance is essential to avoid a falsely labeled compromise.

— THE JOURNEY

From advisory agents to autonomous hunts

Autonomy scales with the stakes. Advisory agents, like a query builder, teach junior analysts as they work. Investigation agents run phishing-click investigations end to end, then a human reviews the result. Scheduled hunts run on their own when the agent is **at least 95% confident**. **Decisions on containment stay with humans**.

ADVISORY

Teach while they work

A query builder helps junior analysts learn the SIEM

SUPERVISED

Agents investigate, humans review

Phishing-click investigations run end to end

AUTONOMOUS

Hunts run on a schedule

Only when the agent is at least 95% confident

"AI always wants to say it has the answer. In our process, the reviewer agent comes in and challenges it, so it has to actually defend it with reasoning and evidence."

Security Operations Leader, national staffing and professional services firm

— THE RESULTS

Proactive hunting at machine speed

During a password spray that compromised one account, the team caught and contained it quickly. Scoping the rest by hand would have taken a **full 40-hour investigation**. Strike48 reduced the investigation time to only 10 hours. Across account-compromise investigations, agents now build the queries and review the logs, **cutting analyst time by 75%**. Phishing-click investigations that once meant pulling logs for a dozen recipients finish in minutes, and email header analysis dropped **from an hour to five minutes**.

Next, the team plans to extend its SOAR work into **automated containment** under the same review gates.

"Our threat hunting was 100% manual before this. Now it's 95% automated, with just a couple of human gates."



Security Operations Leader

National staffing and professional services firm

Learn how Strike48 can help you build a team of agents and workflows customized to your environment

Request a Demo

strike48.com/demo

Strike48™

The Agentic Orchestration Platform for Security and IT