Strike48

How ELLKAY Used Strike48 Agents to Find an Exposure Manual Checks Missed

Company: ELLKAY | Industry: HEALTHCARE TECHNOLOGY

1
PHP exposure found after a manual check reported none

~200
hosts scanned through Microsoft Defender in one request

312
alerts closed across 13 cases after agent-led tuning

48 hrs
of focused platform time to move several jobs onto agents

"Someone sent an email saying they didn't discover any PHP in our system. I had the Strike48 Threat Analyst scan the environment, and it found one instance on a staging server."

Tyler Theel
Security Incident & Threat Management Team Lead | ELLKAY

ABOUT THE CUSTOMER
ELLKAY is a healthcare data management and interoperability company that connects practices, labs, hospitals and health systems.

THE CHALLENGE

When manual checks fail

1 analyst
DEDICATED TO INCIDENT AND THREAT RESPONSE

PHP + Node.js
ADVISORIES LANDING TOGETHER

0 found
BY THE MANUAL CHECK

In October 2026, a run of PHP vulnerabilities landed alongside new Node.js advisories and signing-certificate news. Security teams across industries dropped everything to **check their exposure**.

At ELLKAY, that job fell to Tyler Theel on the **incident and threat response team**. Once the NSA issued its PHP warning, the security team needed to confirm exposure and report to leadership before anyone outside security had to ask.

An internal check had already reported back by email: **no PHP found in the environment.** That answer was wrong.

THE SOLUTION

An agent that scans your complete environment

Tyler handed the question to a Strike48 **Threat Analyst agent**, one of a team of security micro-agents ELLKAY runs. The agent queried Microsoft Defender (MDE and MDA) across every device Defender could see, **roughly 200 hosts**. Because Strike48 queries data where it lives, the scan needed **no new log ingestion**, working across ELLKAY's environment.

IN PRACTICE
Tyler pasted the full advisory email into a chat with the Threat Analyst. The agent returned **one host running PHP**, a staging server, with the details needed to act. Based on the agent's output, Tyler opened a ticket for remediation. The server running PHP, which was no longer needed, was shut down the same day.

THE JOURNEY

From one scan to a full agent team

The PHP scan was one of several jobs Tyler moved onto agents within his **first 48 hours** using the Strike48 platform. Each one handed a manual task to a specialist agent.

ALERT TUNING

Clear the noise

The SOC Manager agent traced LSASS credential-dumping alerts to Qualys and Microsoft tooling: 312 alerts across 13 cases, which were then closed. The agent updates related cases and tests tuning changes against open cases before they ship.

ORCHESTRATION

One front door

A Team Manager agent routes every task to one of seven specialist agents (Detection Engineer, SIEM Administrator, SOC L1 and L2, SOC Manager, Threat Hunter and Threat Analyst), choosing the correct agent for the task automatically.

> **"I like to think of myself as a director, and the Strike48 agents are my team."**
>
> **Tyler Theel**, Security Incident & Threat Management Team Lead, ELLKAY

THE RESULTS

Ahead of the news cycle with a one-person threat function

1	2 scans	Same day	312
EXPOSURE CLOSED	CONSISTENT RESULTS	TICKET + SHUTDOWN	ALERTS CLOSED

The Strike48 Threat Analyst agent found **a PHP instance a manual review missed** and gave Tyler everything needed to submit the ticket for immediate remediation.

The agent also produced a written report about the vulnerability, which Tyler turned into an **ELLKAY-branded PDF for executives**. Leadership had its answer before anyone outside of security team had to ask.

> **"The Threat Analyst Agent found the vulnerability and gave me everything I needed to get it remediated. The agent also produced a detailed report that I shared with leadership."**
>
> **Tyler Theel**
> Security Incident & Threat Management Team Lead
> ELLKAY

Next, ELLKAY is building a standing job: when a new CVE drops, an agent checks exposure and sends the CISO a branded **"affected or not" report**. The team is also connecting other systems, like NinjaOne, Salesforce and Jira, to Strike48 without migrating any data.

Answer "are we impacted?" before leadership asks

Whatever your stack and however small your team, Strike48 turns the next zero-day from a scramble into a report. Request a demo to see it in your environment.

Request a Demo strike48.com/demo

Strike48™

The Agentic Orchestration Platform for Security and IT