AUTONOMOUS SECURITY OPERATIONS · HEALTHCARE

A 250-node phishing playbook, migrated off XSOAR to under 25.

How one of the ten largest federally qualified health centers in the United States of America moved its entire phishing response off Palo Alto XSOAR onto Alaris Workflows, rebuilt as a handful of nodes and several AI agents.

OUTCOMES · PHISHING MIGRATION · PLATFORM-REPORTED

<25

WORKFLOW NODES

Rebuilt from a 250-node XSOAR playbook

1

SOAR PLATFORM RETIRED

Phishing runs entirely on Workflows

0

PROCESS CHANGES

The email intake path was untouched

<1 hr

TO REBUILD ON WORKFLOWS

What took the team weeks to build on XSOAR

INDUSTRY	ENVIRONMENT	MIGRATED FROM	SCOPE	PUBLISHED
Healthcare, federally qualified health center	90+ care sites, one of the ten largest FQHCs	Palo Alto XSOAR	Phishing response, end to end	July 2026

IN THIS STUDY

MODULES DEPLOYED

- Workflows
- Alert Triage + Investigation
- Containment + Response
- Reporting

INTEGRATIONS IN SCOPE

Palo Alto XSOAR
SOAR · MIGRATED FROM

ManageEngine
ITSM / TICKETING

Email Intake
PRESERVED

01

The situation

The customer is one of the ten largest federally qualified health centers in the United States of America, running more than 90 care sites and serving hundreds of thousands of patients a year. Its security function is a small team responsible for everything from detection to audit response across a footprint that never closes.

Phishing was the team's most developed automation. Every reported email ran through a 250-node playbook on Palo Alto XSOAR that pulled context, scored the message, and routed a response. It worked, but it had grown into one of the most complex things the team owned.

02

The pressure

WHY IT MATTERS

Phishing is the workflow most teams automate first and maintain longest. It is where SOAR complexity accumulates.

Two hundred and fifty nodes is two hundred and fifty places for a change to break. Every new phishing pattern meant editing branching logic and testing the whole path, and the playbook leaned on a platform and a skill set the small team had to keep current.

250

Nodes in the phishing playbook the team maintained on Palo Alto XSOAR. Every change meant regression-testing the whole path.

The response was effective but heavy. Keeping it running took a dedicated full-time hire whose entire job was maintaining the XSOAR playbook, and even then the depth of the branching made it hard to explain why the playbook had reached any given verdict.

What the team wanted was the same phishing response with far less to maintain: no change to how staff reported suspicious email, no break to the intake the organization already trusted, and a verdict it could actually explain.

THE ARITHMETIC

A 250-node playbook is 250 places for a change to break. Every phishing update was a full-path regression test.

03

The migration

HELD THE INTAKE

Nothing about how staff reported phishing changed. The migration was invisible to the rest of the organization.

Alaris migrated the phishing response off Palo Alto XSOAR and onto Workflows as a full replacement, not a partial integration. The goal was the same behavior with a fraction of the moving parts.

On Workflows, the hundreds of conditional branches gave way to a small set of nodes and several AI agents working together. The nodes carry the flow; the agents reason about each reported email and return an evidence-based conclusion on its source and intent. The 250-node playbook became fewer than 25, and what had taken the team weeks to build on XSOAR was rebuilt in under an hour.

HOW THE MIGRATION RAN

250 NODES TO UNDER 25

01 Captured intent

Took the XSOAR playbook and the exact behavior it had to preserve.

02 Mapped the flow

Traced every data source, integration, and the email intake path.

03 Held the intake

Confirmed nothing about how phishing reports arrive had to change.

04 Nodes plus agents

Recreated on Workflows as a few nodes with AI agents for judgment.

BEFORE AND AFTER

METRIC	BEFORE	WITH ALARIS
Phishing platform	Palo Alto XSOAR	Alaris Workflows
Playbook complexity	250 nodes	Under 25 nodes
Build time	Weeks	Under an hour
Decision logic	Hand-built branching	Nodes + AI agents
Playbook upkeep	Dedicated full-time role	No dedicated role
Email intake	Existing path	Unchanged

The migration was end to end and invisible to staff: same intake, far fewer paths, evidence attached to every verdict.

04

The result

METHODOLOGY

Node counts and scope are platform-reported from the migration record.

Phishing response now runs on Workflows in under 25 nodes. Reported emails still arrive the same way, AI agents return an evidence-based read on source and intent, and the team maintains a fraction of what it used to.

Palo Alto XSOAR is retired for this workflow, and the full-time role that existed to maintain it is no longer spent on upkeep. The behavior the team relied on survived the move; the complexity did not. A change that once took weeks now takes under an hour.

WHAT CHANGED IN PRACTICE

01 A tenth of the parts

250 nodes became under 25, so a change touches a handful of steps instead of a sprawling tree.

02 Nodes and agents

A few nodes carry the flow; AI agents reason about each reported email and attach the evidence behind every verdict.

03 Invisible to staff

The email intake path was preserved, so no one outside the security team had to change anything.