AUTONOMOUS SECURITY OPERATIONS · HEALTHCARE

30,000 Sophos alerts a week. Thirty days to quiet the queue.

How one of the ten largest U.S. federally qualified health centers took 30,000 weekly Sophos alerts out of the analyst queue, through alert clustering, account-aware auto-close, and connector filtering. Told in its own numbers.

OUTCOMES · FIRST 30 DAYS · PLATFORM-REPORTED

30,000
SOPHOS ALERTS A WEEK
Recurring endpoint events, before tuning

~1%
REACH A HUMAN NOW
Clustering and auto-close absorb the rest

0
SOC HEADCOUNT ADDED
The same team, different work

30 days
TO STEADY STATE
Simple filters first, then autonomous close

INDUSTRY	ENVIRONMENT	SECURITY TEAM	PRIOR AUTOMATION	PUBLISHED
Healthcare, federally qualified health center	Top-ten FQHC, 90+ care sites	Small team, no dedicated SOC	Demisto SOAR playbooks, since replaced	July 2026

IN THIS STUDY

MODULES DEPLOYED

- Detection Engineering
- Alert Triage + Investigation
- Threat Hunting
- Containment + Response
- Reporting
- Workflows

INTEGRATIONS IN SCOPE

Sophos
ENDPOINT DETECTION

ManageEngine
ITSM · TICKET SYNC

Demisto
SOAR · REPLACED

01

The situation

This organization is one of the ten largest federally qualified health centers in the country, operating 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.

The tooling was in place: Sophos on the endpoint, ManageEngine for tickets, and a Demisto SOAR carrying a set of hand-built playbooks. The problem was volume. Sophos alone produced roughly 30,000 alerts a week, and the great majority were recurring events from a handful of service accounts and a few noisy detection rules.

02

The pressure

FIELD NOTE

The four pressures on this page are the same four we hear on nearly every first call with a mid-market health system.

Most of those 30,000 weekly alerts were duplicates of each other: the same rule firing on the same host, the same service account tripping the same benign check, over and over. Spread across a small team, the queue was impossible to work, so most alerts were never truly investigated.

~99%

Share of weekly Sophos alerts that were recurring or duplicate events, carrying no new information for an analyst.

The volume was not just a people problem. The mass of alerts slowed the platform and made the ManageEngine sync brittle, so tickets lagged and the record the team relied on could not be trusted to be current.

The pressure was no longer internal. A peer health system in the region had just disclosed a breach, the board wanted evidence of continuous coverage, and the next HIPAA audit was on the calendar. The team needed the queue answered, not summarized.

THE ARITHMETIC

30,000 alerts a week, at even two minutes each, is 1,000 hours of triage. The team had about 120.

03

The deployment

HOW TRUST RAMPS

Filtering started conservative. Simple filters and grouping first; as the system proved out, clustering and auto-close moved to more aggressive policies, tuned per account.

Alaris connected read-only first and sat with the SOC analysts to trace where the noise came from: which service accounts, which users, and which detection rules were firing the same benign events again and again. The team started with simple connector filters and alert grouping, then widened the policy as each step proved safe.

Alert clustering now collapses recurring and duplicate alerts before they reach the queue. A new alert is compared against recent open alerts from the same source, matched on title similarity and shared entities, and an agent confirms a genuine duplicate before collapsing it under a parent. The agent investigates the cluster once; the analyst sees one item, not twenty. Known-benign accounts auto-close on their own and surface in a single weekly recap, so the team reviews unique occurrences instead of thousands of tickets. The Demisto playbooks were rebuilt as agent workflows, with fewer branching paths and evidence-based conclusions on the source and intent of each email.

NOISE LEDGER · WEEKLY AT STEADY STATE · CLUSTERED, THEN AUTO-CLOSED

~29,600	~20:1	1	0
REMOVED FROM QUEUE	DUPLICATES PER CLUSTER	RECAP PER ACCOUNT	BENIGN EVENTS TO A HUMAN

THE QUEUE, BEFORE AND AFTER

METRIC	BEFORE	WITH ALARIS
Weekly Sophos alerts ingested	~30,000	~30,000
Alerts reaching an analyst	~30,000	~300
Recurring or duplicate alerts	Thousands	Collapsed to one
ManageEngine sync under load	Brittle	Stable
Analyst hours on Sophos, weekly	~90	~5

Ingest volume is unchanged by design. Alaris does not stop Sophos from firing, it answers what fires.

04

The result

METHODOLOGY

Figures reflect a 30-day post-deployment window, platform-reported and measured against the deployment record.

Steady state looks unremarkable, which is the point. Recurring Sophos events collapse before they reach anyone, benign service-account activity closes itself and surfaces once a week in a recap the team actually reads, and the ManageEngine record stays current. The team spends its hours on the alerts that are genuinely new.

WHAT CHANGED IN PRACTICE

01 One review, not thousands

Benign account activity closes itself and lands in a single weekly recap the team reviews in minutes.

02 Duplicates collapse

Recurring alerts cluster under one parent; the agent investigates once instead of twenty times.

03 Tuned to their risk

Reasoning mode, auto-close policy, and clustering are set per account and dialed up as trust builds.

Alaris Security

Move faster than your adversaries

BOOK A WORKING SESSION

alaris.security