

CUSTOMER STORY: SECURITY

Public sector · City government · Legacy SIEM → Elastic Security

How a major U.S. city government scaled Elastic Security across 12,000+ agents

After its prior SIEM dropped log data it could not ingest fast enough, one of the largest U.S. city governments moved to Elastic Security on Elastic Cloud, bringing 12,000+ agents under continuous monitoring with automated, one-click SOC response.

12,000+

Agents under continuous monitoring

~1,000

Network devices normalized to ECS

170+

Active detection rules, custom + built-in

Manual → 1-click

SOC response actions now automated

The challenge

- ✗ Prior SIEM dropped log data under volume, leaving detection coverage gaps.
- ✗ Response actions ran manually and inconsistently across SOC analysts.
- ✗ No built-in alert automation; case closures reconciled by hand.

The solution

- ✓ Elastic Security on Elastic Cloud ingests every source, normalized to ECS.
- ✓ 170+ rules (custom + Elastic Security Labs) detect across the full estate.
- ✓ Tines integration enriches cases and runs one-click response actions.
- ✓ Elastic AI Assistant flags anomalies before they become outages.

How the workflow runs

1. Ingest & normalize

12,000+ agents, ~1,000 devices into ECS

2. Detect

170+ rules fire on complete data

3. Enrich & case

Alerts route to Tines via API

4. Respond

One-click isolation, reset, block

5. Sync

Case closure syncs back to Elastic

Before

- Logs dropped under volume, coverage gaps
- Manual, inconsistent response steps
- Case closures reconciled by hand

After

- Continuous ingestion across the full environment
- One-click, auto-documented response
- Cases pre-enriched; closures sync automatically

“These actions run with a **click of a button** and automatically leave notes within the case for record keeping.”

— Senior member of the city's security operations team (anonymized)

Why it matters beyond one SOC

The team is extending the same ingestion layer into Elastic Observability, already using it to right-size servers and troubleshoot network outages. For a government managing cost and complexity across a large, heterogeneous estate, one platform that ingests everything reliably is both a security and a budget argument, whether the environment is a few hundred endpoints or tens of thousands.

[See how Elastic Security gives public sector teams continuous detection and automated response or start a free trial →](#)