

CUSTOMER STORY: SECURITY Software & technology · Global SOC · Self-managed on-prem → Elastic Cloud

Siemens reclaims ~5,000 SOC analyst hours a year on Elastic Security

Siemens runs Elastic as a common data platform across global cyber defense and its Amberg lighthouse factory, reclaiming roughly 5,000 analyst hours a year and shifting constrained teams from firefighting to prevention.

~5,000 hrs

Analyst hours reclaimed per year

6B/day

Events correlated to ~170 cases/day

<1 week

Detection-rule delivery, was weeks

1.2 PB

Queried across 300,000+ endpoints

The challenge

- ✗ The security team lost ~2.5 to 3 people a year to patching, hypervisor management, and infrastructure upkeep.
- ✗ Scaling capacity meant a purchase order, a rack, and cabling, not a configuration change.
- ✗ Standing up a new detection rule joined a three to four week backlog.
- ✗ Correlating telemetry across siloed data pools was slow and stitched together by hand.

The solution

- ✓ Security analytics moved to Elastic Cloud with Elastic Security on top.
- ✓ A unified data layer correlates 6 billion events a day into ~170 cases for human judgment.
- ✓ Machine learning flags behavioral deviations, keeping false positives down.
- ✓ AutoOps on the self-managed factory stack deployed in about 10 minutes.

How the workflow runs

1. Ingest & normalize

Logstash pulls in 6B events a day

2. Correlate & score

~11,000 alerts aggregate to ~170 cases

3. Detect with ML

Anomaly models cut false positives

4. Triage & investigate

Analysts judge the cases that matter

Before

- ~2.5 to 3 people a year absorbed by data center operations
- New detection rules waited three to four weeks
- Problems surfaced from a complaint email or a slow query

After

- ~5,000 hours a year redirected to security work
- New detection rules delivered in under a week
- The platform surfaces the signal first via correlation, ML, and AutoOps

“We have effectively given our team 5,000 hours back every year, time we now invest in staying ahead of adversaries rather than catching up with logs.”

— Ricardo Oliveira, Head of Engineering Protection and Automation Solutions, Siemens

Why it matters beyond one estate

The lesson is portable whether a team protects a few hundred endpoints or 300,000: a platform that lets a constrained team spend its time on the mission, not the machinery, changes what that team can do. Next, Siemens is moving toward AI-assisted operations with Elastic AI Agent, Attack Discovery, and agentic workflows and extending ingestion to cover more operational technology data.