elastic

Chainguard

CUSTOMER STORY: AGENTIC SECURITY OPERATIONS

New team, fragmented tooling → Elastic

1 billion events a day, 900+ detection rules as code, built by a months-old team on Elastic Security

Chainguard, the trusted source for hardened, production-ready open source, runs detection and response on Elastic Security Serverless: 900+ detection rules managed as version-controlled code, enriched with entity context, and stood up by a cyber resiliency team only months old.

~1 billion
Events a day ingested on Elastic Security

900+
Detection rules, 280+ custom, as code

32
Log sources; 27 live without custom code

21 of 26
Critical sources covered, gaps tracked

The challenge

- ✕ A months-old cyber resiliency team inherited a fast-moving, fragmented environment with no single home for an investigation
- ✕ Dozens of log sources across many vendors and hundreds of alerts a day, with thin institutional knowledge
- ✕ At least 100 alerts a day, each needing manual investigation, pulling engineers off engineering
- ✕ Cloud-native by design, with no capacity to run clusters, tune performance, or operate security infrastructure

The solution

- ✓ Standardized on Elastic Security Serverless, vendor-managed, with nothing for the team to operate
- ✓ Every source normalized to a common schema (ECS); 900+ rules managed as version-controlled code in git
- ✓ Entity analytics and lookup indices add entity context to prioritize higher-risk identity and endpoint activity
- ✓ An Elastic Agent Builder triage skill reconstructs each case and recommends a human-reviewed verdict

How it works

1. Sources
32 sources normalized to ECS

2. Detections
900+ rules, most run as code

3. Cases
150 to 200 cases a day

4. Triage
AI recommends, a human decides

5. Escalation
Confirmed findings route out

Before

- Log sources scattered across many vendors, no single home
- Nearly every alert investigated by hand; triage entirely manual
- Would have required managing clusters and tuning performance

After

- → 32 sources on one platform, 27 onboarded without custom code
- → 150 to 200 cases a day, about 60% auto-resolved within minutes
- → Serverless, with nothing for the team to operate

> "We're a security company, so anything we do needs to be audited and documented. Anything our AI SOC isn't more than 95% confident about gets routed to a human for approval."
>
> — Joaquin Nafstad, Senior Security Engineer, Chainguard

Why it matters beyond one team

The portable lesson: invest early in schema and query fluency, cut noise deterministically before sending alerts to a model, and reserve AI for synthesis while a human owns anything uncertain. Near-term work is taking the triage skill into everyday operation, closing the remaining critical-source gaps, and evaluating Attack Discovery on a cost-aware path, with consolidation onto Elastic over roughly six months.

See how Elastic Security brings detection, triage, and response into one agentic platform or start a free trial →

