elastic

SANS | Research Program

PRODUCT BRIEFING

An Agentic SOC Without the Black Box: How Elastic Security Closes the SOC's Cost and Consolidation Gap

Insights from the 2026 SANS SOC Survey

June 2026

The 2026 SANS SOC Survey outlines a SOC dissatisfied with the tool it depends on most, migrating to the cloud faster than that tool was built to follow, and paying to store data it never uses. SIEM ranks among the least satisfying technologies SOC teams run, even as cloud adoption outpaces what legacy SIEM architecture can support. Elastic Security was built to replace that architecture directly, pairing Elasticsearch's speed with pricing that lets teams keep the data they need without paying to store what they never use.

The Real Cost of Legacy SIEM Economics

The 2026 SOC Survey's findings matter for procurement because they describe one architecture from three angles: Teams are dissatisfied with it, outgrowing it, and paying more each year to keep it running. Every added integration and every dataset held back to control costs adds friction without reducing the volume the SOC must manage.

Elastic Security was designed to replace that architecture rather than patch around it. Attack Discovery distills overwhelming telemetry into prioritized, actionable intelligence, and the AI Assistant handles the manual work of triage, summarizing alerts, generating detection queries, and suggesting remediation using models built into the platform rather than layered on top of it. Because pricing is tied to what teams act on rather than what they store, ingesting more data does not mean paying more to keep it around, an approach the platform calls resource-based pricing.

Key Findings

SIEM ranks among the least satisfying tools in the SOC.

Asked to grade satisfaction with nearly 60 security technologies, respondents rated SIEM third from the bottom, behind only EDR/XDR and next-generation firewalls, and worse than SOAR, threat intelligence platforms, and cloud tools like CASB and CSPM. Elastic Security is built to replace that architecture rather than sit inside it, giving analysts the speed legacy SIEM platforms were never built to deliver.

Cloud migration is outpacing legacy SIEM architecture.

The share of SOCs running cloud-based services is projected to climb from 42% today to 58% within 12 months, the largest architecture shift in the survey, while reliance on a single centralized SOC continues to decline. Legacy SIEM platforms built for on-premises, single-location environments are increasingly asked to correlate data across infrastructure they were never designed to reach. Elastic Security consolidates that visibility on a single platform, using Elasticsearch's speed and ES|QL's cross-source correlation so analysts have one place to investigate across legacy and cloud.

Indiscriminate data ingestion is quietly driving up SOC costs.

34% of respondents send all available data into their SIEM or syslog with no selection criteria, and the resulting storage and licensing costs tend to outpace the value that data produces in an investigation, often forcing teams to limit what they ingest and trade visibility for budget. Elastic Security's resource-based pricing lets teams ingest what an investigation needs and pay only when they act on it.

Platform Capabilities

Most enterprise SOCs still run on legacy SIEM architecture built for a smaller, slower data environment never designed for multicloud volumes. Migrating off that architecture while keeping detection coverage intact is where consolidation projects stall. Elastic Security replaces that architecture directly, giving teams one platform for ingestion, detection, and response across legacy and cloud workloads.

AI Assistant and Attack Discovery

Elastic's AI Assistant uses generative AI and transparent large language models to summarize alerts, generate detection queries, and suggest remediation steps. That's work that would otherwise fall to a Tier 1 analyst case by case. Attack Discovery distills overwhelming telemetry into prioritized, actionable intelligence, saving analysts from the manual review alert fatigue is built on (see Figure 1). Because the underlying models are visible, analysts can verify why the platform reached a conclusion instead of taking it on faith.

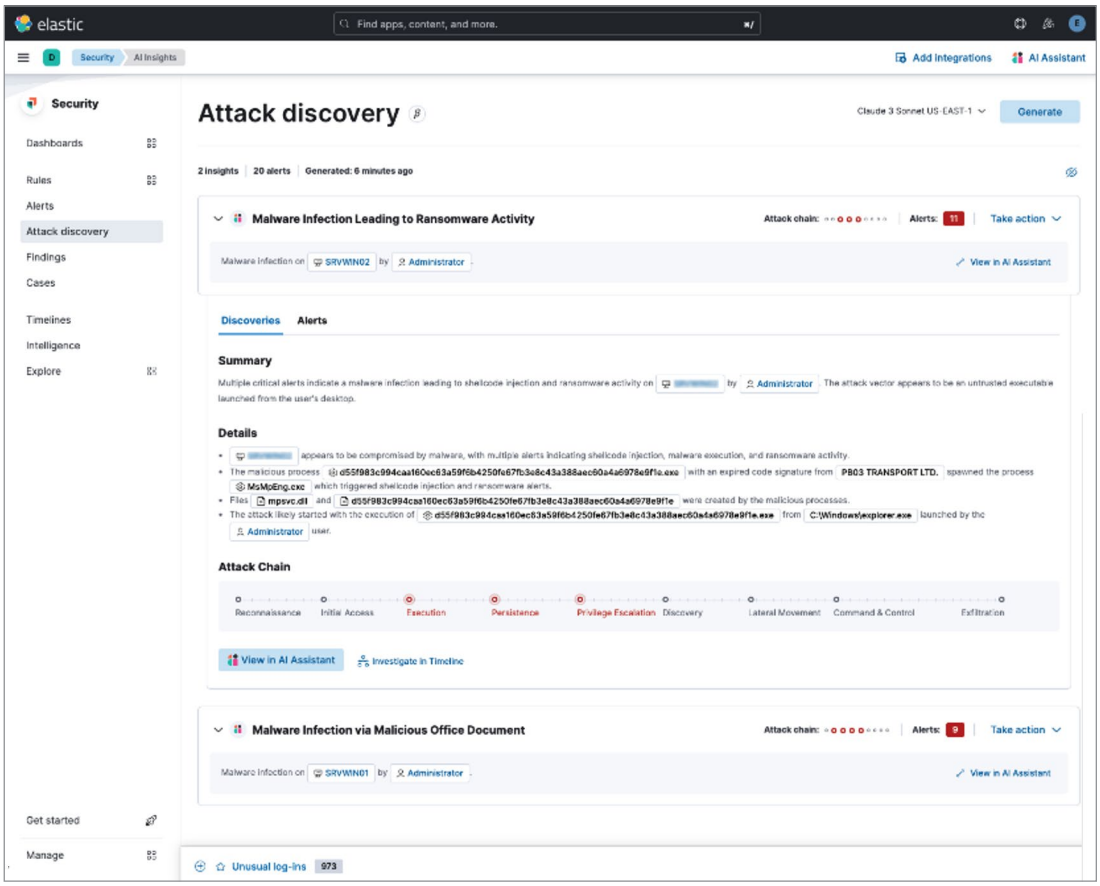

Figure 1. Elastic Security Attack Discovery and AI Assistant Interface

Resource-Based Pricing

Elastic Security's resource-based pricing means teams can ingest the data they need and pay only when they act on it, rather than being charged for retention regardless of whether that data ever gets used. That model gives analysts richer context than volume-capped ingestion allows, without forcing SOC leaders to choose between visibility and budget.

SIEM Consolidation Across Legacy and Cloud

ES|QL, Elasticsearch's pipe-based query language, lets analysts navigate, filter, and correlate data across sources without rebuilding queries for each platform. Paired with SOAR capabilities that orchestrate responses to known threats, Elastic Security lets Tier 1 analysts focus on complex incidents instead of routine triage, consolidating legacy and cloud workloads onto one platform.

Request a Demo