Anvilogic Data Sheet

Modular Detection & Investigation for the AI Era

Anvilogic is an adaptive AI SOC platform that unifies and enhances threat detection & investigation across diverse security data sources without centralization. It's designed for SOC analysts, detection engineers, threat hunters, and incident responders seeking to overcome the limitations of traditional SIEM-centric approaches.

Key Features

Federated Detection Execution

Run detections across Splunk, Sentinel, Snowflake, Databricks, S3, and more, without data duplication.

Detection-as-Code (DaC)

Version, test, and deploy detection content with CI/CD workflows. Treat your detections like sofware code.

AI Copilot & Autonomous Agents

Our agent suite help build, tune, triage, and maintain detections, reducing manual SecOps workloads by 90%.

Advanced Correlations

Drag-and-drop MITRE TTPs across multiple stages to build advanced attack chains. Instead of point detections, Anvilogic lets you model and detect stealthy, multi-stage threats that single-event detections and in-stream models routinely miss.

Triage & Investigation

Cut 45% of alert noise with 98% confidence. Investigate from a single MITRE-mapped panel enriched with verdicts, context, and playbooks that scale analyst decisions across the SOC.

Challenges

- Are SIEM costs or ingest limits forcing you to cut back on visibility?
- How many tools does your SOC have to investigate across today?
- Are detection engineers stretched thin managing rules across multiple tools?
- SIEM alert fatigue creating unmanageable backlog, difficulty upkeep with emerging coverage
- Do you have security data sitting in S3 not being used for detection?

How We're Different

Anvilogic is an adaptive AI SOC platform that unifies and enhances threat detection & investigation across diverse security data sources without centralization. It's designed for SOC analysts, detection engineers, threat hunters, and incident responders seeking to overcome the limitations of traditional SIEM-centric approaches.

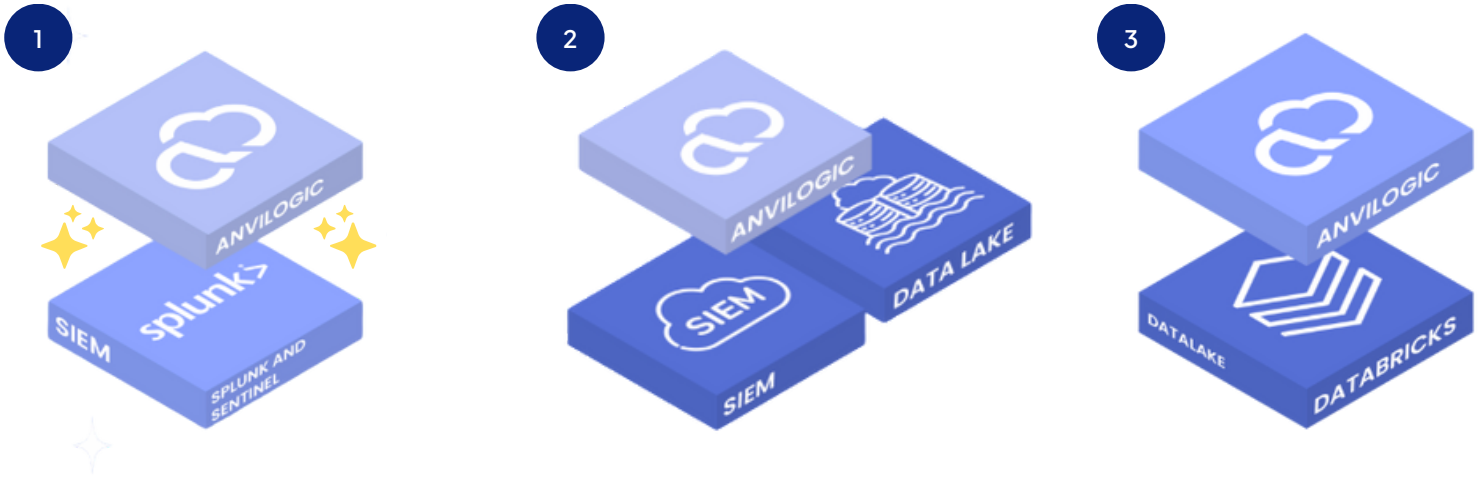
Problem	Legacy Tools	ANVILOGIC™
Analytics tied to storage	Requires centralized ingest	Decoupled detection logic
SIEM pricing model	Based on ingest/query volume	80% cheaper than Splunk & Sentinel
Rule maintenance	Manual, tool-specific	AI-tuned Detection-as-Code
Detection Content	Shelf ware blackbox hard to customize	90% of our library is actively deployed
Cloud telemetry	Expensive to ingest & egress	Run detections in place (e.g., S3)
Multi-platform detection	Not supported	Native feature

Who is it for?

- Security teams tired of SIEM costs and limits
- Detection engineers juggling multiple tools
- SOCs moving to Snowflake, Databricks, or cloud-native storage
- CISOs looking to reduce vendor lock-in and SIEM tax
- Mid-market and enterprise orgs modernizing their architecture without blowing up ops

Adoption Strategy

Anvilogic is built to meet you where you are—not force a rip-and-replace.



Our 3 Primary Deployments:

1. **Augment your SIEM**
   Keep running Splunk and/or Sentinel. Let us run detection & triage smarter.
2. **SIEM + Data Lake Modernization**
   Expand detections onto lower-cost data lakes.
3. **Replace legacy SIEM**
   components entirely, running directly on data lakes and lakehouses. ex) Databricks or Snowflake

Use Cases We Crush

Improving SIEM Value

- Splunk/Sentinel alert fatigue
- Detections against custom data source
- Apply schema to unify disparate data
- Translate atomic rules into reusable logic

Hybrid Detection

- Detection across hybrid cloud (AWS, Azure, GCP)
- Offloading heavy data feeds (VPC, Application, Full EDR telemetry) to cheaper data lakes

Improving Alert Effectiveness

- Enrich and tune detections with context
- Simulate cross-platform threat correlation
- Build scenario-based detections from multiple alerts
- Improve signal-to-noise ratios

Full SIEM replacement for budget-conscious SOCs

- Validate business-aligned threat detections
- Route alerts through modeled workflows

Best Selling Points

- A validated framework for scalable, unified detection
- Operationalized detection scenarios tied to real threats
- Tuning optimization for rules and integrations
- Agentic workbench for detection lifecycle management

Rakuten streamlined detection engineering, reduced 43% manual alert triage, and saved thousands of analyst hours without increasing headcount. Holds the record for most custom-built detections across Anvilogic customers (270+).

SAP ran Splunk and Databricks in dual mode for two years, using Anvilogic as the bridge to modernize detection. Starting with the Enterprise Cloud Services business, SAP scaled detection-as-code across platforms, cut alert noise by 90%, and proved the model before expanding organization-wide, gaining speed, coverage, and full control over their full security data strategy.

Kroll fully exited Splunk by moving to Anvilogic + Snowflake, rapidly deploying 395 detections, integrating 49 tools in under a month, and scaling global security services with speed and depth.