PARTNERSHIP DATA SHEET

Cribl + Anvilogic

Complete data-to-detection pipeline for modern security operations

Cribl routes security data to cost-effective data lakes. Anvilogic layers intelligent detection and guided triage on top—activating that data to reduce real-world risk.

Data Control

Cribl Stream and Edge route, reduce, and transform security telemetry before it lands in Snowflake, Databricks, or Azure Data Explorer—reducing ingestion costs while maintaining full visibility.

Detection Intelligence

The Anvilogic AI SOC Platform overlays behavioral detections, AI-driven tuning, and streamlined triage workflows directly on your data lake, delivering SIEM detection outcomes without legacy SIEM costs.

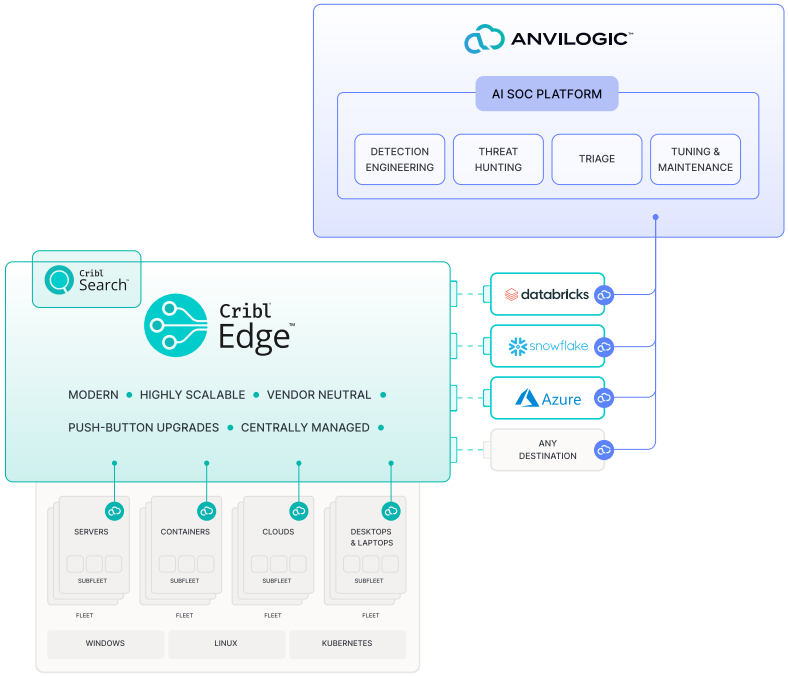
Joint Value

Together, Cribl and Anvilogic enable customers to break free from legacy SIEM constraints, leverage data lake economics, and deploy 1000+ MITRE-aligned detections in weeks vs months.

Vendor Neutrality

Without the need to rip-n-replace or vendor lock in from traditional legacy SIEM. Cribl governs data routing. Anvilogic governs detection logic. Both integrate seamlessly with your existing stack: Splunk, Sentinel, Tines, ServiceNow, and more.

Architecture



ROUTE

Control data flow with Cribl Stream and Edge

STORE

Land in Snowflake, Databricks, or Azure ADX

DETECT

Deploy Anvilogic detections and workflows

RESPOND

Triage with Monte AI and orchestrate response

Joint Value Proposition

Cribl	ANVILOGIC™
Controls and routes security data to cost-effective destinations	Deploys, tunes, and correlates detections on that data, wherever it lands
Reduces ingestion costs and unlocks flexibility	Replaces rigid SIEM rules with scalable, AI-assisted detection pipelines
SIEM ingestion reduction and legacy offload	SIEM replacement or overlay, without ripping anything out
Simple onboarding via packs and pipelines	Rapid deployment of 100+ MITRE-aligned detections in weeks
No detection or security logic	**Full detection lifecycle: build, tune, triage, correlate, retire**

Ideal Customer Profile

- Already using Cribl to route data to S3, Snowflake, or Databricks
- Looking to reduce SIEM costs while maintaining detection coverage
- Need to deploy behavioral detections faster than legacy SIEMs allow
- Seeking SIEM replacement or overlay without rip-and-replace
- Want AI-powered detection tuning (90% alert reduction proven)
- Require MITRE ATT&CK coverage at enterprise scale

Proof Points

98% triage accuracy
with Monte AI assistant

90%+ alert reduction
in production environments

1000+ MITRE-aligned detections
deployed in weeks, not months

Detection lifecycle acceleration
from build to retirement

About Cribl

Cribl, the Data Engine for IT and Security, empowers organizations to transform their data strategy. Customers use Cribl's vendor-agnostic solutions to analyze, collect, process, and route all IT and security data from any source or in any destination, delivering the choice, control, and flexibility required to adapt to their ever-changing needs.

About Anvilogic

Anvilogic is an AI SOC platform that enables security teams to build, maintain, and scale detection engineering programs without legacy SIEM constraints. With 1000+ MITRE-aligned detections, AI-assisted tuning, and native support for Snowflake, Databricks, and Azure Data Explorer, Anvilogic delivers enterprise-grade threat detection & response at data lake scale.

Learn more: www.cribl.io | www.anvilogic.com

©2024 Cribl, Inc. and Anvilogic, Inc. All Rights Reserved. All trademarks are the property of their respective owners.