SOLUTION BRIEF

Detection visibility and coverage at scale

Turn up real security signals, turn down noise.
Expand detection coverage and cut SIEM costs.

The challenge

Legacy SIEM platforms helped handle detection and response in an outdated era, with models that encourage SOCs to collect as many logs as possible, then normalize and store data with monolithic data infrastructure for detection coverage.

Today your environment is multi-cloud, SaaS-heavy, containerized, API-driven, and identity-centric, which creates far more data and far more complexity. As volumes explode, legacy SIEM licensing forces a choice: either you keep paying more to store everything, or ingest less and live with blind spots. Teams that move to modern data pipelines and data lakes get better scale, flexibility, and cost control - and they need a smarter way to turn all that security telemetry into high-quality detections that expand coverage and make the SOC more effective.

The solution: Better together

CardinalOps is not a SIEM. It sits on top of your existing SIEM, EDR, and XDR tools as an AI-powered detection engineering layer that continuously measures and improves coverage. **Cribl Edge** and **Cribl Stream** collect, shape, and route the right security telemetry into those tools. **Cribl Search** and **Cribl Lake** give you access to cheaper, long-term telemetry for testing and investigations. Together, Cribl and CardinalOps turn your modern security data architecture into targeted, contextualized detections instead of more noise.

AI-powered tuning workflows autonomously find and fix broken, noisy SIEM detection rules as telemetry sources evolve and configurations drift. Together, Cribl and CardinalOps cut wasteful SIEM data costs, eliminate blind spots, and unmask stealthy adversaries, so you never miss another threat.

The challenge

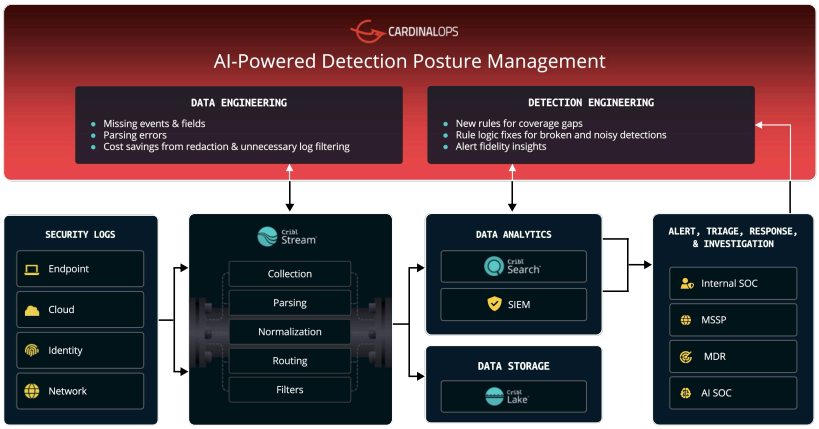
- Exploding data volumes from complex enterprise environments
- Legacy SIEM platforms have inflexible, monolithic data infrastructures
- Outdated licensing models forcing tradeoffs between coverage and budget

The solution

- Flexible, modular data architecture for the right security context, in the right format, at the right time
- AI-powered detection engineering workflows that continuously expand threat coverage

The benefits

- Full visibility of security data, no matter its source, location, or format
- Drastic reductions in SIEM data costs, eliminating tradeoffs between coverage and budget
- More effective, efficient SIEM detection programs



The benefits of using Cribl and CardinalOps

OPERATIONALIZE SECURITY DATA FOR DETECTIONS

Cribl gives you full visibility of your security data, no matter its source, location, or format, amplifying the security signals needed for CardinalOps automated detection engineering workflows to expand detection coverage.

SAY GOODBYE TO COVERAGE GAPS

Cribl's flexible, scalable infrastructure helps teams put contextual data into action, enabling CardinalOps to eliminate coverage gaps with new SIEM and EDR detection rules. CardinalOps automated detection engineering workflows find and fix broken, noisy rules that result from drifting configurations and log schemas.

BOOST EFFECTIVENESS AND REDUCE COSTS

CardinalOps delivers intelligence and context to feed back into Cribl Stream, Search, and Lake. You can tune pipelines to send exactly the events your SIEM needs, keeping high-value data in hot storage ready for real-time detection. Identifying missing events, fields, and parsing errors helps refine Cribl's collection and normalization logic, increasing detection effectiveness. Pinpointing unnecessary, redundant security logs informs filtering logic to drastically cut SIEM data costs.

Summary

Cribl and CardinalOps helps your SOC turn modern security data architecture into stronger, more effective detections. Cribl's data infrastructure gives you full visibility across diverse security log sources, while CardinalOps continuously expands threat coverage and keepsSIEM rules effective as environments change. Together, Cribl and CardinalOps turn your security data into action, maximizing detection coverage, eliminating blind spots, and cutting wasted spend from outdated SIEM licensing models.

Cribl | CARDINALOPS

Get started with Cribl and CardinalOps today

Contact us to learn how embedding detection engineering into your data pipeline and storage workflows unlocks more effective, efficient, and scalable threat coverage.

ABOUT CARDINALOPS

CardinalOps enables enterprise security teams to proactively eliminate risk by continuously validating and expanding threat detection coverage, remediating broken and noisy detections, and enabling threat-informed defenses. Powered by Cardinal AI, CardinalOps identifies detection gaps and automatically covers them with targeted detections and cost-effective remediations, reducing risk, maximizing the potential of existing security tools, and protecting organizations from the threats that matter most.

Learn more at https://cardinalops.com/

ABOUT CRIBL

Cribl, the AI Platform for Telemetry, empowers enterprises to manage and analyze telemetry for both humans and agents. Trusted by organizations worldwide, including half of the Fortune 100, Cribl bridges the gap between AI ambition and infrastructure reality. No lock-in. No data loss. No compromises. Cribl's vendor-agnostic platform ensures data remains portable and interoperable. By cost-effectively handling increasing data volume and variety without delay, Cribl gives enterprises the choice, control, and flexibility to build what's next. Founded in 2018, Cribl is a remote-first workforce with an office in San Francisco, CA.

Learn more at cribl.io | Join our Slack community
Try Cribl Sandboxes | Follow us on LinkedIn and X

SB-0071-EN-1-0526

Cribl