CASE STUDY | HOSPITALITY

How a global hospitality leader turned security telemetry into a strategic asset

with Deloitte and Cribl

Executive overview

When a global hospitality leader faced escalating security information and event management (SIEM) costs, rising compliance pressure, and fragmented observability, the engineering team turned to Deloitte to architect a modern data strategy. As primary systems integrator, Deloitte partnered with Cribl to implement an Amazon Web Services (AWS)-based cybersecurity data lake that now anchors unified security and observability operations for the hospitality organization.

Deloitte positioned Cribl as the intelligent data control plane between diverse sources and analytics platforms, including their SIEM, Dynatrace, and Amazon Security Lake. Together, we deployed technology that helped the organization reshape how they manage and get value from telemetry.

The business challenge

The hospitality company had reached a breaking point with its SIEM. Telemetry volume had pushed the platform to its performance and cost limits, with annual spending threatening budgets yet still failing to ingest all required security data. The organization also faced a hard compliance deadline to ingest and retain all Tier 1 security data by year-end to meet New York State Department of Financial Services (NYDFS) and other regulatory requirements, but critical data was either locked in expensive SIEM storage or scattered across siloed systems.

Beyond security, the company also struggled with fragmented observability tools. Its SIEM, Dynatrace, and cloud-native services all operated in isolation without a unified data strategy. That created blind spots and prevented the organization from using telemetry for advanced analytics and artificial intelligence (AI), and machine learning (ML) initiatives.

Pairing Deloitte's transformation and regulatory expertise with Cribl's vendor-agnostic data engine gave the customer **a flexible, future-ready telemetry architecture.**

Highlights

- Replaced a SIEM-centric architecture with an AWS- based cybersecurity data lake powered by Cribl and Amazon Security Lake
- Onboarded more than 75 data sources into a unified, OCSF-aligned telemetry platform
- Achieved up to 20× faster searches in the data lake compared to the legacy SIEM
- Met a year-end NYDFS Tier 1 security data deadline with all critical telemetry centralized in an auditable repository
- Reduced SIEM and storage costs through tiered routing while increasing total data retention
- Enabled cross-domain analytics across security, IT operations, and AI/ML initiatives from a single data control plane

Cribl | Deloitte.

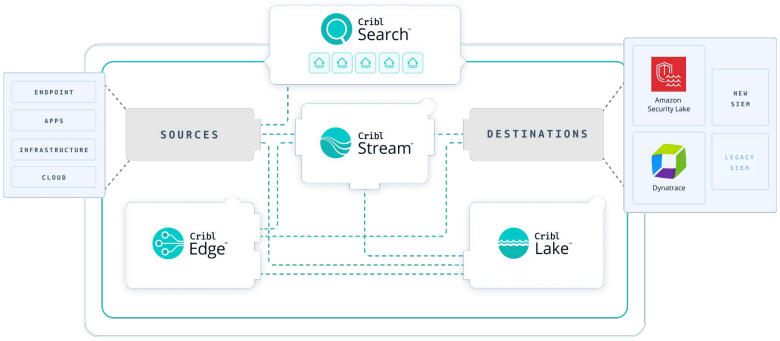
The Deloitte-Cribl solution

Deloitte served as the primary integrator and strategic advisor, defining an enterprise data strategy that positioned Amazon Security Lake, powered by Cribl, as the authoritative source for security and compliance data. Working across cybersecurity, IT operations, compliance, and enterprise architecture teams, Deloitte designed a tiered routing strategy where hot data flows to the SIEM for real-time alerting while bulk telemetry routes to cost-effective storage in Amazon Security Lake.

Deloitte's engineering team onboarded more than 75 data sources and built Cribl pipelines to normalize data, convert it to the Open Cybersecurity Schema Framework (OCSF) for Amazon Security Lake, and implement Cribl Search. These pipelines enabled searches against the lake to run up to 20× faster than comparable queries in the SIEM.

Deloitte also developed custom cyber workflows and laid the groundwork for advanced threat hunting and future cybersecurity AI/ML use cases.

Most importantly, Deloitte expanded the vision beyond security. By routing IT telemetry and application logs from Dynatrace and other observability tools through Cribl into Amazon Security Lake, the team enabled cross-domain analytics and reuse across security, operations, and AI/ML initiatives. This integration shows how the Deloitte-Cribl alliance delivers value beyond security and helps extend Cribl into broader observability environments.



Results and business impact

The transformation delivered immediate, measurable results. Large-scale searches against the data lake ran up to 20× faster than the legacy SIEM, while tiered data routing significantly reduced costs and simultaneously increased total data retention. The organization also met its year-end regulatory deadline, with all Tier 1 security data centralized in a comprehensive, auditable repository.

Beyond performance and compliance gains, Cribl's SIEM-independent routing layer introduced long-term strategic flexibility. Now the team can direct data to best-of-breed tools as requirements change, without

Deloitte brought immense value to the deployment:

- Built pipelines and stood upCribl Packs to help schematize and route data
- Brought expertise and led implementation strategy that brings everything together
- Enabled hospitality leader to begin onboarding conversational search logs with Cribl

rebuilding their data pipelines. The unified platform supports security, fraud detection, compliance, insider threat, and risk management, with AI/ML-driven analytics continuously refined to strengthen threat detection.

The data lake is now expanding into fraud analytics, customer experience insights, business intelligence, and operational optimization. Together, Deloitte and Cribl delivered a transformative outcome by combining strategic advisory, deep regulatory expertise, and hands-on technical implementation. The alliance drives sustained business value well beyond the initial deployment.

TL; DR

- A global hospitality leader now gets up to 20× faster searches in their data lake compared to the legacy SIEM.
- The team uses Cribl to tier their data for increased retention at lower cost.
- Now they have one data foundation for security, fraud, and customer analytics.

ABOUT DELOITTE

To learn more about how Deloitte and Cribl can transform your organization's data architecture, **contact the Deloitte-Cribl alliance team**.

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

CS-0051-EN1-0526

Cribl