>SOLUTION BRIEF_

Davinsi Labs Achieves Data Agility with Cribl

HIGHLIGHTS

- Onboarded new data sources in minutes using Cribl's automated pipelines
- Normalized and enriched data across 200+ customers for shared detection logic
- Centralized engineering enabled SOC team to focus on threat response
- Validated detections and trained analysts using Cribl Replay
- Integrated seamlessly into Terraform and Ansible workflows for zero-touch deployment

As Davinsi Labs transitioned from a consultancy and product reseller into a managed security services provider (MSSP), it needed a scalable, consistent way to onboard and manage customer data. With a growing customer base, diverse technology stacks, and high expectations for operational efficiency, Davinsi Labs found its solution in Cribl Stream, enabling rapid onboarding, consistent normalization, and scalable data engineering.

Faster, repeatable customer onboarding

Davinsi Labs' move to a fully managed detection and response (MDR) model meant they had to handle telemetry from hundreds of customer environments, each with different firewalls, cloud platforms, and logging tools. To scale effectively, it needed a consistent way to collect, normalize, and route data.

Cribl Stream provided that consistency. It allows Davinsi Labs to ingest and process log data directly from customer environments, whether on premises or cloud, and prepare it for use in their hosted SIEMs and analytics tools.

Each customer has its own SIEM environment, which makes it even more important to have a repeatable, automated onboarding process. Cribl Stream fits seamlessly into Davinsi Labs' deployment model, allowing the team to bring new data sources online quickly by updating configuration files and triggering CI/CD pipelines.

> **"In many cases, onboarding a new data source is as simple as updating a file and triggering our automation pipeline. You can press a button, take a coffee break, and when you're back it's up and running."**
>
> **— Tom Horré,** Chief Strategy and Commercial Officer at Davinsi Labs

Standardized data that powers a shared detection model

Davinsi Labs doesn't just collect telemetry; it builds detection logic and applies it across all its customers. That model only works if the underlying data is consistent, regardless of whether it comes from a Fortinet firewall, AWS CloudTrail, or a legacy on-prem DNS server. Cribl makes that possible by transforming and normalizing data before it ever hits the SIEM.

The team uses Cribl Stream to enrich logs at the edge, resolving common MSSP challenges like overlapping IP address spaces. They also encrypt all data in the customer's data center before transmission, ensuring integrity in transit. Cribl then routes that telemetry to the appropriate destination, whether it's a production SIEM, development environment, or a test sandbox.

> **"Cribl doesn't just help us move data, it makes our detection model possible. Without it, we'd be stuck rewriting rules for every customer. With it, we can scale security outcomes without scaling operational complexity."**
>
> **— Tom Horré,** Chief Strategy and Commercial Officer at Davinsi Labs

Scalable, centralized data engineering

> **"Cribl gives us a standardized way to move and shape data at scale. It's not just a transport layer; it's the foundation for everything we build on top."**

Davinsi Labs treats data engineering as a core part of its MDR strategy. Cribl makes that possible. By acting as a central data layer, Cribl Stream allows Davinsi Labs to decouple data transformation from security analysis.

A dedicated data engineering team manages Cribl, maintaining high-quality pipelines that normalize, enrich, encrypt, and route telemetry throughout the stack, all without burdening the SOC.

This separation of duties allows the security team to focus on detection logic and incident response, while data engineers maintain consistent, automated pipelines behind the scenes. Cribl's flexibility and automation-ready design make it the glue that holds this model together.

Reliable, secure data delivery

> **"Once data hits Cribl, we know it's safe. Even if a connection fails temporarily, we can trust the pipeline to recover without losing visibility."**

In security operations, dropped logs can mean missed threats. That's why Davinsi Labs routes all customer telemetry through Cribl Stream, where persistent queues on both the source and destination sides provide built-in protection against connectivity issues. If a VPN tunnel drops or a destination system goes down, Cribl buffers the data until the path is restored, preventing loss and maintaining integrity across the pipeline.

Improved detection and security operations training

Cribl's Replay feature allows Davinsi Labs to continuously test detection logic and train SOC analysts, all integrated into the CI/CD pipeline. When engineers update a rule, the pipeline automatically replays real-world attack data to verify that detections still fire as expected. The team builds these test cases from anonymized samples collected during actual incidents.

Cribl Replay also supports hands-on training. Engineers create purpose-built pipelines that simulate full attack scenarios, allowing analysts to investigate them just as they would in a live environment. Davinsi Labs uses these simulations for onboarding, skills development, and tabletop exercises.

"Replay lets us reuse real attacks to test detections and train analysts in a safe, controlled way. It's tightly integrated into our workflow and adds real operational value."

— Tom Horré, Chief Strategy and Commercial Officer at Davinsi Labs

"If a feature isn't automatable, we're not using it. Cribl fits right into our CI/CD workflows, allowing us to onboard new sources and scale securely without slowing down."

Automation-friendly design

Davinsi Labs manages its entire production environment using infrastructure-as-code, and Cribl fits cleanly into that model. All Cribl Stream deployments are handled through automated pipelines using Ansible and Terraform, enabling a zero-touch workflow that keeps operational overhead low, even as the number of customers grows.

Cribl's configuration-as-code approach and robust API support make it easy to version, deploy, and manage pipelines programmatically – a must-have for a security provider operating at scale.

TL;DR

- Davinsi Labs used Cribl to accelerate onboarding, bringing new data sources online in minutes through automated pipelines
- Standardized detection with normalized and enriched data across 200+ customers, enabling a single detection model to scale
- Davinsi Labs' centralized data engineering team manages all data flows through Cribl, freeing the SOC to focus on threat detection
- Built-in resilience with persistent queues prevents data loss during connectivity issues
- Automation-first deployment with seamless integration into Davinsi Labs' Terraform and Ansible pipelines

ABOUT DAVINSI LABS

At Davinsi Labs, our team is everything. We believe in their talent, commitment, and the value they add to our company and customers. We are proud to say that we are a team of 100 specialized professionals. Thanks to their dedication and passion, we can deliver our customers the highest level of expertise, go the extra mile, and be the ideal partner for organizations striving for digital resilience. The digital world is constantly changing. We help customers to secure and optimize their data and digital services in these challenging times. Davinsi Labs operates under Proximus NXT. Want to stay informed of all developments? Follow us on LinkedIn.

ABOUT CRIBL

Cribl makes open observability a reality for today's tech professionals. The Cribl product suite defies data gravity with radical levels of choice and control. Wherever the data comes from, wherever it needs to go, Cribl delivers the freedom and flexibility to make choices, not compromises. It's enterprise software that doesn't suck, enables tech professionals to do what they need to do, and gives them the ability to say "Yes." With Cribl, companies have the power to control their data, get more out of existing investments, and shape the observability future. Founded in 2017, Cribl is a remote-first company with an office in San Francisco, CA.

Learn more: www.cribl.io | Try now: Cribl sandboxes | Join us: Slack community | Follow us: LinkedIn and Twitter

CS-0004-EN-2-0624