Cribl | PRESIDIO

>CASE STUDY_

A Faster Path to Risk Reduction: Cribl Transforms the Security Operations Center at Presidio Networked Solutions

Presidio provides professionally managed services, specializing in the design, implementation, and management of agile and secure digital platforms. Their solutions enable clients to move faster and innovate in how they interact with their own customers, employees and partners.

When Ryan Pinga, Presidio's Vice President of Managed Services, was brought in to help overhaul the Security Operations Center (SOC) providing the organization's Managed Detection and Response (MDR) offering, he started by evaluating different log pipeline solutions on the market. His goal was to shift towards a more flexible and modular setup enabling Presidio to support multiple technologies with a scalable and flexible platform that would exceed customer expectations

Ryan and his team started by looking at the classic solutions (mostly open source), but noticed that each of them had too much overhead or required deep (and costly) engineering expertise to get running at scale. Then, they stumbled across Cribl.

HIGHLIGHTS

- Went from purchasing Cribl Stream to first deployment in less than two weeks
- Reduced time to onboard clients by an average of 70%.
- Cut engineering team workload by 50%.

> **"About 45 minutes into researching, we knew we wanted Cribl. It was an immediate no-brainer. It had everything we needed from a technical and architectural perspective to enhance our managed service offering, with the perfect balance of flexibility without massive engineering overhead."**
>
> **— Ryan Pinga,** Vice President of Managed Services

Unification of Data Collection

Cribl Stream is now Presidio's behind-the-scenes engine that powers all log collection for their MDR clients. They use it to collect customer data from Syslog, API collectors, Beats agents, leading security tools, and other sources. Each client has dedicated worker nodes which send raw data to S3 buckets, then routes normalized and shaped data to a multi-tenant SIEM.

"Cribl Stream does all of our log source reduction, standardization, and normalization for every one of our data sources. It gives us a clean UI, making it easy to do all of our parsing, rewrites, and transforms on various data sources across the board."

— Ryan Pinga, Vice President of Managed Services

"The improved analytics and visibility we get by incorporating Cribl are foundational. We get a level of granularity that is difficult or impossible without it."

When the data hits the SIEM, it's ready to add value. Clean data accelerates the performance of the SIEM because correlation searches don't have to churn through irrelevant data. And investigators have enriched, normalized data giving them the context they need to quickly respond to alerts and investigations.

Delivering Risk Coverage and Value, Fast, for Clients

By using Cribl Stream, Presidio has been able to stand out among its competitors — not only in their ability to tackle any data source, but also in quickly delivering the risk coverage their customers need.

"Instead of being beholden to other vendors to build and maintain parsers or index certain things, everything is now completely within our control with Cribl Stream. It's a big differentiator for us to tell clients that there's no data source we can't work with – and Cribl makes that possible for us."

— Ryan Pinga, Vice President of Managed Services

Ryan and his team can now accelerate data onboarding and provide clients with immediate functionality and value — something that other providers who are not using Crbil Stream aren't able to do nearly as easily. The team uses Cribl Packs to help customers quickly get a handle on managing risk. Packs bundle up knowledge related to a given data source along with pre-built routes and pipelines making it easy to port configurations from one worker group to the next. Since most of Presidio's MDR clients have similar security data sources, utilizing Cribl Packs and leveraging scalable pipelines saves a lot of time.

"Since we put Stream in place and started leveraging Cribl Packs, we basically moved from an average onboarding time of 60-90 days to about 15-30 days."

— Ryan Pinga, Vice President of Managed Services

Cribl Packs enable scalability that didn't exist before. They allow Ryan and his team to onboard data simply by reusing pipelines, making modifications only to credentials, authentication, and IPs. This results in minimal delays when onboarding a new client, instilling confidence in the product's functionality and their onboarding process.

> "With Cribl Stream, we can easily send full raw logs to S3 for compliance purposes and send reduced, normalized versions to our SIEM platform."

Many Packs in the Cribl Dispensary are Open Cybersecurity Schema Framework (OCSF) compliant, meaning they can be deployed to easily utilize this standard schema, and take advantage of the schema event class to more accurately interpret the information contained in the record, and often accelerating performance of downstream tools for detection, monitoring, and analytics.

Reduced Engineering Costs

Optimized performance along with reductions in log volumes help Presidio pass cost-savings on to the customer, but Ryan's biggest savings is around engineering resources. Rather than spending engineering hours to build a solution from open source products, Cribl Stream provides the needed functionality with a low barrier to entry for configuration, maintenance, and operation.

> **"Building and maintaining alternative solutions would take three to five engineers to do at scale. I can operate Cribl Stream with half the amount of engineering resources because it's such a solid, well-maintained, and extremely flexible product."**
>
> **— Ryan Pinga**, Vice President of Managed Services

Ryan is excited for a future that includes new tools that will complement and enhance their current offering. Cribl Edge will help optimize tools by replacing proprietary, single vendor agents that are prone to dropping events or are difficult to manage. Cribl Search will allow them to easily search-in-place all the data that is routed to their clients' S3 buckets for compliance and more.

> "Our confidence in the Cribl Stream platform, its roadmap, and focus gives us a lot of confidence to do things at scale."

TL;DR

- Presidio used Cribl Stream to shift towards a more flexible, modular infrastructure.
- Cribl Stream powers all log collection for Presidio's MDR clients.
- Improved service offerings by being able to work with every data source.