Cribl | SIEMENS

>CASE STUDY_

Siemens Simplifies Security Operations with Cribl and Amazon Security Lake

HIGHLIGHTS

- Data volume reduced from approximately 7-8 TB input to a significantly smaller output.
- Aggregating over 15-30 minute time periods, instead of handling individual events.
- Overcame volume restrictions to onboard data sources they didn't previously have room for.

The Cloud Security Operations team at Siemens Foundational Services manages over 800 cloud accounts and environments for their internal customers. Historically, managing the enormous amounts of data from these clients was a monumental challenge. Since adopting Cribl Stream, they've been able to send much more crucial data into their Security Information and Event Management System (SIEM), and boost their threat detection capabilities.

One of the team's goals is to continuously improve the security monitoring of their environment. Gaining more visibility into VPC flow logs and other high volume data sources had been a top priority for a while, but they were held back by the financial restrictions from their SIEM license.

The combination of Cribl and Amazon Security Lake finally opened up the possibility for getting the data they needed into Splunk.

> "Ingesting that much data straight up from our different accounts wasn't possible – until we learned about Cribl Stream. Now we have the flexibility to transform the data from Amazon Security Lake on its way to Splunk."
>
> —**Pedro Borges**, Senior Security Engineer

Streamlined Data Onboarding Across the Entire Organization

Managing, onboarding, and routing logs from all these accounts used to require set up time from both the Cloud Security Operations (CSO) team and their internal clients. Now, Siemens uses Amazon Security Lake to aggregate logs from all accounts and regions into one central place and adjust data lifecycles as necessary.

But without a way to easily get that data to Splunk, the switch to Amazon Security Lake wouldn't have been as beneficial.

"Without Cribl, data we need doesn't make it into splunk, and we lose access to critical intel."

– **Pedro Borges**,
Senior Security Engineer

"Cribl has become part of our critical path, but we're just kind of scratching the surface of what we can do. We're leveraging so much more as each week goes by."

– **Scott Schwartz**,
Software Engineering
Senior Manager

"Cribl Stream came to our rescue by letting us simplify the ingestion into our SIEM. We no longer have to take time away to set up infrastructure to accommodate the passing of data from one environment to the next – we just use Cribl to send it right to our Splunk environment."

—**Scott Schwartz**, Software Engineering Senior Manager

Significant Reduction in Data Volumes

Since Amazon Security Lake supports Open Cybersecurity Schema Framework (OCSF) formatting, large, detailed file sizes are the norm, as are extra fields that don't really have any relevance to Siemens and the security detections they implement. The ability to easily reduce this data made Cribl Stream the perfect complement to their Amazon Security Lake integration.

"We use the Cribl pipelines to take this massive JSON log format and just extract the fields that are critical to us. If we only really care about 10 specific fields, we reduce events to those 10 and that's it."

—**Pedro Borges**, Senior Security Engineer

For VPC flow logs and S3 data, the team at Siemens also aggregates events over time, so they don't use up bandwidth sending them one-to-one.

"We're also using Cribl Stream to combine events. From a security detection standpoint, it's great because our analysts can just see if an endpoint was hit, instead of seeing the same event multiple times in a Splunk search. Then we can pivot into when and how many times, or dive into the raw data if we need to."

—**Pedro Borges**, Senior Security Engineer

Leveraging Cribl Search for Incident Investigations

The Cloud Security Operations team at Siemens is all in on Cribl Stream, and is just starting to realize the benefits of Cribl Search. During a recent investigation, they needed to figure out what was accessing some S3 objects, and found an easy solution.

"We had all the data in Amazon Security Lake, but I wasn't ready to start setting up Athena to start reading it. I decided to use Cribl Search instead, and within 5-10 minutes, I was able to start searching. It was relatively easy to implement, and I was able to get the data that I needed quickly."

—**Scott Schwartz**, Software Engineering Senior Manager

> "The plan is for any new applications and log sources to go through Cribl, so that we can transform the data and replay it whenever we need to."
>
> – **Pedro Borges**, Senior Security Engineer

More Cribl in the Future

Siemens has had a lot of success so far with Cribl, and the team is excited to continue further down the same path to see what else they can do with it. Both EKS audit logs and WAF logs are next on their list of sources to tackle.

> **"We've struggled with WAF logs in the past, just due to the sheer volume. Using Cribl to do some similar reductions and summarizations is going to allow us to bring that data in and run it against the threat Intelligence detections that we have in place."**
>
> **—Scott Schwartz**, Software Engineering Senior Manager

Historically, when their internal clients wanted to send application logs, the CSO team would provide them with the right token, endpoint, index, source type, etc., so they could directly send data to Splunk. This workflow did work well, but didn't always have the most efficient output.

> **"With our previous process, it was great that we were able to get those logs, but sometimes they contained a lot of noise. We've updated our process so that instead of going directly to Splunk HEC, they'll be going through the Cribl-Splunk HEC input, and we'll get a lot of that space back."**
>
> **—Pedro Borges**, Senior Security Engineer

> "We're keeping a lot of data in amazon security lake for compliance and retention purposes, because we know we can just use Cribl to replay it back into splunk if we need it."
>
> – **Scott Schwartz**, Software Engineering Senior Manager

TL;DR

- Using Cribl to process logs from Amazon Security Lake before ingesting them into Splunk
- Eased log aggregation with Amazon Security Lake; enabled flexible transformation and search of that data with Cribl
- Simplified ingestion of high-volume data sources like VPC flow logs, Route53 DNS resolver query logs, and CloudTrail S3 data events.
- Reduced, transformed, enriched security log data before sending to Splunk for analysis
- Extracted only relevant fields from verbose OCSF format logs for efficiency
- Enhanced threat detection capabilities by enabling the ingestion and analysis of high-volume data sources previously unfeasible

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. Cribl's product suite, which is used by Fortune 1000 companies globally, is purpose-built for IT and Security, including Cribl Stream, the industry's leading observability pipeline, Cribl Edge, an intelligent vendor-neutral agent, Cribl Search, the industry's first search-in-place solution, and Cribl Lake, a turnkey data lake. Founded in 2018, Cribl is a remote-first workforce 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-0030-EN-1-1124