Cribl | YaleNewHavenHealth

>CASE STUDY_

Yale New Haven Health reduces burden on SIEM and revamps security infrastructure.

Yale New Haven Health is Connecticut's largest healthcare system. Their cybersecurity team brought in Cribl Stream to help manage data from 30,000+ endpoints, reduce their SIEM license spend, and assist with security tool migration.

When Yale New Haven's cybersecurity team noticed a surprise 30-45% increase in the volume of their firewall logs, they went to work looking into the issue. It turned out that a software update was responsible for adding 63 fields to each of their Palo Alto logs — a problem tailor-made for Cribl Stream to solve.

HIGHLIGHTS

- 40% reduction in Palo Alto log volume.
- Two-week transition from Splunk to Sentinel.
- Centralized collection of data from 30,000+ endpoints.

40% reduction in Palo Alto Networks log volume.

The increase in volume pushed them way over their 400 GB/day Splunk license. The additional data was a combination of null fields, verbose descriptions of the logs, and other data that wasn't anything of value to the organization.

> **"Cribl Stream made it easy to strip the extra fields out and get those logs right back under control. We didn't lose any log fidelity or important data – we just took out some of the garbage."**
>
> **— Robert Arbuckle**, Information Security Analyst

The reduction had an immediate impact on Yale New Haven's SIEM license usage.

> **"Cribl really changed the way that our Splunk spend worked. We were constantly using about 600 – 700 GB/day of our 400 GB license, but were able to bring it down to less than 400 GB – just by using Stream to make a couple of changes to Palo Alto Networks logs."**
>
> **— Robert Arbuckle**, Information Security Analyst III

Smooth, two-week cutover from Splunk to Sentinel.

Even with the reduction in Palo Alto logs, Splunk's latest upgrade made it too cost-prohibitive for Yale New Haven to continue using it. With the help of Security Risk Advisors (SRA), a cybersecurity consulting firm, they quickly built a cost-effective solution — moving to Microsoft Sentinel as their SIEM and Azure Data Explorer (ADX) as their data lake.

> **"Having Cribl Stream in place made switching from Splunk super easy — we just had to point the outputs to Sentinel instead. We stood up the new SIEM and populated our data lake within two weeks."**
>
> **— Robert Arbuckle**, Information Security Analyst III

Once Robert and the team set up all their routes, pipelines, and access controls, SRA gave them even more functionality than anticipated.

> **"We did some prep work, then SRA came in to pull some levers, and we started filling the data lake — which turned out to be awesome from day one."**
>
> **— Frank Heaven**, Senior Information Security Specialist

> "Cribl Stream greatly reduces the cost of our SIEM, cuts white noise from logs, and makes them more meaningful."

All the logs for all the teams.

Now that the team at Yale New Haven Health has Cribl Stream, Sentinel, and ADX in place, they have the foundation to continue improving their security posture. They've onboarded logs from Microsoft, Netscaler, Cisco, Infoblox, Epic, and more — and there are also fewer restrictions on the other logs they consider bringing in.

> **"Now If there's a log with a good use case, that's reason enough for us to bring it on with Cribl. Cost just isn't as big of a driver as it was before."**
>
> **— Robert Arbuckle**, Information Security Analyst III

It's also easier for Robert to meet requests from different groups within the Yale New Haven Health system — like the identity team that wanted to onboard the organization's password self-service website logs. They can also easily give and control access to all of the company's data.

> **"If another team wants to bring their data in, we don't necessarily have to worry about them being able to see stuff that's not theirs. We can easily give them access to just that piece of the database using role-based access."**
>
> **— Robert Arbuckle**, Information Security Analyst III

A central location for all syslog and UDP traffic.

Since they're receiving data from so many endpoints, Yale New Haven Health is happy to have Cribl as a central spot to send all their syslog and UDP traffic.

> **"We have a pretty distributed workforce and about 5,000 people that work remotely, so we're sending data from about 30,000 endpoints to Cribl now. Having that central location has made a huge difference."**
>
> **— Frank Heaven**, Senior Information Security Specialist

> **"We love the ability to send the same data to multiple sources — and it's actually very intuitive. If i can use Cribl, most people can."**

By sending these disparate data sources through Cribl, it's easier to normalize and filter incoming data, which makes analysis easier and significantly cuts storage costs. Centralizing data collection also improves security by providing a unified view of network activity, aiding in identifying potential threats. Easily reducing data also improves downstream pipeline performance by reducing noise sent to other tools.

In the future, Yale New Haven Health plans to use Cribl to build out their internal Security Operations Center (SOC) and make new tool acquisition easier and faster to evaluate, implement and realize value. They plan to build more on-site nodes to use the Windows Event Collector (WEC) feature and pull in events from all their servers, not just the domain controllers. As they are onboarding Epic logs, they are using Cribl's data masking feature to ensure the security and privacy of sensitive information, which has the added benefit of reducing the amount of time spent with auditors.

TL;DR:

- Reduced data ingest from 600-700 GB/day down to 400 GB/day without losing context or fidelity for downstream tools.
- 40% reduction in Palo Alto Networks log volume.
- Two week cutover from Splunk to Microsoft Sentinel.
- More room to onboard other log sources without worrying about cost.
- Easy access control for teams within the organization.
- Created central location to receive all syslog and UDP traffic.