>CASE STUDY_

How the University of Pittsburgh Streamlined Security Data Processing with Cribl

HIGHLIGHTS

- Successfully migrated from Splunk to Microsoft Sentinel in just 68 days
- Achieved unified, searchable logs from all sources via lightweight pipelines
- Optimized ingest costs through smart filtering and compression
- One-pane control streamlines admin for a small team
- Seamless rollout to 1,000+ servers with easy upgrades

For years, the University of Pittsburgh used Splunk Cloud to manage its ever-growing security event data demands. However, the IT Security team realized that they were unable to fully leverage the value of their data. Despite investing considerable time and effort in cleaning and parsing specific datasets to enable searchability and identify incidents, the vast majority lacked the necessary structure and normalization.

After onboarding **Splunk** Enterprise Security (ES), the team identified a need to enhance Common Information Model (CIM) for compliance across varied data sources. They sought to streamline log formats from various environments, including firewalls, Windows, Linux, and cloud systems.

In pursuit of optimizing their security data management, the University made the strategic decision to transition to Microsoft Sentinel. They implemented **Cribl Stream** and **Cribl Edge** to facilitate a seamless transition, allowing for data transformation and enrichment in-flight, ensuring adherence to Sentinel's formatting and analytic requirements before reaching the SIEM.

Streamlined SIEM Migration in Just 68 Days

The migration from Splunk to Sentinel was completed efficiently in just 68 days, thanks to Cribl's pivotal role in expediting the process. By integrating Cribl, the team established pre-processing pipelines that parsed, **normalized**, and enriched log data in real-time, readying it for immediate ingestion and analysis by **Sentinel**.

> **"Compared to our previous setup, Cribl has significantly improved our data management, making operations smoother. As a small team with extensive responsibilities, Cribl has been an invaluable asset."**
>
> **—Richard McIver**, Senior Security Engineer at the University of Pittsburgh

Because the University of Pittsburgh team leveraged Cribl to parse, filter, and compress data, and eliminate unnecessary fields, for their migration, they not only achieved their primary goal but also realized a major added benefit: significant cost savings.

For a large organization generating approximately 4TB of data daily, the resulting reduction in data volume sent to Sentinel was a key priority for senior leadership due to the substantial ingestion costs.

Ease of Use and Centralized Management

The University of Pittsburgh's IT Security team greatly valued the simplicity and efficiency of Cribl's unified platform, which streamlined their operations compared to the multiple tools and complex configuration files they navigated in their previous stand-alone Splunk environment.

Being able to manage all their data processing, normalization, and routing through a single pane of glass in Cribl Stream and Cribl Edge has streamlined their workflows and made them much more efficient. What's more, the intuitive interfaces and cross-training Cribl provides enabled their small team to get up to speed quickly.

TL;DR

- The University of Pittsburgh migrated from Splunk to Microsoft Sentinel in just 68 days.
- The migration addressed long-standing challenges related to data parsing and normalization, improving searchability and maximizing data value.
- Cribl Stream and Cribl Edge enabled the team to normalize data from many disparate sources into a usable format for Microsoft Sentinel, while reducing ingest costs and streamlining data management.
- Cribl Edge simplified configuration management across 1,000+ servers.
- Cribl's intuitive UI and centralized control allowed the small security team to gain full visibility into their data, detect and respond to threats faster, and operate more efficiently across the board.

> **"Having everything in one place so we can work with all our data in a single pane of glass is helpful. And, you know, for those local file sources that we're pulling in, just manipulating that data and working with it is much easier now."**
>
> **—Richard McIver**, Senior Security Engineer, University of Pittsburgh

Smooth Implementation across 1000+ Servers

The University of Pittsburgh IT Security team anticipated that rolling out Cribl Edge across over 1000 servers would be a major challenge. However, in reality, the process was remarkably smooth.

The team was able to work with system and service owners to easily push out the Cribl Edge agents, organize the nodes, and share configurations across their different server groups. What's more, updating these agents has also been simple, allowing the team to keep the platform up-to-date with minimal effort.

> **"Upgrading the agents has been really easy. We're in the middle of doing our first upgrade, but so far, it's been very, very smooth and easy. Organizing the nodes and the fleets to help keep them organized and share configs across different groups of systems has been helpful."**
>
> **—Richard McIver**, Senior Security Engineer, University of Pittsburgh

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 X

CS-0039-EN-1-0625