>CASE STUDY_

Academic Health System Accelerates SIEM Migration with Cribl

HIGHLIGHTS

- Rapid SIEM migration to CrowdStrike's FalCon Next-Gen SIEM (under 60 days)
- Centralized location for processing 5TB data per day across 40,000 endpoints
- Enhanced scalability, improved data flow visibility, and reduced EPS limitations.

As a premier academic healthcare institution providing world-class medical education, groundbreaking research, and specialized care to diverse populations, this Health System relies heavily on securely managing vast amounts of telemetry data from various sources. Typically, medical and research facilities have multiple systems for collecting and analyzing this data. These systems often store data in different formats, making it a challenge to manage and use effectively.

The Health System's cybersecurity team identifies, assesses, and prioritizes security risks while developing strategies to safeguard sensitive data. With over 2TB/day streaming in from various sources including Windows Event, Azure, Authentication, and Audit logs, having a robust security information and event management (SIEM) solution is mission-critical. Unfortunately, the existing SIEM solution was failing to meet performance and safety requirements. The existing SIEM's unreliable log ingestion was creating gaps in security coverage, while its limited alerting and triaging capabilities hindered the team's ability to respond to threats quickly.

With a looming, extremely tight migration deadline, the team chose CrowdStrike Falcon Next-Gen SIEM and Cribl Stream to streamline log management and enhance their security posture.

Accelerating SIEM migrations

The Health System's cybersecurity team evaluated multiple solutions, including homegrown SIEM providers and managed services. Ultimately, the timing was perfect for the team to deploy CrowdStrike Falcon Next-Gen SIEM, which offered seamless integration with their existing CrowdStrike EDR and Identity records.

> "When it came time to pick out the next SIEM, we were looking for a tool that would give us the right coverage and keep us safe."
>
> — Security Architect

To enable the rapid migration and ensure flexibility in data management, the Health System selected Cribl Stream. With Cribl quickly installed as their centralized data processing platform, they could easily direct data to the CrowdStrike Falcon platform and other tools as needed. The team succeeded in deploying both solutions in under two months, ensuring uninterrupted security operations..

> **"We had to get off our old platform as quickly as possible and onto the new one in under two months. The thought was that we could get Cribl and then all we would have to do is point it over to CrowdStrike."**
>
> **— Security Architect**

A new era of flexibility and reliability

The combination of Cribl and the CrowdStrike Next-Gen SIEM has transformed the way the Health System's security team manages data. Not only has it significantly improved reliability, Cribl also provides enhanced visibility into data flows, enabling the ability to monitor and troubleshoot log ingestion in real time.

> **"Cribl has helped get all our logs centralized into one point. It's a win just having that in place. We have more flexibility with Cribl in the middle than we would have without it – it is a massive timesaver."**
>
> **— Security Architect**

Furthermore, Cribl's ability to simplify data transformation, such as converting email logs to JSON, has eliminated manual processes and reduced errors. The platform's flexibility has allowed them to onboard new data sources without worrying about EPS limitations or reconfiguring existing setups. This scalability ensures that the Health System's security infrastructure can grow alongside their evolving needs, essentially future-proofing operations.

> **"Before Cribl, we would burn through EPS constantly. It made the SIEM impossible to use. Now, we are free to do anything. We can actually onboard anything right now without a problem."**
>
> **— Security Architect**

TL;DR

- Migrated to CrowdStrike Falcon Next-Gen SIEM in under two months
- Centralized log ingestion and data processing with Cribl Stream, managing ~2TB/day across 40,000 endpoints
- Enhanced visibility and reliability of log ingestion, improving threat detection and response
- Eliminated EPS limitations, enabling seamless onboarding of new data sources
- Improved visibility and control with centralized log management
- Future-proofed security architecture with flexible data routing and transformation

Commitment to continuous improvement

Looking ahead, the Health System is focused on enhancing its security and data management practices with several key initiatives. They plan to eventually refine their log parsing and formatting processes to optimize data flow and improve clarity for analysis. Custom correlation rules for their Next-Gen SIEM deployment are under development, which will enable more effective threat detection tailored to their specific needs.

> **“Anytime anyone asks us about Next-Gen SIEM, we tell them: if you’re going to do that, you’ve got to get Cribl. Cribl is the secret sauce.”**
>
> **— Security Architect**

Additionally, they are exploring the implementation of a data lake for long-term storage to meet a new state-mandated 6-year data retention requirement. These efforts reflect the team’s commitment to maintaining a robust, adaptable, and scalable security infrastructure.

CS-0047-EN-1-1225