>CASE STUDY_

Reddit Streamlines Security Data Management with Cribl

HIGHLIGHTS

- Transitioned from ELK to Splunk to a homegrown SIEM using Cribl.
- Enabled data streaming via Kafka for rapid threat detection.
- Cut ELK's maintenance overhead.
- Simplified data management and eliminated vendor reliance.

Reddit

Reddit, one of the world's most popular online community platforms, was relying on an ELK stack to ingest and analyze security-related data. However, as data volumes grew, the operational overhead of maintaining this infrastructure became unsustainable. To address this challenge, Reddit used Cribl Stream to smoothly transition to Splunk Cloud and, eventually, a homegrown system without disrupting security operations.

Streamlining Data Management and Migration

By implementing **Cribl Stream** as its central data pipeline, Reddit seamlessly ingested, **normalized**, and **routed** audit data from internal systems, third-party tools, and network infrastructure logs into Splunk. Cribl's flexibility and scalability reduced operational complexity and made data management more efficient.

> **"Cribl's consistent performance and reliability give us confidence in our data infrastructure."**
>
> **—Chad Anderson**, Manager of Reddit Security Intelligence Center

Cribl also helped Reddit future-proof its security strategy. Because Reddit routed all data through Cribl during its initial **migration**, Reddit was able to rapidly transition to a homegrown SIEM without having to reconfigure individual data sources, helping it complete the migration in just six months.

> **"Sending all our logs through Cribl allowed us to roll out our homegrown SIEM very quickly."**
>
> **—Chad Anderson**, Manager of Reddit Security Intelligence Center

Enhancing Security Analytics and Detection Capabilities

As Reddit's data infrastructure evolved, Cribl allowed Reddit to stream data to Kafka in milliseconds, meaning they could leverage Kafka's distributed processing capabilities for near-real-time threat detection. Moreover, leveraging BigQuery for storage has enabled Reddit to run AI and machine learning models for more advanced analysis.

> **"With Cribl, we achieve powerful real-time data stream analysis, transferring data to Kafka in milliseconds, and leveraging BigQuery for backend storage, which offers robust query options."**
>
> **—Chad Anderson**, Manager of Reddit Security Intelligence Center

Lowering Maintenance Overhead

Cribl Stream has significantly lowered the **maintenance overhead** for Reddit's data infrastructure. Keeping its ELK infrastructure stable and running – managing upgrades and patches and ensuring the overall reliability of the system – required too much time and was putting a significant strain on the team's resources. With Cribl, that maintenance burden has been all but eliminated.

> **"Keeping the ELK stack running was almost a person's full-time job. Cribl, however, just works, and we don't have to worry about it. It's super easy to go in and configure new data sources and push data through, and it scales up easily. We don't have to manage Cribl at all right now."**
>
> **—Chad Anderson**, Manager of Reddit Security Intelligence Center

TL;DR

- Reddit transitioned from an ELK stack to Cribl Stream to streamline data ingestion and reduce operational overhead.
- Cribl enabled a smooth migration to Splunk Cloud and later a homegrown SIEM without disrupting security operations.
- The flexible data routing simplified migration, allowing Reddit to complete the transition in just six months.
- Cribl enhanced security analytics facilitating the use of Kafka for real-time threat detection and integrating with BigQuery for advanced analysis.
- Maintenance overhead was significantly reduced, eliminating the need for full-time management of the ELK stack.

ABOUT CRIBL

Cribl, the Data Engine for IT and Security, empowers organizations to transform their data strategy. Powered by a data processing engine purpose-built for IT and Security, Cribl's product suite is a vendor-agnostic data management solution capable of collecting data from any source, processing billions of events per second, automatically routing data for optimized storage, and analyzing any data, at any time, in any location. With Cribl, IT and Security teams have the choice, control, and flexibility required to adapt to their ever-changing data needs. Cribl's offerings–**Stream**, **Edge**, **Search**, and **Lake**–are available either as discrete products or as a holistic solution.

Learn more: www.cribl.io | Join us: Slack community | Follow us: LinkedIn and Twitter

CS-00038-EN-1-0625