Cribl

SIEM Migration with Cribl Stream

HOW-TO GUIDE

CONTENTS

INTRODUCTION

Understanding the challenge: complexities of SIEM migration

Telemetry data is growing exponentially, adversaries are moving faster than ever, and the number of companies sending data to multiple SIEM products increased by 45% last year.[1]

Many of those companies are choosing modern SIEM platforms. Migrating to a modern security information and event management (SIEM) platform is now essential for organizations to improve their security operations. However, this process is often complex and fraught with challenges. Organizations must maintain their security posture during the transition, optimize data to fit the requirements of the new SIEM platform, ensure data quality and control, and manage costs effectively.

Traditional migration methods can lead to disruptions in security operations, data loss, or increased expenses. These issues arise because legacy systems are ill-equipped to handle modern data volumes or adapt to evolving security needs. IT and Security teams need a solution that minimizes risk while ensuring operational continuity. Cribl Stream does both—and more.

28%	Rate at which telemetry data is growing annually (CAGR)
51 seconds	Fastest recorded eCrime breakout time[2]
45%	Percent of companies sending data to multiple SIEMS

[1] Cribl's Navigating the data current report, 2024.

[2] Crowdstrike 2025 Global Threat Report.

Business value: Why migrate?

A SIEM migration is more than just a vendor or technology swap. Migrating to a modern SIEM platform transforms your organization's ability to detect and respond to threats, optimize costs, and future-proof your security infrastructure.

Modern SIEMs offer enhanced threat detection capabilities by using machine learning and behavioral analytics to identify threats in real time. Unlike legacy systems that rely on static rules, these platforms adapt to evolving attack patterns, reduce false positives and improve incident response times.

Cost efficiency is another critical benefit. Legacy systems often lead to spiraling costs due to indiscriminate log storage and inefficient data processing. Modern SIEMs, especially when paired with Cribl Stream, allow organizations to optimize data ingestion, tier storage based on access frequency, and eliminate redundant or low-value data—significantly reducing operational expenses.

Scalability is a major advantage as well. Legacy SIEMs can struggle to handle the exponential growth in telemetry data. Modern platforms scale seamlessly, ensuring consistent performance even as data volumes increase.

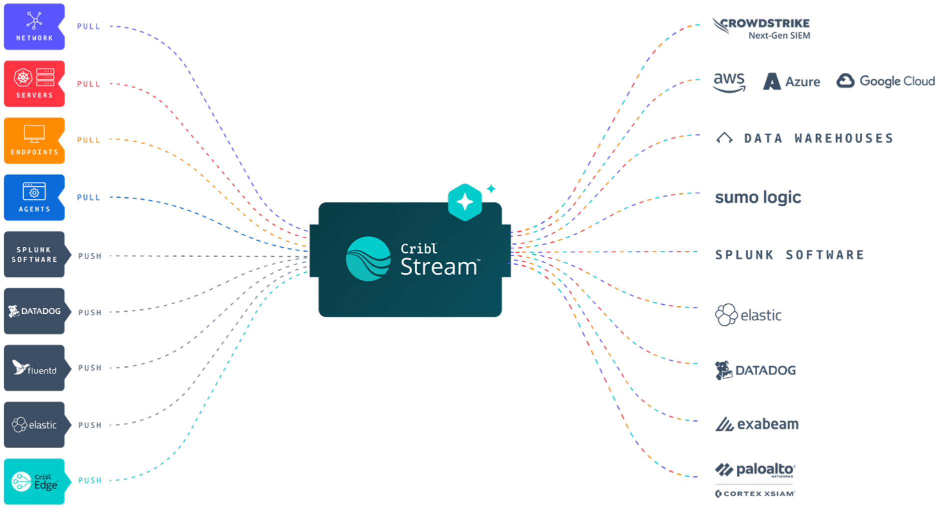
Compliance becomes easier with modern SIEMs that provide automated reporting, robust data retention policies, and audit trails. These features simplify adherence to regulatory requirements while maintaining transparency in security operations.

Operational efficiency also improves dramatically. Modern SIEMs streamline workflows through automation and intuitive dashboards, enabling security operations center (SOC) teams to focus on high-priority incidents rather than repetitive tasks.

Finally, migrating with Cribl Stream introduces vendor agnosticism into your security strategy. **By decoupling data ingestion from specific SIEM vendors, organizations gain flexibility in tool selection and avoid vendor lock-in—empowering them to choose the best solutions for their goals.**

Cribl Stream: an overview

Cribl Stream is a telemetry pipeline that gives your organization complete control over your data during SIEM migration, making the process smoother and more efficient. By decoupling data ingestion from specific platforms, Cribl Stream lets you route data simultaneously to both your legacy system and the new SIEM without disruption. This ensures operational continuity while allowing you to test and validate the new system with live production data.



Example customer environment

Stream allows you to filter, shape, enrich, redact, normalize, and transform telemetry to meet the unique requirements of your security environment. Sensitive information can be secured through redaction, while irrelevant or low-value data is filtered out to reduce storage costs and improve analytics performance. You can dynamically route specific datasets to different destinations based on business necessities, ensuring your SIEM receives only the data it needs.

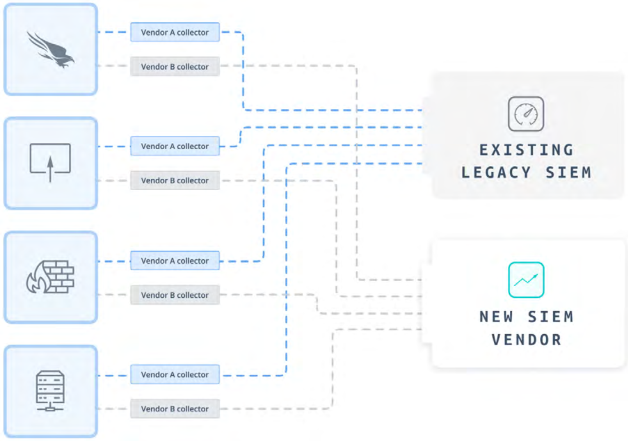
Stream also allows you to clone production data streams for testing or troubleshooting without impacting live operations. Its vendor-agnostic design supports diverse sources and destinations, giving you the freedom to evaluate multiple SIEM options without committing upfront. Whether you're working with petabyte-scale data or integrating across complex environments, Cribl Stream adapts seamlessly to your requirements.

By using Cribl Stream during migration, you can optimize data quality, reduce costs, and maintain a strong security posture while preparing your organization for future scalability and flexibility.

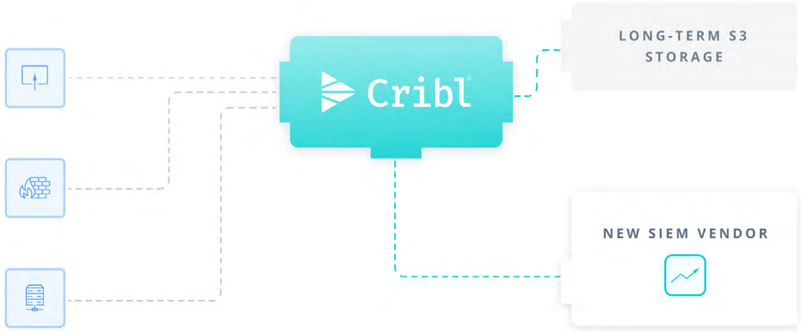
How Cribl Stream Facilitates SIEM Migration

Cribl Stream makes SIEM migration seamless by enabling phased transitions while maintaining operational continuity. It allows you to clone production data from your legacy system into the new platform without disrupting day-to-day operations. This dual-forwarding setup ensures thorough testing of new configurations with live production data before fully cutting over.

TRADITIONAL SIEM MIGRATION



MIGRATION WITH CRIBL STREAM



The platform also optimizes incoming telemetry by filtering out unnecessary noise and enriching valuable fields for better insights in the new system. Its vendor-agnostic design supports multiple collection agents and destinations simultaneously, reducing lock-in risks and increasing flexibility during migration.

By maintaining both systems in parallel during testing phases, Cribl Stream minimizes risk while ensuring your security posture remains intact throughout the transition process.

Implementing a streamlined SIEM migration with Cribl Stream

1 | Assess current SIEM environment

Begin by evaluating your existing use cases, data sources, and security requirements. Identify gaps or inefficiencies in your current setup that need addressing during migration. This assessment will help you define clear objectives for the process. For assessment tips and best practices, you can refer to our whitepaper.

2 | Define migration objectives

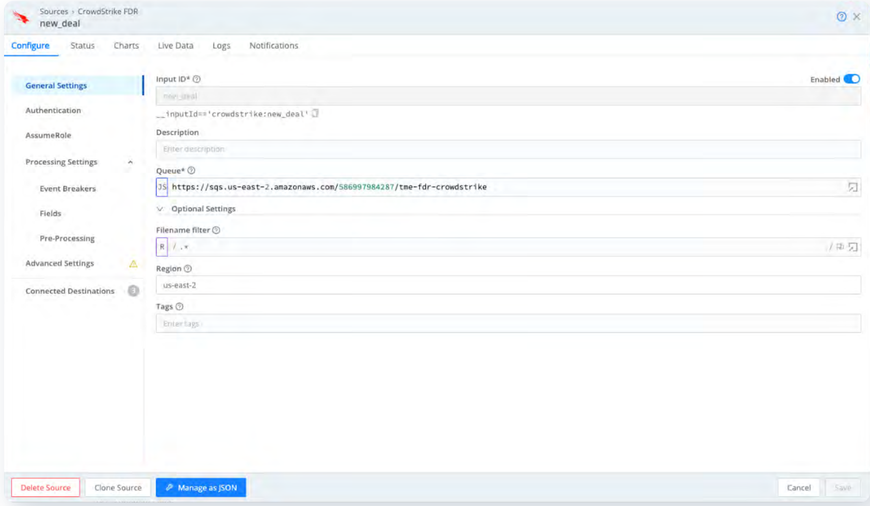
Set priorities for what you want to achieve with the migration, whether it's improving threat detection capabilities, optimizing costs, or enhancing compliance measures. Establish success criteria that align with these goals.

3 | Set up Cribl Stream

Install and configure Cribl Stream as your central telemetry pipeline. Configure it to ingest data from your existing sources and route it simultaneously to both legacy and new SIEMs. The intuitive interface makes setup straightforward, even for teams unfamiliar with telemetry pipelines. Check out our Getting Started Guide for a hands-on guide to Stream's core features and to learn how to set up a basic deployment.

4 | Configure Sources

Connect all relevant sources—like firewalls, VPN logs, audit trails—to Cribl Stream. Stream's visual UI, QuickConnect, is a great way to swiftly get data sources connected to your desired destinations. From there, you can use QuickConnect to parse, normalize, and enrich incoming telemetry in flight on its way to the destination(s). Use "Routes" for more flexible configurations tailored to your specific needs.



Sources › CrowdStrike FDR
new_deal

Input ID*: new_deal

Enabled

`__inputId=='crowdstrike:new_deal'`

Description: Enter description

Queue*: `https://sqs.us-east-2.amazonaws.com/586997984287/tme-fdr-crowdstrike`

Optional Settings

Filename filter: `/.*`

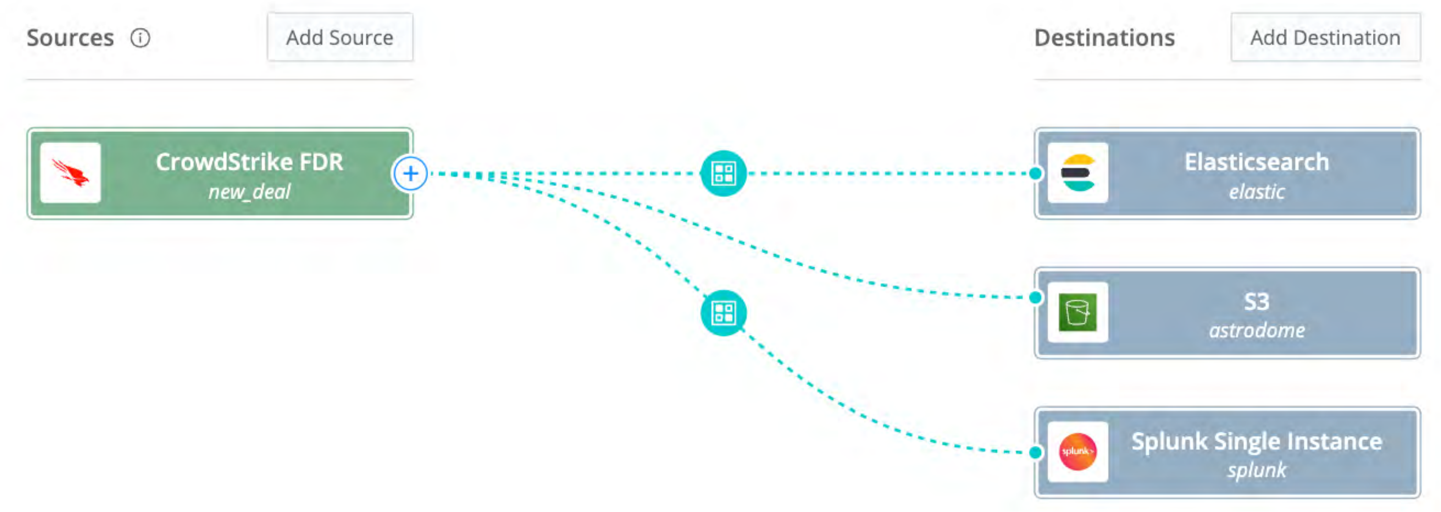
Region: us-east-2

Tags: Enter tags

Implementing a Streamlined SIEM Migration with Cribl Stream *(continued)*

5 | Implement phased migration

Use Stream to clone production data into the new SIEM while keeping the legacy system operational. Gradually transition use cases like insider threat detection or account activity monitoring from one system to the other. This phased approach allows you to test new configurations thoroughly before fully cutting over.



5 | Validate and optimize

Test dashboards, alerts, and use cases in the new SIEM using live production data routed through Cribl Stream. Refine configurations based on performance metrics gathered during testing phases. Adjust routing rules within Stream for further optimization as needed.

Monitor and adjust your migration strategy

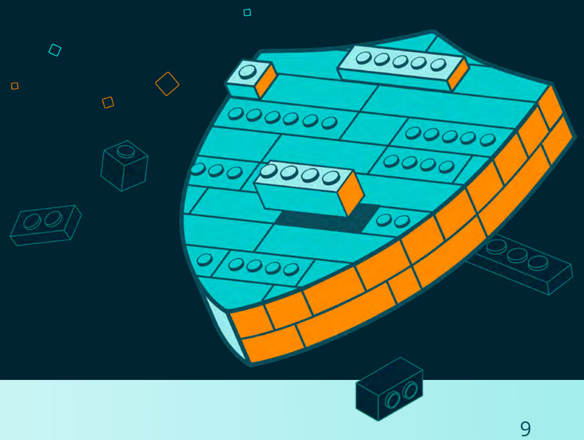
A successful SIEM migration doesn't end with the deployment of a new platform. Continuous monitoring and adjustment are essential to ensure the new system delivers on its promises of improved threat detection, operational efficiency, and cost optimization. By using Cribl Stream in your migration strategy, you can maintain visibility into performance, identify areas for improvement, and adapt to evolving security needs.

With Cribl Stream, teams can monitor ingestion rates, alert accuracy, and system performance throughout the migration process. This visibility allows security teams to identify bottlenecks, data drift, and inefficiencies that could impact the effectiveness of the new SIEM. By tracking these metrics, organizations can proactively address issues and maintain their security posture.

Post-migration, Stream's flexibility supports evolving security demands. Teams can adapt to new threats by adding data sources, refining filtering rules, or enhancing enrichment pipelines. Additionally, benchmarking SIEM performance, such as search times or alert reduction rates, ensures the system continues to meet business objectives. Regular tuning sessions and red team attack simulations can help further optimize detection accuracy and operational efficiency.

For a deeper dive into refining your SIEM migration strategy, including detailed steps on benchmarking and adapting workflows, take a look at our Eight Steps to Mastering Your SIEM Migration whitepaper.

This asset provides actionable insights to help security teams maximize the value of their new SIEM while maintaining a robust security posture.



Conclusion

Migrating to a modem SIEM platform is an opportunity to transform how your organization approaches security operations. By using Cribl Stream during migration, your organization can:

- **Reduce risk** through phased transitions
- **Gain flexibility** in tool selection without vendor lock-in
- **Improve data quality** while optimizing costs
- **Ensure operational continuit**y while future-proofing your security architecture

Cribl Stream empowers organizations to migrate SIEM confidently while laying the groundwork for more flexible and efficient security operations in the long term.

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: cribl.io | Try now: Cribl sandboxes Join us: Slack community
Follow us: LinkedIn and X (Twitter)

EB-0008-EN-1-0525