>SOLUTION BRIEF_

Cribl and CrowdStrike Falcon Next-Gen SIEM.

THE INDUSTRY CHALLENGES

- As cyber threats get more sophisticated, organizations must continuously update their defensive strategies to secure their digital landscapes.
- Enterprises face the challenge of securing an increasingly complex IT environment with dispersed data, integrating new tools effectively with legacy SIEM, and overcoming siloed visibility across point products that delay threat detection and response.
- Organizations must navigate a growing array of regulations governing data security and privacy, requiring sophisticated compliance mechanisms.

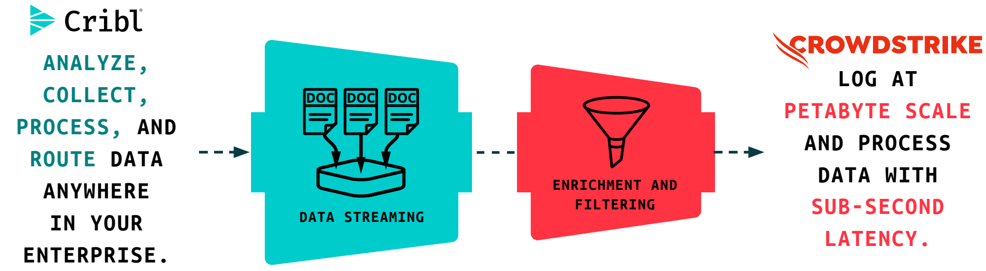
THE SOLUTION

Cribl and CrowdStrike Falcon® Next-Gen SIEM integrate best-in-class platforms to help teams overcome these challenges, manage their security landscape more effectively, unify visibility, and maintain compliance with ease.

Changes across the industry.

Organizations today face a complex cybersecurity landscape, where managing a vast volume of security data and effectively responding to threats quickly becomes paramount. Today's SOCs struggle to keep up with adversaries, and are dealing with a 133% annual global growth in cyber assets and 28% data growth year over year. With cybersecurity threats growing in sophistication and speed, companies struggle with integrating, managing, and analyzing the vast amounts of data from disparate sources needed to combat them. This complexity can cause gaps in visibility and slowed operations, hindering threat detection and response while increasing risk.

Through a strategic partnership, Cribl and CrowdStrike have developed a robust solution that unifies and streamlines the management of cybersecurity data. This approach enhances visibility, improves threat detection and response capabilities, and gets more of the right data to Next-Gen SIEM.



ANALYZE, COLLECT, PROCESS, AND ROUTE DATA ANYWHERE IN YOUR ENTERPRISE.

LOG AT PETABYTE SCALE AND PROCESS DATA WITH SUB-SECOND LATENCY.

Cribl and Falcon Next-Gen SIEM for unified security management.

By integrating Cribl and Falcon Next-Gen SIEM, teams get the combined benefit of Cribl's data stream management excellence with CrowdStrike's advanced AI-native SOC platform, helping to easily unify dispersed data sources for faster, more accurate threat detection and response. With security data seamlessly streamed, stored, and analyzed in one threat-centric console, Cribl and CrowdStrike simplify complex security operations and help to maximize the effectiveness of existing security solutions— no matter where the data is located.

With Cribl and Falcon Next-Gen SIEM, teams can:

- Integrate data and tooling: Consolidate various data sources, including log files, network traffic data, endpoint data, threat intel feeds and more into the Falcon platform enhances threat detection and response.
- Better manage data: Use filtering and enrichment techniques to minimize noise and focus on high-priority threat indicators, like unusual outbound traffic, unauthorized access attempts, and patterns that scream "malware".
- Scale and flex: Adapt to evolving security needs, ensuring sustainable and robust cybersecurity infrastructure. Support scalability in data management. Efficiently handle more data volumes without degrading system performance. Collect more data, faster and easier. Improve data collection efficiency— critical for the SIEM and SOC.

A closer look at the use cases: Cribl and Falcon Next-Gen SIEM.

Trying out a new SIEM.

For organizations exploring new SIEM technologies or setting up a SIEM for the first time, the Cribl and CrowdStrike solution ensures a smooth implementation. Cribl's robust data management capabilities simplify the integration of existing data sources with CrowdStrike's SIEM, ensuring that data is optimally formatted and enriched from the start.

Augmenting your existing SIEM tool.

Enhance the capabilities of your existing SIEM system with Cribl's data stream management tools. This augmentation allows for better data handling, reducing the load on the SIEM and improving its efficiency and effectiveness in threat detection.

Migrating your SIEM.

Reduce migration risk and streamline the process of moving from one SIEM system to Falcon Next-Gen SIEM. By managing and conditioning the data before, during, and after the migration using Cribl, organizations can ensure continuity, compliance, and performance without disruptions.

GET STARTED WITH CRIBL AND CROWDSTRIKE FALCON NEXT-GEN SIEM TODAY.

Cribl and Falcon Next-Gen SIEM deliver a unified approach to simplify operations and strengthen cybersecurity posture across various industries, giving teams:

- As cyber threats get more sophisticated, organizations must continuously update their defensive strategies to secure their digital landscapes.
- Enterprises face the challenge of securing an increasingly complex IT environment with dispersed data, integrating new tools effectively with legacy SIEM, and overcoming siloed visibility across point products that delay threat detection and response.
- Organizations must navigate a growing array of regulations governing data security and privacy, requiring sophisticated compliance mechanisms.

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 Twitter

SB-0047-EN-1-0624