Cribl

>SOLUTION BRIEF_

Increase data visibility and accelerate attack resolution with Cribl Stream™ and Exabeam New-Scale SIEM™

THE CHALLENGE

Traditional SIEMs struggle in today's complex and expanding environments, creating a growing effectiveness gap fueled by increased data volume, alerts, and costs.

THE SOLUTION

Cribl and Exabeam join forces to address data challenges that hinder security investigations, technology adoption, and compliance — enhancing security teams' visibility into relevant data sets and speeding up TDIR.

THE BENEFITS

- Enable vendor-neutrality and faster data onboarding, ensuring data integrity during migration for Exabeam customers.
- Enhance processing capabilities, optimizing downstream systems and enabling cost-effective data delivery to New-Scale SIEM.
- Improve visibility and context for Exabeam customers, enabling swift response to high-risk activity and incidents involving multiple teams.

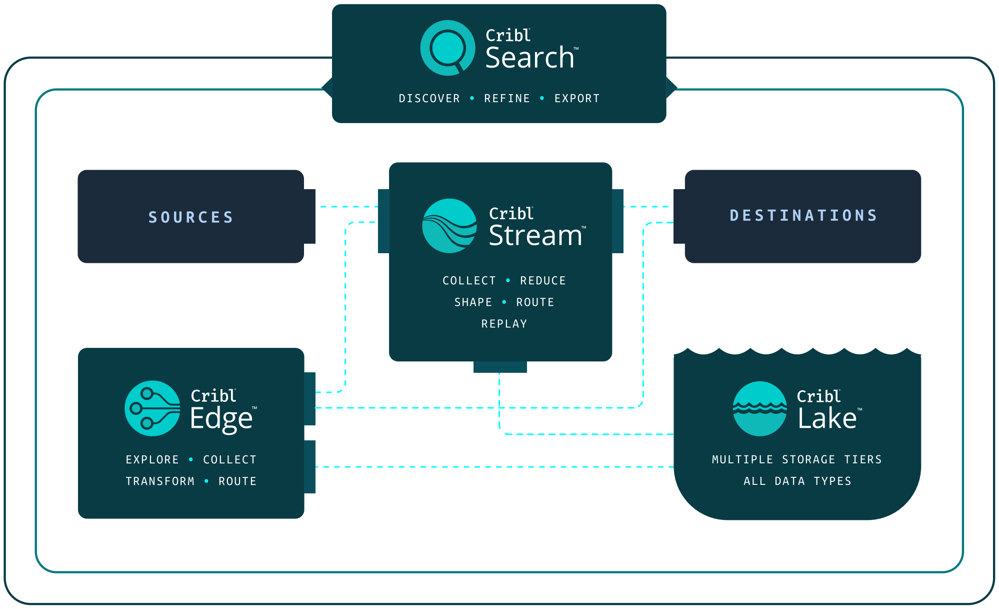
Together, Exabeam New-Scale SIEM and Cribl Stream provide a way for security teams to accelerate threat detection, investigation, and response (TDIR) while increasing data visibility.

The power of Cribl and Exabeam.

Traditional SIEM platforms relying on search and correlation can be expensive and resource-intensive. Security teams grappling with a disconnect between their data needs and SIEM products need a flexible solution to securely gather and analyze data from various sources — at cloud-scale.

Exabeam's cloud-native architecture handles more data sources at higher volumes, offering risk-based prioritization and insights that legacy tools often overlook. The architecture allows for rapid data ingestion, hyper-fast query performance, behavioral analytics, and automated investigation capabilities that enhance security analysts' effectiveness. With Cribl Stream's observability solution, security teams gain extra visibility and control over telemetry data, along with the flexibility to format logs as needed. Stream ensures efficient data ingestion, reducing storage costs by ingesting only the necessary data into the SIEM.

Cribl and Exabeam collaborate to tackle log data challenges that can hinder security investigations, technology adoption, and compliance. Using Exabeam Security Operations Platform and Cribl's data pipelining engine, security teams unlock maximum data ingestion efficiency, reduced costs, and accelerated threat detection, investigation, and response (TDIR).



Cribl and Exabeam collaborate to tackle log data challenges that hinder security investigations, technology adoption, and compliance.

The benefits of using New-Scale SIEM with Stream.

Gain vendor-neutrality and unlock seamless migrations with no data loss.

Cribl Stream facilitates smooth data migration to Exabeam's New-Scale SIEM, ensuring data dependencies are maintained, and provides vendor-neutrality to onboard data efficiently. This seamless migration process guarantees data integrity throughout, preventing any loss of critical information. Exabeam's New-Scale SIEM is designed to handle the complexities of modern environments, offering enhanced scalability and performance.

Optimize data delivery for Exabeam New-Scale SIEM.

Cribl empowers Exabeam customers to optimize data delivery to New-Scale SIEM effectively. By utilizing Cribl Stream, customers can filter out unnecessary fields, ensuring that only relevant data is sent to Exabeam's SIEM. Additionally, Stream allows for the redirection of high-volume data to appropriate downstream systems, avoiding unnecessary strain on the SIEM infrastructure. This optimization ensures better performance and cost-effectiveness of data delivery to New-Scale SIEM.

Enhance visibility and accelerate incident response.

Cribl plays a pivotal role in enhancing visibility and incident response capabilities for joint Exabeam customers. By leveraging Cribl Stream's flexible data collection and enrichment, customers can add additional context to the data, such as GeoIP, asset information, and behavior analytics. This enriched data empowers security teams with comprehensive insights, leading to improved visibility into potential threats and faster, more effective incident response across multiple teams. The combination of New-Scale SIEM and Stream's data enrichment capabilities ensures a robust and proactive security approach.

Summary.

Looking to let go of legacy security tools that struggle to keep up with the latest cyber threats, many enterprises are turning to Exabeam. Exabeam technologies enable SecOps teams to transform and modernize their SOC, so they catch every attack and respond more quickly and maximize their TDIR investments.

Exabeam's cloud-native architecture handles more data sources, offering risk-based prioritization and insights. Its rapid data ingestion, hyper-fast query performance, behavioral analytics, and automated investigation enhance security analysts' effectiveness. With Cribl Stream, security teams gain control over telemetry data and access to top-tier processing, optimizing data ingestion and reducing storage costs.

Cribl and Exabeam collaborate to tackle log data challenges that hinder security investigations, technology adoption, and compliance. Using Exabeam Security Operations Platform and Cribl's data pipelining engine, security teams achieve maximum data ingestion efficiency, cost reduction, and accelerated threat detection, investigation, and response.

> **Together, Cribl and Exabeam Stream provide a way for security teams to accelerate threat detection, investigation, and response (TDIR) while increasing data visibility.**

With Cribl Stream and Exabeam New-Scale SIEM, customers can:

- Enable vendor-neutrality and faster data onboarding, ensuring data integrity during migration.
- Get access to enhanced migration services through partners for on-premises, cloud, multi-cloud, and hybrid deployments.
- Enhance their data processing capabilities, optimizing downstream systems and enabling cost-effective data delivery to Exabeam New-Scale SIEM.
- Maximize internal and channel support on cost-saving and retention initiatives while maintaining platform flexibility.
- Improve visibility and context, enabling swift response to high-risk activity and incidents involving multiple teams.
- Accelerate execution of security playbooks, incident remediation, and efficient data sharing for MSSPs with internal, customer, and vendor teams.

To get started with Exabeam New-Scale SIEM and Cribl Stream today, click here to sign up for Stream Cloud. The Cribl Slack Community is also a great place to connect with leaders from other teams leveraging both Cribl and Exabeam.

ABOUT EXABEAM

Exabeam is a global cybersecurity leader that adds intelligence to every IT and security stack. We are reinventing the way security teams use analytics and automation to solve threat detection, investigation, and response (TDIR), from common security threats to the most critical that are difficult to identify. The Exabeam Security Operations Platform is a comprehensive cloud-delivered solution that leverages machine learning and automation using a prescriptive, outcomes-based approach to TDIR. It is designed and built to help security teams detect external threats, compromised users and malicious adversaries, minimize false positives, and make security success the norm. For more information, visit www.exabeam.com.

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-0030-EN-2-0524