Exabeam and Cribl

Maximize data visibility and reduce costs with New-Scale SIEM™ from Exabeam and Cribl Stream

Legacy SIEM solutions weren’t built for today’s complex, rapidly expanding environments, creating what we call the SIEM effectiveness gap. This gap is widening as data volumes increase, driving up the cost of storage and resources needed to manage security alerts. Platforms that rely primarily on search and correlation are often expensive and resource intensive, requiring knowledge of what you are looking for. When it comes to security, there is often a big difference between what security teams need and what SIEM products deliver. Teams need the flexibility to get data safely from multiple sources while gathering valuable context and insights that accelerate threat investigation, remediation, and response — and do it at cloud scale.

The Power of Exabeam and Cribl

New-Scale SIEM™ from Exabeam manages more data sources at a higher volume and delivers risk-based priorities and insights to uncover and escalate threats that legacy tools and point solutions miss. The combination of rapid data ingestion, hyper-fast query performance, powerful behavioral analytics, and automated investigation helps increase security analysts’ effectiveness.

Cribl’s Stream observability solution provides additional control over telemetry data and the flexibility required to route, filter, and mask data on the fly. Cribl helps to provide efficient data ingestion by ensuring only the correct data gets ingested into Exabeam. By filtering out low-value data, security organizations create additional headroom for new telemetry data while reducing storage costs.

Together, Exabeam and Cribl provide security teams with better visibility into the right data sets to accelerate threat detection, investigation, and response (TDIR).

Data creation in 2025¹: 175ZB
Massive growth in compliance requirements²: $50B²
Massive growth in tooling and complexity³: 54%³

¹ IDC WW Global DataSphere and Global StorageSphere Structured and Unstructured Data Forecast, 2022-2026
² 166ZB of unstructured data - logs, events, metrics and traces + 15ZB of structured data - transactional data commonly held in databases and data warehouses
³ https://www.ibm.com/downloads/cas/3R8N1DZJ)
Data Routing with Cribl

Joint Use Case Scenarios

**Flexible Data Routing** — Route data to and from any security tool in your stack without adding infrastructure or agents

**Data Filtering** — Filter out low-value data from security storage and analytics to increase headroom and boost downstream performance

**Data Shaping and Masking** — Enrich third-party data with threat intel, GeoIP, asset info, and more or mask sensitive PII data in flight for compliance

Primary Benefits of Exabeam and Cribl

- Accelerate the adoption of New-Scale SIEM with no downtime
- Route security log data to multiple destinations
- Reduce storage costs through data filtering
- Pull in quality telemetry data to improve threat detection
- Expand the visibility of security threats and detect abnormal activity
About Cribl

Cribl makes open observability a reality for today's tech professionals. The Cribl product suite defies data gravity with radical levels of choice and control. Wherever the data comes from, wherever it needs to go, Cribl delivers the freedom and flexibility to make choices, not compromises. It's enterprise software that doesn't suck, enables tech professionals to do what they need to do, and gives them the ability to say “Yes.” With Cribl, companies have the power to control their data, get more out of existing investments, and shape the observability future. Founded in 2018, Cribl is a remote-first company with an office in San Francisco, CA.

For more information, visit www.cribl.io or our LinkedIn, Twitter, or Slack community.

About Exabeam

Exabeam is a global cybersecurity leader that created New-Scale SIEM™ for advancing security operations. We help organizations detect threats, defend against cyberattacks, and defeat adversaries. The powerful combination of our cloud-scale security log management, behavioral analytics, and automated investigation experience results in an unprecedented advantage over insider threats, nation states, and other cyber criminals. We understand normal behavior, even as normal keeps changing — giving security operations teams a holistic view of incidents for faster, more complete response.