SOLUTION BRIEF

Supercharge Your Security Insights with Cribl Stream

Drive better visibility across SecOps by taking control of your data

The Challenge

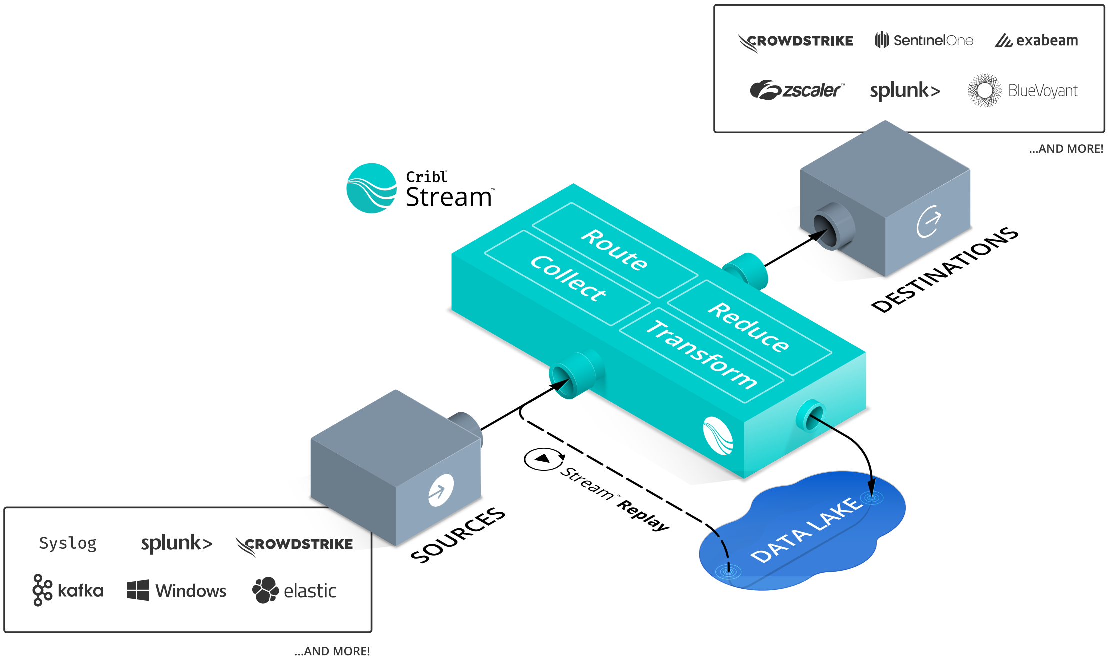
Security teams are inundated with data from multiple sources and formats. Digging through a mountain of noisy, low quality data slows detecting breaches, hunting for new threats, and responding when a breach does occur. Moreover, with multiple security tools deployed, sharing information across tools is impossible.

The Cribl Solution

Use Cribl Stream's data filtering to boost your data's signal, then increase the value of what you choose to keep by enriching it with context – automatically adding related data from external sources – all in real time.

Enrich your data with third party sources like GeoIP and known threats databases before it even gets into your logging and SIEM platforms. Provide greater context to your organization, and enable a deeper, more actionable response of your security and observability data.

Eliminate duplicate fields, null values, and any elements that provide little analytical value. Filter and screen events for dynamic sampling, or convert log data into metrics for access to massive volume reduction, leading to better performance and cost savings.



SOLUTION BENEFITS

- Enrich data from third-party sources for improved context
- Filter low value data from security analytics platforms
- Govern data while masking PII and ensuring regulatory compliance

CRIBL STREAM HELPS YOU GET THE SECURITY DATA YOU WANT, IN THE FORMATS YOU NEED, TO WHEREVER YOU WANT TO GO.

Key Features of Stream

BOOST THE SIGNAL AND REDUCE THE NOISE

Enrich data before it lands in your security tooling to accelerate threat intelligence and incident response efforts. Stream allows you to add context to critical security data sources, like GeoIP, indicators of compromise, and any other threat intelligence database.

EASILY GET DATA IN

Stream acts as a universal collector and receiver of security data sources, allowing you to quickly ingest and normalize data using a best-in-class user experience. On-board new and existing data and send it to any security platforms on your terms.

IMPROVE THREAT HUNTING

On-demand routing of data to the threat hunting tools of your choice to find new threats and feed detection pipeline with new content. Uncover unknown unknowns faster with better observability over all your data.

ACCELERATE INCIDENT RESPONSE

Shape all of the data you need to drive decisions about your environment. Translate and transform data from all of your sources to the tools you choose. Get a more complete picture of your data by enriching logs with third-party data. Stream collects data from all of your sources, and shapes it into actionable logs and metrics for analysis.

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 2017, 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.