Cribl

>SOLUTION BRIEF_

Cribl for the Intelligence Community.

Optimize IC mission outcomes with a data processing engine purpose-built for IT and Security.

The challenge.

Public sector agencies, including those in the intelligence community, face the challenge of managing sensitive data that requires special handling, classification, and heightened access monitoring to mitigate insider threats. With incidents like the Wikileaks and Snowden disclosures compromising national security, there is a pressing need for comprehensive solutions to monitor and control data access and dissemination.

The solution.

Public sector agencies, both civilian and within the intelligence community, are tasked with managing sensitive data that requires special handling, classification, and heightened access monitoring to address insider threats. This is in accordance with guidelines such as the Office of Management and Budget (OMB) Memorandum M-21-31, NIST Special Publication 800-53, and Intelligence Community Standard (ICS) 500-27, and recent incidents have underscored the need for robust solutions that monitor and control data access and dissemination to safeguard national security.

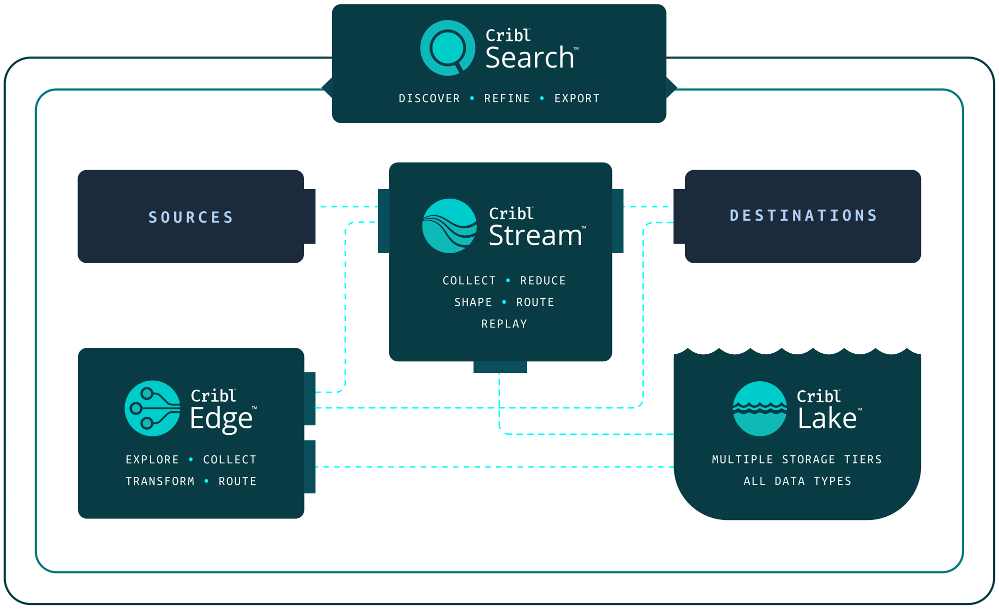
Cribl offers a comprehensive suite of products tailored to the specific challenges faced by public sector agencies in detecting and mitigating insider threats. By leveraging advanced data collection, analysis, and monitoring capabilities, Cribl enables agencies to proactively identify and respond to insider threats while aligning with the requirements set forth in M-21-31, NIST 800-53, and ICS 500-27. This ensures compliance and enhances the security posture of agencies' sensitive information and operations.

The Cribl suite of products encompasses a range of capabilities designed to address the unique needs of public sector agencies in combating insider threats. Cribl solutions facilitate the comprehensive collection and ingestion of vast amounts of structured and unstructured data from diverse sources, including IT system and security logs (as outlined in NIST 800-53), organizational context data, and external context data, adhering to the guidelines of M-21-31 and ICS 500-27. This allows agencies to gather a holistic view of employee activities, enabling in-depth analysis and anomaly detection.

THE INTELLIGENCE COMMUNITY + DATA MANAGEMENT

- Public sector agencies face insider threat challenges with sensitive data, necessitating monitoring and control.
- Compliance with guidelines such as OMB Memorandum M-21-31, NIST Special Publication 800-53, and ICS 500-27 is crucial for public sector agencies to effectively manage sensitive data and ensure national security.
- Cribl solutions aligns with those regulations and more, enabling proactive insider threat detection and compliance with enhanced security measures.

> "Having the flexibility to pivot destinations based on the type of data is really powerful. We're able to give the analysts and the users of these tools a much easier experience and save them valuable time."
>
> **Josh Brunvoll,**
> Consulting Engineer at a large federal agency



Use cases:

Collect and route data to the right destinations.

Get data where it needs to go in support of M-21-31, NIST 800-53, and ICS 500-27.

Effectively combat insider threats.

Ensure interagency and internal teams have the necessary insights to stop bad actors.

Cribl for the IC.

The Cribl suite of products is tailored to the specific challenges faced by public sector agencies, including detecting and mitigating insider threats. By leveraging advanced data collection, analysis, and monitoring capabilities, Cribl enables the intelligence community to proactively identify and respond to insider threats while aligning with the requirements set forth in M-21-31, NIST 800-53, and ICS 500-27, ensuring compliance and enhancing the security posture of agencies' sensitive information and operations.

Capabilities:

- Collect and ingest vast amounts of structured and unstructured data from diverse sources, including IT system and security logs (as outlined in NIST 800-53), organizational context data, and external context data, adhering to the guidelines of M-21-31 and ICS 500-27.
- Perform ad hoc or automated queries across multiple data sources, enabling in-depth analysis of anomalous employee behaviors and potential insider threats in accordance with M-21-31 and NIST 800-53.
- Integrate organizational context data from HR databases and other business systems, along with external context data specified in ICS 500-27, providing a holistic view of employee activities and motivations, enhancing the accuracy of threat detection.
- Support continuous evaluation of cleared personnel, facilitating real-time identification of suspicious activities and prompt response to potential threats, as required by M-21-31 and NIST 800-53.
- Vendor-agnostic integration with IC ecosystems, bolstering analysis capabilities and providing pre-built content for streamlined insider threat investigations.

Cribl Stream™

A vendor-neutral collection, reduction, enrichment, and routing system for IT and security data.

Cribl Edge™

An intelligent, scalable, edge-based data collection system for logs, metrics, and application data.

Cribl Search™

Perform federated "search-in-place" queries on any data, in any form.

Cribl Lake™

A simplified data lake solution to easily store, manage, and access data.

Benefits:

With Cribl, the intel community can:

- Proactively detect and mitigate insider threats, aligning with the proactive approach advocated in M-21-31 and NIST 800-53, thus reducing the risk of sensitive information leaks and national security breaches.
- Enhance visibility into employee activities, enabling more effective identification of potential insider threats, as stipulated in NIST 800-53.
- Streamlines the insider threat detection process, saving valuable time and resources for agencies, in accordance with M-21-31 and NIST 800-53.
- Respond promptly to potential threats, minimizing the impact of insider incidents and aligning with the timely response requirements outlined in M-21-31.
- Comply and govern data in accordance with industry guidelines, standards, and memorandums.

Cribl helps the intelligence community bring data to every mission, enabling proactive identification and response to insider threats, aligning with the requirements set forth in M-21-31, NIST 800-53, and ICS 500-27, and enhancing the security posture of agencies' sensitive information and operations.

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-0040-EN-1-0524