>SOLUTION BRIEF_

Accelerate EO 14028 Compliance While Controlling Log Ingestion Costs

THE CHALLENGE

U.S. Federal agencies are tasked with building effective cybersecurity practices and workflow in an ever-changing threat environment, while optimizing their SIEMs for cost , scale, and complexity.

THE SOLUTION

Cribl Stream gives federal agencies the power of an observability pipeline, enabling them to accelerate EO 14028 compliance, follow memorandum guidance to the letter, and control log ingestion costs.

THE BENEFITS

- Achieve best-in-class SIEM optimization and data reduction
- Effectively address the requirements of M-21-31
- Easily comply with data enrichment and routing directives
- Accelerate your Zero Trust Architecture (ZTA) strategy for network and data with respect to M-22-09

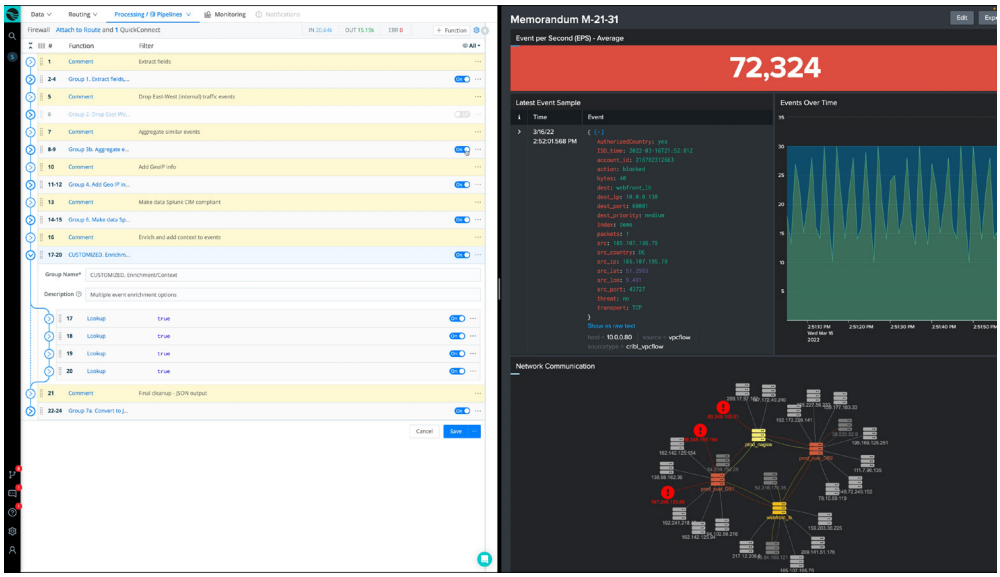
When federal agencies integrate Cribl Stream into their environment, they can quickly and securely optimize their SIEM for cost and performance, while complying with the latest OMB mandates.

It's no secret that U.S. federal agencies are on a mission: to protect the American people and continuously improve our nation's approach to cybersecurity. It's a daunting task, but agencies can get there by optimizing their security, incident, and event management tooling, to comply with Executive Order (EO) 14028, and following the guidance issued in memorandums M-21-31, M-22-01, and M-22-09. By integrating the leading observability pipeline Cribl Stream into their environment, federal agencies can accelerate EO 14028 compliance and follow memorandum guidance to the letter, reduce complicated architecture, and control ingestion costs.

Achieve Best-in-Class SIEM Optimization and Data Reduction

With the Cribl product suite, organizations can free up valuable analytic capacity in their SIEM by sending data to the most cost-effective destinations, like object storage, for long-term retention. This separates companies' SIEM instance – or system of analysis – from their system of record, enabling them to route data to the best tool for the job – or all the tools for the job – by translating and formatting data into any tooling schema they require. Cribl Stream processes data in flight, meaning agencies can remove extraneous fields, null values, mask sensitive and PII fields, and eliminate duplicate events, leading to log volume reductions on average of 30% or more – all while keeping a full-fidelity copy in low-cost storage to replay if needed.

Executive order (EO) 14028: improving the nation's cybersecurity emphasizes cybersecurity as a national priority and mandates each federal agency to adapt to today's continuously changing threat environment.



Effectively Address the Requirements of M-21-31

The Biden Administration's Executive Order (EO) 14028: Improving the Nation's Cybersecurity emphasizes cybersecurity as a national priority and mandates each federal agency to adapt to today's continuously changing threat environment. EO 14028 directs federal agencies to take decisive action to improve cybersecurity investigative and remediation capabilities. Effective policies around logging, retention, and management are essential for improving these capabilities, and OMB-issued memorandum M-21-31 details a maturity model for event log management. With Cribl Stream, a streamlined approach to advanced maturity is finally within reach for federal agencies. These mandates provide direction for Federal agencies to reach basic logging maturity by August 2022, and achieve the highest maturity level by August 2023. Cribl Stream supports the most critical elements of each maturity level by augmenting your current logging environment.

STREAM SUPPORT ACROSS MATURITY LEVELS		
EL1	**EL2**	**EL3**
• Basic Logging Categories • Minimum Logging Data • Time Standards • Event Forwarding • Protecting & Validating Log Info • CISA & FBI Access Requirement • Basic Centralized Access	• Intermediate Logging Categories • Inspection of Encrypted Data • Intermediate Centralized Access	• Advanced Logging Categories • Advanced Centralized Access

Cribl Lake gives IT and security teams the power to eliminate vendor lock-in, streamline workflows, and analyze more faster.

Easily Comply with Data Enrichment and Routing Directives

A second memorandum, M-22-01, directs the federal government to adopt a robust endpoint detection and response (EDR) solution to bolster agency's abilities to respond to increasingly sophisticated threat activity on Federal networks. Real-time continuous monitoring and collection of all endpoint data is crucial to those efforts. Cribl Stream is able to perform data enrichment in order to address data attribution issues and help you answer the question, "Who performed this action?" As a universal router and receiver, Cribl Stream can bring in endpoint data from any source, and send it to any destination for consolidation, retention, and archival – making it the perfect tool to help you achieve M-22-01 compliance.

Accelerate your ZTA strategy for network and data with respect to M-22-09

Finally, memorandum M-22-09 puts forth a zero trust architecture (ZTA) strategy for all federal agencies. The Zero Trust Model is built on the tenet that no actor, system, network, service operating outside or within the security perimeter is trusted. Data categorization, monitoring sensitive data, and information sharing are additional components of zero trust and critical to national security. Cribl Stream provides out of the box capabilities to address each of these challenges through data enrichment, masking and removing sensitive data, and allowing agencies to format data when sharing across multiple destinations. With an observability pipeline like Cribl Stream in place, federal agencies get a centralized control plane that adheres to the Zero Trust model, so they can securely manage device data and traffic flow.

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-00XX-EN-X-XX24