>SOLUTION BRIEF_

Augment your SIEM with Microsoft Sentinel, Azure Data Explorer, and Cribl

THE CHALLENGE

Long retention requirements, unpredictable costs, and rapid data growth leave customers struggling with limitations in their current self-managed SIEMs and looking to modernize to full-service SIEM platforms like Microsoft Sentinel.

THE SOLUTION

Cribl Stream provides a vendor-agnostic observability pipeline to help you route, parse, restructure, and enrich data in flight. Giving you the power to write directly to Microsoft Sentinel and ADX while allowing multiple SIEMs to run in parallel until a full cutover is appropriate for improved security posture.

THE BENEFITS

- Scalable and resilient data collection.
- Efficient analysis and long-term storage.
- Selectively route data to improve security posture.
- Cross-cloud consolidation.

Onboard security data from non-Azure source into Microsoft Sentinel, while managing costs by offloading high-volume, low-value data to Azure Data Explorer's data analytics platform.

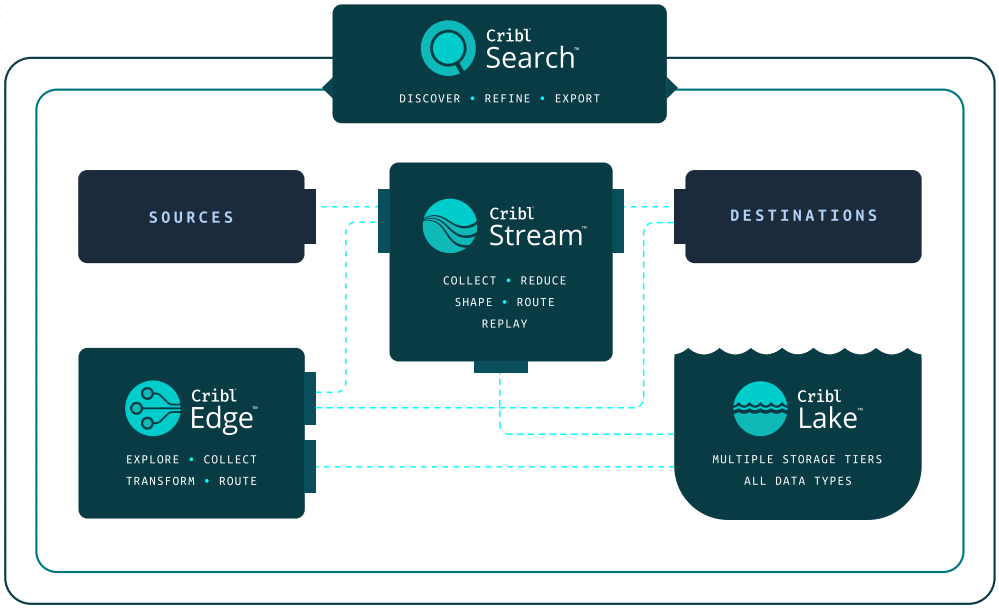
The challenge.

Limitations of traditional SIEM tools with long retention requirements, unpredictable costs, and rapid data growth isn't sustainable. Designed for real-time analysis, these tools weren't meant to be used for storing and managing the exponential growth of data. It's simply too expensive to retain data in the tools used to analyze it. You need a centralized security data platform that gives you the freedom to unlock third party data for your cloud-native SIEM while routing low priority data to a data lake, keeping it at arms reach without blowing their infrastructure budget.

The solution.

Organizations opt for Microsoft Sentinel's comprehensive SIEM for its robust SOAR and threat intelligence capabilities, and seamless integration with Microsoft's suite. However, to achieve true enterprise-wide threat intelligence, security teams need a centralized platform to bring in data from third-party sources and maintain threat detection and response alongside existing tooling.

Cribl defies data gravity with radical levels of choice and control by simplifying data management and giving you the flexibility to route, parse, restructure, and enrich data in flight, enabling a fast and cross-cloud consolidation for efficient migration of workloads to Sentinel. This streamlines operations compared to managing multiple OSS tools. Transform data into default or custom tables within Log Analytics Workspace, and write directly to Azure Data Explorer (ADX) or Blob Storage with the ability to replay data as needed to any destination, reducing intermediary steps and streamlining your security infrastructure. Whether you're adopting a new SIEM strategy, going multi-SIEM, or in negotiations with your current SIEM vendor, gain the power to run Microsoft Sentinel in parallel with the rest of your tech stack until a full cutover is appropriate for improved security posture.



CUSTOMER STORY:

Edward Jones shifts to a modern, cloud-native architecture

"With Cribl Stream, we can get the data our old SIEM collected, as well as any other data we want to collect. It allows us to serve other platforms and the other teams using their own processes within our organization the right data. We can all work together now to collect data once and get it to everybody that needs it, in the optimal format."

— Christopher Simpson,
Sr. Technical Architect, Edward Jones

Watch Case Study Webinar

The benefits of using Cribl with Microsoft Sentinel and Azure Data Explorer:

Scalable and resilient data collection.

Onboard data from any third-party source and transform it to any format required within Log Analytics Workspace including CommonSecurityLog, SecurityEvents, Syslog, and WindowsEvents tables — leveraging Cribl's direct tile integration to skip any complex reconfigurations.

Selectively route data to improve security posture.

By routing priority data to Sentinel, eliminate duplicative data streams with IT Ops and avoid SIEM down-time or outages.

Separate system of analysis from system of detection.

Route high-quality data to Sentinel for immediate threat alerting and detection, while forking a full-fidelity copy to ADX for long-term data ingestion, querying, visualization, and management.

Efficient analysis and long-term storage.

Store low-priority data in ADX to leverage its high-performance big data analytics capabilities while meeting compliance standards. Replay data as needed back to Sentinel for threat huntingand investigations.

Cross-cloud consolidation.

Simplify data integrations from multiple clouds into ADX and Sentinel with Cribl. A smoother migration into security data warehouses gives enhanced visibility, cost-effectiveness, and a more flexible data analytics framework.

USE CASES

Vendor-neutral routing

- Onboard and route data from any on-premises, cloud platforms, or open-source tools to Microsoft Azure with the flexibility to move that data wherever it needs to go in the future.

SIEM augmentation

- Enhance threat detection and incident response by routing specific data to dedicated tools and workflows including Microsoft Sentinel.

Storage and compliance

- Fork a copy of your data to ADX to meet compliance requirements, with the ability to replay data ad hoc to any destination.

Summary

Customers are choosing Microsoft Sentinel for its powerful SOAR capabilities and threat intelligence features, while looking towards ADX for its high-performance analytics and querying capabilities. Cribl gives these customers the flexibility to seamlessly integrate non-Azure data into Sentinel, while routing low-value data directly to ADX for data exploration, analysis, and cost optimization. Security teams gain data routing and transformation capabilities that enable the efficient onboarding of data to Sentinel and ADX for strengthened security posture.

With Cribl, Sentinel and ADX customers can:

- Simplify data onboarding and get security data into Sentinel and ADX.
- Strengthen security posture, with the flexibility for SIEM augmentation and / or migration.
- Increase visibility and save costs, leveraging ADX's querying and analytics capabilities and long-term retention.
- Consolidate security data across clouds and bring in 3rd party data sources from other cloud environments.

To get started with Microsoft Azure and Cribl today, visit **https://cribl.io/microsoft-azure/**. The **Cribl Slack Community** is also a great place to connect with leaders from other teams leveraging both Sentinel and Cribl.

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, and Cribl Search, the industry's first search-in-place solution. 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-0012-EN-1-0224