Cribl | ALPHASOC

_SOLUTION BRIEF

Uncover compromised endpoints, cloud workloads, and user identities with Cribl and AlphaSOC

THE CHALLENGE

Threat hunting is expensive to undertake within XDR and SIEM platforms, as security teams must index and process large volumes of low fidelity telemetry to drive their detections.

THE SOLUTION

Customers send raw telemetry from Cribl to AlphaSOC to drive their own custom detections and hunt for threats within any kind of audit log.

THE BENEFITS

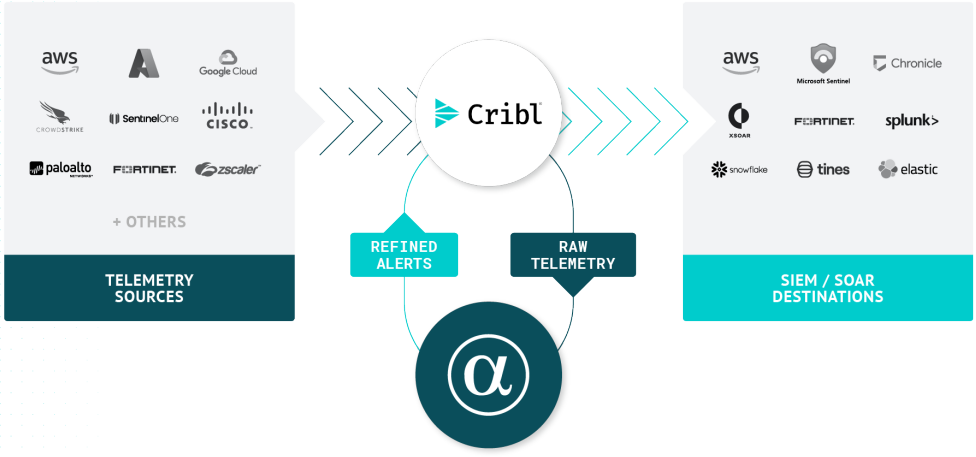
- Detect threats across multiple domains including cloud infrastructure, SaaS applications, and identity providers
- Leverage hundreds of in-built AlphaSOC detections to drive threat hunting across your systems and platforms
- Deploy your own custom detections in Sigma format without having to index telemetry within your SIEM

Combine Cribl Stream and AlphaSOC to detect threats without indexing terabytes of raw audit logs within your SIEM platform. Detect Anything™ with AlphaSOC and build your own detection-as-code pipelines.

Cribl Stream enables security teams to take control over their data to enhance detection and response workflows. Capabilities such as intelligent routing, customizable pipelines, and built-in integrations, allow organizations to optimize, accelerate, and scale their security operations.

Cribl and AlphaSOC provide cost-effective detection coverage for modern security teams. By offloading expensive threat detection processes to the AlphaSOC Analytics Engine, customers can shift resource intensive analytics, enrichment, and time-series analysis outside of their SIEM and reduce unnecessary costs.

Security teams rely on AlphaSOC to highlight threats and anomalies across multiple cloud platforms, SaaS applications, identity providers, operating systems, and networks.



"By eliminating the need for customers to process huge volumes of raw elemetry within their SIEM platforms we can realize significant cost savings and efficiency gains. Cribl and AlphaSOC enable modern teams to build detection-as-code pipelines and embrace open standards for both detection logic (Sigma) and alert output (OCSF). Users can instantly run custom detections without having to load telemetry into a SIEM first."

Why Cribl and AlphaSOC?

Harmonize threat detection logic across multiple platforms

By applying the same unified detection logic and threat intelligence across multiple telemetry sources (e.g., audit logs from AWS, Microsoft Azure, and Google Cloud) security teams can close the blind spots and gaps in coverage between disparate threat detection capabilities.

Detection-as-code support with Sigma rules

AlphaSOC users can instantly deploy thousands of open-source community Sigma rules to drive threat detection across platforms including AWS, Microsoft Azure, Google Cloud, Microsoft 365, Okta, GitHub, Microsoft Windows, Apple macOS, and Linux. Custom Sigma rules can also be deployed to support threat hunting and intelligence gathering.

Reduce threat hunting and detection costs

Security teams avoid data indexing costs by "washing" raw telemetry outside of the SIEM with Cribl Stream and AlphaSOC. The data processing associated with thousands of detection rules is also offloaded to AlphaSOC to further reduce costs. Low volume, high fidelity alerts are then sent from AlphaSOC to any SIEM or Data Lake via Cribl Stream.

Summary

AlphaSOC and Cribl create a scalable threat detection and investigation workflow that maximizes speed, accuracy, and efficiency. Security teams gain extended visibility and the ability to proactively hunt for threats across their environment.

Get started with AlphaSOC and Cribl today at alphasoc.com/cribl

ABOUT ALPHASOC

AlphaSOC provides cutting edge threat detection and analytics software to highlight both known and unknown emerging threats. Security teams rely on AlphaSOC to provide high fidelity alerts and drive their threat hunting and detection programs.

Learn more at alphasoc.com.

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-0059-EN-2-0425