HUNTERS | Cribl

SOLUTION BRIEF

Realize Your Data Lake Strategy with Hunters and Cribl

THE CHALLENGE

SecOps teams need a lightweight solution to send security telemetry to the Hunters SOC Platform, and multiple other destinations.

THE SOLUTION

Using Cribl Stream, teams can easily send telemetry to Hunters in the required formats. When security priorities change, adjusting formats and columns required for Hunters' ingestion pipeline is a frictionless process.

THE BENEFITS

- Easily onboard on-prem data to the Hunters SOC Platform
- Simplify ingest from cloud-based telemetry sources
- Enrich, filter, and transform data in flight
- Route security telemetry to any destination

SOLUTION BRIEF

Realize Your Data Lake Strategy with Hunters and Cribl

Combine Cribl Stream's data ingestion and routing capabilities with the Hunters SOC Platform to accelerate your security data lake rollout.

The Challenge

A security data lake offers the opportunity for unprecedented security analytics. However, realizing those benefits means onboarding a variety of high-volume data sources with different formats and protocols. This crucial part of the data lake equation is often overlooked, and can be a challenge for overworked security teams. Customers are often surprised by the difficulty — and the costs — involved managing the onboarding process.

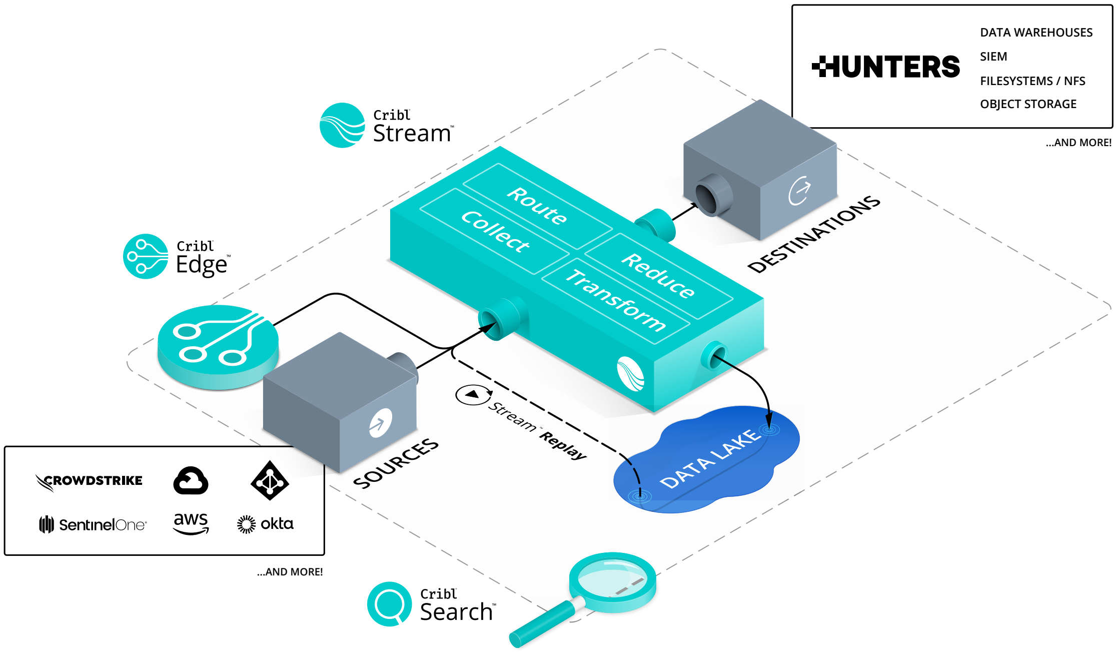
The Solution

Together, Hunters and Cribl make it seamless to move and transform data, no matter the source, into the Hunters SOC Platform. Companies that are looking to replace their SIEM with Hunters can leverage Cribl to expedite the onboarding of their security data and serve as the "data onramp" to Hunters. By combining Cribl Stream's data ingestion and routing capabilities with the advanced capabilities of the Hunters SOC Platform, you can get the most value out of your security data lake.

Recommended Deployment Method

Send data via an S3 bucket to Hunters from Cribl. This recommended method ensures that the data is properly routed and can be easily monitored.

HUNTERS AND CRIBL MAKE IT SEAMLESS TO MOVE AND TRANSFORM DATA, NO MATTER THE SOURCE, INTO THE HUNTERS SOC PLATFORM.



The Benefits of Using the Hunters SOC Platform with Cribl's Observability Solution

EASILY ONBOARD ON-PREM DATA TO THE HUNTERS SOC PLATFORM

Cribl Stream makes ingesting on-prem data into Hunters easy by routing this data to an S3 bucket where Hunters can onboard it into the data lake.

SIMPLIFY INGEST FROM CLOUD-BASED TELEMETRY SOURCES

Cloud logs are high fidelity and an important signal for inclusion in a centralized data lake. In today's cloud SaaS centric environment most customers operate multiple clouds increasing the complexity of getting all cloud logs into the data lake. Cribl makes the process of getting up and running fast without shouldering the burden or costs of managing data onboarding infrastructure.

ENRICH, FILTER, AND TRANSFORM DATA IN FLIGHT

Cribl can transform data into the necessary format (JSON) in order for Hunters to ingest it without having to transform it ourselves. Cribl can also split apart log sources by the different data types for data ingestion into the data lake.

ROUTE SECURITY DATA TO ANY DESTINATION AND REDUCE TOIL

Security teams struggle to route data to their SIEM and long term storage for compliance requirements. Cribl Stream reduces the toil security teams experience having to route data to these multiple destinations.

BY COMBINING CRIBL STREAM'S DATA INGESTION AND ROUTING CAPABILITIES WITH THE ADVANCED CAPABILITIES OF THE HUNTERS SOC PLATFORM, YOU CAN GET THE MOST VALUE OUT OF YOUR SECURITY DATA LAKE.

Summary

With Cribl, Hunters customers can:

- *Easily onboard on-prem data to the Hunters SOC Platform*
- *Simplify ingest from cloud-based telemetry sources*
- *Enrich, filter, and transform data in flight*
- *Route security telemetry to any destination*

Ultimately, Cribl observability solutions help Hunters customers achieve real-time data monitoring capabilities across all enterprise security data sources and unlocks real-time visibility for your data flows for enhanced security operations.

To get started with Hunters and Cribl today, click here. The Cribl Slack Community is also a great place to connect with leaders from other teams leveraging both Hunters and Cribl.

ABOUT HUNTERS

Hunters delivers a Security Operations Center (SOC) Platform that empowers security teams to automatically identify and respond to security incidents across their entire attack surface. The platform enables vendor-agnostic data ingestion and normalization at a predictable cost, and its built-in detection engineering, data correlation, and automatic investigation help teams overcome volume, complexity, and false positives. Hunters mitigates real threats faster and more reliably than SIEMs, ultimately reducing customers' overall security risk. Enterprises like Booking.com, Upwork and Cimpress leverage Hunters SOC Platform to empower their security teams.

Hunters is backed by leading VCs and strategic investors including Stripes, YL Ventures, DTCP, Cisco Investments, Bessemer Venture Partners, U.S. Venture Partners (USVP), Microsoft's venture fund M12, Blumberg Capital, Snowflake, Databricks, and Okta.

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 2018, 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.