CrowdStream

Last updated: Mar. 26, 2025

Overview

CrowdStream is a specialized cloud-hosted version of Cribl Stream to ingest data from a wide range of sources into Falcon Next-Gen SIEM for threat detection, investigation, and response.

Requirements

Subscription: Falcon Next-Gen SIEM

Default roles:

- Falcon Administrator
- NG SIEM Administrator
- NG SIEM Security Lead
- Connector Manager

Permissions required for custom roles: View CrowdStream

CrowdStrike clouds: Available in US-1, US-2, and EU-1.

Additional requirements: The default parser for this integration requires logs ingested in their original format. Dropping and masking log data is allowed as it does not change the format of the original logs. For logs that are not in their original format, a custom parser is required. For more info, see Creating a Parser [https://library.humio.com/data-analysis/parsers-create.html].

Set up CrowdStream

> **Note:** The terms and conditions and privacy notices are displayed for your first login only.

1. In the Falcon console, go to **Next-Gen SIEM > Log management > CrowdStream [/data-connectors/crowdstream]**.
2. Review and check to accept the terms and conditions for CrowdStream.
3. Click **Log in**.
4. Review and check to accept Cribl's terms of service and privacy notice.
5. Click **Continue**
   The CrowdStream Workspace page opens.
6. Follow Cribl's CrowdStream product documentation [https://docs.cribl.io/stream/deploy-crowdstream/] to complete your CrowdStream integration setup.

‹ Fusion SOAR[/documentation/page/v430f1d6/soar-falcon]