

# >INTEGRATION BRIEF\_

Cribl Stream and CrowdStrike Falcon Data Replicator (FDR) Integration

## THE BENEFITS

- Cribl Stream collects data from CrowdStrike Falcon Data Replicator and routes to one or more destinations based on your security analytics and retention requirements.
- Only send the data to your enterprise security platform that is required for detection, investigation, and advanced threat hunting activities within your Security Operations Center (SOC) to optimize ingest costs and platform performance.
- Enrich event data using Cribl Stream with device metadata sourced from CrowdStrike FDR to provide security teams with the entire security picture.
- Use the Replay function in Cribl Stream to move data from a security data lake back into your security analytics platforms to address longer-term investigative needs.

Export CrowdStrike Falcon data using Cribl Stream to address long-term retention requirements and improve threat hunting capabilities.

#### The Challenges

- Deep visibility into the endpoint is required to detect or prevent increasingly complex threats and to align to modern cybersecurity frameworks (CFS) like MITRE ATT&CK.
- This increased visibility results in a large increase in data velocity and processing requirements for enterprise security analytics (SIEM/SOAR) platforms.
- It becomes too expensive to satisfy the long-term retention requirements of this large dataset using enterprise security analytics platforms

### **The Solution**

CrowdStrike Falcon provides deep visibility and response capabilities at the endpoint and are now more relevant than ever considering the move from corporate networks to a remote workforce. CrowdStrike FDR provides access to Falcon data via an AWS S3 bucket within CrowdStrike Security Cloud which is exported by Cribl Stream. This increased visibility results in a large increase in data volumes and processing requirements when sending to enterprise security platforms such as a SIEM or SOAR. Cribl observability solutions give CrowdStrike customers new resources to maximize their security efforts, allowing teams greater speed and agility to transform and route critical data. The integration of Cribl Stream and CrowdStrike FDR data provides visibility into the below activities at the endpoint and more:

- · Behavioral alerts
- Information about processes (create, listen, termination, modification)
- Commands and scripts run
- Registry modifications
- Domain Name Service (DNS) activity
- Netflow
- File activity (create, modify, delete)
- Scheduled task or start-up modifications
- HTTP activity

While these security-relevant event types are among the most important sources to the security and compliance organizations, the verbosity of the events is usually too taxing for most analytics platforms such as a SIEM. Cribl Stream provides the solution for satisfying long-term investigative and compliance requirements while also optimizing the data sent to the analytics platforms as needed.

#### Integrating Cribl Stream with CrowdStrike FDR

It only takes a few minutes to configure Cribl Stream to retrieve data from CrowdStrike FDR. In summary, the steps you'll need to take are:

- 1. Configure Cribl Stream to pull data from the CrowdStrike FDR S3 bucket
- 2. Install the Cribl Pack for CrowdStrike FDR
- 3. Set up any data enrichment you want to perform
- 4. Configure your destinations

Let's get started.



1.Configure the CrowdStrike FDR Stream source tile to pull data from the Falcon Data Replicator AWS S3 bucket

Pull					
splunk Splunk Splunk Search	Amazon Kinesis	Amazon SQS	Amazon S3 2	Azure Event Hubs	Azure Blob Storage
Google Cloud Pub/Sub	Office 365 Services	Office 365 Activity	Office 365 Message Trace	Prometheus Scraper	Kafka
Confluent Cloud	CrowdStrike FDR				

Provide an Input ID, the name, URL, or ARN of the SQS queue to read notifications from, then select the region from the dropdown.

Sources > CrowdStrike FDR New Source			⊘ ×
General Settings	Input ID* ③	Enabled	@ Yes 🔵
Authentication	CrowdStrike_FDR		
Assume Role	nputla== crowastrike:crowastrike_FDR'		
Processing Settings	arn:aws:sqs:us-east-1:11111111111:Crowdstrike-2222222222-bucket		5
Event Breakers	OPTIONAL SETTINGS  Filename filter ⑦		
Fields	/ .*		/ 🕫 🗐
Pre-Processing	Region ⑦		
Advanced Settings	US East (Ohio)		$\sim$
Connected Destinations	Tags ⊘ Enter tags		
12			
🖉 Manage as JSON		Cancel	Save

Configure access to the bucket on the Authentication tab using AWS IAM policies or access/secret key pairs.

uthentication assume Role	Auto ⊘	Manual ⑦	Secret ⊘	
uthentication				
ssume Role				
In section of Cottings				
rocessing settings				
Event Breakers				
Fields				
Pre-Processing				
dvanced Settings				
onnected Destinations				

2. Download and install the Crowdstrike FDR Pack from the Cribl Pack Dispensary to quickly transform, reduce, drop, or enrich data that will be routed to a security analytics platform.

← → C	nbl.lo		Q () \$	0 0 0 7 0 * 0 0
╞ Cribl	Packs Dispensary	P, Search D(spensary		Tublish Rick SIGN IN
Filters				Sort: Last updated 🖂 4
Built by Cribi	SentinelOne Cloud Funnel	Cisco FTD >>	Cribl Pack for Infoblex	Crowdstrike FDR Pack
DATA TYPE     Events/Logs	Interfaces with the S3 sourced EDR data provided by SentineROne's Cloud Funnel service to transform, route, enrich, or drop events. This pack supports both version 1	Drop, Extract, Suppress based on certain ETD codes in lookup tables	Clean and parse infobiox logs	Transform, enrich, drop, and reduce event size of various Crowdstrike FDR events
Metrics Traces	and version 2 formatting of the Cloud Funnel data Jim Apger - Cribi Ver 2.0.1 2023-02-23	(on Rust - Crib) Ver 1.1.7 2023-02-21	jan Rust- crial Ver	Ahmed Kira - Cribi Vie 1.0.2 2023-02-02
Reduction	cc-greynoise-enrich cc-greynoise-enrich	Microsoft Windows Events	Redis Knowleo 🖈 🏓	NetflowLogic NetFow Optimizer cc-NetFlow_Logic
Filtering	Leverage Greynoise Intel via Redis to enrich events in Stream	Streamlining Windows Events - Support for XML Classic and NXLog event formats	Common use cases for Redis	Process logs from NetFlawLagic s NetFlaw Optimizer solution
	Blue Cycle LLC Ver 0.1.5. 2023-01-27	David Malslin - Cribl Ver 1.0.3 2023-01-19	Cribl - Ahmed Kira Ver 10.1 2023-01-19	Olga Fed., tFlow Logic Ver 1.0.2 2022-12-21
Cisco PaloAito	Ubiquiti Unifi Syslog	Cisco ASA >>	Syslog Pre-processing	Synology Events ct-symblogy events
Ande 🛃 🌖	Clean up and extracts for Ubiquit syslog data	Orop, Extract, Suppress based on certain ASA codes in lookup tables	Pre-process data received over Syslog, for volume reduction and enrichment. Timestamp normalization is implemented	Process, reduce, and transform Synology NAS logs.

**3.**Configure destination tiles for your analytics platforms and security data lake then route data to those destinations. The below example accomplishes the following

Filter events that were sourced from Crowdstrike FDR, route them through the Crowdstrike FDR pack, then send the optimized events to the SIEM.

Filter events that were sourced from Crowdstrike FDR, route them through the Crowdstrike FDR pack, then send the optimized events to the SOAR platform.

Route all events (filter=true) via the passthrough pipeline into the AWS S3 security Data Lake.

📚 Stream 😑	Home Manage Monitoring Settings		Q Search Stream	٥
Group defaultHy	brid 🔻 Overview Data 🔻 Routin	Processing  Group Settings		♦ 75c91c4 ∨ Co
Data Routes				
Search rou	tes			Add Route
≎ III All •	Route	Filter	Pipeline/Output	Events (In) 🕶
1	Send to SIEM	inputId=='crowdstrike:CrowdstrikeFDR'	PACK cribl_crowdstrike (Crowdstrike FDR Pack)	0.000%
2	Send to SOAR	inputId=='crowdstrike:CrowdstrikeFDR'	PACK cribl_crowdstrike (Crowdstrike FDR Pack)	0.000%
3	Send to security Data Lake	inputId=='crowdstrike:CrowdstrikeFDR'	passthru	0.000%
4	default	true	main	0.000%
$\rightarrow$	endRoute - Data reaching this point will be routed to	the Default Destination (devnul)		

#### 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

©2024 Cribl, Inc. All Rights Reserved. 'Cribl' and the Cribl Flow Mark are trademarks of Cribl, Inc. in the United States and/or other countries. All third-party trademarks are the property of their respective owners.

SB-00XX-EN-X-XX24