>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

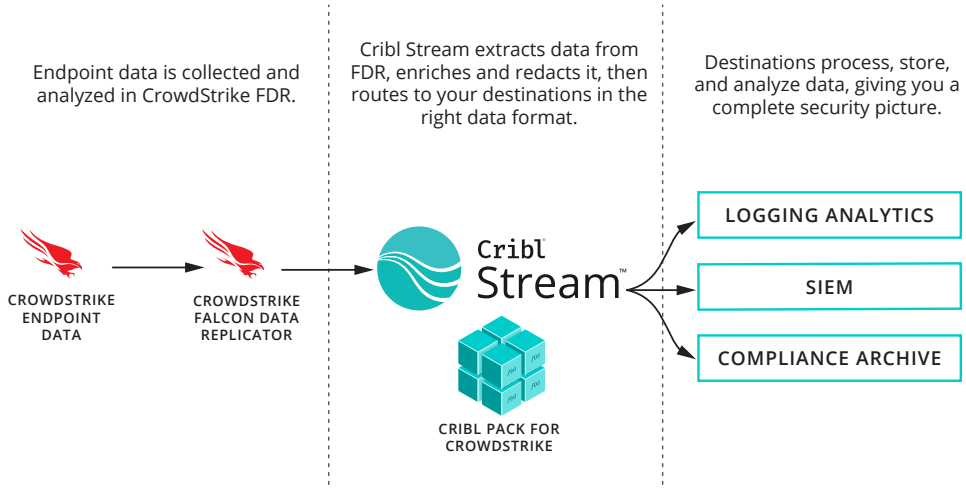
While these security-relevant event types are among the most important sources to the security and compliance organizations, the verbosity of the events is usually too taxing for most analytics platforms such as a SIEM. Cribl Stream provides the solution for satisfying long-term investigative and compliance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

Integrating Cribl Stream with CrowdStrike FDR

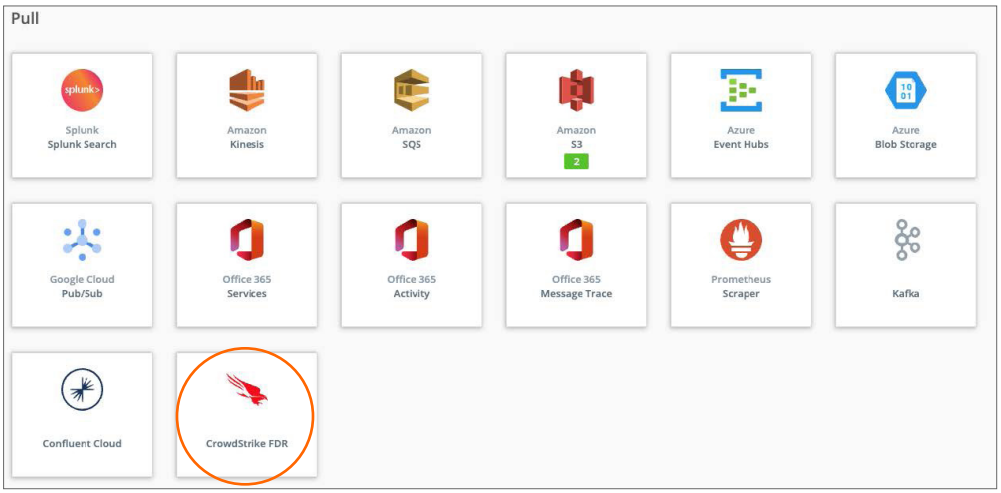
It only takes a few minutes to configure Cribl Stream to retrieve data from CrowdStrike FDR. In summary, the steps you'll need to take are:

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

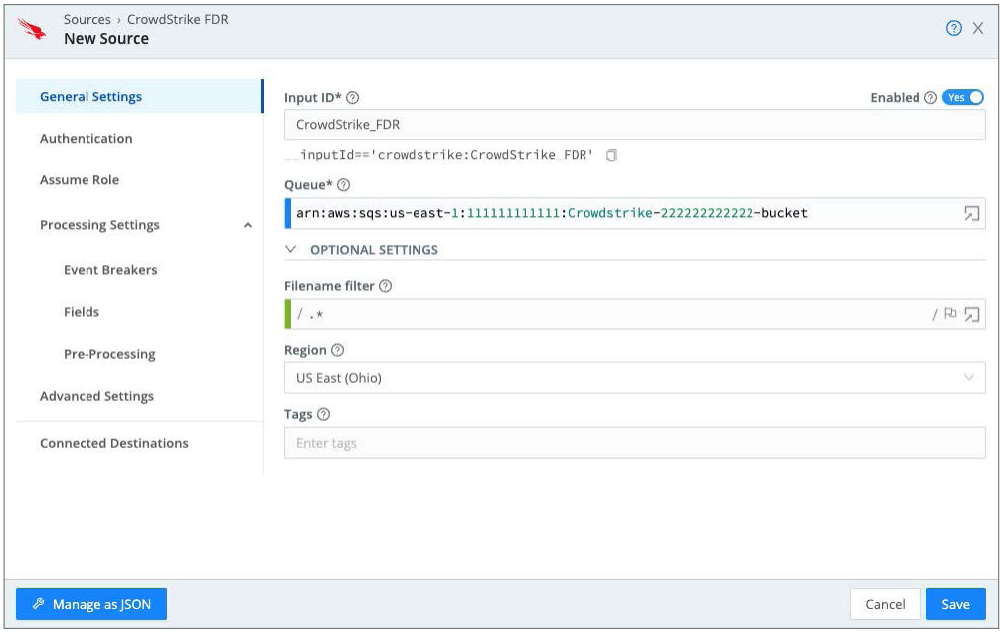
Let's get started.



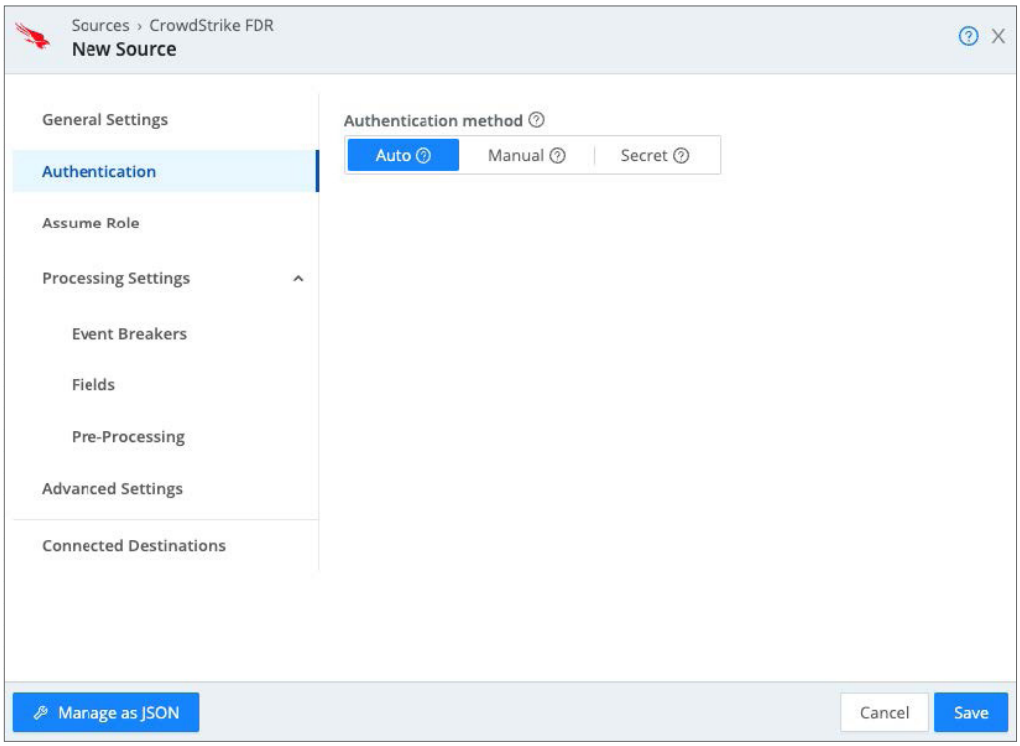
1. Configure the CrowdStrike FDR Stream source tile to pull data from the Falcon Data Replicator AWS S3 bucket



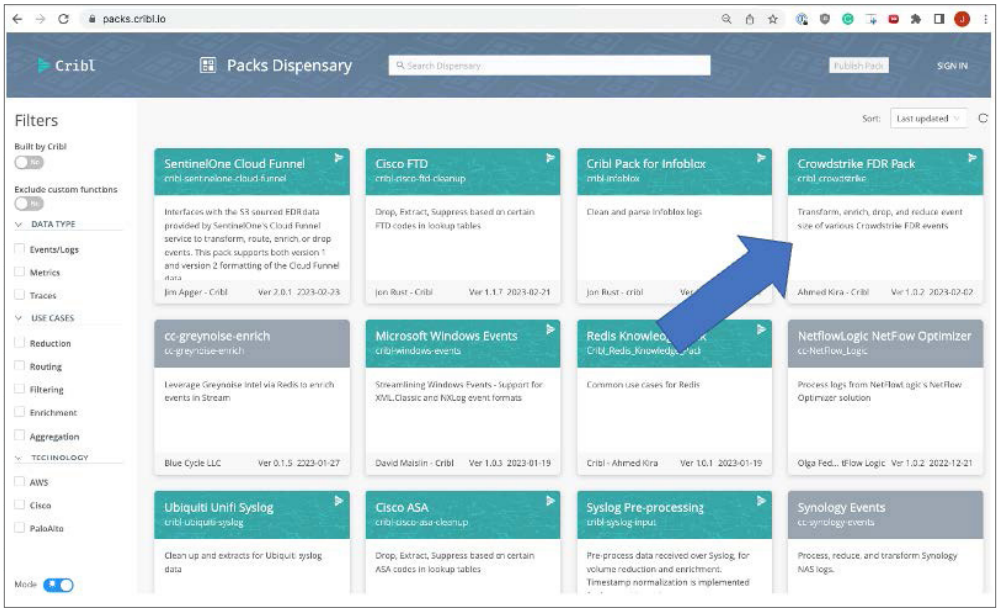
Provide an Input ID, the name, URL, or ARN of the SQS queue to read notifications from, then select the region from the dropdown.



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



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.

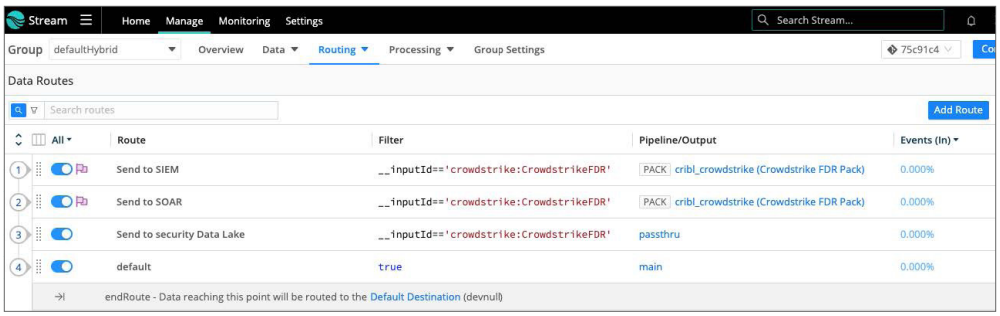


3. Configure destination tiles for your analytics platforms and security data lake then route data to those destinations. The below example accomplishes the following

   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.



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

SB-00XX-EN-X-XX24