Crowdstrike Integrations

Introduction

This integration is for CrowdStrike products. It includes the following datasets for receiving logs:

falcon dataset consists of endpoint data and Falcon platform audit data forwarded from Falcon SIEM Connector.

fdr dataset consists of logs forwarded using the Falcon Data Replicator.

Assumptions

The procedures described in Section 3 assume that a Log Collector has already been setup.

Compatibility

This integration supports CrowdStrike Falcon SIEM-Connector-v2.0.

Requirements

Logs

Falcon

Contains endpoint data and CrowdStrike Falcon platform audit data forwarded from Falcon SIEM Connector.

FDR

The CrowdStrike Falcon Data Replicator (FDR) allows CrowdStrike users to replicate FDR data from CrowdStrike managed S3 buckets. CrowdStrike writes notification events to a CrowdStrike managed SQS queue when new data is available in S3.

This integration can be used in two ways. It can consume SQS notifications directly from the CrowdStrike managed SQS queue or it can be used in conjunction with the FDR tool that replicates the data to a self-managed S3 bucket and the integration can read from there.

In both cases SQS messages are deleted after they are processed. This allows you to operate more than one Elastic Agent with this integration if needed and not have duplicate events, but it means

you cannot ingest the data a second time.

CrowdStrike Integration Procedures

Please provide the following information to CyTech:

Collect CrowdStrike Falcon Data Replicator logs (input: aws-s3) Option 1

1. AWS: Access Key ID
2. AWS: Secret Access Key
3. AWS: Queue URL - URL of the AWS SQS queue that messages will be received from.

Collect CrowdStrike logs via API. Option 2 (Recommended)

1. Client ID: Client ID for the CrowdStrike.
2. Client Secret: Client Secret for the CrowdStrike.
3. URL: Token URL of CrowdStrike.

Revision #2
Created 23 April 2024 11:36:44
Updated 19 June 2024 06:54:01