CrowdStrike Falcon SIEM Connector

Coralogix provides seamless integration with CrowdStrike Falcon, allowing you to correlate security-related events with your application and infrastructure logs and detect and respond to security incidents more effectively.

While this integration allows you to choose your preferred log shipper, we **strongly recommend** using OpenTelemetry as a best practice. Other available shippers can be found here.

> **NOTE**
>
> This integration has been replaced. Refer to our new integration document.

Configuration

The following is an example configuration.

STEP 1. Install the Crowdstrike Falcon SIEM connector.

STEP 2. Configure it to stream CrowdStrike events into a local file. By default the SIEM connector stores its data in /var/log/crowdstrike/falconhoseclient/. Change the default data storage location if necessary.

STEP 3. Download OpenTelemetry on the SIEM connector host. Get started here.

Example

Use the example below as a basis for shipping your logs, which adopt a multiline logs pattern.

Replace the `private_key` with your Coralogix Send-Your-Data API key and `domain` with your Coralogix domain.

```
receivers:
  filelog:
    start_at: beginning
    include:
      - /var/log/crowdstrike/falconhoseclient/output
    multiline:
      line_start_pattern: "^{"
    operators:
      - type: json_parser
```

```
        parse_to: body
exporters:
  coralogix:
    domain: "coralogix.com"
    private_key: "your Send-Your-Data API key"
    application_name: "open-test-app"
    subsystem_name: "CrowdStrike-Falcon"
    timeout: 30s
service:
  pipelines:
    logs:
      receivers: [ filelog ]
      exporters: [ coralogix ]
```

Support

Need help?

Our world-class customer success team is available 24/7 to walk you through your setup and answer any questions that may come up.

Feel free to reach out to us **via our in-app chat** or by sending us an email at support@coralogix.com.

Last updated: October 8, 2024

Was this helpful?

Leave your feedback here.

◯ **Yes** ◯ **No**

Send