Kandji

Kandji is a device management platform that helps businesses manage and secure Apple devices. It allows IT teams to automate tasks such as setting up devices, enforcing security settings, and keeping software up-to-date, making it easier to manage a large number of devices across a company.

Integrate Kandji into Coralogix via OpenTelemetry (OTel) Collector to send Threat-Details logs. These logs track and record security-related events, including potential threats and vulnerabilities, within an organization's Apple devices managed through Kandji.

Prerequisites

- Permission to create API token on a Kandji account.
- Access to Coralogix account.
- A virtual machine to run automated script and OTel.

Integration

1. Create a read-access API token on your Kandji account. API token should have read access.
2. Set up automated script to pull Kandji Threat-Details logs and save them to a file. Use the following cron expression for your cron job.

```
0 0 * * * rm /var/log/kandji.json; rm /var/log/log.json; rm
/var/log/kandji.log; curl --location -g
'https://{sub_domain}.api.kandji.io/api/v1/threat-details' --header
'Authorization: Bearer <api_token>' --header 'date_range: 1' >>
/var/log/kandji.json; jq '.results' /var/log/kandji.json >>
/var/log/log.json; cat /var/log/log.json | jq ".[]" >> /var/log/kandji.log
```

where:

- `{sub_domain}` is your Kandji sub-domain.
- `<api_token>` is the token generated in step 1.
- Set up OTel Collector to read logs from the `/var/log/kandji.log` file and send them to Coralogix.
- Replace the OTel configuration file with the following:

```
receivers:
```

```
  filelog:
    start_at: beginning
    include:
      - /var/log/kandji.log
    multiline:
      line_start_pattern: "^{"
    operators:
      - type: json_parser
        parse_to: body
exporters:
  coralogix:
    domain: "<coralogix_domain>"
    private_key: "your Send-Your-Data API key"
    application_name: "<your-app-name>"
    subsystem_name: "<your-subsystem-name>"
    timeout: 30s
service:
  pipelines:
    logs:
      receivers: [ filelog ]
      exporters: [ coralogix ]
```

where:

- `private_key` is your Coralogix Send-Your-Data API key.
- `domain` is your Coralogix domain.

Last updated: March 12, 2025

Was this helpful?

Leave your feedback here.

◯ **Yes** ◯ **No**

Send