CYLUS

Integration Manual

CylusOne and Google SecOps

Overview

This document describes the integration between CylusOne and Google Security Operations (formerly Chronicle). The integration provides bi-directional capabilities:

1. **Log Ingestion**: Forward security alerts, system health logs, and audit logs from CylusOne to Google SecOps using Syslog via Bindplane
2. **Response Integration**: Execute response actions in CylusOne directly from Google SecOps SOAR playbooks

CylusOne is a rail cybersecurity Platform that provides OT/IoT threat detection and monitoring for railway and critical infrastructure environments. This integration enables security teams to centralize CylusOne alerts within their Google SecOps SIEM and orchestrate automated responses through SOAR workflows.

Data Flow:

1. CylusOne generates security alerts, system health logs, and audit events
2. Logs are exported via Syslog (CEF format) to Bindplane agent
3. Bindplane normalizes and forwards logs to Google SecOps ingestion API
4. Google SecOps parses logs using the CylusOne parser (if available) or generic Syslog/CEF parser
5. Analysts can trigger response actions in CylusOne through SOAR playbooks

Prerequisites

CylusOne Requirements

- CylusOne Platform access with administrative privileges
- Network connectivity from CylusOne to Bindplane agent (port 514 TCP)
- CylusOne API key for response integration

Google SecOps Requirements

- Google SecOps instance (Standard or Enterprise)
- Bindplane access (included with Google SecOps)
- Ingestion API credentials (service account JSON key)
- SOAR module enabled (for response integration)

Network Requirements

- Outbound connectivity from Bindplane to Google SecOps ingestion endpoints:
  - `malachiteingestion-pa.googleapis.com` (gRPC)
  - `dataplane-pa.googleapis.com` (HTTPS DataPlane API)
- Firewall rules allowing Syslog traffic from CylusOne to Bindplane
- Outbound HTTPS (443) from Google SecOps to CylusOne API endpoint

---

Log Ingestion via Bindplane

Configure CylusOne Syslog Export

Step 1: Navigate to Integrations

1. Log in to the CylusOne Platform
2. Navigate to **Settings** (gear icon in left sidebar)
3. Click on **Integrations**

Step 2: Add Syslog Integration

1. In the Integrations page, click on the **Library** tab
2. Locate the **SYSLOG** integration card
3. Click **Add** to configure a new Syslog integration

Step 3: Configure Syslog Parameters

Configure the following fields in the "Add Integration - SYSLOG" dialog:

Parameter	**Description**
Address	IP address or hostname of the Bindplane agent
Port	Syslog port (default 514)
Message format	Log format (recommended: CEF)
Protocol	Transport protocol (recommended: TCP)
Integration Name	Descriptive name for this integration

Step 4: Select Content Types

Choose which log types to forward to Google SecOps:

- **Security Alerts** - Threat detections, anomalies, and security events
- **System Health Logs** - Platform health, connectivity, and performance metrics
- **Audit Logs** - User actions, configuration changes, and administrative events

Step 5: Configure Additional Fields (Optional)

Select additional metadata to include in Syslog messages:

- **Alert Description** - Detailed description of security alerts
- **Affected Assets** - Railway assets, devices, or networks involved in the event

Step 6: Save Configuration

1. Click **Confirm** to save the integration
2. The integration will appear in the "My Integrations" tab with an **Active** status
3. Note the assigned display name (e.g., "Syslog 1") and configured address

Configure Bindplane for Log Collection

Install Bindplane Agent

Before configuring Bindplane, you need to install the Bindplane agent on a Linux server that will receive Syslog data from CylusOne and forward it to Google SecOps.

Installation Command (Linux):

```shell
sudo sh -c "$(curl -fsSlL https://github.com/observIQ/bindplane-otel-collector/releases/latest/download/install_unix.sh)" install_unix.sh
```

> **Note**: The installation script automatically starts the `observiq-otel-collector` service on systems with systemd.

Service Management Commands:

```shell
# Start the service
sudo systemctl start observiq-otel-collector

# Restart the service (after configuration changes)
sudo systemctl restart observiq-otel-collector

# Stop the service
sudo systemctl stop observiq-otel-collector

# Check service status
sudo systemctl status observiq-otel-collector
```

Important File Locations:

File	Location
Configuration file	`/opt/observiq-otel-collector/config.yaml`
Log file	`/opt/observiq-otel-collector/log/collector.log`

View Bindplane Logs:

```shell
sudo tail -F /opt/observiq-otel-collector/log/collector.log
```

Verification:

After installation, verify the agent is running:

```shell
sudo systemctl status observiq-otel-collector
```

You should see an "active (running)" status.

Step 1: Configure Bindplane config.yaml

Edit the Bindplane configuration file at `/opt/observiq-otel-collector/config.yaml`:

Complete Configuration Example:

```
receivers:
  tcplog:
    listen_address: "0.0.0.0:514"
    # Optional: Enable TLS for encrypted syslog
    # tls:
    #   cert_file: "/path/to/server.crt"
    #   key_file: "/path/to/server.key"

exporters:
  chronicle/cylusone:
    compression: gzip
    # Path to your Google SecOps service account credentials file
    creds_file_path: '/opt/observiq-otel-collector/auth.json'
    # Replace with your Google SecOps customer ID
    customer_id: '<your-customer-id>'
    endpoint: malachiteingestion-pa.googleapis.com
    # The Log type for CylusOne logs is CEF (ARCSIGHT_CEF)
    log_type: 'ARCSIGHT_CEF'
```

```
    raw_log_field: body

service:
  pipelines:
    logs/cylusone:
      receivers:
        - tcplog
      exporters:
        - chronicle/cylusone
```

Configuration Notes:

- Replace `<your-customer-id>` with your actual Google SecOps customer ID
- Ensure the `creds_file_path` points to your service account JSON key file
- The receiver listens on port 514 for TCP syslog traffic
- For TLS encryption, uncomment the TLS section and provide certificate paths

Step 2: Deploy Configuration

1. Save the Bindplane configuration
2. Restart or reload the Bindplane agent to apply changes
3. Verify the agent status shows the pipeline as active

Verify Log Ingestion

Method 1: Test Integration from CylusOne

1. In CylusOne, navigate to **Settings > Integrations > My Integrations**
2. Locate your Syslog integration
3. Click **Test Integration**
4. CylusOne will send test logs to the configured Syslog endpoint

Method 2: Check Bindplane Metrics

1. In Bindplane, navigate to the monitoring/metrics dashboard
2. Verify the `syslog/cylusone` receiver shows incoming messages

3. Check the `chronicle/cylusone` exporter shows successful exports

Method 3: Query Google SecOps

1. Log in to Google SecOps
2. Navigate to **Search** or **Investigation**
3. Run a UDM query to verify CylusOne logs:

```
SQL
metadata.vendor_name = "Cylus"
```

4. Verify log fields are properly parsed and populated

Response Integration (SOAR)

The CylusOne response integration enables Google SecOps SOAR to execute actions within the CylusOne platform, such as updating alert statuses, retrieving asset information, or triggering incident response workflows.

Add CylusOne Integration to Google SecOps

Step 1: Access SOAR Integrations

1. Log in to Google SecOps
2. Navigate to **SOAR** > **Integrations** or **Settings** > **Integrations**
3. Search for **CylusOne** in the integrations catalog

> **Note**: The CylusOne integration is available in the Google SecOps content hub repository under third-party response integrations.

Step 2: Install Integration

1. Click **Install** or **Add Integration** on the CylusOne card
2. Review the integration description and required permissions
3. Confirm installation

Configure Authentication

Step 1: Obtain CylusOne API Credentials

1. Log in to CylusOne Platform
2. Navigate to **Settings > API Tokens** (or **Integrations > API Tokens**)
3. Click **Generate New Token** or **Create API Key**
4. Provide a descriptive name: `Google SecOps Integration`
5. Copy the generated API key (it will only be shown once)

Step 2: Configure Integration Parameters

In Google SecOps, configure the CylusOne integration with the following parameters:

Parameter	Type	Required	Description
Base URL	String	Yes	The base URL for your CylusOne instance
Cylus API Key	Password	Yes	API key for authenticating to CylusOne
Verify SSL	Boolean	Yes	Enable SSL certificate validation

Step 3: Test Connection

1. Click **Test** or **Validate** to verify connectivity
2. Google SecOps will attempt to authenticate and retrieve basic information
3. Confirm the test succeeds and shows a green status

Step 4: Save Configuration

1. Click **Save** or **Create** to store the integration configuration
2. The integration will now be available in SOAR playbooks

Available Actions

The CylusOne response integration provides the following actions for use in SOAR playbooks:

Action Name	Description
Enrich Asset Information	Retrieve details about railway assets or network devices from CylusOne
Ping	Test connectivity and authentication to the CylusOne Platform

> **Note**: Specific action parameters and response formats are defined in the integration files in the Google SecOps content hub repository.