CYBRAICS

nLighten™

Cylance Integration Guide

CYBRAICS

Introduction

Cybraics provides a log ingress for processing Cylance Protect + Optics Events. The customer needs to make the changes provided in this document in order to have nLighten process these events.

Requirements

Requirements are as follows:

- Cylance Portal access

The following is provided by Cybraics:

- IP/Domain of destination host
- Port of destination host

The following needs to be provided to Cybraics before enabling:

- Tenant ID – provided by Cylance

Configuration

From within the Cylance Portal,
navigate to **Settings** -> **Application** and select the **Syslog/SIEM** checkbox.

This brings up the options for configuring the destination host for your Cylance Events.

Configure :

- **Event Types** – select all that apply to your environment
- **SIEM** – “Splunk”
- **Protocol** – “TCP”
- **TLS/SSL** – select the checkbox
- **IP/Domain** – “nc01.nl.cybraics.com”
- **Port** – “10514”
- **Severity** – “Warning”
- **Facility** – “Internal”
- **Custom Token** – place your Tenant ID here

Click “**SAVE**”.

Your Cylance Portal is now configured to forward its events to your nLighten environment.

Sample Configuration