ESET Threat Intelligence Integrations

ESET Threat Intelligence provides advanced, real-time insights into global cybersecurity threats, empowering you to proactively defend your network and systems. By leveraging a vast database of threat data, it enables you to detect and respond to emerging threats, track attack trends, and enhance your security posture with actionable intelligence. With ESET Threat Intelligence, you can make informed decisions to protect your organization from sophisticated cyber threats.

Setup:

1) Log Collector must be installed.

2) Prepare the information from the ESET Threat Intelligence Account:

- Ensure that you have access to **ESET Threat Intelligence** feeds (via ESET Threat Intelligence API or downloadable data).
- Please prepare the **Username** and **Password** that you have received from ESET during their onboarding process.

References Information:

Data streams

This integration connects with the ESET Threat Intelligence **TAXII version 2 server**. It includes the following datasets for retrieving logs:

Dataset	TAXII2 Collection name
apt	apt stix 2.1
botnet	botnet stix 2.1
cc	botnet.cc stix 2.1

Dataset	TAXII2 Collection name
domains	domain stix 2.1
files	file stix 2.1
ip	ip stix 2.1
url	url stix 2.1

Obtaining an API Key for ESET Threat Intelligence

Usage of the ESET Threat Intelligence (ETI) API

The **ESET Threat Intelligence (ETI) API** can be used directly in a web browser's address bar as a REST API, meaning that it does not necessarily require implementation in a programming language. This allows for a straightforward integration of threat intelligence data without the need for additional software development.

Authentication

Authentication with the ETI API is managed via a **token**. This token can be generated in the profile section of the ESET Threat Intelligence portal. It is important to note that each token is valid for **only one hour**, ensuring secure access to the API.

To generate a token, users can either manually generate it through the portal interface or use a **CURL request**. This approach provides flexibility, allowing automated generation of tokens for integration or scheduled use.

> **"**
> ## Generate via CURL Request
>
> Step 1: Open a Command-Line Interface (CLI)
>
> - **Windows**: Open Command Prompt (cmd) or PowerShell.
> - **macOS/Linux**: Open Terminal.
>
> Step 2: Enter the CURL Command
>
> In the command-line interface, use the following CURL command to generate an authentication token:
>
> **curl -F name="YOUR-USERNAME" -F pass="YOUR-PASSWORD" ETI_URL/auth/**

> Step 3: Copy and save the authentication token

Note.
After 10 failed login attempts within 5 minutes, the user will be blocked for 15 minutes.
After 20 failed attempts from a specific IP address within 5 minutes, all login attempts from that IP will be blocked for 15 minutes.

If you need further assistance, kindly contact our support at support@cytechint.com for prompt assistance and guidance.