NG SIEM - Abusech Integration

This integration is designed to collect and process **AbuseCH threat intelligence logs**. It retrieves indicators from multiple AbuseCH APIs and makes them available for security monitoring and analysis.

Supported Datasets

The integration provides the following datasets:

- **URL Dataset**
  - Retrieves **URL-based indicators** from the AbuseCH API.
  - Data source: URLhaus API Documentation
- **Malware Dataset**
  - Retrieves **malware-based indicators** from the AbuseCH API.
- **MalwareBazaar Dataset**
  - Retrieves indicators from **MalwareBazaar**, a community-driven project hosted by AbuseCH.

URL Logs

The **AbuseCH URL data stream** fetches threat intelligence indicators from the following API endpoint:

```
https://urlhaus-api.abuse.ch/v1/urls/recent/
```

This stream provides details on recently observed malicious URLs that can be used for detection, correlation, and blocking in security systems.

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

Revision #3
Created 23 September 2025 08:15:08 by Richmond Abella
Updated 3 October 2025 12:38:07 by Richmond Abella