OpenCTI Feed Aggregation Connector

Introduction

This connector was created to address the limitations in using RSS Feeds and . It’s implemented as an external-import connector which triggers every 24hours

The plan

List of sites filtered

The Hacker News: <https://feeds.feedburner.com/TheHackersNews>   
Bleeping Computer: <https://www.bleepingcomputer.com/feed/>   
Other sites?

Brief Steps taken

1. Identify RSS Feed availability
2. Parse RSS Feeds to extract entries
3. Filter out the feeds we want using rules (e.g. category type, title does not contain…)
4. Convert entries into Stix2 format and send to opencti

Dockerisation Process

Docker build and add image into services into opencti docker-compose.yml