Introduction
The GOSINT, is an Open Source Threat Intelligence platform that helps us to identify and process the threat intelligence. GOSINT analyses structured and unstructured threat intelligence and helps a security analyst to identify different Indicators of Compromise (IOC) which can be driven into other tools like CRITs, MISP, or directly into log management systems or SIEM.

Once installed, the default installation path will be `/home/gosint/projects/src/GOSINT/`

Use the command `./gosint` inside this directory to start GOSINT server. Dashboard can be accessed by entering `localhost/` inside your web browser.

Generating API keys
Alien vault:
2. Login to the account.
3. Go to the API tab to obtain the API key.

Virus Total:
2. Login to the account.
3. Go to settings and go to API key tab to obtain the API key.
Twitter:
1. Go to apps.twitter.com and Login.
2. Click on Create a new app.
3. Fill all the necessary details and click on create.
4. Go to Keys and Access Tokens tab to obtain the API Keys.

Cisco Umbrella:
Similarly, Cisco Umbrella API can also be integrated to GOSINT. It is a paid service.

https://umbrella.cisco.com/
Configuration and Use

Settings

The GOSINT has a settings page that lets us to configure the different endpoints associated with the application. The API keys, consumer secret and other tokens generated from the third-party sources are to be provided here so as the GOSINT to access these services.

Indicator Feeds

Indicator Feeds allows us to add different feeds from the internet as input. Threat intelligence feeds are constantly updating streams of indicators or artifacts derived from a source outside the organization. By comparing threat feeds with internal telemetry you can automate the production of highly valuable operational intelligence. There is no limit to the number of indicator sources you can add.
Dashboard
The GOSINT dashboard allows us to view and modify all the stages that GOSINT requires human interaction. It is generally divided into Pre Processing, Post Processing and Transfer Station. It has other supportive functions like Ad Hoc Operations which allows you to analyze a single URL using the provided API such as Alienvault, VirusTotal, ThreatCrowd etc.

The Indicator Metrics allows you to visualize the Indicators that are currently loaded into GOSINT categorized as Indicators Sources or Indicators Type as shown in figure.
Pre-Processing Stage

All the feeds that are entered in indicator feeds are transferred into the preprocessing stage. An analyst can run these indicators through Cisco Umbrella, ThreatCrowd, VirusTotal, and other sources. The output from these sources can be used to reach a verdict whether the indicator is false positive or add more details. It also allows customizing the result so that the analyst can get a clearer context in determining the threat which can used in future for further clarification.
Ad-Hoc Operations

Ad-hoc operations allows us to insert a single URL rather than fetching a set of URL from feeds or API as input. It also allows us to perform analysis on specific IOCs using Threat Crowd, Virustotal etc.
Post Processing

After filtering and processing the scrapped results from Pre-Processing stage, the indicators are moved into the post processing stage. Here, we can observe and modify the content so as to fit the needs of the organization before it is transferred to the next stage.
Transfer Station

The results in post processing stage can be selectively or collectively exported as CSV files or directly be streamed into CRIT or MISP using the export feature.

A Sample exported csv file is given below:

<table>
<thead>
<tr>
<th>gold</th>
<th>date</th>
<th>indicator</th>
<th>type</th>
<th>source</th>
<th>context</th>
<th>tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>b7fle5594kvc0hfkg</td>
<td>2018-01-04T17:00:00+02:00</td>
<td><a href="https://i2.wp.com/malwarebreakdown.com">https://i2.wp.com/malwarebreakdown.com</a></td>
<td>url</td>
<td>malwarebreakdown.com/feed/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b7fle5594kvc0hfkg</td>
<td>2018-01-04T17:00:00+02:00</td>
<td>btmnkkvm.com</td>
<td>domain</td>
<td>malwarebreakdown.com/feed/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b7fle5594kvc0hfkg</td>
<td>2018-01-04T17:00:00+02:00</td>
<td>ptt.nvds.com</td>
<td>domain</td>
<td>malwarebreakdown.com/feed/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b7fle5594kvc0hfkg</td>
<td>2018-01-04T17:00:00+02:00</td>
<td>upwddodqnyqoxys.com</td>
<td>domain</td>
<td>malwarebreakdown.com/feed/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b7fle5594kvc0hfkg</td>
<td>2018-01-04T17:00:00+02:00</td>
<td>194.87.94.11</td>
<td>ip</td>
<td>malwarebreakdown.com/feed/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b7fle5594kvc0hfkg</td>
<td>2018-01-04T17:00:00+02:00</td>
<td>edokjm.com</td>
<td>domain</td>
<td>malwarebreakdown.com/feed/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b7fle5594kvc0hfkg</td>
<td>2018-01-04T17:00:00+02:00</td>
<td>193.38.117.100</td>
<td>ip</td>
<td>malwarebreakdown.com/feed/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b7fle5594kvc0hfkg</td>
<td>2018-01-04T17:00:00+02:00</td>
<td>anyalikyafelpcrdfs.com</td>
<td>domain</td>
<td>malwarebreakdown.com/feed/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b7fle5594kvc0hfkg</td>
<td>2018-01-04T17:00:00+02:00</td>
<td>f0jrmfscunauov.com</td>
<td>domain</td>
<td>malwarebreakdown.com/feed/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b7fle5594kvc0hfkg</td>
<td>2018-01-04T17:00:00+02:00</td>
<td>46.165.254.211</td>
<td>ip</td>
<td>malwarebreakdown.com/feed/</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A Sample CSV File containing Threat indicators such as domains, IPs and URLs is attached below. This file can be fed to SIEM tool an configured accordingly to protect against attacks and blacklist them.

If the type chosen is CRIT, the data will be exported to the CRITS Repository. Once Exported, data will be deleted from the GOSINT Database.
Recipe Managers

The Recipe manager acts as a filter to the sources and allows users to set up task automation inside GOSINT. It can be used with a predefined set of indicators specified by used to carry out a particular set of operations, such as to always scan a particular source from an example site using VirusTotal every time you can use Recipe Manager. The Recipe Manager is so powerful that we can define an entire Indicator to automatically push to the production.