# Introduction and Objective

The objective of this document is to provide an initial list of open-source Incident Data Management systems which we can customize with minimal development effort.

This is a high-level document, it does not go into details how each and every evaluated applications work. It takes a layman’s view of how approachable an application is to get the job done.

An objective list of benchmark is in the next section.

# Incident Management Apps Benchmarks

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Open-source apps / Benchmarks** | [**MANTIS**](#_MANTIS) | [**MISP**](#_MISP) | [**FIR**](#_FIR) | **[threat\_](#_threat_note)**  **[note](#_threat_note)** | [**SCOT**](#_SCOT) | [**CYPHON**](#_CYPHON) | **[SOLTRA](#_SOLTRA_EDGE)**  **[EDGE](#_SOLTRA_EDGE)** |
| Data Entry UI |  | ✓ | ✓ | ✓ | ✓ |  | ✓ |
| Data Entry UI STIX Compliant |  |  |  |  |  |  | ✓ 1.2 |
| Ease of Installation and Maintenance (dev, test, prod)  (KISS) | Installation  Failed  Not fix |  | ✓ | ✓ |  | Installation  Failed | ✓ |
| Usability   * Concepts alignment * Productivity |  |  | ✓ |  |  |  | ✓ |
| Customization with minimum Coding   * Categories * Attributes |  |  | ✓ |  |  |  |  |
| OOB Statistics |  |  | ✓ |  |  |  |  |
| STIX | 1.2 | 2.0 |  |  |  |  | ✓1.2 |
| Language | Python | Python | Python | Python | Perl | Python |  |
| Open-source | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | Commercial |
| **Total Ticks** | **1** | **2** | **6** | **3** | **2** | **1** | **5** |
| Issues Open | 4 | 860 | 32 | 43 |  |  |  |
| Issues Closed | 14 | 1328 | 143 | 64 |  |  |  |
| Commits | 74 | 6861 | 401 | 396 | 7380 |  |  |
| Last update | 4 years ago | 10 days ago | 10 months ago | 1 year ago | 21 days ago |  |  |

# MANTIS

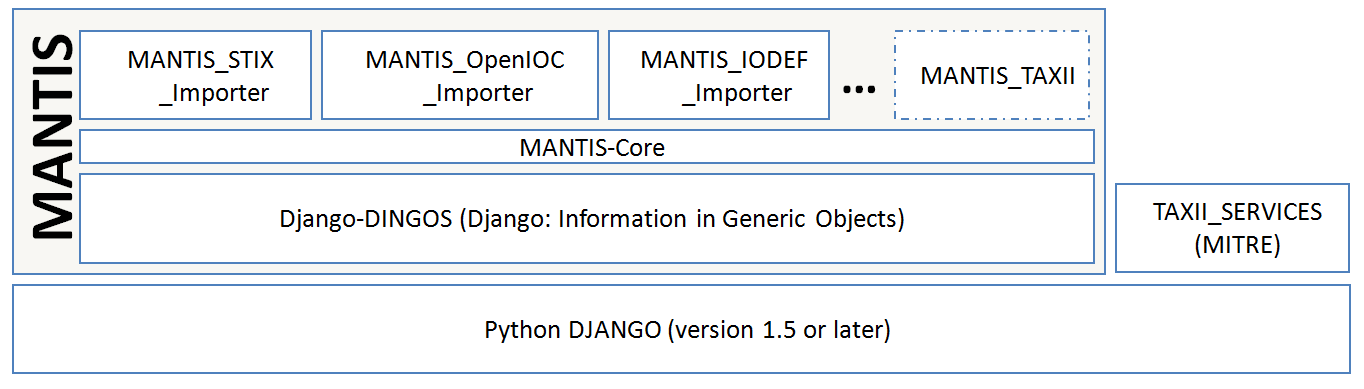
<http://django-mantis.readthedocs.io/en/latest/>

<https://github.com/siemens/django-mantis>

In a nutshell, no data input UI available. It is an import and visualization tool.

|  |
| --- |
| Installation Failed not fix - Error while installing libxml2-python #12  <https://github.com/siemens/django-mantis/issues/12>  <https://github.com/siemens/django-mantis/issues/22> |

## Architecture

[](http://django-mantis.readthedocs.io/en/latest/_images/mantis_architecture.PNG)

*MANTIS architecture*

## What MANTIS is and isn’t

isn’t a finished tool or even project: we like to think that it provides a solid basis on which cyber-threat intelligence management can be built up upon, but if you expect something that out of the box covers all aspects of cyber-threat intelligence management, MANTIS isn’t for you.

(currently) isn’t a tool fit for importing huge datasets. It can import fairly large XML documents such as the MITRE STIX conversion of the APT-1 report, but this takes a while (expect 20-30 minutes or so.) So do not expect to be able to throw, e.g., dozens and dozens of MAEC files with sizes of several 100MBs into the system: the generic importer is not fit for such sizes.

This situation may change at some point of time with more stream-lined importers, but MANTIS is really not intended to deal with very big data the way log management solutions such as Splunk et al. are.

## What MANTIS is:

MANTIS provides an example implementation of a framework for managing cyber threat intelligence expressed in standards such as STIX, CybOX, IODEF, etc. The aims of providing such an example implementation are:

To aide discussions about emerging standards such as STIX, CybOX et al. with respect to questions regarding tooling: how would a certain aspect be implemented, how do changes affect an implementation? Such discussions become much easier and have a better basis if they can be lead in the context of example tooling that is known to the community.

To lower the entrance barrier for organizations and teams (esp. CERT teams) in using emerging standards for cyber-threat intelligence management and exchange.

To provide a platform on the basis of which research and community-driven development in the area of cyber-threat intelligence management can occur.

Even though MANTIS is in no way a complete system, it already does cover a first use case: MANTIS provides an information repository into which cyber threat intelligence received in STIX/CybOX, OpenIOC and IODEF can be imported in a meaningful way that allows browsing, filtering and searching for information. Thus, MANTIS can be used as information base for keeping all the information you receive and information you generate yourself that is expressed in one of the currently supported standards. Because the importer is highly configurable, importers for other structured data should not be too difficult to write (and will hopefully be shared with the community ...).

# MISP

<https://github.com/MISP/MISP>

OOB not for the faint-hearted.

You need to “re-interpret” its concepts / fields for your own purpose.

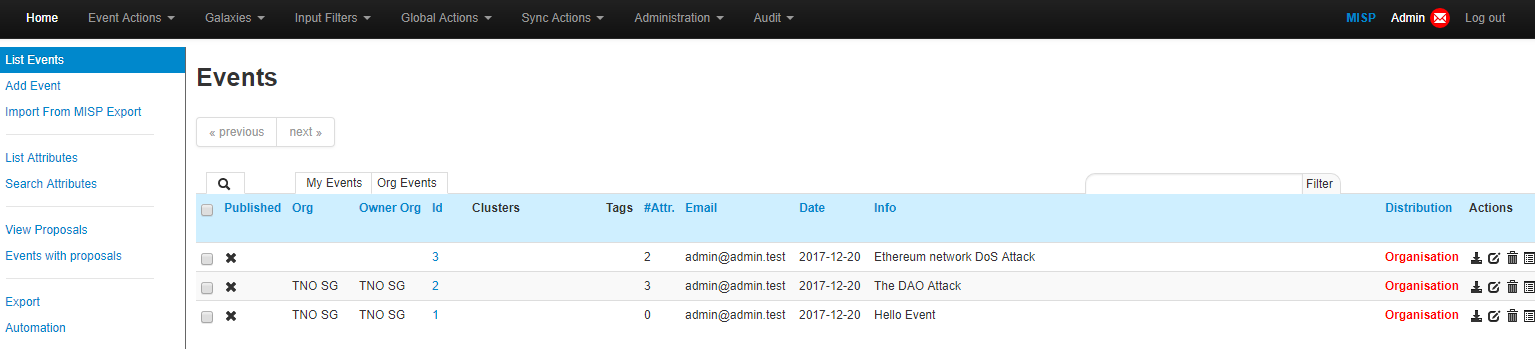
Customizability not for the faint-hearted, there is a learning curve for each components,

Need to write scripts/codes for customizing e.g. Categories, Attributes

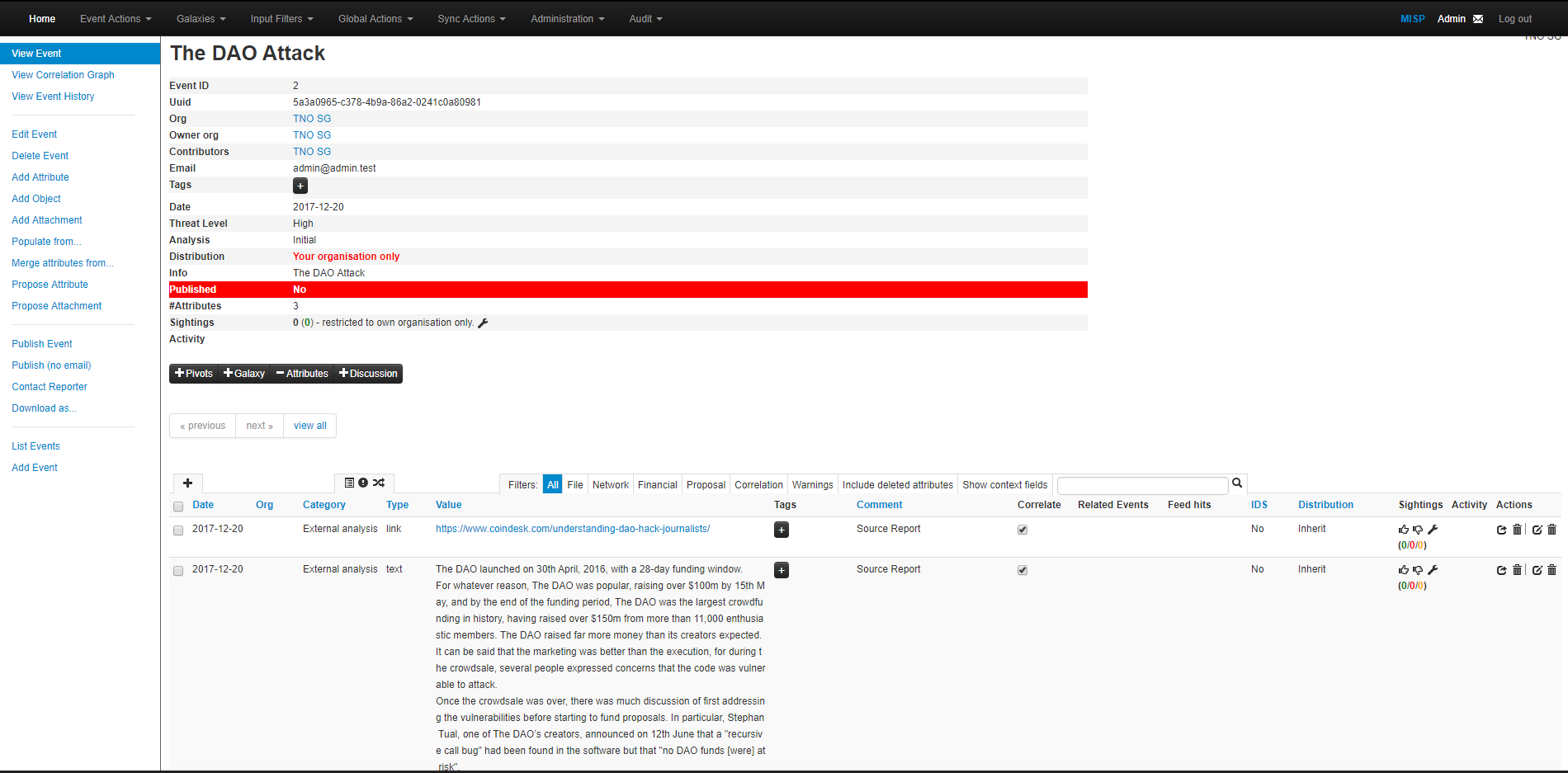
It is a full global enterprise multi-sites information sharing application.

|  |
| --- |
| VMware - MISP\_v2.4.84  http://192.168.9.129/  GUI Admin: [admin@admin.test](mailto:admin@admin.test) : admin (it's the site admin account with full rights, feel free to create other users)  Shell/SSH: misp / Password1234 |

## Events List (interpreting events as incidents)



## View Event Edit Example



# FIR

<https://github.com/certsocietegenerale/FIR/>

<https://github.com/certsocietegenerale/FIR/wiki/Architecture>

OOB - by far the most usable.

Unlike other frameworks, its setup instructions actually works!

OOB customization without going into codes is actually possible, see screenshots below.

|  |
| --- |
| VMware - Ubuntu 64-bit FIR  sebtno : sebtno  cd dev/FIR  ./startFIR.sh  open <http://localhost:8000/>  admin : admin  dev : dev |

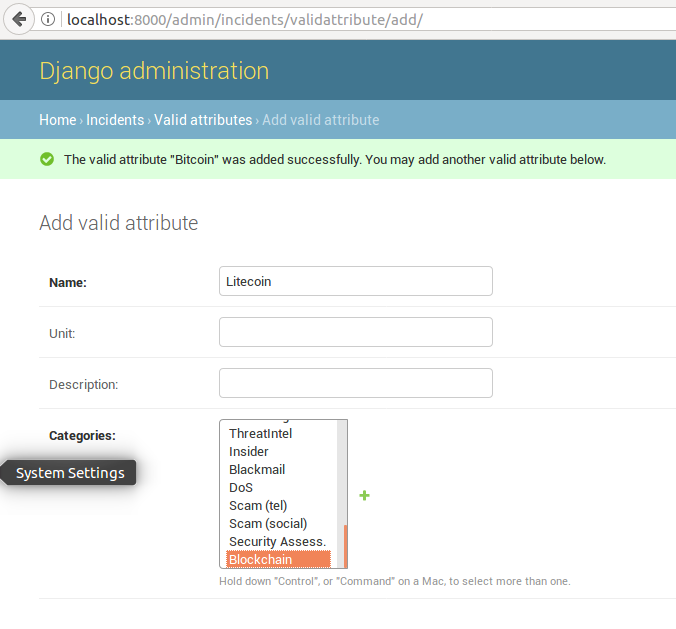
## Categories and Attributes

Login as admin, go to Admin panel

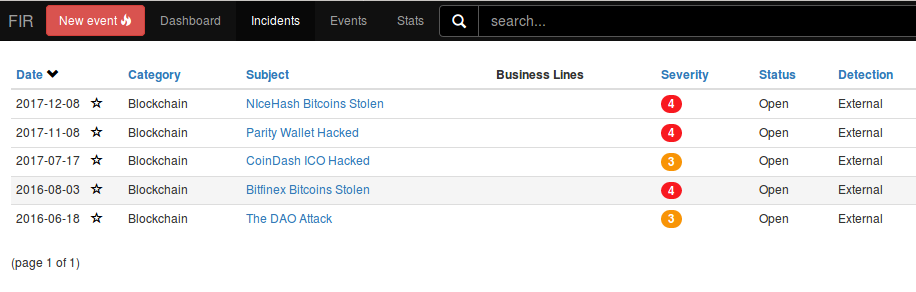


OR open

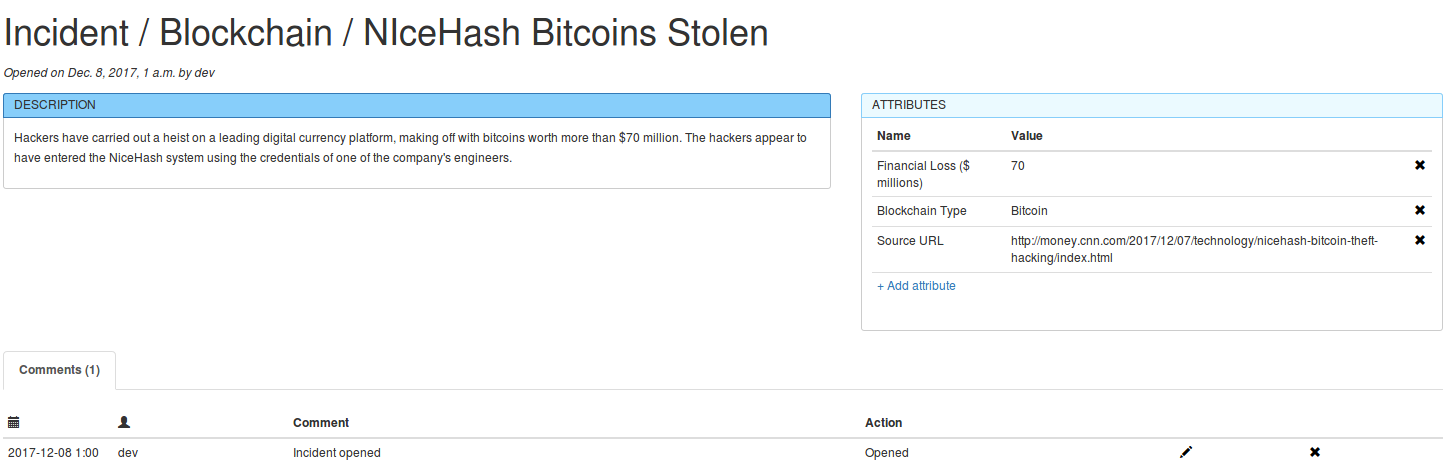
<http://localhost:8000/admin/login/?next=/admin/>



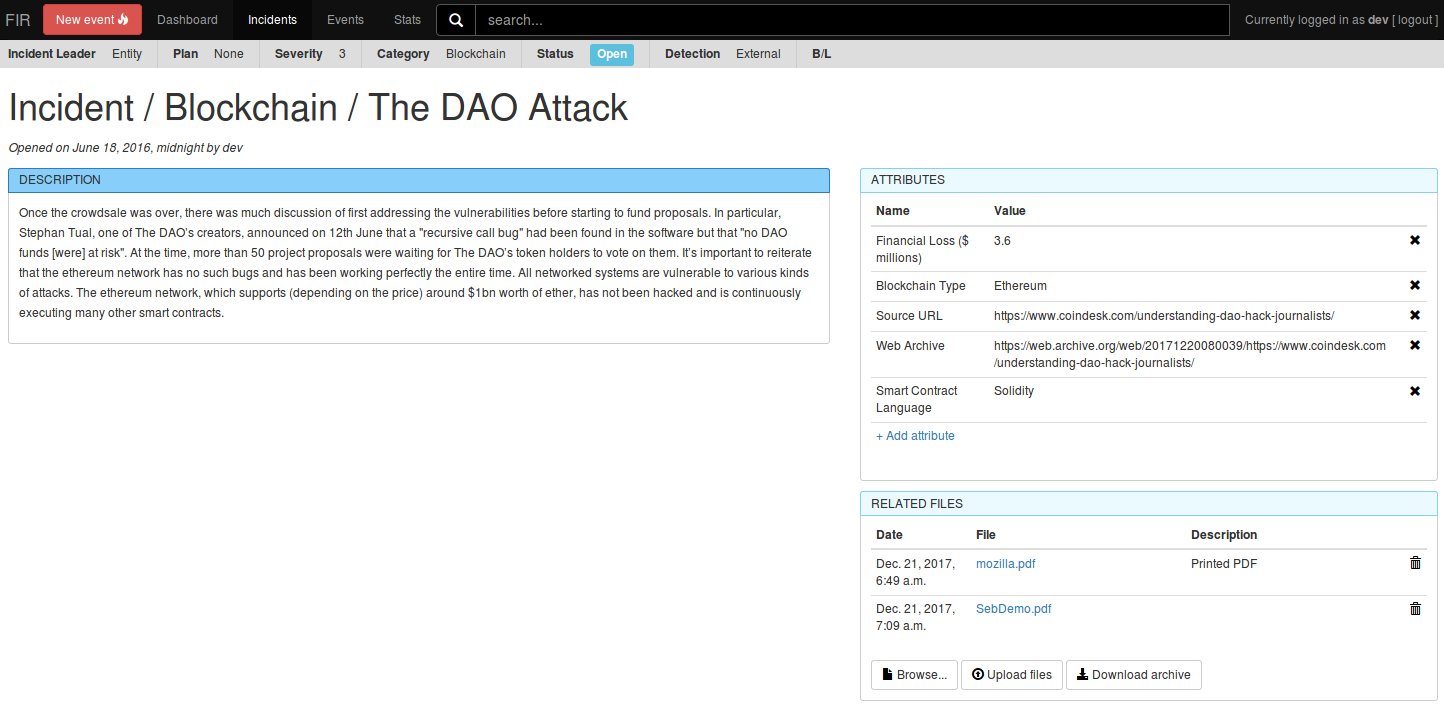
## Incidents List



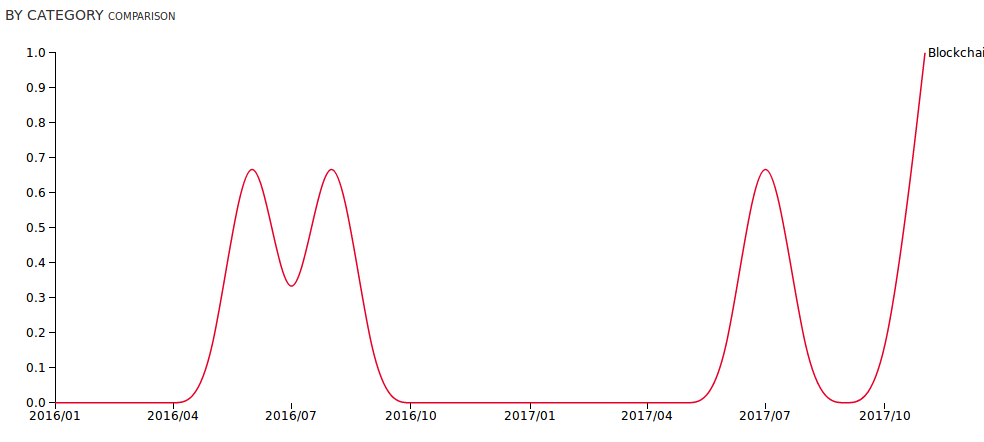
## Incident Edit Example 1



## Incident Edit Example 2



## Statistics Example 1



## Statistics Example 2



# threat\_note

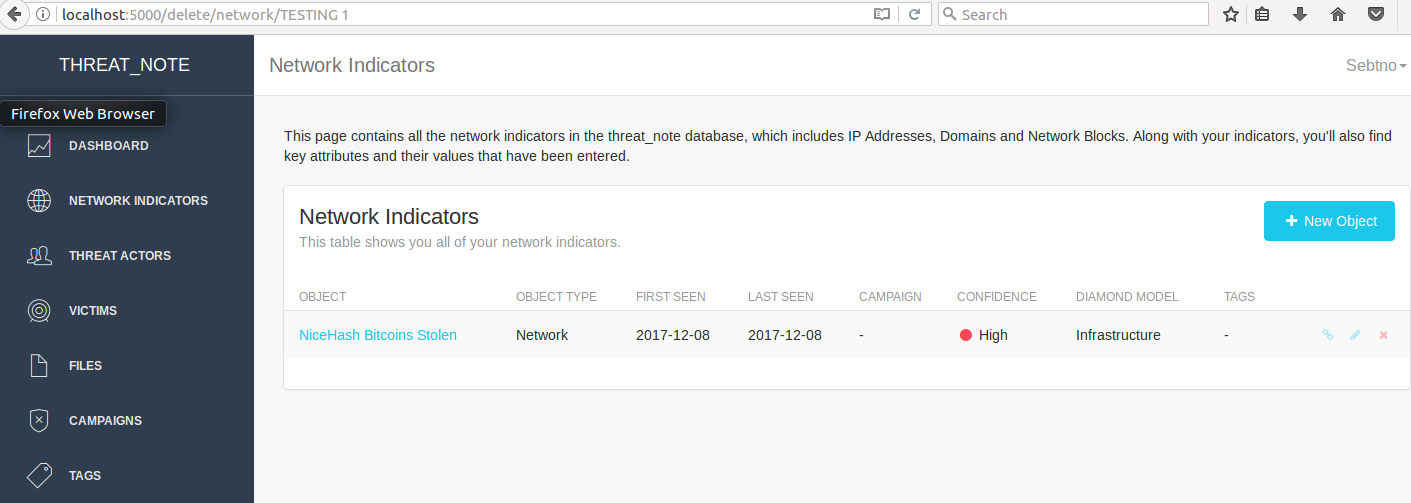
<https://github.com/defpoint/threat_note>

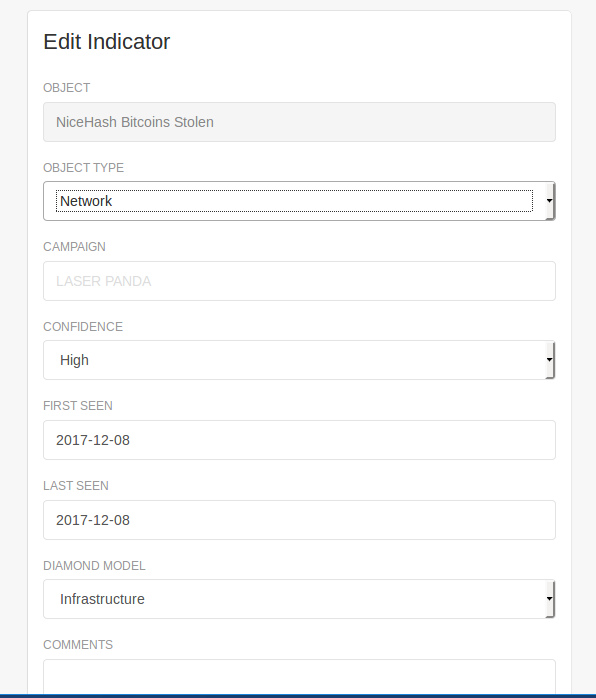
|  |
| --- |
| VMware- Ubuntu 64-bit threat\_note  login sebtno : sebtno  cd dev/threat\_note  check ifconfig for VM IP address  Run "honcho start"  - listing on port 5000  From host machine, ping <VM IP address>  From host machine web browser, open <VM IP address>:5000  From VM, just open http://localhost:5000/  user/password: sebtno/sebtno |

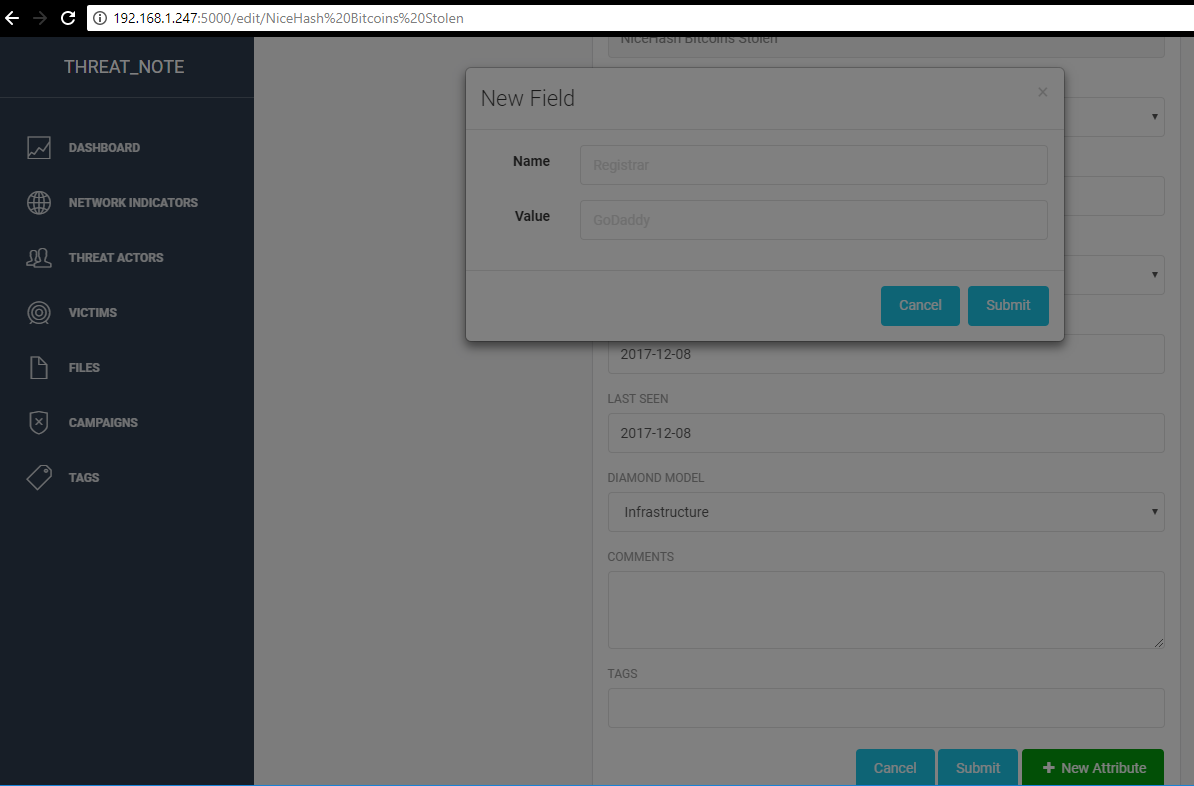
From edit Indicator, new attributes can be added to specific entry only.

Bug still open - when using New Attribute. <https://github.com/defpoint/threat_note/issues/152>

Basic framework for you to change source codes and database definitions.



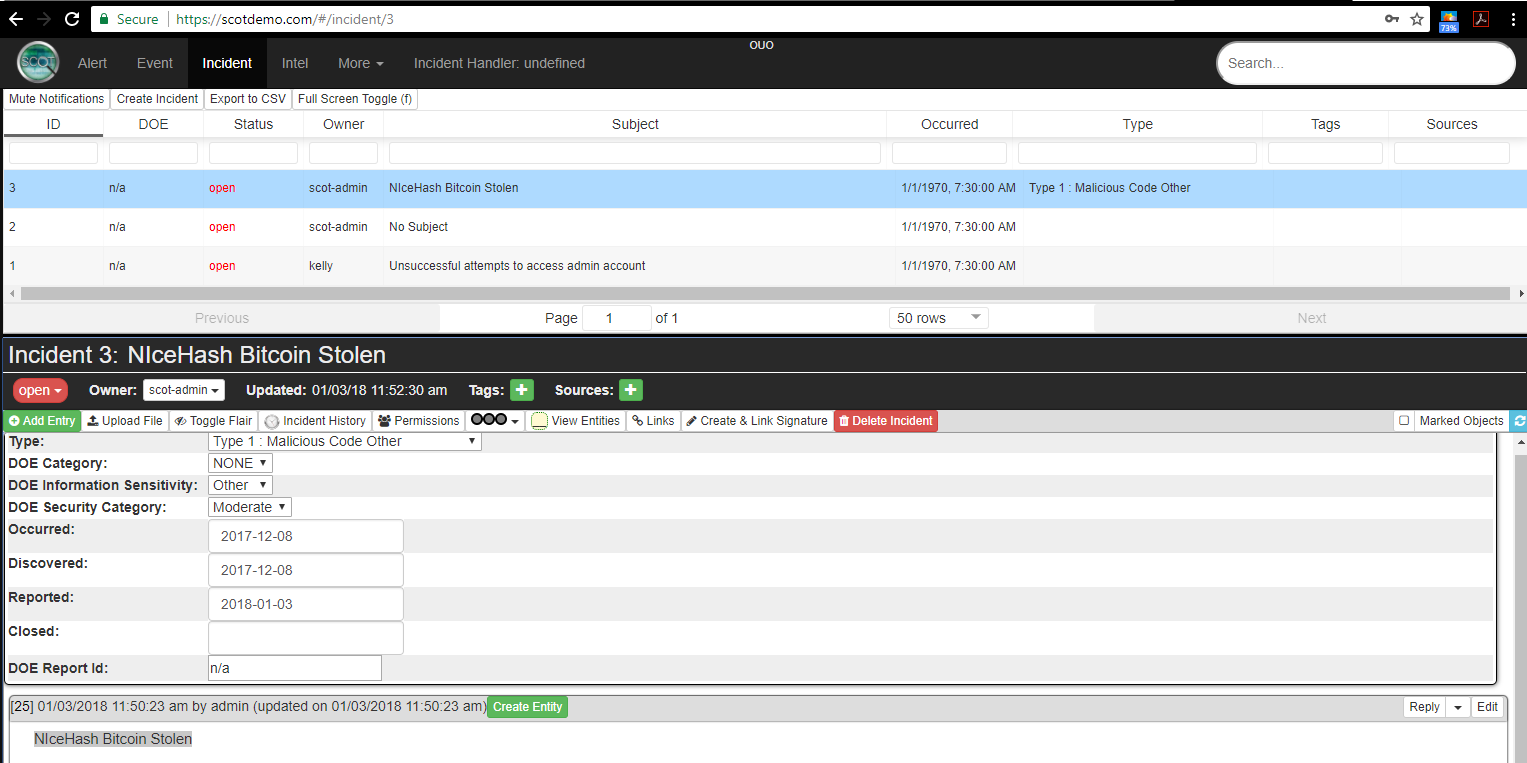




# SCOT

<https://github.com/sandialabs/scot>

Open [https://scotdemo.com](https://scotdemo.com/) with the **username**: admin/ **password**: admin



# CYPHON

<https://github.com/dunbarcyber/cyphon>

<http://cyphon.readthedocs.io/en/latest/getting-started/install-cyphon.html>

<https://www.cyphon.io/cyphon-vm/>

Installation failed

$ ifconfig eth0 <-- device not found !!! Wireless network adapter cannot work.

Changed the network adapter to Paravirtualized network adapter (virtio-net) in network settings.

<https://github.com/dunbarcyber/cyphon/issues/271>

# SOLTRA EDGE

<https://soltra.com/en/>

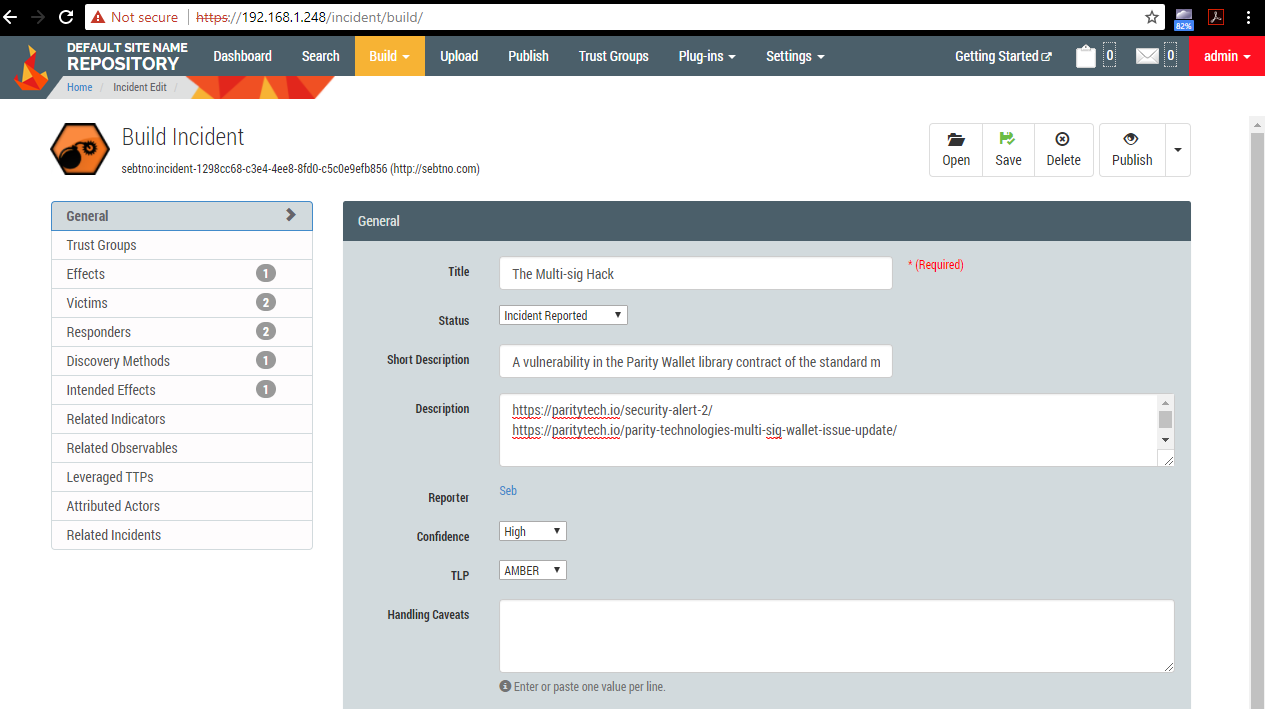
<https://soltra.com/en/documentation/ctx-soltra-edge/installation-and-vm-configuration/>

Commercial Software USD15,000 per year

STIX 1.2 Compliant Data Entry UIs

|  |
| --- |
| Virtual Box - RedHat Soltra Edge  Start the vm without connection to TNO domain network  Login:admin  password:sebtno  observe the IP displayed  https://<IP>/ |

## Create Incident

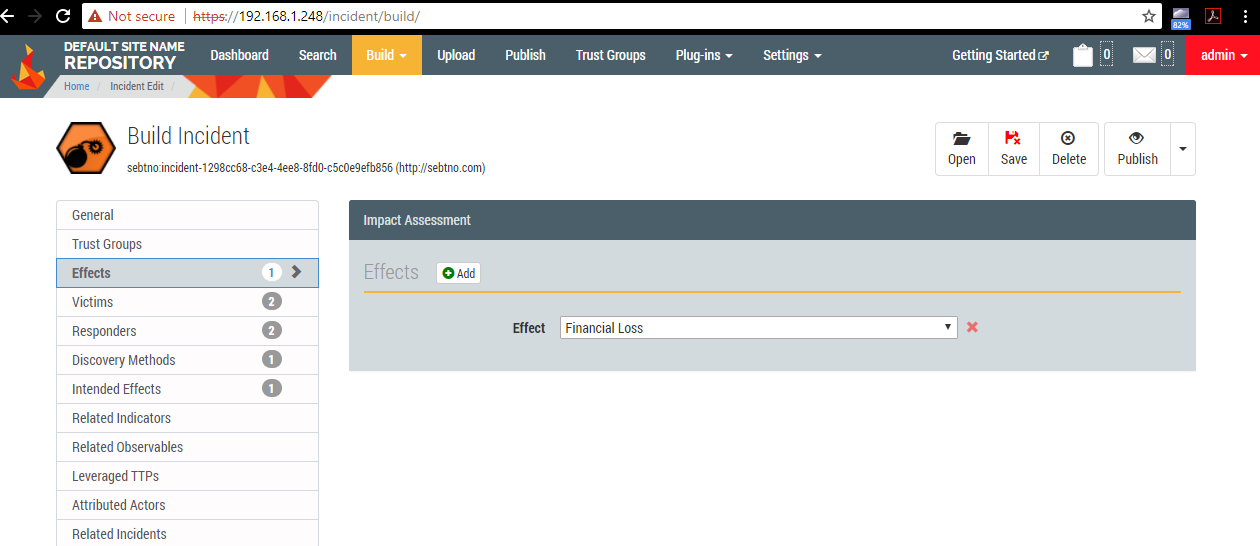


WARNING – missing customization

STIX has no custom field for related URL links, Web Archive Links. Adding them to Description.

STIX has no custom object to store uploaded files.

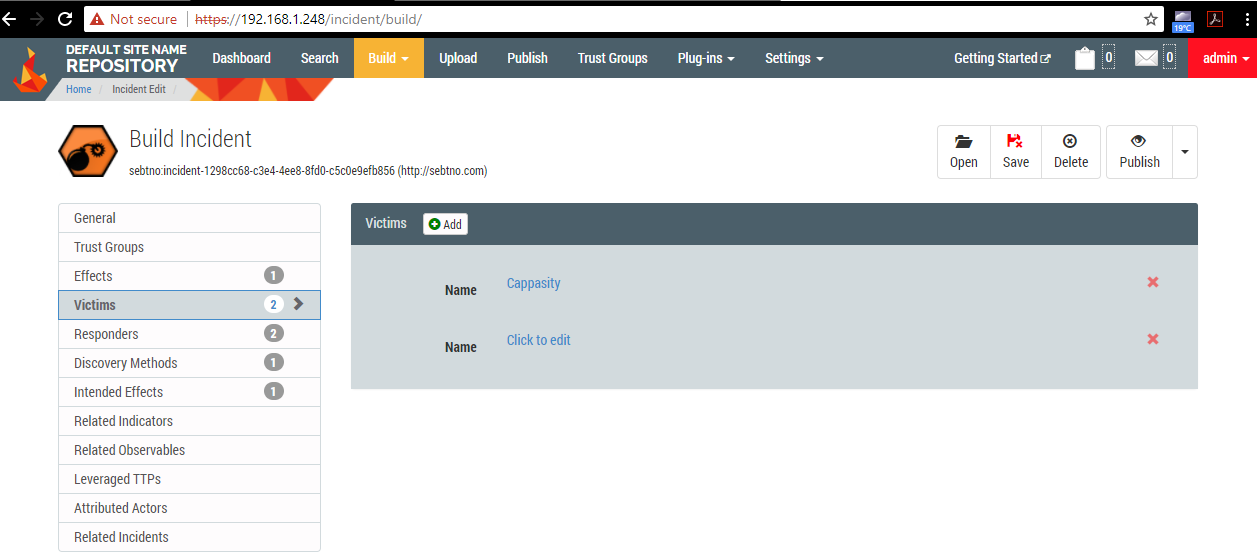
### Incident Effects



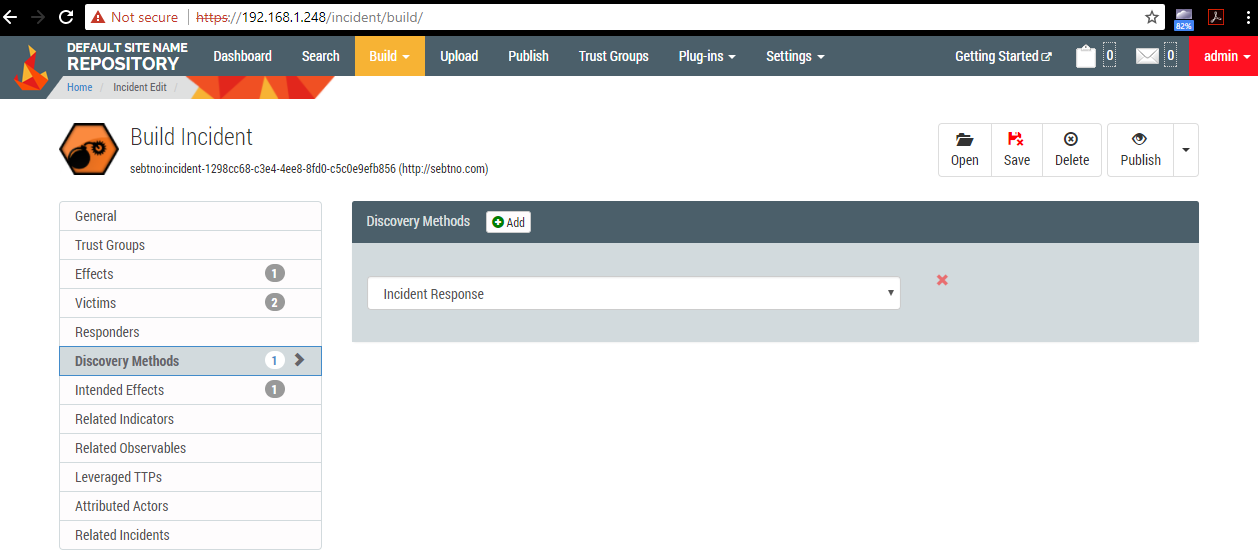
WARNING – missing customization

STIX has no custom field for Amount lost

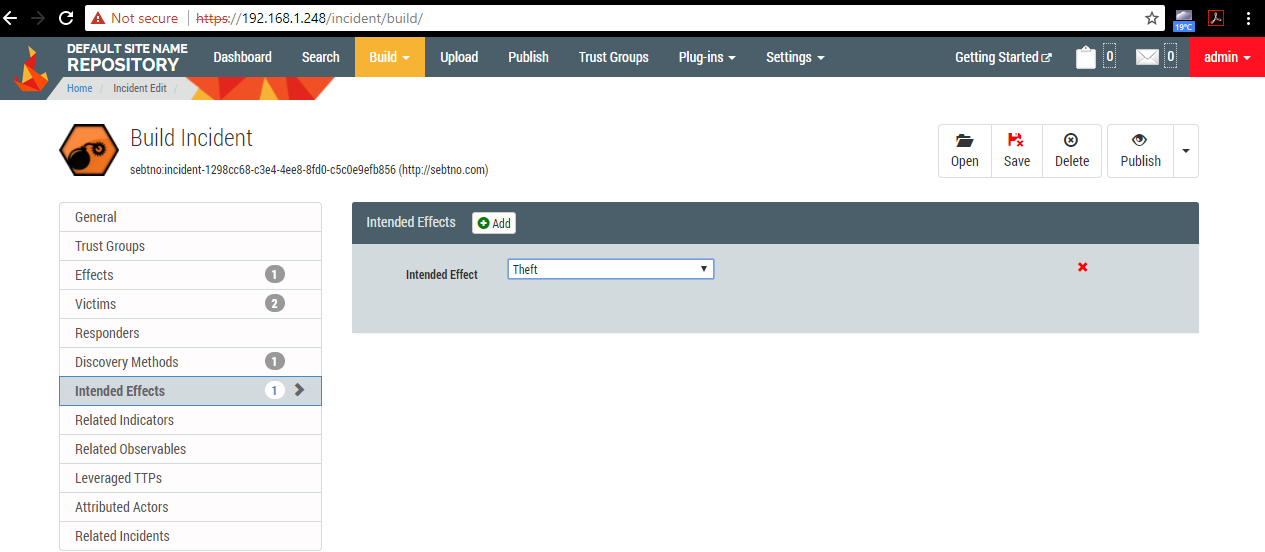
### Incident Victims



### Incident Discovery Methods



### Incident Intended Effects



## Create TTP

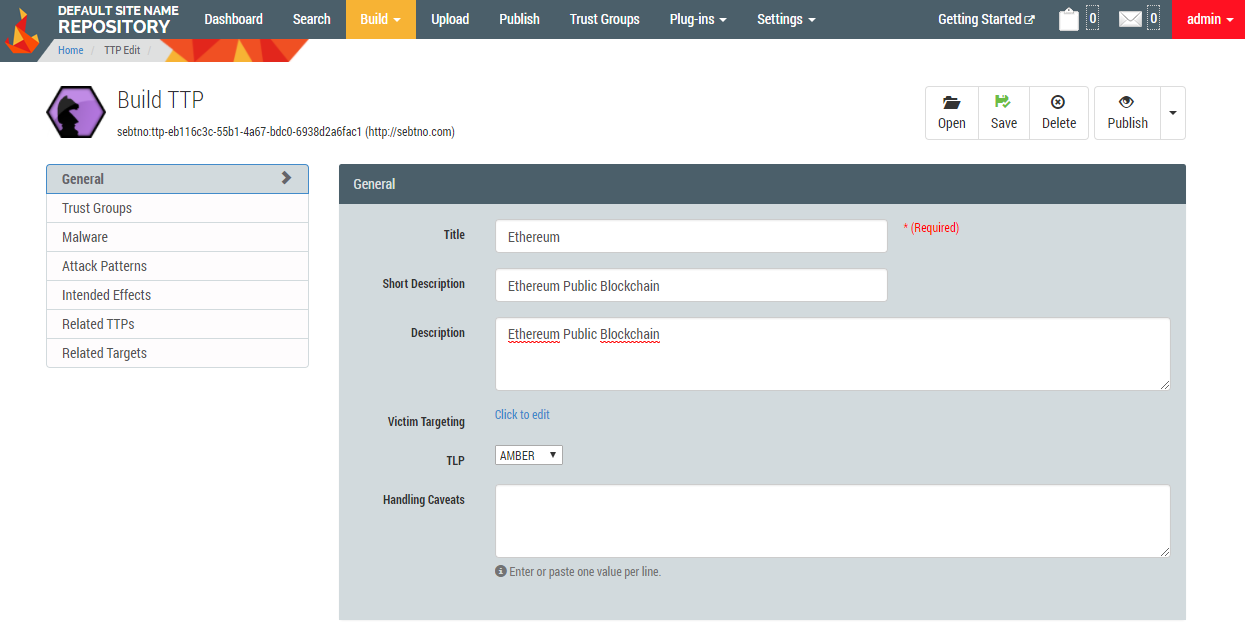
### Missing TTP Objects

WARNING - Missing TTP objects:

<http://stixproject.github.io/data-model/1.2/ttp/ResourceType/>

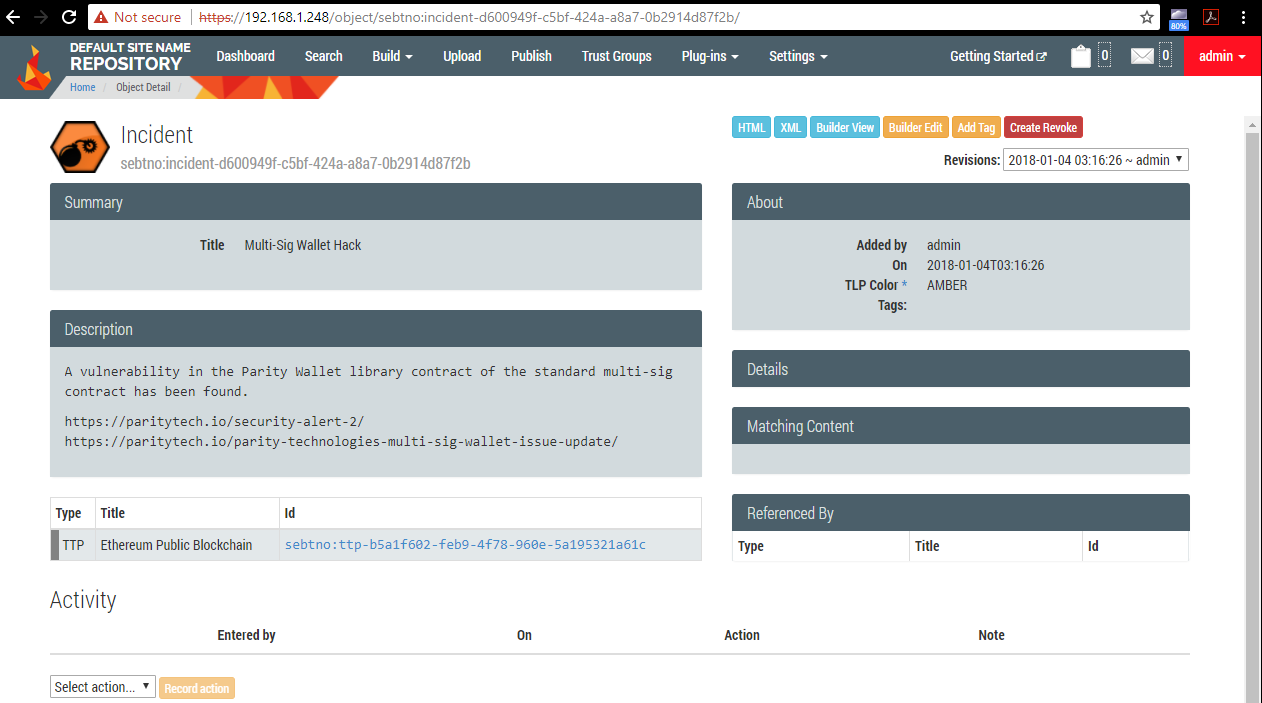
<http://stixproject.github.io/data-model/1.2/ttp/InfrastructureType/>

<http://stixproject.github.io/data-model/1.2/ttp/ToolsType/>



## Publish

After creating TPP and Incident, then Publish



### Exported STIX XML

