Start using Screener

Now, when the setup is done. It is time to start using the tool.
If it is not set up yet, please refer to these articles:
Install Screener in Linux
Setup Tutorial for VMware
Setup Tutorial for Virtualbox

Step 1: Domain and SSL certificate

As the first step it is highly recommended to setup Domain and SSL. However, it is not necessary. MSI plugin is able to work with no SSL over IPv4.
This step is a must to make O365 plugin operational, it can not operate via IP address.

Also, with the domain name configured you can create an MX record for the owned domain name to receive reports over SMTP protocol.

At this stage, if an MX record is configured, the Screener is already able to accept the reports. Simply forward a suspicious email as an attachment to the anyname@yourdomain.com.

Step 2: Configure the Plugin

Configure the plugin in Settings → Plugins.
it is necessary to define, which version is going to be used, O365 or MSI.

Step 3: Configure Automatic analyze rules

Configure or leave by default Yara Dictionaries.
Configure or leave by default Yara Rules.
Configure or leave by default Custom Rules.
Configure or leave by default Analyzer Score.

Step 4: Users

Configure additional users if necessary.
Each user has equal permissions, but it is possible to configure different timezones per user.

Step 5: Deploy the plugin

Download and deploy the O365 or MSI plugin.

Step 6: Report an incident

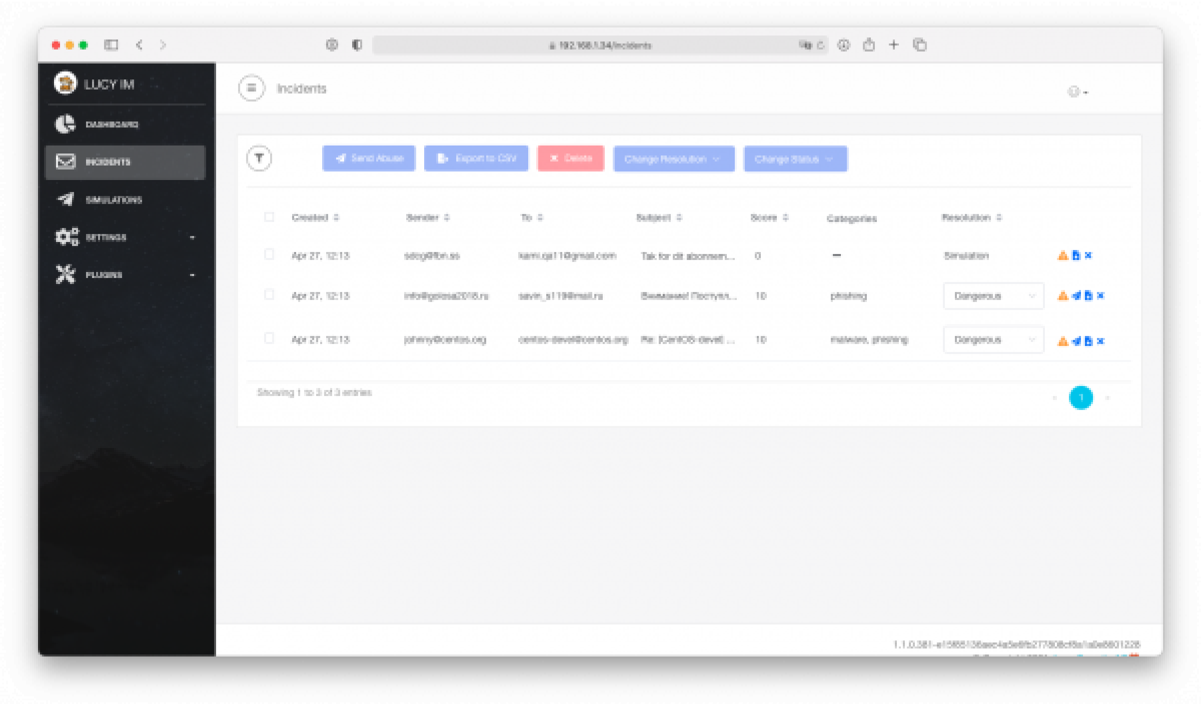
As soon as installed, a button should appear in the Outlook interface.
Simply select a suspicious email in the list and click the button.
The suspicious email is reported and now should appear in the Screener Incidents section.
Or, it can appear in the "Simulations" sections in case if a LUCY email message was reported.

The screener always listens to port 25, so in case if you are planning to report incidents over SMTP, it is enough to create an MX record of the screener domain.

For example:
There is a domain name screener.com pointing to the instance. Simply use randomemailaddress@screener.com and the Screener will accept the report.

Step 7: Review the incident

It is possible to review the incoming incidents.
The system will do an automatic analysis of an incident as soon as it is received.
The automatic scan will happen according to the Analyze rules. It will receive some spam score.
The amount of the spam score is unlimited, however, it'll be cut of to 10 since it is a maximum value for an incident.



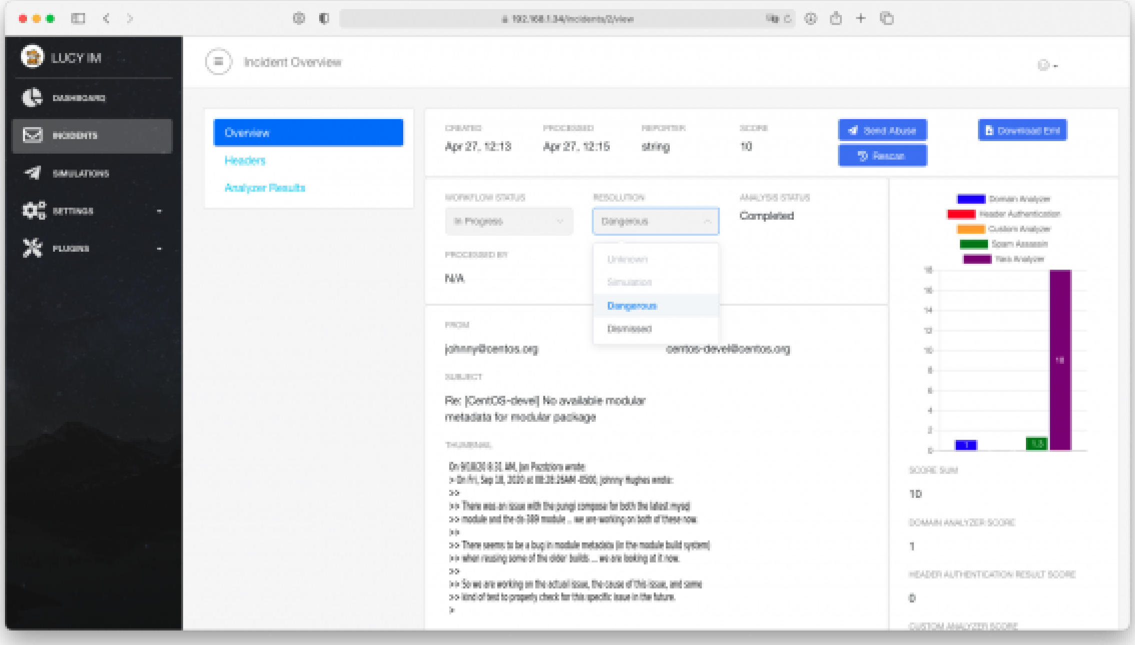
	Created	Sender	To	Subject	Score	Categories	Resolution
□	Apr 27, 12:13	sdog@fbn.ss	kami.ga11@gmail.com	Tak for dit abonnem...	0	–	Simulation
□	Apr 27, 12:13	info@golosa2018.ru	savin_s11@mail.ru	Внимание! Поступл...	10	phishing	Dangerous
□	Apr 27, 12:13	johnny@centos.org	centos-devel@centos.org	Re: [CentOS-devel] ...	10	malware, phishing	Dangerous

Showing 1 to 3 of 3 entries

Step 8: Define the threat

Change the workflow status from Open to In Progress.
Define what should be done with the incident.
Should a user send an abuse?

Should a user rescan the incidents?
As soon as the incident is reviewed by a user, it is possible to define the Resolution for the incident. It can be Dangerous or Dismissed. As soon as the Resolution is defined, the workflow status for the incident will be automatically set to "Closed".



CREATED Apr 27, 12:13

PROCESSED Apr 27, 12:15

REPORTER string

SCORE 10

WORKFLOW STATUS In Progress

RESOLUTION Dangerous

ANALYSIS STATUS Completed

PROCESSED BY N/A

FROM johnny@centos.org

centos-devel@centos.org

SUBJECT Re: [CentOS-devel] No available modular metadata for modular package

THUMBNAIL

```
On 9/18/20 8:31 AM, Jan Pazdziora wrote:
> On Fri, Sep 18, 2020 at 08:28:29AM -0500, Johnny Hughes wrote:
>>
>> There was an issue with the pungi compose for both the latest mysql
>> module and the ds-389 module .. we are working on both of these now.
>>
>> There seems to be a bug in module metadata (in the module build system)
>> when reusing some of the older builds ... we are looking at it now.
>>
>> So we are working on the actual issue, the cause of this issue, and some
>> kind of test to properly check for this specific issue in the future.
>
```

SCORE SUM 10

DOMAIN ANALYZER SCORE 1

HEADER AUTHENTICATION RESULT SCORE 0

CUSTOM ANALYZER SCORE

From:
https://wiki.lucysecurity.com/ - **LUCY**

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=start_using_screener

Last update: **2021/04/27 19:08**