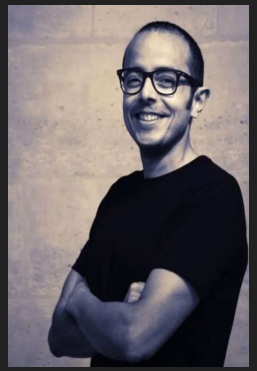
TheHive Project

GRAIL SECUTIRY SISTEMS S.L.

Fundadors TheHive Project

Nabil Adouani

Thomas Franco



Saad Kahi

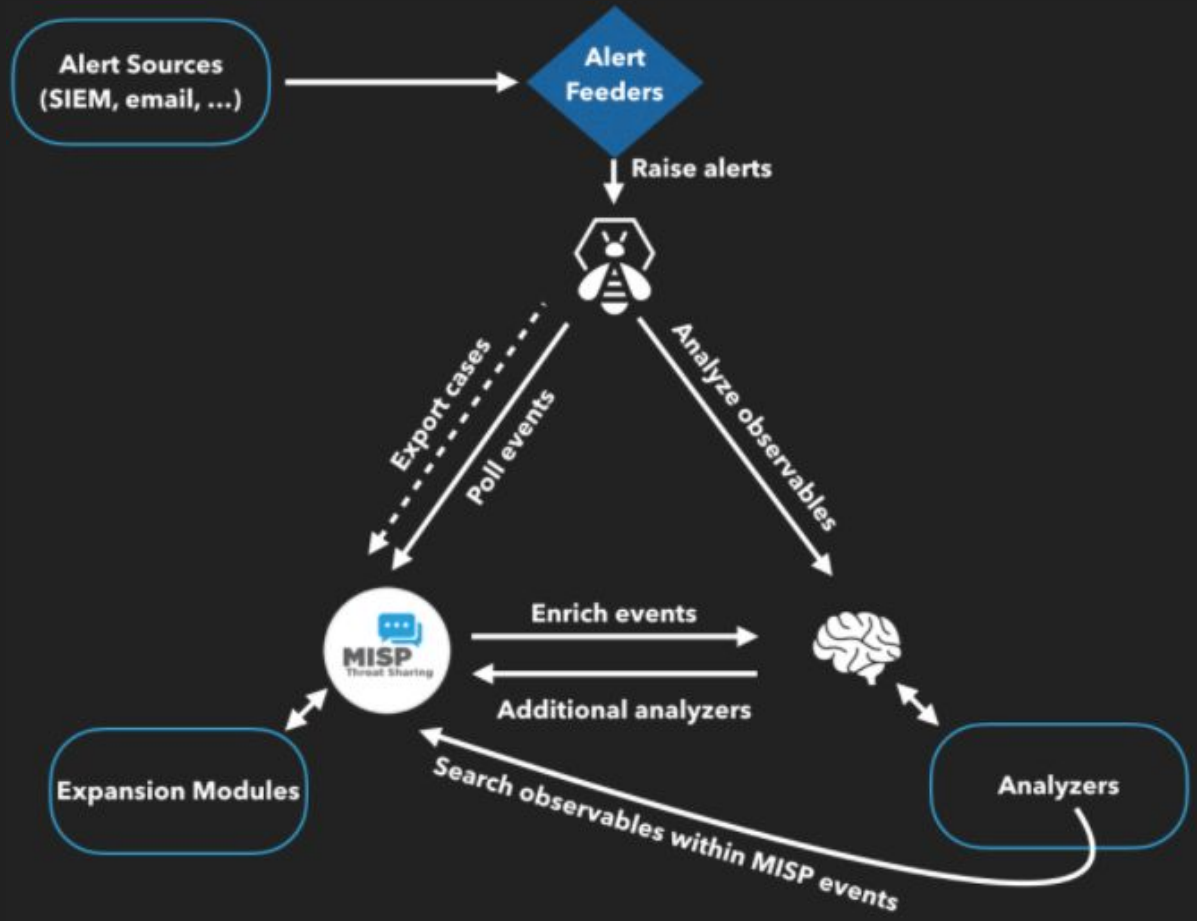
Jérome Leonard

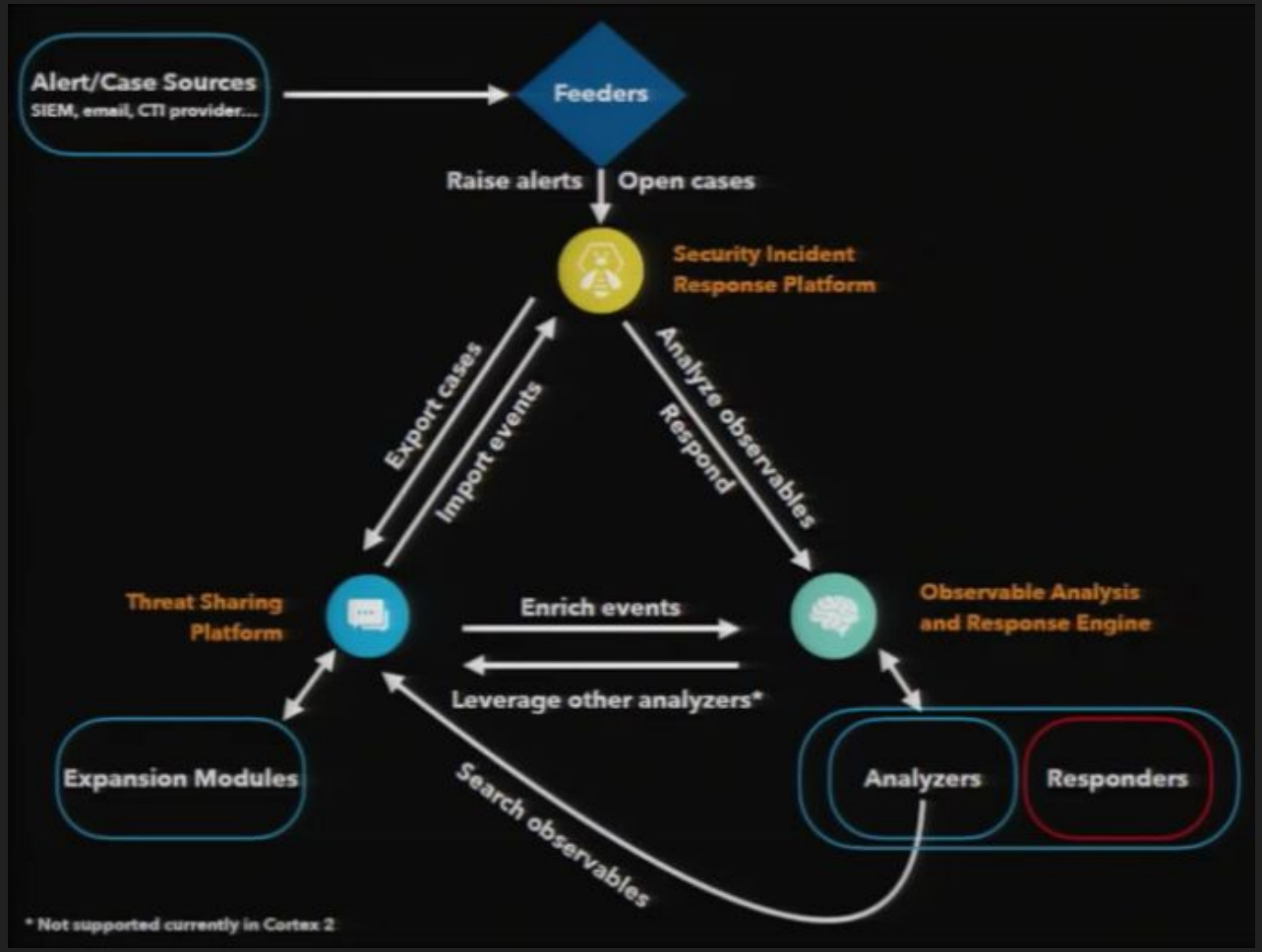
Danni Co

Nils Kuhnert

Què és i per a què serveix?

TheHive Project és una plataforma de resposta lliure d'incidents de seguretat de codi obert 3 en 1 escalable dissenyada per facilitar la vida a SOCs, CSIRTs, CERT i qualsevol professional de la seguretat de la informació que s'encarregui d'incidents de seguretat que hagin de ser investigats i actuats ràpidament. És l'empresa perfecta per MISP. Podeu sincronitzar-lo amb una o diverses instàncies MISP per iniciar investigacions sobre esdeveniments MISP. També podeu exportar els resultats d'una investigació com a esdeveniment MISP per ajudar els vostres companys a detectar i reaccionar als atacs que heu tractat. A més, quan TheHive s'utilitza conjuntament amb Cortex, els analistes i investigadors de seguretat poden analitzar fàcilment els dissenys, si no centenars, d'observables.


Alert Sources
(SIEM, email, ...)
Alert
Feeders
Raise alerts
Export cases
Poll events
Analyze observables
MISP
Threat Sharing
Enrich events
Additional analyzers
Expansion Modules
Analyzers
Search observables within MISP events


Alert/Case Sources
SIEM, email, CTI provider...
Feeders
Raise alerts
Open cases
Security Incident Response Platform
Export cases
Import events
Analyze observables
Respond
Threat Sharing Platform
Enrich events
Leverage other analyzers*
Observable Analysis and Response Engine
Expansion Modules
Search observables
Analyzers
Responders
* Not supported currently in Cortex 2

TH4

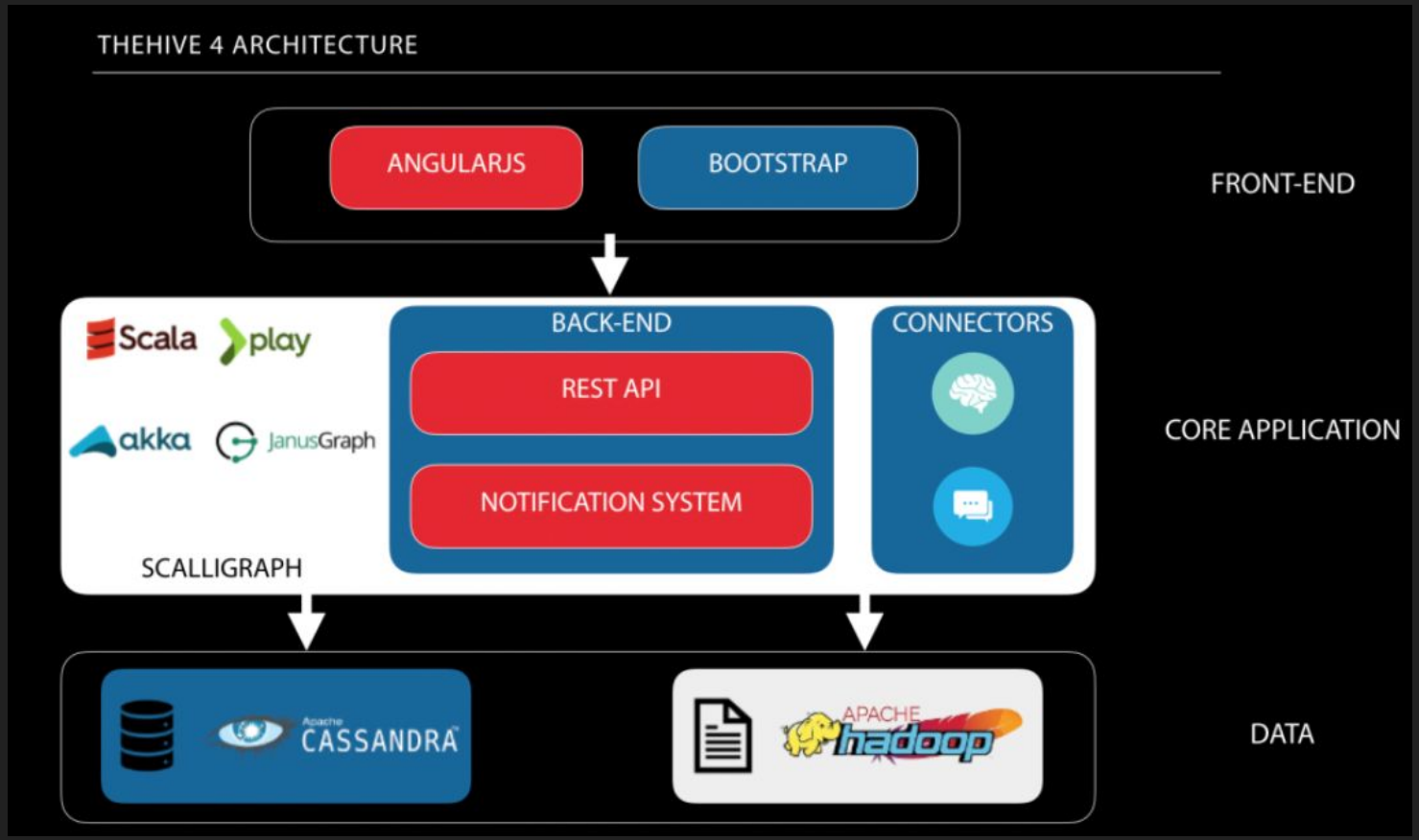
TheHive4 estructura la informació en gràfics i l'emmagatzema en una base de dades d'Apache Cassandra. Tots els fitxers que adjunteu als registres de tasques o que afegiu com a observables s'emmagatzemen en un sistema de fitxers distribuït de Hadoop (HDFS).

Característiques TH4

Apache Cassandra és un sistema d'administració de bases de dades distribuïdes de codi obert dissenyat per manipular grans quantitats de dades en diversos servidors, oferint una alta disponibilitat sense un únic punt de fallada. Ofereix un suport robust per a 'clusters' que abasteixen diversos centres de dades.

Apache Hadoop és un entorn de programari emprat per a l'emmagatzemament i processat distribuït de dades usant el model de programació MapReduce. Consisteix en clústers d'ordinadors construïts mitjançant maquinari estàndard.

TheHive4


THEHIVE 4 ARCHITECTURE
ANGULARJS
BOOTSTRAP
FRONT-END
Scala
play
akka
JanusGraph
SCALLIGRAPH
BACK-END
REST API
NOTIFICATION SYSTEM
CONNECTORS
CORE APPLICATION
Apache CASSANDRA
APACHE hadoop
DATA

Característiques TH3

Arquitectura

Està escrit a Scala i utilitza Elasticsearch. La seva API REST és apàtrida, cosa que li permet escalar horitzontalment. La utilitat frontal és AngularJS amb Bootstrap.

Bases de dades

TheHive utilitza el motor de cerca Elasticsearch per emmagatzemar totes les dades com a documents persistents. Elasticsearch no forma part del paquet TheHive. S'ha d'instal·lar i configurar com una instància autònoma que es pugui localitzar a la mateixa màquina.

TheHive utilitza el port http d'Elasticsearch (per defecte, 9200 / tcp).

Es requereixen tres paràmetres per connectar-se a Elasticsearch:

- nom base de l'índex
- nom del clúster
- adreça i els ports de la instància d'Elasticsearch

Akka és un conjunt d'eines i un temps d'execució gratuït i de codi obert per crear aplicacions altament concurrents, distribuïdes i tolerants a fallades.

Scala és un llenguatge de programació BSD (programari lliure) modern multi-paradigma dissenyat per a expressar patrons de programació generals d'una manera concisa, elegant i segura respecte als tipus.

Play Framework és un marc d'aplicacions web de codi obert.

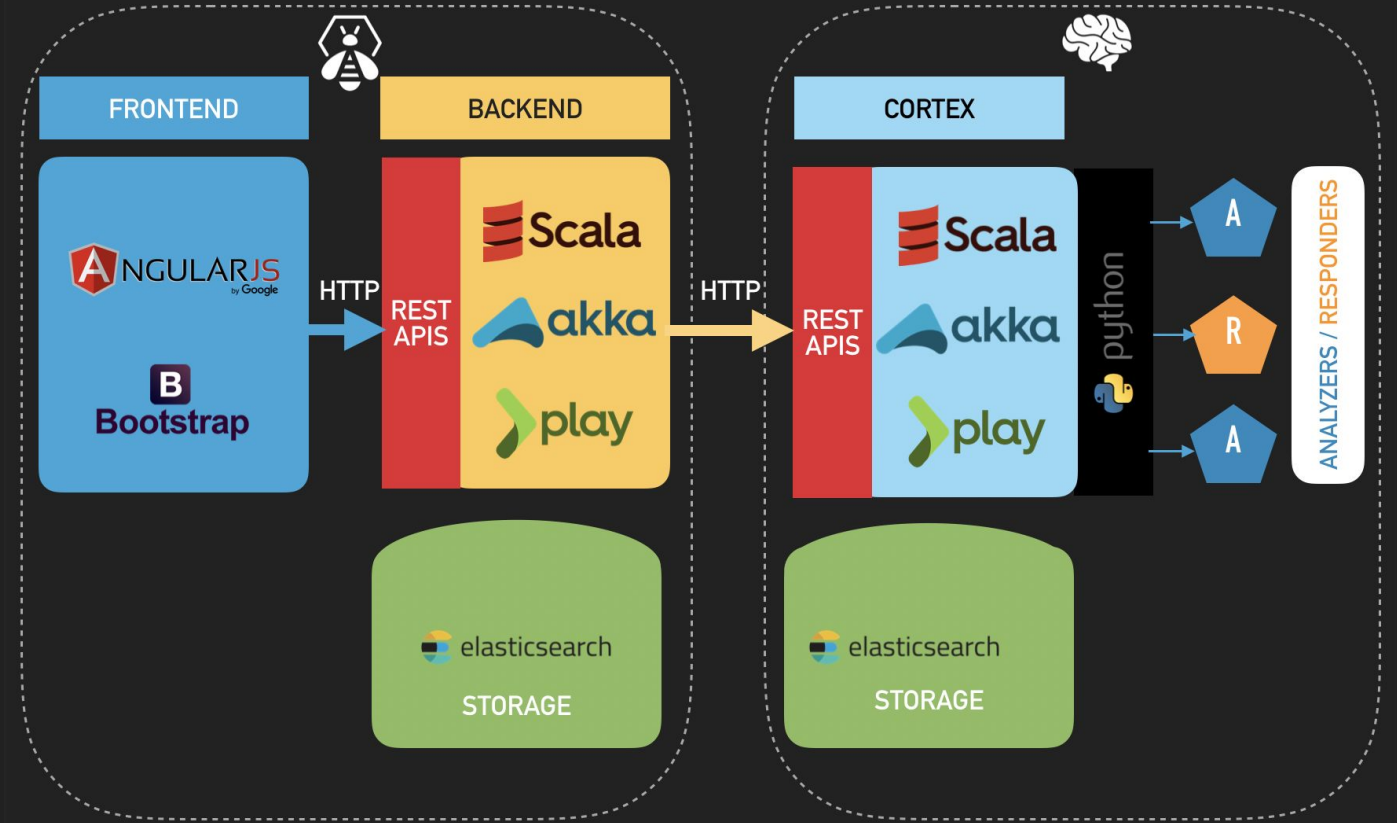
Elasticsearch us permet emmagatzemar, cercar i analitzar enormes volums de dades de manera ràpida i gairebé en temps real i retornar respostes en mil·lisegons. Pot obtenir respostes de cerca ràpides perquè en lloc de cercar directament el text, cerca un índex. **Elasticsearch** és NoSQL **database**. Això vol dir que emmagatzema dades de manera no estructurada i que no podeu utilitzar SQL per consultar-les.

AngularJS és un framework de JavaScript de codi obert que s'utilitza per crear i mantenir aplicacions web d'una sola pàgina.

Bootstrap és una biblioteca multiplataforma o conjunt d'eines de codi obert per al disseny de llocs i aplicacions web. Conté plantilles de disseny amb tipografia, formularis, botons, quadres, menús de navegació i altres elements de disseny basat en HTML i CSS, així com a extensions de JavaScript addicionals. Només ocupa el desenvolupament front-end.

Python és un llenguatge de programació interpretat.

TheHive3


FRONTEND
BACKEND
CORTEX
ANGULARJS
by Google
Bootstrap
HTTP
REST APIS
Scala
akka
play
HTTP
REST APIS
Scala
akka
play
python
A
R
A
ANALYZERS / RESPONDERS
elasticsearch
STORAGE
elasticsearch
STORAGE

Què és TheHive? (SIRP)

TheHive, com SIRP, ens permet investigar incidents de seguretat de forma ràpida i col·laborativa. Diversos analistes poden treballar simultàniament en tasques i casos. Si bé els casos es poden crear des de zero, TheHive pot rebre alertes de diferents fonts gràcies als alimentadors d'alertes que consumeixen esdeveniments de seguretat generats per múltiples fonts i els alimenten TheHive utilitzant la biblioteca **TheHive4py** esmentada.

Ón es pot instal·lar?

La instal·lació es pot fer:

- En un servidor **Debian** o **Centos** on cal fer la instal·lació i configuració.
- En contenidors de **Docker** on únicament cal fer la configuració extesa.
- Es pot instal·lar fàcilment en qualsevol distribució estàndard de GNU / Linux
- **Red Hat Package Manager** o **RPM** (eina d'administració de paquets), **DEB package** (paquets instal·ladors de programari), **Binaris**, or **Build it Yourself**.

API REST -> Serveix per comunicarse entre apps dades de forma eficaç i fiable.

Una **API** (interfície de programació d'apps) es un conjunt de requisicions (documents que permeten una adquisició) que permet la comunicació d'informació entre apps. La API fa ús de requisicions HTTP que s'encarreguen de les operacions bàsiques pel tractament de dades.

Les principals **sol·licituds** son:

POST: crea dades al servidor

GET: lectura de dades al host

DELETE: esborra la informació

PUT: registre d'actualitzacions

REST (de la arquitectura) es l'abreviació de Representational State Transfer, és un conjunt de restriccions que s'usen perquè les sol·licituds d'abans compleixin amb les directrius definides en la arquitectura

Les regles de la arquitectura son:

- Client-server
- Etc.

Comunicació

TheHive4PY

És un API en Python que es propia de TheHive. Ens permet la interacció entre diferents solucions com un SIEM.

Autenticació

TheHive compleix la connexió local, LDAP, Active Directory (AD) o Auth2 / OpenID Connect per a l'autenticació. Per defecte, depèn de les credencials locals emmagatzemades a Elasticsearch.

Els mètodes d'autenticació s'emmagatzemen al *auth.provider* paràmetre, que té diversos valors. Quan un usuari inicia la sessió, cada mètode d'autenticació s'intenta en ordre fins que s'aconsegueix. Si no funciona cap mètode d'autenticació, torna a ser un error i utilitzar-lo no pot iniciar la sessió.

Per habilitar l'autenticació mitjançant AD, LDAP o O Auth2 / OpenID Connect, editariem *application.conf i donariem els valors del entorn, etc.*

Cortex en TheHive

Pot utilitzar un o diversos motors d'anàlisi Cortex per obtenir informació addicional sobre els observables. Quan es configuren, els analitzadors disponibles a Cortex es poden usar en TheHive.

MISP en TheHive

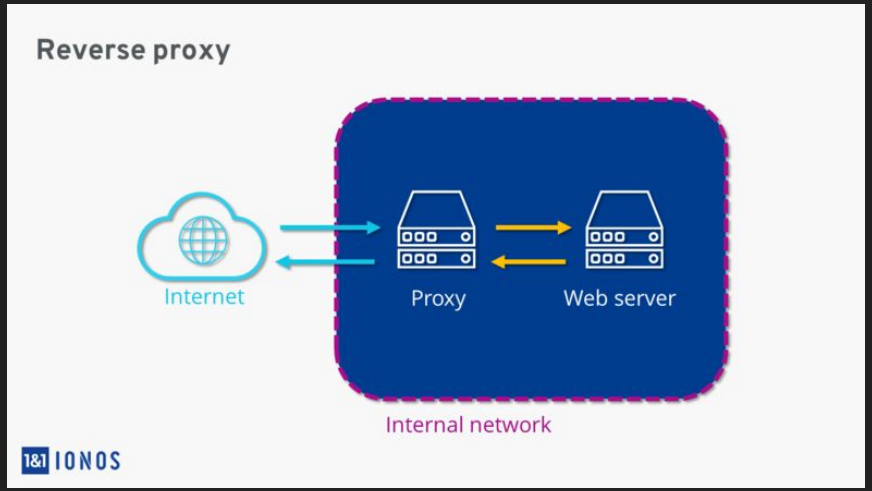
TheHive pot interactuar amb MISP de dues maneres: importar un esdeveniment MISP per crear un cas en TheHive i exportar un cas TheHive per crear un esdeveniment MISP. Per defecte, qualsevol instància/es de MISP que s'afegeixi a la configuració de TheHive s'utilitzarà per importar esdeveniments i exportar casos.

Els esdeveniments MISP només seran importats per TheHive si tenen al menys un atribut i van ser publicats.

(haurà de crear una plantilla de cas abans d'importar esdeveniments de MISP i apareixeran com alertes dins de l'Alertspanel)

HTTPS

Es pot habilitar HTTPS en l'aplicació TheHive o afegir un servidor intermediari invers davant de TheHive. Es recomana l'última solució.



Proxy Invers

- **Load balancing** -> permet l'accés a un recurs web eficaçment i distribueix la càrrega de sol·licituds web en diversos servers garantitzant amb el seu rol que tracti de igual forma la quantitat de sol·licituds per no desbordar.
- **Caché** -> Pot fer com a cau.
- **Protecció d'atacs** -> Al no revelar la IP del Server, s'enmascara la IP real.
- **Xifrat SSL** -> Desxifra les sol·licituds web que es generin i quan tingui resposta per part del server, la xifra i la envia al client i el server utilitzi altres recursos per millorar rendiment.

Quin contingut té TheHive?

- Alertes (de molts tipus)
- Plantilles per als casos
- Report templates
- Observables
- Casos
- Panells de control
- Mètriques
- Users

Aixecament

```
root@grail-VB:/home/grail/docker# docker-compose up
Starting docker_elasticsearch_1 ...
Starting docker_elasticsearch_1 ... done
Starting docker_cortex_1 ...
Starting docker_cortex_1 ... done
Starting docker_thehive_1 ...
Starting docker_thehive_1
```

root@grail-VB: /home/grail/docker

File Edit View Search Terminal Help

GNU nano 2.9.3 docker-compose.yml

```
version: "2"
services:
  elasticsearch:
    user: $USER
    image: elasticsearch:7.9.1
    environment:
      - http.host=0.0.0.0
      - discovery.type=single-node
      - script.allowed_types=inline
      - thread_pool.search.queue_size=100000
      - thread_pool.write.queue_size=10000
    ulimits:
      nofile:
        soft: 65536
        hard: 65536
    volumes:
      - $PWD/elasticsearch/data:/usr/share/elasticsearch/data
      - $PWD/elasticsearch/logs:/usr/share/elasticsearch/logs
  cortex:
    image: thehiveproject/cortex:latest
    environment:
      - job_directory=/tmp/cortex-jobs
    volumes:
      - /var/run/docker.sock:/var/run/docker.sock
      - /tmp/cortex-jobs:/tmp/cortex-jobs
    depends_on:
      - elasticsearch
    ports:
      - "0.0.0.0:9001:9001"
  thehive:
    image: thehiveproject/thehive:latest
    depends_on:
      - elasticsearch
      - cortex
    ports:
      - "0.0.0.0:9000:9000"
    command: --cortex-port 9001 --cortex-key ewv6cimImNzifmsqiDtx8Ho/pb3t5gbw
```

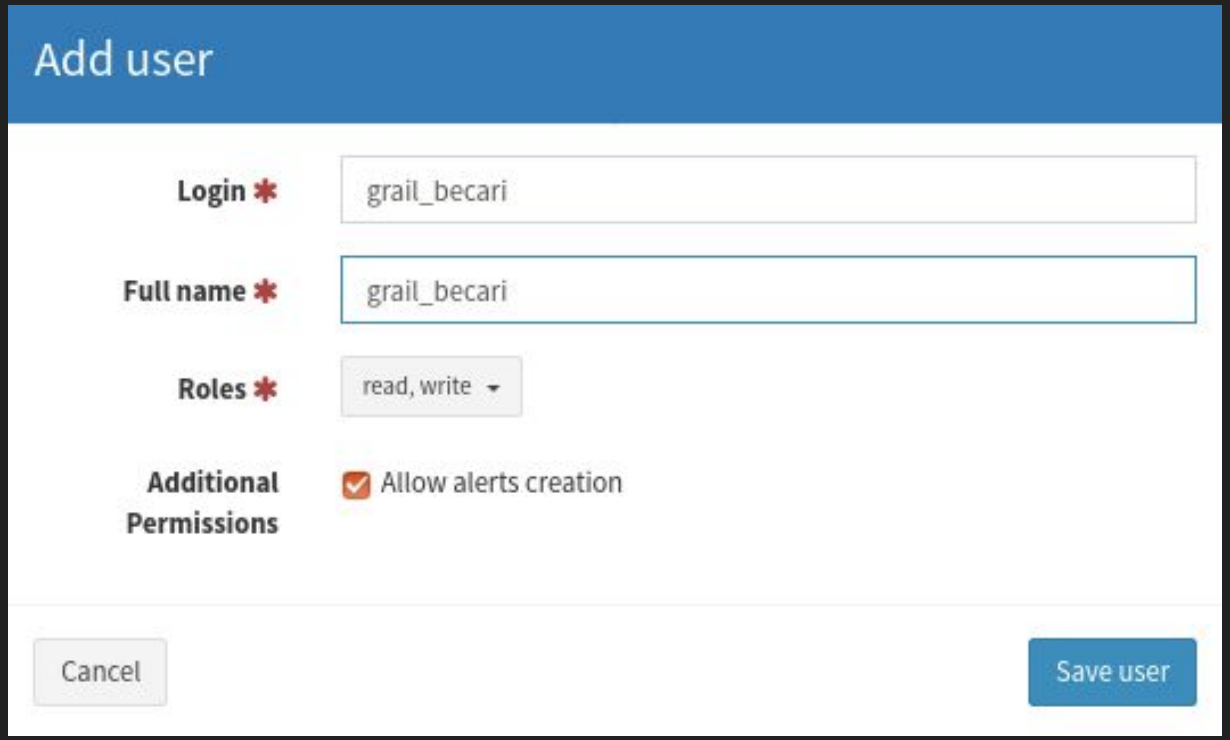
Users

Podem afegir múltiples usuaris amb diferents rols dins del SOC amb diferents permissos assignats.

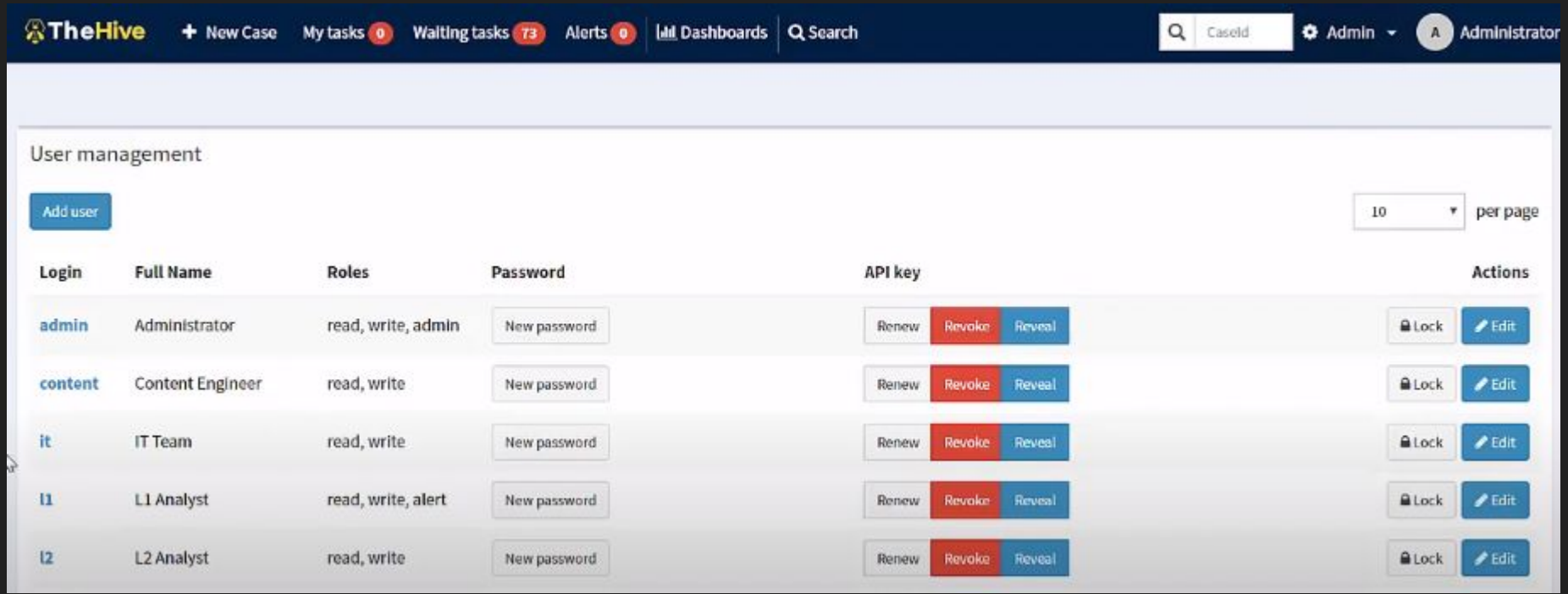
Hi ha 4 funcions:

- **read**: es poden llegir totes les dades no sensibles. Amb aquesta funció, un usuari no pot fer cap canvi. No poden afegir cap cas, tasca, registre o observable. Tampoc no poden executar analitzadors.
- **write**: crear, eliminar i canviar dades de qualsevol tipus. Aquesta funció és per als usuaris estàndard. **write** el paper hereta els **read** drets.
- **admin**: Els usuaris amb aquesta funció poden gestionar comptes d'usuari, mètriques, crear plantilles de casos i tipus de dades observables. **admin** hereta **write** drets.
- **alert**: els usuaris amb aquesta funció només poden crear alertes.

Exemple


Add user
Login *
grail_becari
Full name *
grail_becari
Roles *
read, write
Additional Permissions
Allow alerts creation
Cancel
Save user

Exemple llista users



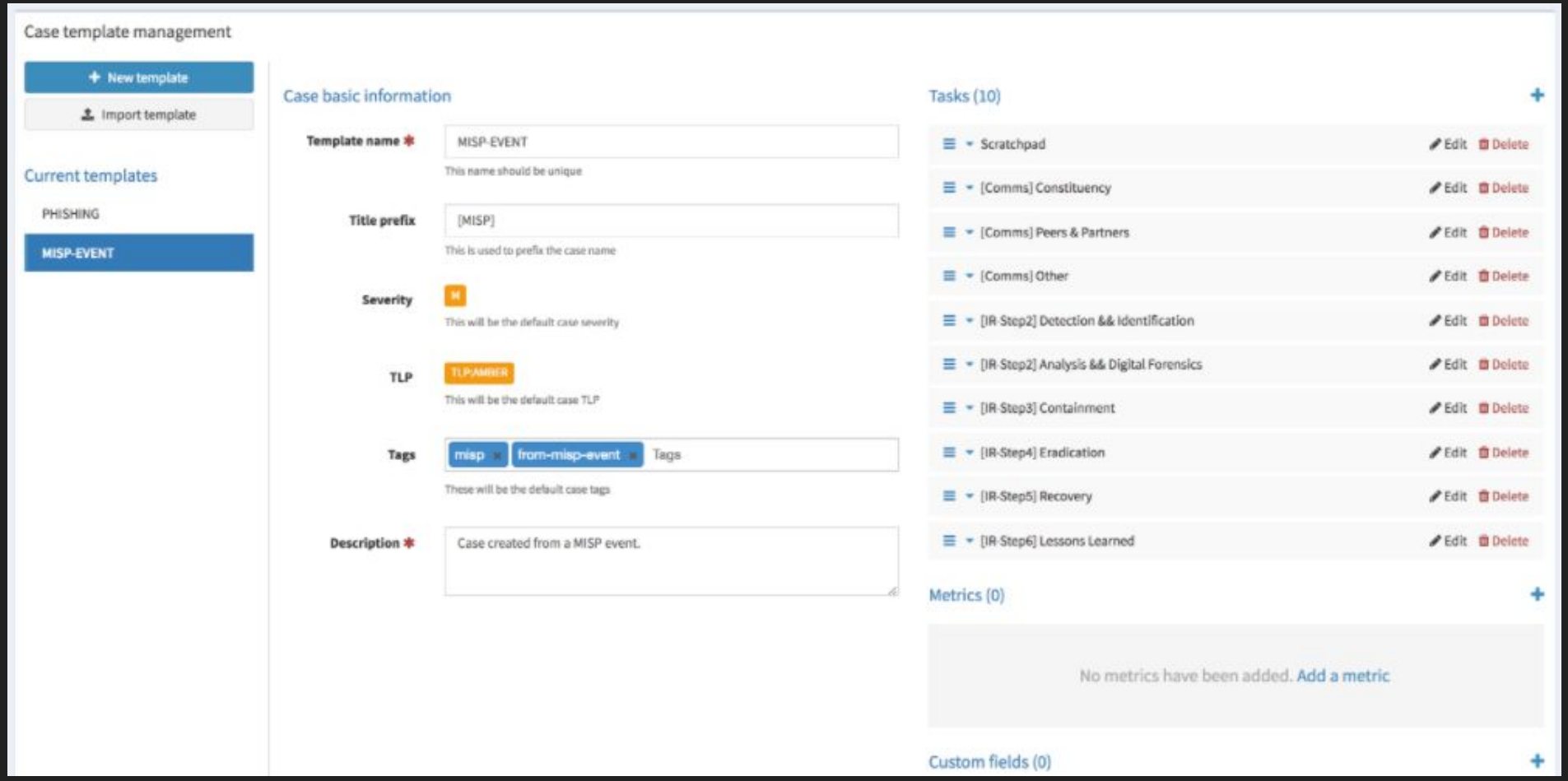
Templates

Quan TheHive està connectat a un servidor Cortex, es poden analitzar els observables per obtenir-ne informació addicional. Cortex genera informes en format JSON. Per tal que els informes siguin més llegibles, podeu configurar les plantilles d'informes. Les plantilles d'informes converteixen JSON a HTML mitjançant el motor de plantilles AngularJS.

Per a cada analitzador disponible a **Cortex** podeu definir dos tipus de plantilles: curtes i llargues. Un informe breu exposa informació sintètica, que es mostra a la part superior de la pàgina observable. Amb informes breus podeu veure un resum de tots els analitzadors d'execució. Els informes llargs només mostren informació detallada quan l'usuari selecciona l'informe. Les dades sense format en format JSON sempre estan disponibles.

Les plantilles d'informes es poden configurar al menú **Admin**> **Report templates**. Oferim plantilles d'informes per a analitzadors Cortex predeterminats. Es pot descarregar un paquet amb totes les plantilles d'informes a https://dl.bintray.com/thehive-project/binary/report-templates.zip i es pot injectar mitjançant el Import templates botó.

Templates


Case template management
+ New template
Import template
Current templates
PHISHING
MISP-EVENT
Case basic information
Template name *
MISP-EVENT
This name should be unique
Title prefix
[MISP]
This is used to prefix the case name
Severity
M
This will be the default case severity
TLP
TLP:AMBER
This will be the default case TLP
Tags
misp
from-misp-event
Tags
These will be the default case tags
Description *
Case created from a MISP event.
Tasks (10)
Scratchpad
[Comms] Constituency
[Comms] Peers & Partners
[Comms] Other
[IR-Step2] Detection && Identification
[IR-Step2] Analysis && Digital Forensics
[IR-Step3] Containment
[IR-Step4] Eradication
[IR-Step5] Recovery
[IR-Step6] Lessons Learned
Edit
Delete
Metrics (0)
No metrics have been added. Add a metric
Custom fields (0)

Observables

Els diferents tipus de observables que tenim:

dataType
other
uri_path
regexp
file
registry
ip
mail_subject
mail
url
hash
domain
autonomous-system
filename
fqdn
user-agent

Mètriques

Les mètriques s’han integrat per tenir indicadors rellevants sobre casos.

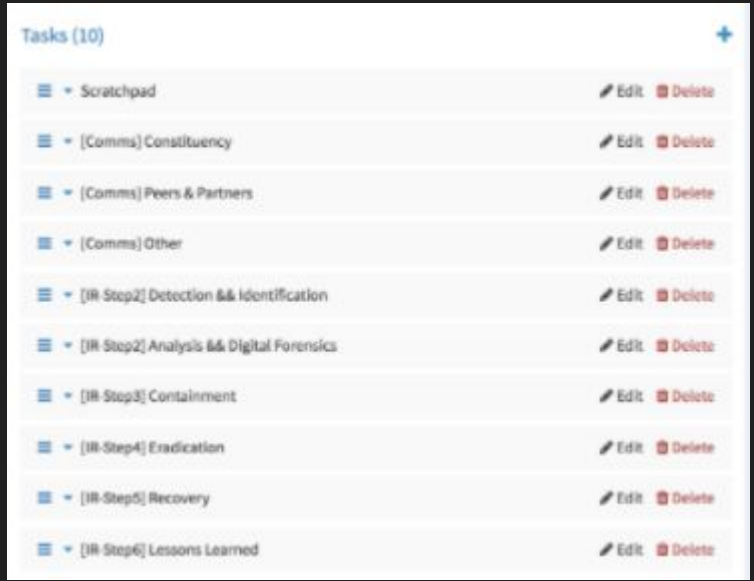
Les mètriques són valors numèrics associats a casos (per exemple, el nombre d'usuaris afectats). Cada mètrica té un **nom**, un **títol** i una **descripció**, definits per un **administrador**.

Les mètriques es defineixen globalment. Per crear mètriques, com a administrador, aneu al menú d'administració i obriu l'element "Mètriques de majúscules i minúscules".

Les mètriques s’utilitzen per crear estadístiques (element “Estadístiques” al menú del perfil d’usuari). Es poden filtrar per intervals de temps i majúscules i minúscules amb etiquetes específiques.

Tasks

És quadre ón l'analista de turn pot ingresar de forma detallada les seves observacions respecte el cas, és a dir, són tasques que ha de fer l'analista, etc. i exposar el seu tractament.



Protocols TLP i PAP

TheHive té la capacitat d'identificar automàticament els observables que ja s'havien vist en casos anteriors. Els observables també es poden associar a un TLP i un PAP i a la font que els ha proporcionat o ha generat mitjançant etiquetes.

Protocol TLP: Nivells

S'ha d'utilitzar TLP: **RED** quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, reputació o operacions si és mal utilitzada.

S'ha d'utilitzar TLP: **AMBER** quan la informació requereix ser distribuïda de forma limitada, però suposa un risc per a la privacitat, reputació o operacions si és compartida fora de l'organització.

S'ha d'utilitzar TLP: **GREEN** quan la informació és útil per a totes les organitzacions que hi participen, així com amb tercers de la comunitat o el sector.

S'ha d'utilitzar TLP: **WHITE** quan la informació no suposa cap risc de mal ús, dins de les regles i procediments establerts per a la seva difusió pública.

Protocol PAP: Nivells

(PAP: **VERMELL**) Només accions no detectables. Els destinataris no poden utilitzar informació PAP: RED a la xarxa. Només accions passives en registres que no es poden detectar des de l'exterior.

(PAP: **AMBRE**) Comprovació passiva de creu. Els destinataris poden utilitzar la informació PAP: AMBER per realitzar controls en línia, com ara l'ús de serveis prestats per tercers (per exemple, VirusTotal), o configurar un test de control.

(PAP: **VERD**) Es permeten accions actives. Els destinataris poden utilitzar informació PAP: VERD per fer ping a l'objectiu, bloquejar el trànsit entrant / sortint des de / cap a l'objectiu o configurar específicament les zones de mel per interactuar amb l'objectiu.

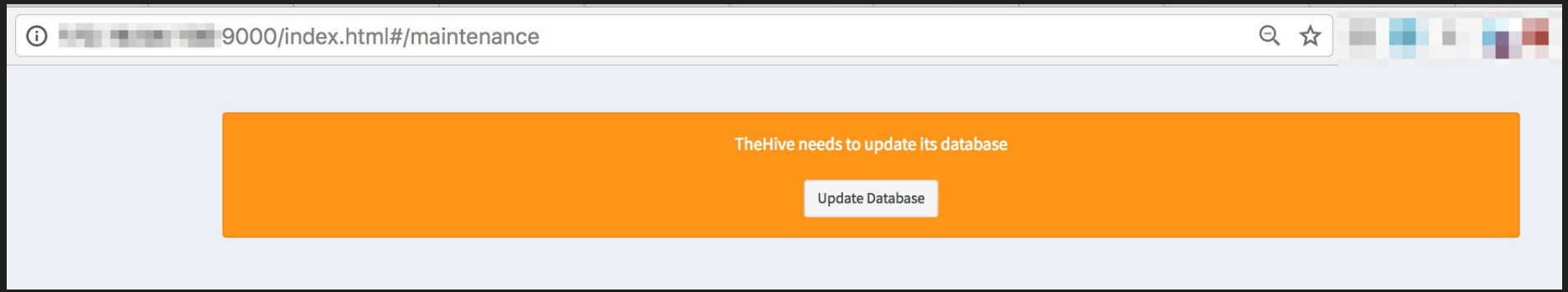
(PAP: **BLANC**) No hi ha restriccions en l'ús d'aquesta informació.

Per què utilitzar-lo?

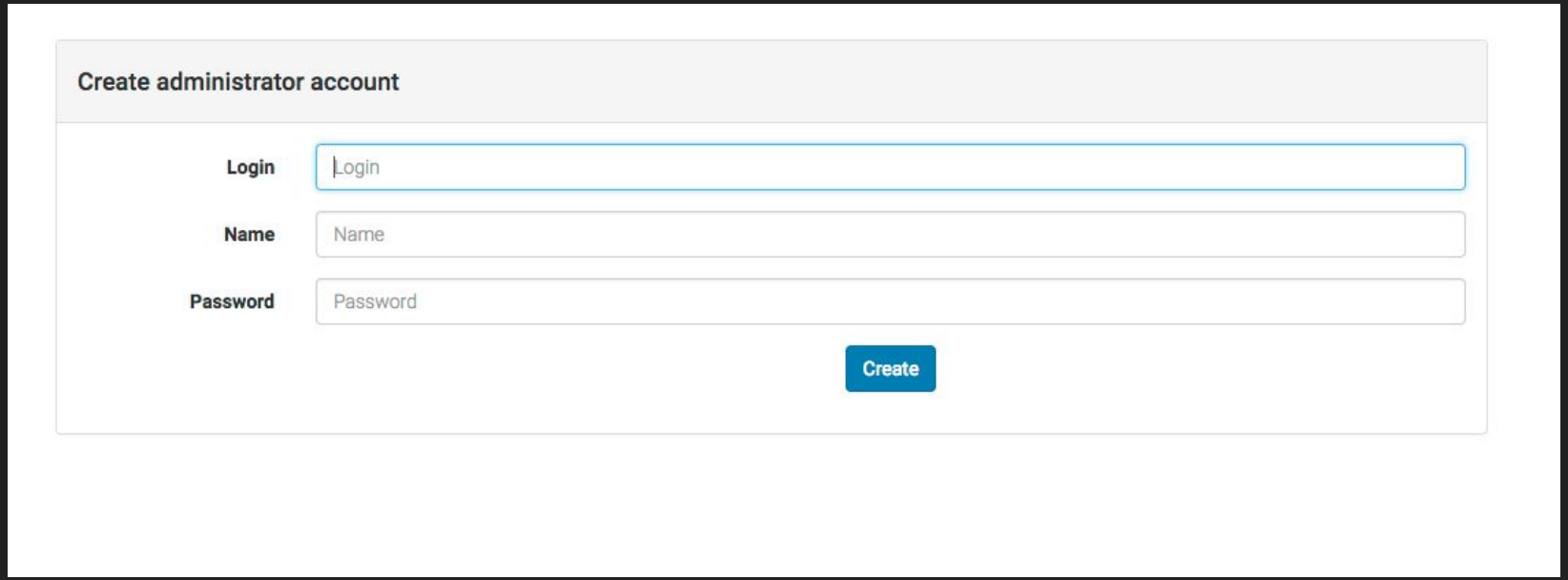
TLP va ser creat per a fomentar un millor intercanvi d'informació sensible (però no classificada) en l'àmbit de la seguretat de la informació, és a dir, garantitzaar que la compartició de les dades és amb la audiencia adecuada.

És utilitzat per organitzacions públiques i privades en el sector de la ciberseguretat.

La primera vegada que us connectem, haureu de crear l'esquema de la base de dades.

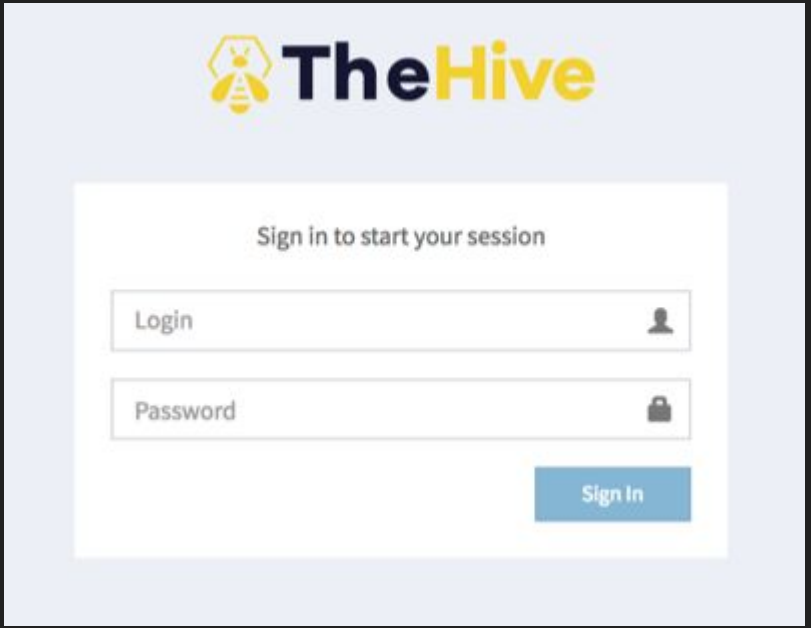


Un cop acabat, hauríem de ser redirigit a la pàgina per crear el compte de l'administrador.

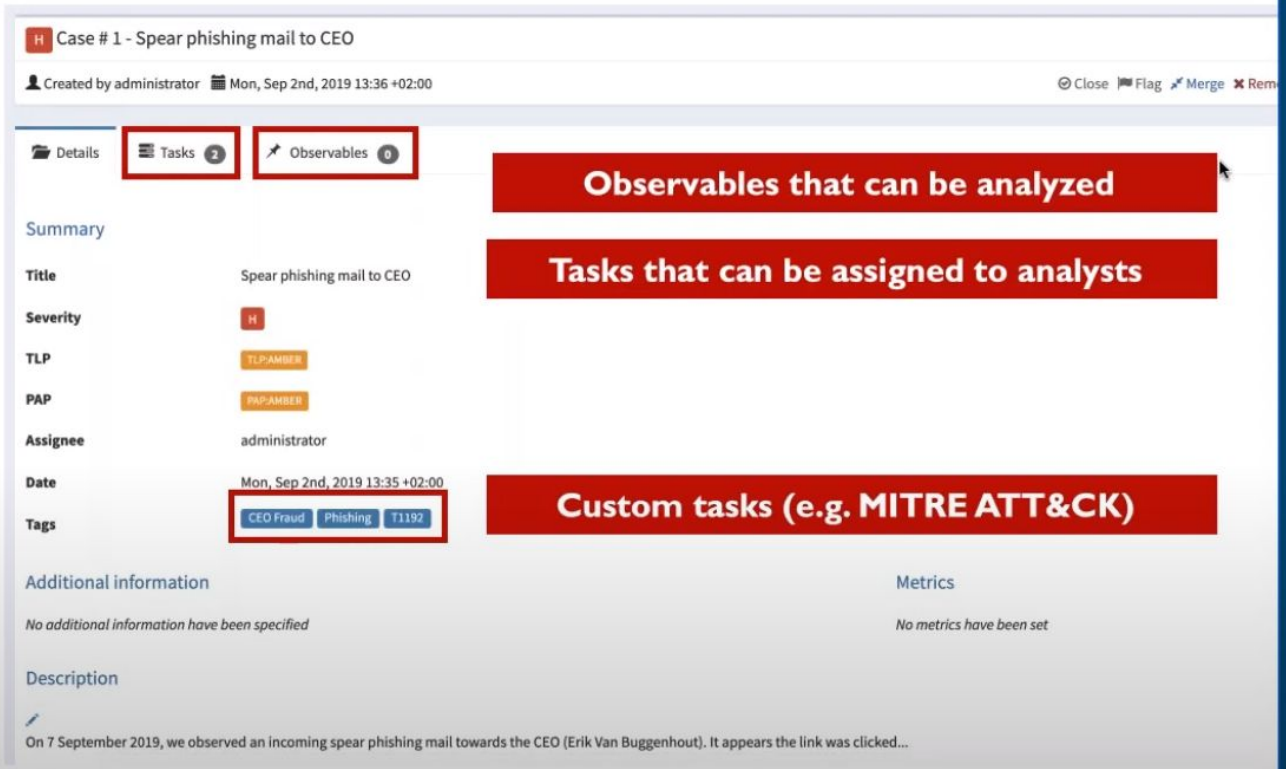


Un cop creat, hauriem de ser redirigits

a la pàgina d'inici de sessió.



TheHive interface - Cases



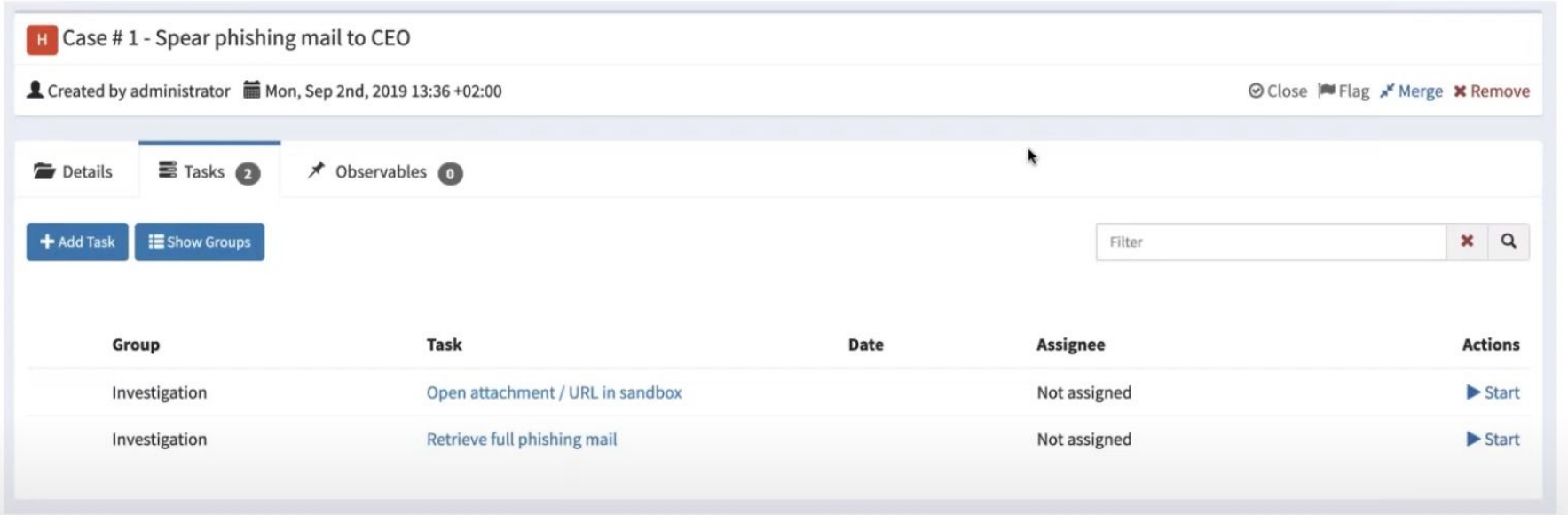
TheHive focuses on three core pillars:

Collaborate – multiple SOC and CERT analysts can simultaneously work on an investigation and collaborate.

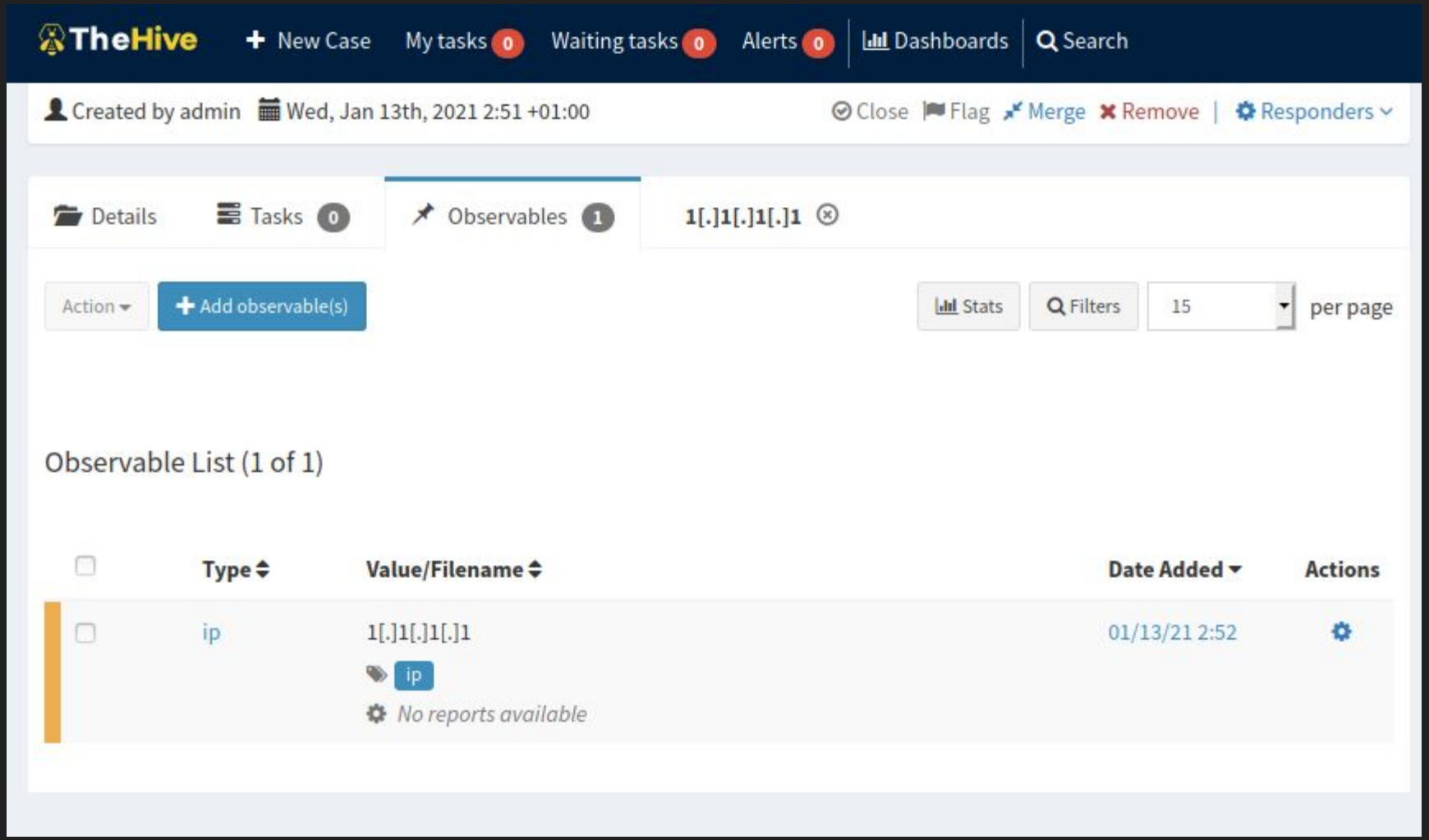
Elaborate – TheHive allows you to create flows and templates to speed up and automate tedious tasks.

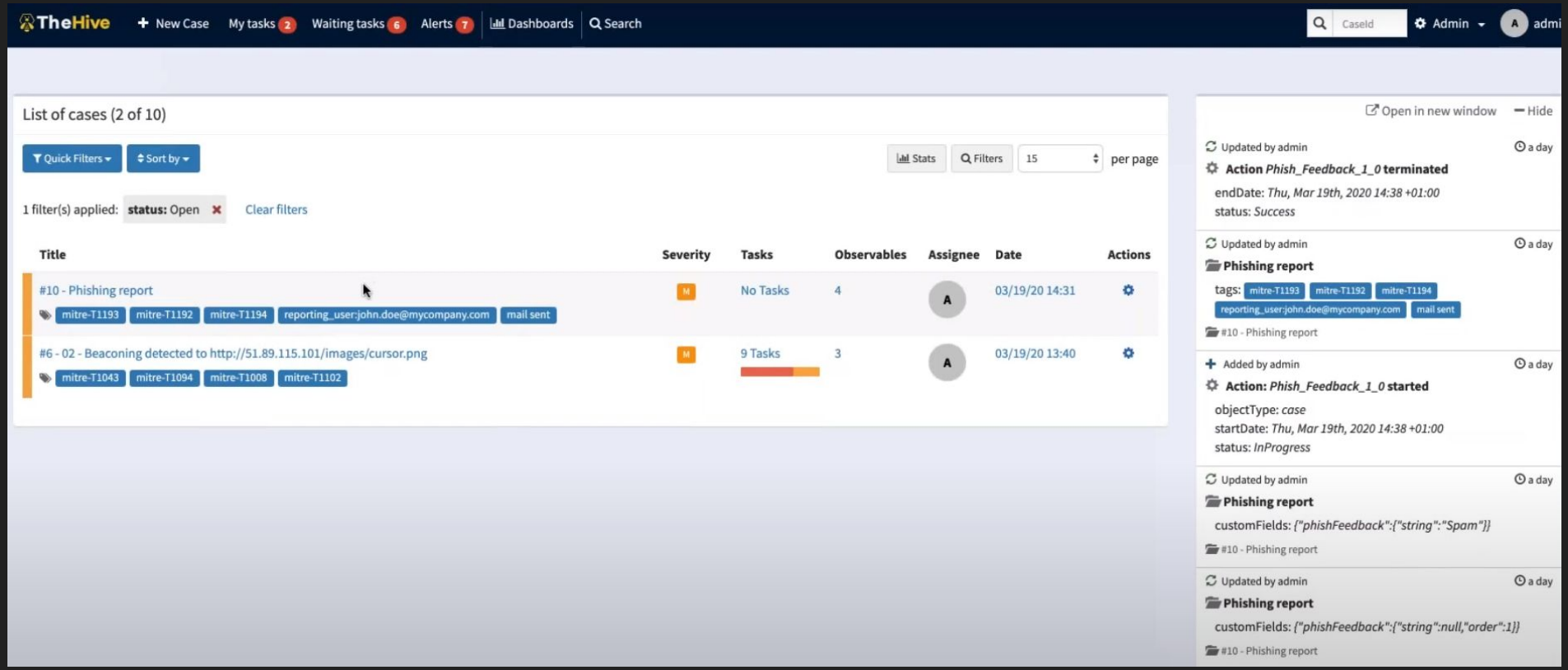
Analyze – TheHive tightly integrates with MISP, which allows for bi-directional communication. The platform allows for quick triage and filtering of IOCs.

TheHive interface - Tasks



In the above screenshot, we see a number of tasks that have been created for an example case (currently not assigned to an analyst). We can also create templates in TheHive which include a number of built-in tasks!

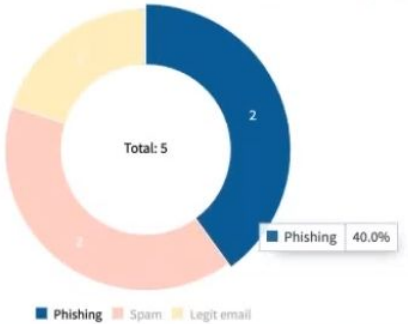

TheHive
New Case
My tasks 0
Waiting tasks 0
Alerts 0
Dashboards
Search
Created by admin
Wed, Jan 13th, 2021 2:51 +01:00
Close
Flag
Merge
Remove
Responders
Details
Tasks 0
Observables 1
1[.]1[.]1[.]1
Action
Add observable(s)
Stats
Filters
15
per page
Observable List (1 of 1)
Type
Value/Filename
Date Added
Actions
ip
1[.]1[.]1[.]1
01/13/21 2:52
ip
No reports available


TheHive
+ New Case
My tasks 2
Waiting tasks 6
Alerts 7
Dashboards
Search
CaseId
Admin
admi
List of cases (2 of 10)
Quick Filters
Sort by
Stats
Filters
15
per page
1 filter(s) applied: status: Open
Clear filters
Title
Severity
Tasks
Observables
Assignee
Date
Actions
#10 - Phishing report
mitre-T1193
mitre-T1192
mitre-T1194
reporting_user:john.doe@mycompany.com
mail sent
M
No Tasks
4
A
03/19/20 14:31
#6 - 02 - Beaconing detected to http://51.89.115.101/images/cursor.png
mitre-T1043
mitre-T1094
mitre-T1008
mitre-T1102
M
9 Tasks
3
A
03/19/20 13:40
Open in new window
Hide
Updated by admin
a day
Action Phish_Feedback_1_0 terminated
endDate: Thu, Mar 19th, 2020 14:38 +01:00
status: Success
Updated by admin
a day
Phishing report
tags: mitre-T1193 mitre-T1192 mitre-T1194 reporting_user:john.doe@mycompany.com mail sent
#10 - Phishing report
Added by admin
a day
Action: Phish_Feedback_1_0 started
objectType: case
startDate: Thu, Mar 19th, 2020 14:38 +01:00
status: InProgress
Updated by admin
a day
Phishing report
customFields: {"phishFeedback":{"string":"Spam"}}
#10 - Phishing report
Updated by admin
a day
Phishing report
customFields: {"phishFeedback":{"string":null,"order":1}}
#10 - Phishing report

TheHive Reporting

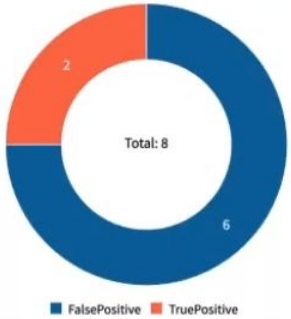
Phishing Feedback

Save as Image CSV



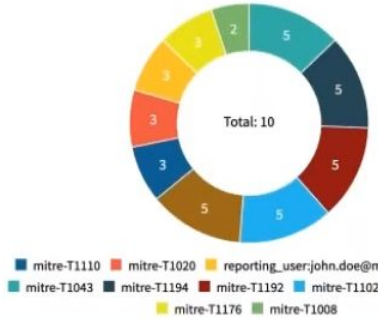
Revolved cases by resolution

Save as Image CSV



Case tags

Save as Image CSV

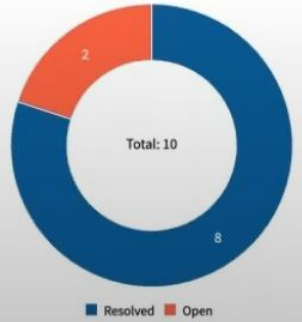


Owner of open cases

Save as Image CSV

Cases by status

Save as Image CSV



Què és Cortex?

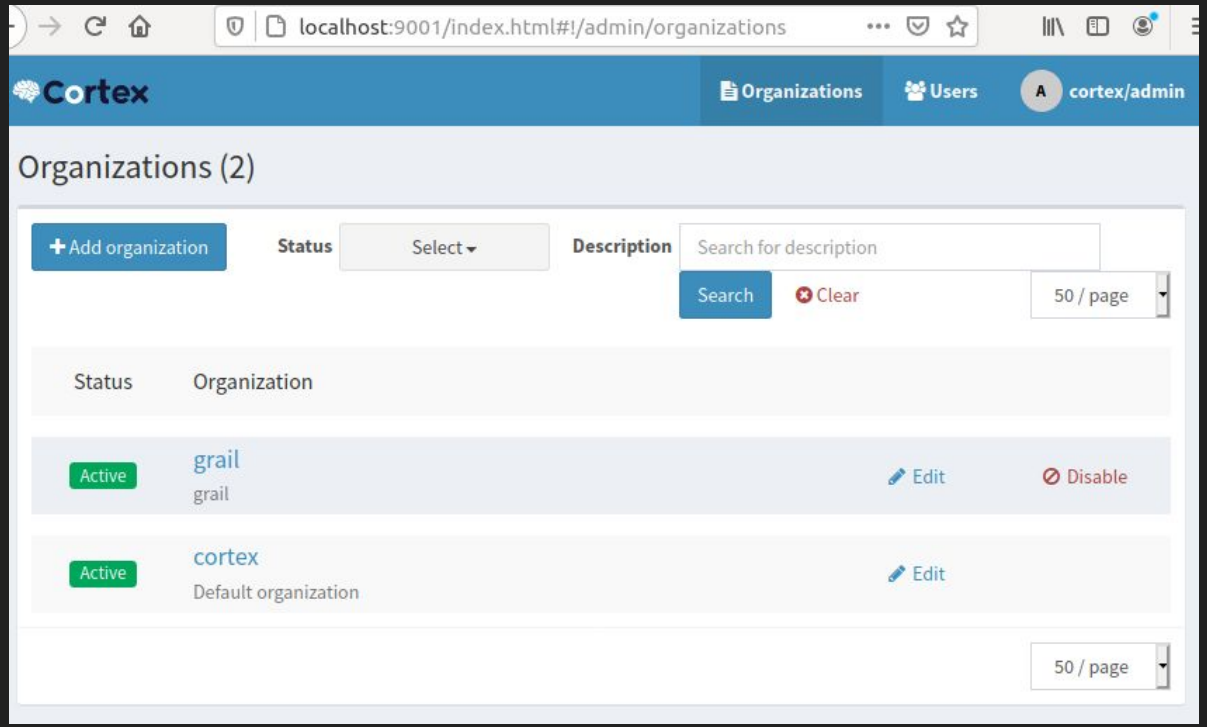
És un motor d'anàlisi independent i un company perfecte per TheHive i MISP. Els analistes poden utilitzar-lo per analitzar observables utilitzant la seva interfície web d'usuari, en aquest cas poden enviar només d'un en un. El poder realment entra en joc quan fem servir la seva API REST. TheHive parla nativament a Cortex (com ho fa MISP).

També olla invocar Mòduls d'Expansió MISP. Aquests són normalment utilitzats per MISP per enriquir a els atributs dins de dels esdeveniments, però Cortex también olla aprofitar-les per ANALITZAR a els observables.

Quin contingut té Cortex?

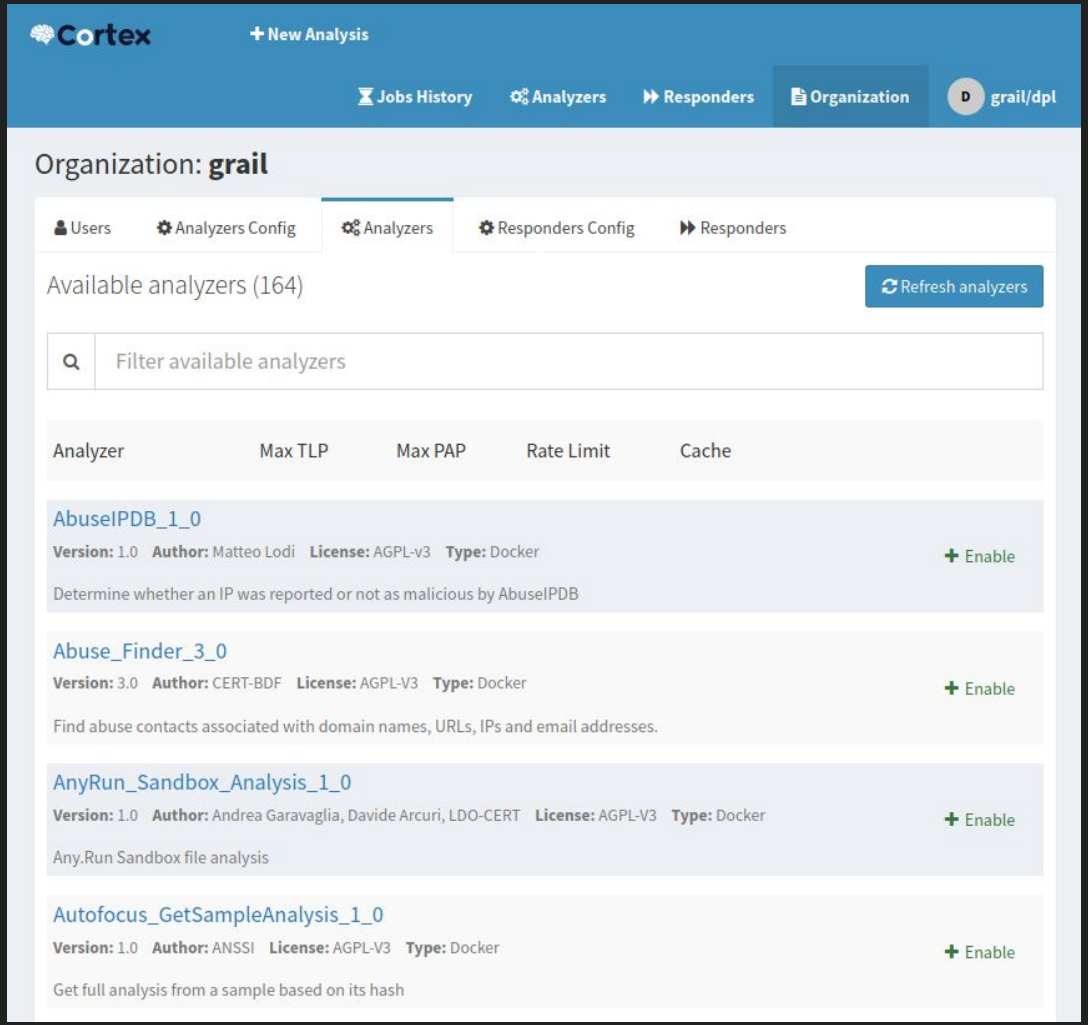
- Organitzacions
- Usuaris (amb diferents rols)
- Analitzadors
- Respostes

Organitzacions



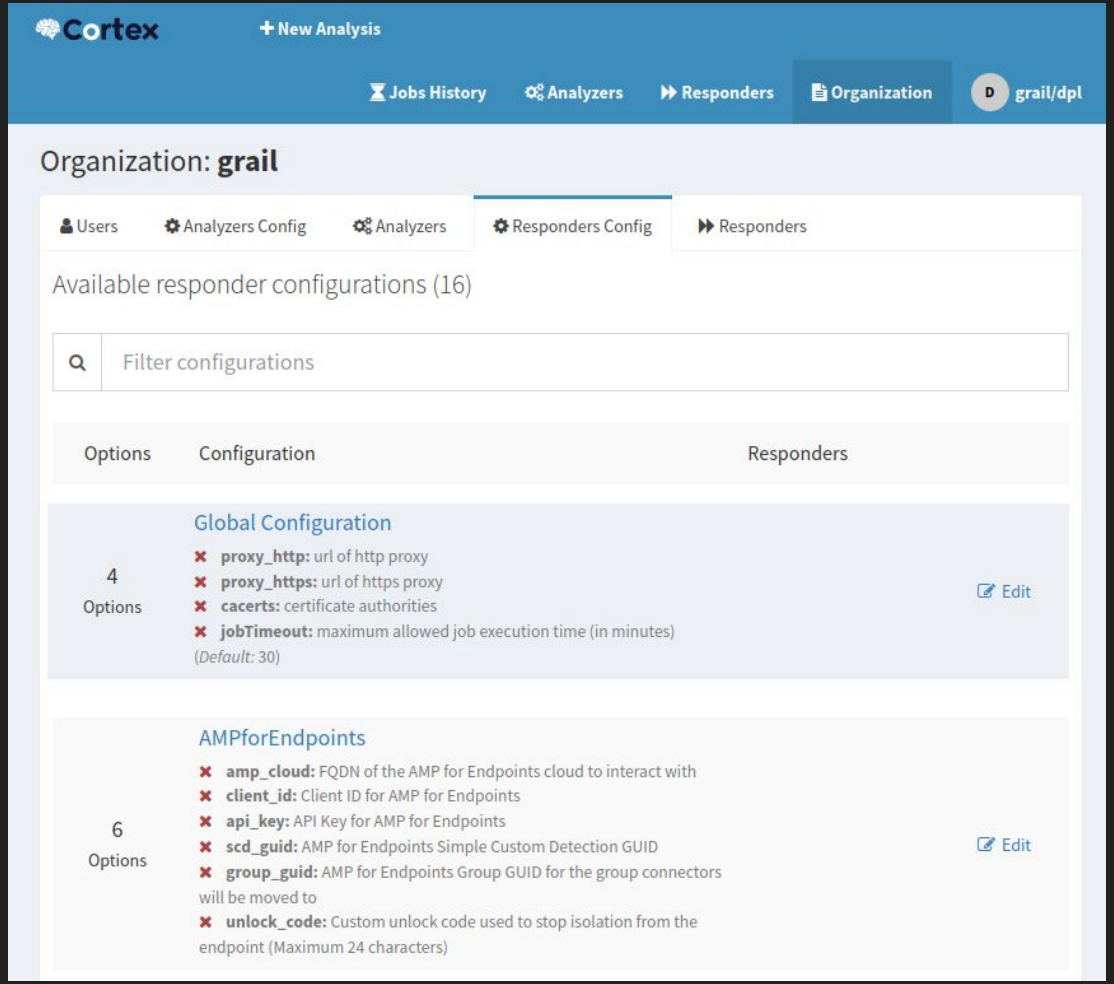
Analitzadors

Té 39 analitzadors. Un analitzador pot escriure en qualsevol llenguatge de programació admès per Linux, encara que tots els seus analitzadors actuals estan escrits en Python. Això es deu al fet que proporcionem una biblioteca de Python anomenada Cortexutils que conté un conjunt de classes d'utilitat que fan que sigui més fàcil escriure un analitzador en Python.


Cortex
+ New Analysis
Jobs History
Analyzers
Responders
Organization
D
grail/dpl
Organization: grail
Users
Analyzers Config
Analyzers
Responders Config
Responders
Available analyzers (164)
Refresh analyzers
Filter available analyzers
Analyzer
Max TLP
Max PAP
Rate Limit
Cache
AbuseIPDB_1_0
Version: 1.0 Author: Matteo Lodi License: AGPL-v3 Type: Docker
+ Enable
Determine whether an IP was reported or not as malicious by AbuseIPDB
Abuse_Finder_3_0
Version: 3.0 Author: CERT-BDF License: AGPL-V3 Type: Docker
+ Enable
Find abuse contacts associated with domain names, URLs, IPs and email addresses.
AnyRun_Sandbox_Analysis_1_0
Version: 1.0 Author: Andrea Garavaglia, Davide Arcuri, LDO-CERT License: AGPL-V3 Type: Docker
+ Enable
Any.Run Sandbox file analysis
Autofocus_GetSampleAnalysis_1_0
Version: 1.0 Author: ANSSI License: AGPL-V3 Type: Docker
+ Enable
Get full analysis from a sample based on its hash

Responders

Els responders són programes que té Cortex per poder combatre les amenaces, ja sigui, denegar IP’s, dominis, etc. Es poden executar en el mateix TheHive.


Cortex
+ New Analysis
Jobs History
Analyzers
Responders
Organization
D
grail/dpl
Organization: grail
Users
Analyzers Config
Analyzers
Responders Config
Responders
Available responder configurations (16)
Filter configurations
Options
Configuration
Responders
4
Options
Global Configuration
proxy_http: url of http proxy
proxy_https: url of https proxy
cacerts: certificate authorities
jobTimeout: maximum allowed job execution time (in minutes)
(Default: 30)
Edit
6
Options
AMPforEndpoints
amp_cloud: FQDN of the AMP for Endpoints cloud to interact with
client_id: Client ID for AMP for Endpoints
api_key: API Key for AMP for Endpoints
scd_guid: AMP for Endpoints Simple Custom Detection GUID
group_guid: AMP for Endpoints Group GUID for the group connectors will be moved to
unlock_code: Custom unlock code used to stop isolation from the endpoint (Maximum 24 characters)
Edit

Què és MISP? (CyDefSIG)

És una plataforma per compartir amenaces i és un programari de codi obert i gratuït que ajuda a compartir informació de la intel·ligència sobre amenaces, recopilar, emmagatzemar i correlacionar indicadors de compromís d'atacs específics, intel·ligència d'amenaces, informació sobre fraus financers, informació sobre vulnerabilitats o fins i tot informació contra el terrorisme.

Què fa MISP?

- Emmagatzema informació tan tècnica com no tècnica sobre malware i atacs ja detectats.
- Crear automàticament relacions entre malware i els seus atributs.
- Emmagatzema dades en un format estructurat, permetent així un us automatizat de sistemas de detecció o eines forenses .
- Generar regles NIDS per després importarse a IDS.
- Compartir els atributs de malware i amenaces amb altres organitzacions i grups de confiança.

Quin contingut té?

- Usuaris
- Organitzacions
- Events (per difundir-los)
- Rols
- Dashboard
- Etc. a la següent diapositiva

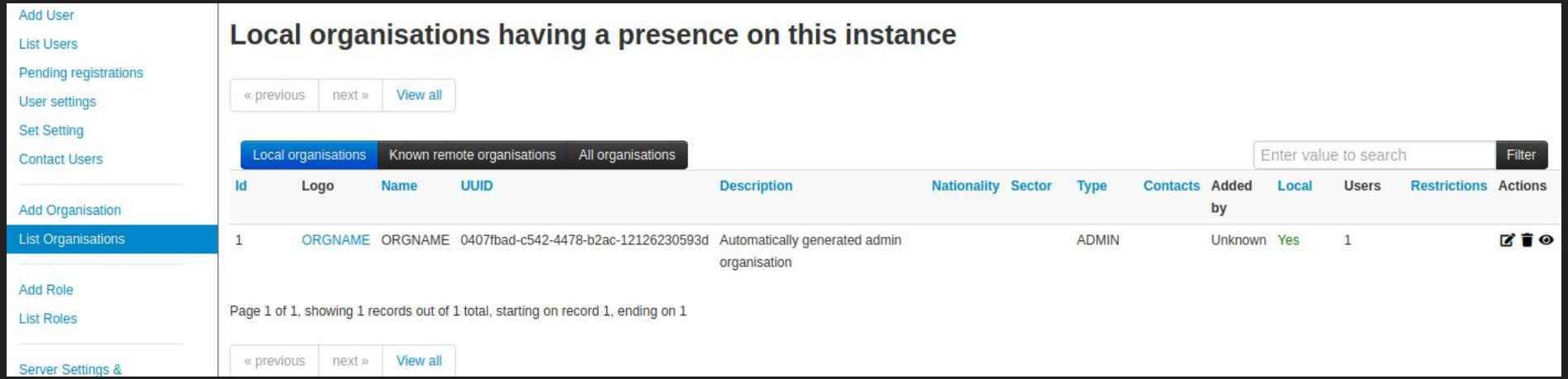
- **Taxonomies** -> ens permet classificar els events.
- **Galaxies** -> ens permet agrupar diferents grups d'events (peçes de malware) i entendre tendències de malware.
- **Atributs i categories (del atribut no del event)** -> antivirus, network activity…
- **Atributs (tipus) que es comparteixen** -> md5, filename, hostname, ip-src, ip-dst…
- **Warning-list** -> ens permet treballar amb falsos positius (indicadors que no es apliquen a nosaltres ja que són d'altres regions…)
- **TLP** -> etiqueta per com compartir l'event
- **Feeds** -> proporcionen intercanvi d'informació a través de HTTP, USB...

¿I què és un esdeveniment?

No és més que el registre d'una mostra amb les seves IOC (indicadors de compromís) que hagim descobert o se'ns hagi remès des d'un SIEM, IDS o IPS, i així poder-lo correlacionar amb la nostra llista de feeds.

Què són els Feeds?

Bàsicament són recursos (obtinguts de fonts remotes o locals) que generen tercers amb informació i que podem recollir per afegir-la en la nostra instància de MISP. Aquesta informació ve estructurada en format MISP, CSV o text pla, i conté indicadors que poden importar automàticament en MISP en intervals predefinits.


Add User
List Users
Pending registrations
User settings
Set Setting
Contact Users
Add Organisation
List Organisations
Add Role
List Roles
Server Settings &
Local organisations having a presence on this instance
« previous
next »
View all
Local organisations
Known remote organisations
All organisations
Enter value to search
Filter
Id
Logo
Name
UUID
Description
Nationality
Sector
Type
Contacts
Added by
Local
Users
Restrictions
Actions
1
ORGNAME
ORGNAME
0407fbad-c542-4478-b2ac-12126230593d
Automatically generated admin organisation
ADMIN
Unknown
Yes
1
Page 1 of 1, showing 1 records out of 1 total, starting on record 1, ending on 1
« previous
next »
View all

Add User
List Users
Pending registrations
User settings
Set Setting
Contact Users

Add Organisation
List Organisations

Add Role
List Roles

Server Settings & Maintenance
Update Progress

Jobs

Scheduled Tasks
Event Block Rules
Blocklists Event
Manage Event Blocklists
Blocklists Organisation
Manage Org Blocklists

Admin Add User

Email

auditor@grail.com

Set password

Organisation

ORGNAME

Role

admin

Authkey

BTdoa3g2Mnp6iki8eEoWMLgzM

NIDS SID

Sync user for

Not bound to a server

PGP key

Paste the user's PGP key here or try to retrieve it from the CIRCL key server by clicking on "Fetch PGP key" below.

Fetch PGP key

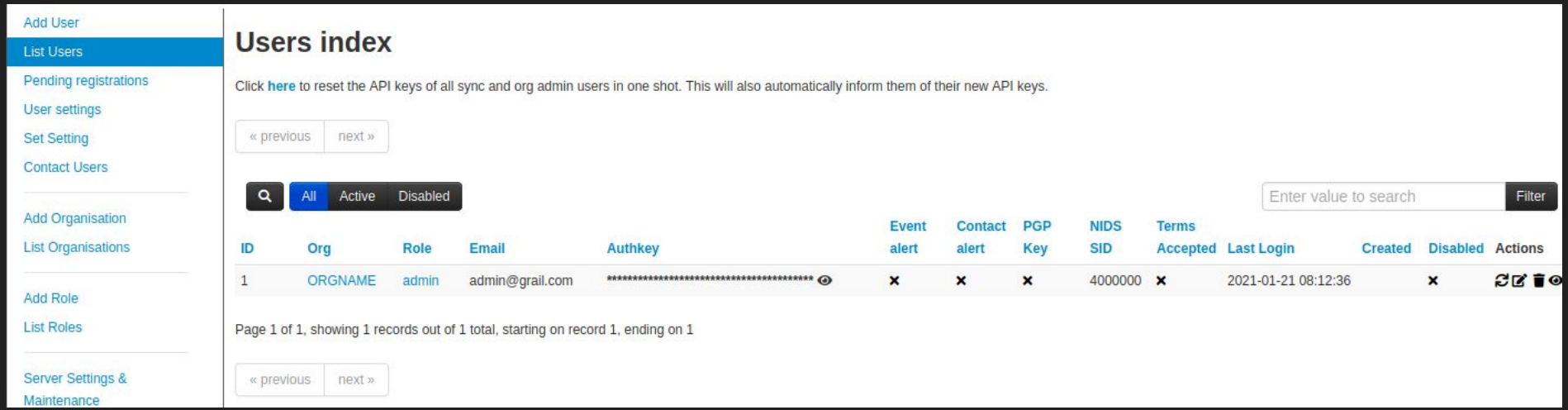
Receive email alerts when events are published

Receive email alerts from "Contact reporter" requests

Disable this user account

Send credentials automatically

Create user


Add User
List Users
Pending registrations
User settings
Set Setting
Contact Users
Add Organisation
List Organisations
Add Role
List Roles
Server Settings & Maintenance
Users index
Click here to reset the API keys of all sync and org admin users in one shot. This will also automatically inform them of their new API keys.
« previous
next »
All
Active
Disabled
Enter value to search
Filter
ID
Org
Role
Email
Authkey
Event alert
Contact alert
PGP Key
NIDS SID
Terms Accepted
Last Login
Created
Disabled
Actions
1
ORGNAME
admin
admin@grail.com
4000000
2021-01-21 08:12:36
Page 1 of 1, showing 1 records out of 1 total, starting on record 1, ending on 1
« previous
next »

Roles

Instance specific permission roles.

« previous next »

Add role

Enter value to search Filter

ID	Default	Name	Site Admin	Admin	Sync	Audit	Auth	Regexp Access	Tagger	Tag Editor	Template	Sharing Group	Delegate	Sighting	Object Template	Galaxy Editor	Decaying	Publish Zmq	Publish Kafka	Memory Limit	Max execution time	Searches / 15 mins	A
1	☐	admin	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	2048M	300 s	Unlimited	
2	☐	Org Admin	✗	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	2048M	300 s	Unlimited	
3	☐	User	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	2048M	300 s	Unlimited	
4	☐	Publisher	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✓	✓	✗	✗	✓	✓	✓	2048M	300 s	Unlimited	
5	☐	Sync user	✗	✗	✓	✗	✓	✗	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	2048M	300 s	Unlimited	
6	☐	Read Only	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	2048M	300 s	Unlimited	

List Taxonomies
Update Taxonomies

Taxonomies

« previous 1 2 3 next »

ID	Namespace	Description	Version	Enabled	Required	Active Tags	Actions
121	workflow	Workflow support language is a common language to support intelligence analysts to perform their analysis on data and information.	10	No		0 / 26	
120	vocabulaire-des-probabilites-estimatives	Ce vocabulaire attribue des valeurs en pourcentage à certains énoncés de probabilité	3	No		0 / 5	
119	veris	Vocabulary for Event Recording and Incident Sharing (VERIS)	2	No		0 / 1992	
118	use-case-applicability	The Use Case Applicability categories reflect standard resolution categories, to clearly display alerting rule configuration problems.	1	No		0 / 8	
117	type	Taxonomy to describe different types of intelligence gathering discipline which can be described the origin of intelligence.	1	No		0 / 11	
116	trust	The Indicator of Trust provides insight about data on what can be trusted and known as a good actor. Similar to a whitelist but on steroids, reusing features one would use with Indicators of Compromise, but to filter out what is known to be good.	1	No		0 / 12	
115	tor	Taxonomy to describe Tor network infrastructure	1	No		0 / 4	
114	tlp	The Traffic Light Protocol - or short: TLP - was designed with the objective to create a favorable classification scheme for sharing sensitive information while keeping the control over its distribution at the same time.	5	No		0 / 5	
113	threats-to-dns	An overview of some of the known attacks related to DNS as described by Torabi, S., Boukhtouta, A., Assi, C., & Debbabi, M. (2018) in Detecting Internet Abuse by Analyzing Passive DNS Traffic: A Survey of Implemented Systems. IEEE Communications Surveys & Tutorials, 1–1. doi:10.1109/comst.2018.2849614	1	No		0 / 18	

List Taxonomies
View Taxonomy
Delete Taxonomy
Update Taxonomies

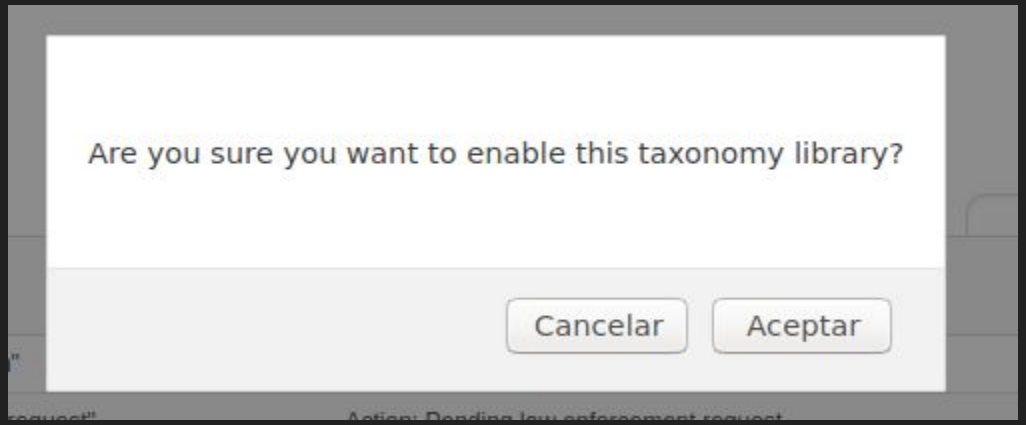
PHISHING Taxonomy Library

Id	95
Namespace	phishing
Description	Taxonomy to classify phishing attacks including techniques, collection mechanisms and analysis status.
Version	4
Enabled	No (enable)

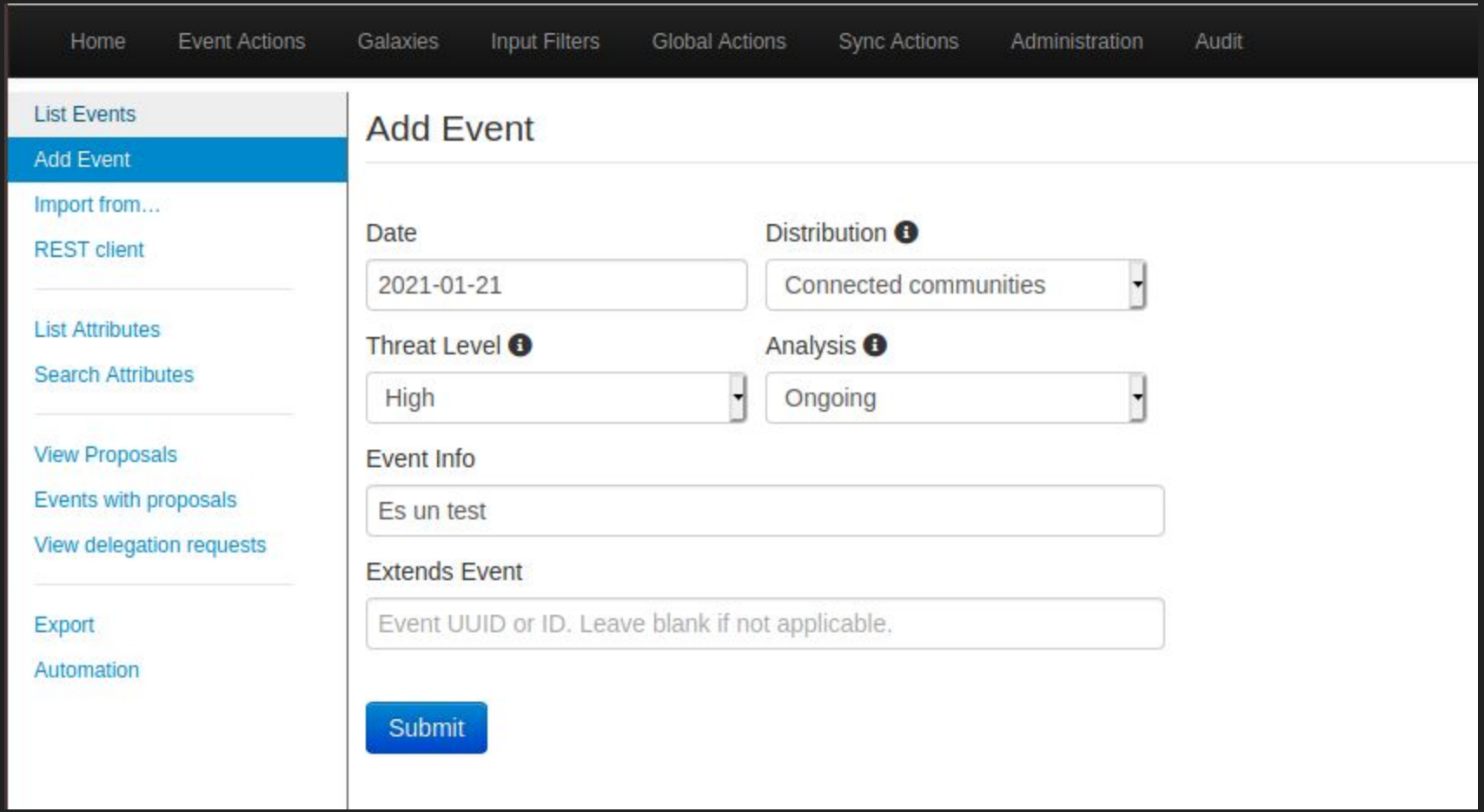
« previous next »

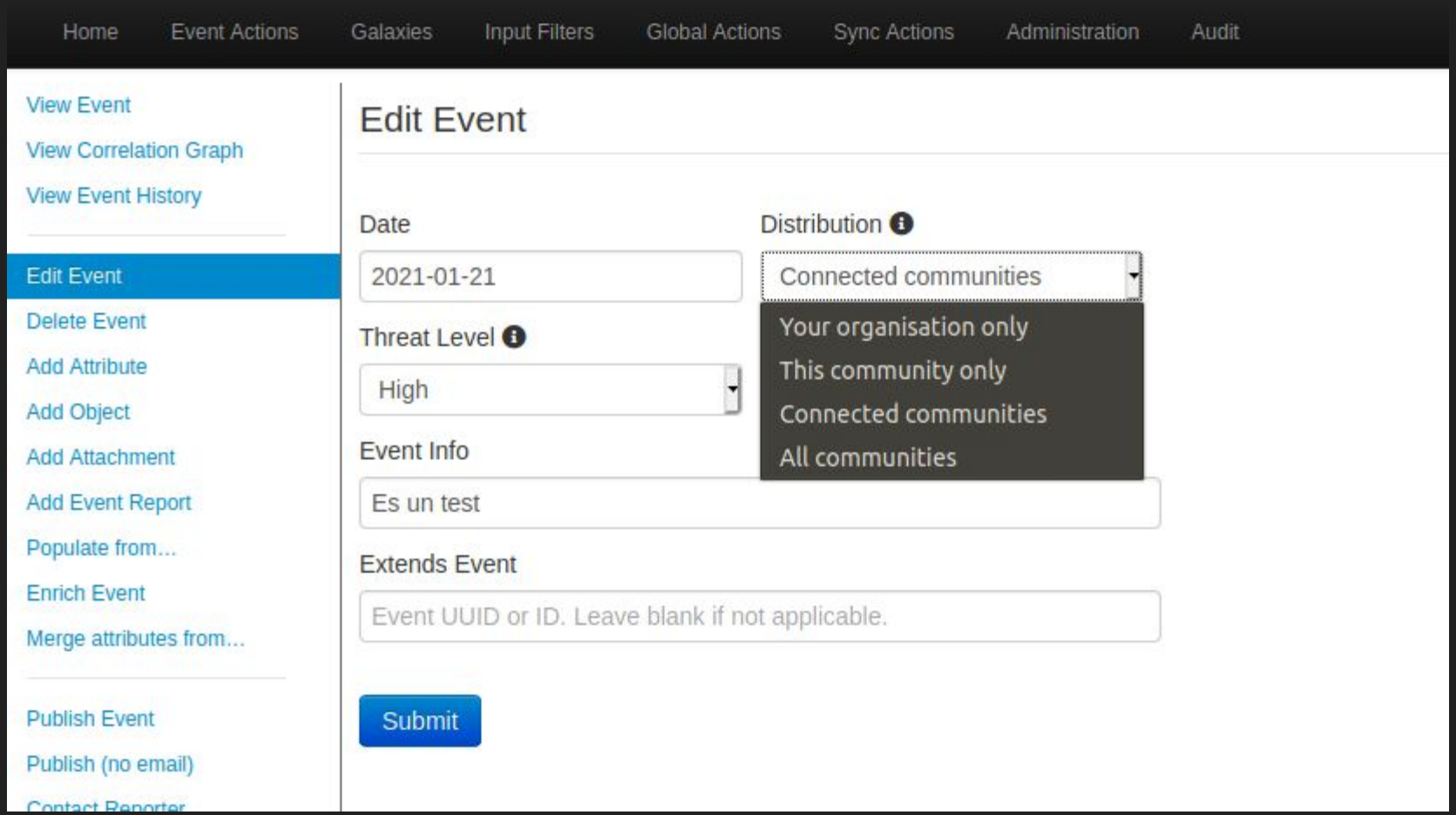
Filter

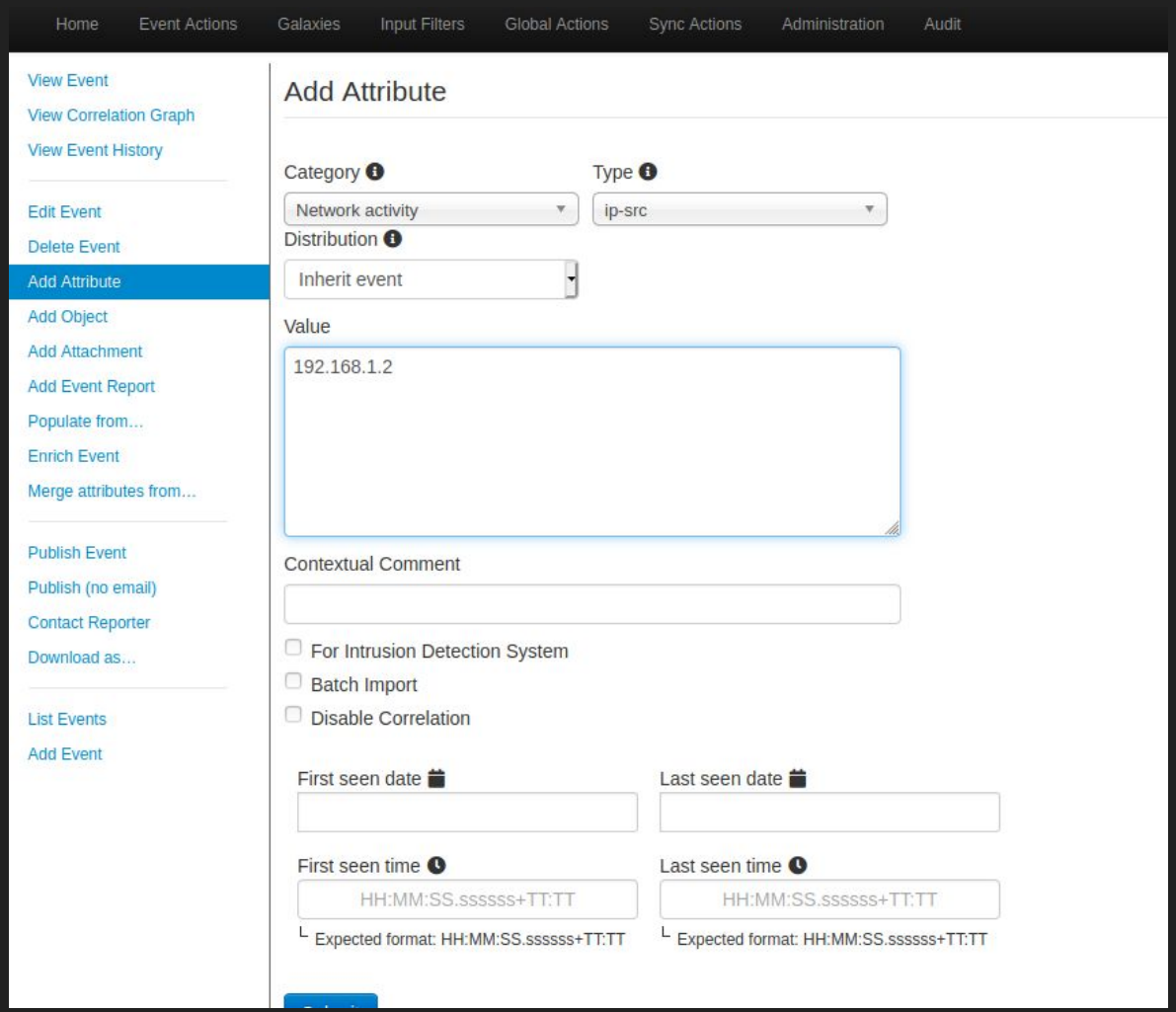
Tag	Expanded	Numerical value	Events	Attributes	Tags	Action
phishing:action="pending-dispute-resolution"	Action: Pending dispute resolution		N/A	N/A		N/A
phishing:action="pending-law-enforcement-request"	Action: Pending law enforcement request		N/A	N/A		N/A
phishing:action="take-down"	Action: Take down		N/A	N/A		N/A
phishing:distribution="bulk-phishing"	Distribution: Bulk phishing		N/A	N/A		N/A
phishing:distribution="spear-phishing"	Distribution: Spear phishing		N/A	N/A		N/A
phishing:distribution="whaling"	Distribution: Whaling phishing		N/A	N/A		N/A
phishing:principle-of-persuasion="authority"	Principle of Persuasion: Society trains people not to question authority so they are conditioned to respond to it. People usually follow an expert or pretense of authority and do a great deal for someone they think is an authority.		N/A	N/A		N/A
phishing:principle-of-persuasion="commitment-reciprocation-consistency"	Principle of Persuasion: People feel more confident in their decision once they commit (publically) to a specific action and need to follow it through until the end. This is true whether in the workplace, or in a situation when their action is illegal. People have tendency to believe what others say and need, and they want to appear consistent in what they do, for instance, when they owe a favour. There is an automatic response of repaying a favour.		N/A	N/A		N/A

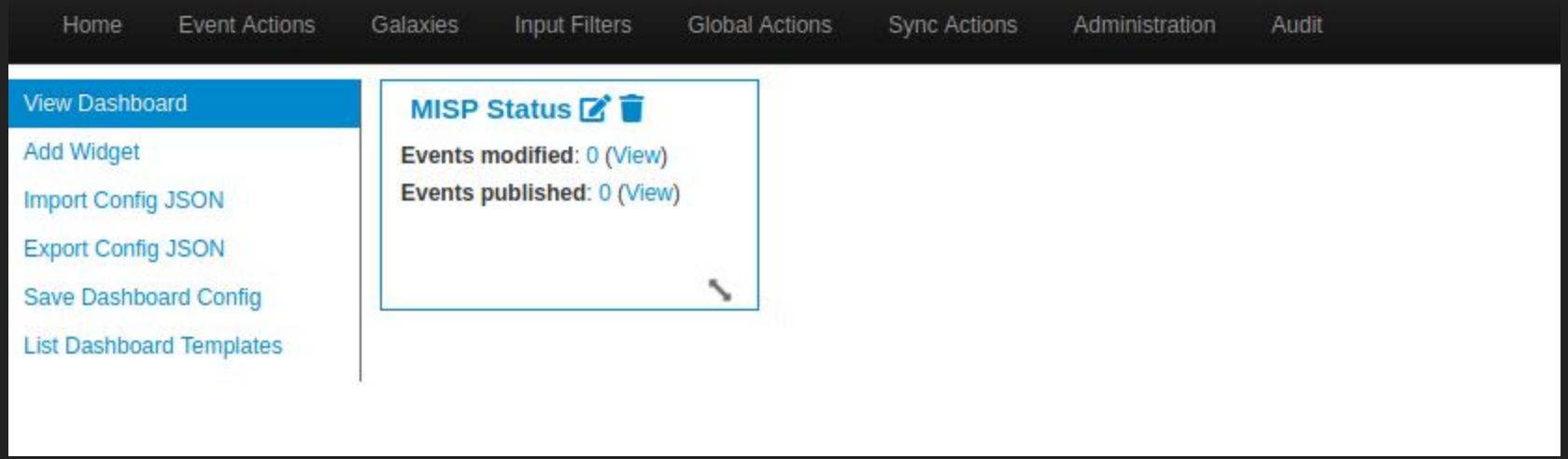


Taxonomy enabled.


Home
Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
List Events
Add Event
Import from…
REST client
List Attributes
Search Attributes
View Proposals
Events with proposals
View delegation requests
Export
Automation
Add Event
Date
2021-01-21
Distribution
Connected communities
Threat Level
High
Analysis
Ongoing
Event Info
Es un test
Extends Event
Event UUID or ID. Leave blank if not applicable.
Submit


Home
Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
View Event
View Correlation Graph
View Event History
Edit Event
Delete Event
Add Attribute
Add Object
Add Attachment
Add Event Report
Populate from...
Enrich Event
Merge attributes from...
Publish Event
Publish (no email)
Contact Reporter
Edit Event
Date
2021-01-21
Distribution
Connected communities
Your organisation only
This community only
Connected communities
All communities
Threat Level
High
Event Info
Es un test
Extends Event
Event UUID or ID. Leave blank if not applicable.
Submit


Home
Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
View Event
View Correlation Graph
View Event History
Edit Event
Delete Event
Add Attribute
Add Object
Add Attachment
Add Event Report
Populate from...
Enrich Event
Merge attributes from...
Publish Event
Publish (no email)
Contact Reporter
Download as...
List Events
Add Event
Add Attribute
Category
Network activity
Type
ip-src
Distribution
Inherit event
Value
192.168.1.2
Contextual Comment
For Intrusion Detection System
Batch Import
Disable Correlation
First seen date
Last seen date
First seen time
Last seen time
HH:MM:SS.ssssss+TT:TT
Expected format: HH:MM:SS.ssssss+TT:TT
Expected format: HH:MM:SS.ssssss+TT:TT


Home
Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
View Dashboard
Add Widget
Import Config JSON
Export Config JSON
Save Dashboard Config
List Dashboard Templates
MISP Status
Events modified: 0 (View)
Events published: 0 (View)

WARNING: This functionality is deprecated and will be removed in the near future. Use the REST client to refine your search conditions and export in any of the given formats with much more control.

Warning, you are logged in as a site admin, any export that you generate will contain the FULL UNRESTRICTED data-set. If you would like to generate an export for your own organisation, please log in with a different user.

List Events
Add Event
Import from…
REST client

List Attributes
Search Attributes

View Proposals
Events with proposals
View delegation requests

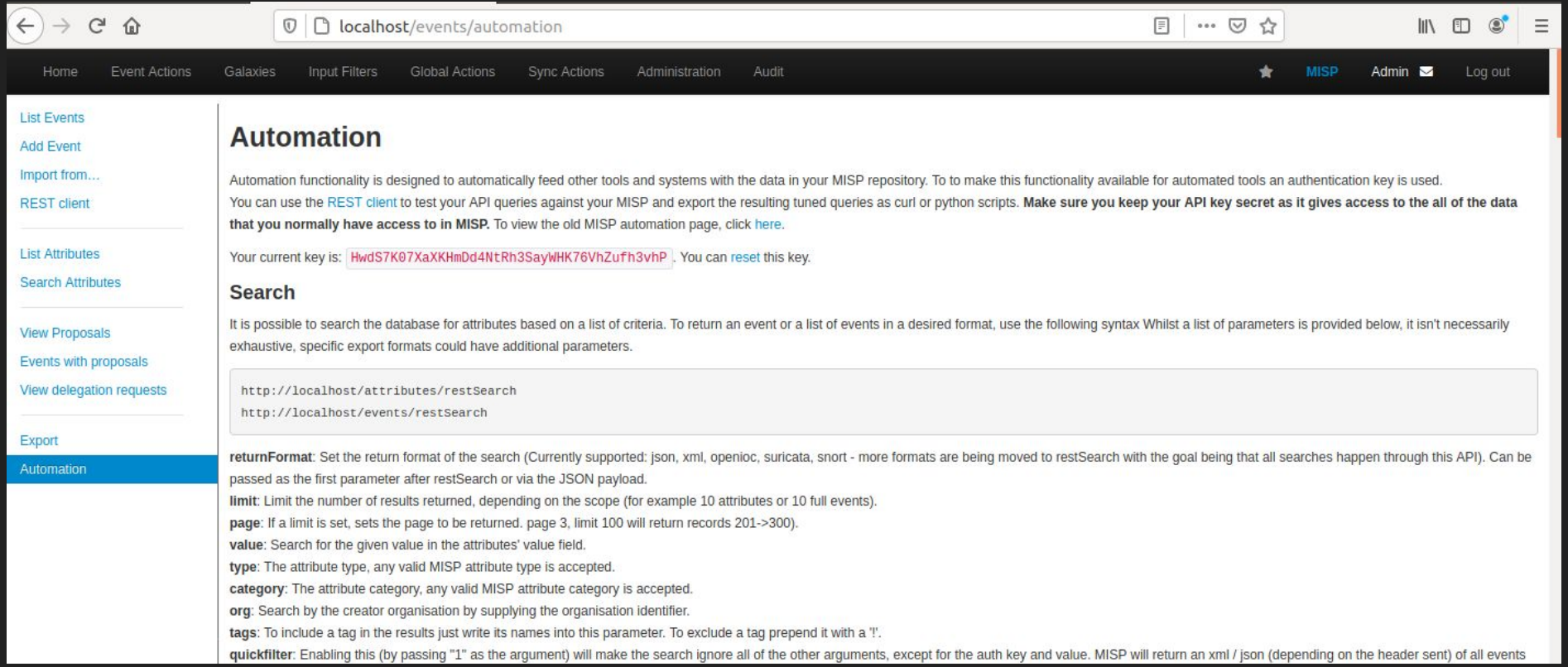
Export
Automation

Export

Export functionality is designed to automatically generate signatures for intrusion detection systems. To enable signature generation for a given attribute, Signature field of this attribute must be set to Yes. Note that not all attribute types are applicable for signature generation, currently we only support NIDS signature generation for IP, domains, host names, user agents etc., and hash list generation for MD5/SHA1 values of file artifacts. Support for more attribute types is planned.

Simply click on any of the following buttons to download the appropriate data.

Type	Last Update	Description	Outdated	Filesize	Progress	Actions
JSON	N/A	Click this to download all events and attributes that you have access to in MISP JSON format. Attachments are enabled on this instance.	Yes	N/A	N/A	Download Generate
XML	N/A	Click this to download all events and attributes that you have access to in MISP XML format. Attachments are enabled on this instance.	Yes	N/A	N/A	Download Generate
CSV_Sig	No valid events	Click this to download all attributes that are indicators and that you have access to (except file attachments) in CSV format.	No	N/A	Queued	Download Generate


localhost/events/automation
Home
Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
MISP
Admin
Log out
List Events
Add Event
Import from…
REST client
List Attributes
Search Attributes
View Proposals
Events with proposals
View delegation requests
Export
Automation
Automation
Automation functionality is designed to automatically feed other tools and systems with the data in your MISP repository. To to make this functionality available for automated tools an authentication key is used.
You can use the REST client to test your API queries against your MISP and export the resulting tuned queries as curl or python scripts. Make sure you keep your API key secret as it gives access to the all of the data that you normally have access to in MISP. To view the old MISP automation page, click here.
Your current key is: HwdS7K07XaXKHmDd4NtRh3SayWHK76VhZufh3vhP . You can reset this key.
Search
It is possible to search the database for attributes based on a list of criteria. To return an event or a list of events in a desired format, use the following syntax Whilst a list of parameters is provided below, it isn't necessarily exhaustive, specific export formats could have additional parameters.
http://localhost/attributes/restSearch
http://localhost/events/restSearch
returnFormat: Set the return format of the search (Currently supported: json, xml, openioc, suricata, snort - more formats are being moved to restSearch with the goal being that all searches happen through this API). Can be passed as the first parameter after restSearch or via the JSON payload.
limit: Limit the number of results returned, depending on the scope (for example 10 attributes or 10 full events).
page: If a limit is set, sets the page to be returned. page 3, limit 100 will return records 201->300).
value: Search for the given value in the attributes' value field.
type: The attribute type, any valid MISP attribute type is accepted.
category: The attribute category, any valid MISP attribute category is accepted.
org: Search by the creator organisation by supplying the organisation identifier.
tags: To include a tag in the results just write its names into this parameter. To exclude a tag prepend it with a '!'.
quickfilter: Enabling this (by passing "1" as the argument) will make the search ignore all of the other arguments, except for the auth key and value. MISP will return an xml / json (depending on the header sent) of all events

API MISP i REST

MISP inclou una potent API REST que us permet automatitzar la difusió de la intel·ligència i les dades sobre les amenaces. Si no esteu familiaritzat amb l'API, podeu explorar-ne les funcions (i la documentació en línia) mitjançant Event Actions, client REST.

A les últimes versions de MISP, el client de l'API REST admet l'autocompleció.

PyMISP és una biblioteca Python per accedir a plataformes MISP mitjançant la seva API REST PyMISP permet obtenir esdeveniments, afegir o actualitzar esdeveniments / atributs, afegir o actualitzar mostres o buscar atributs.

Les etiquetes són els vocabularis que fem servir per classificar esdeveniments i atributs.

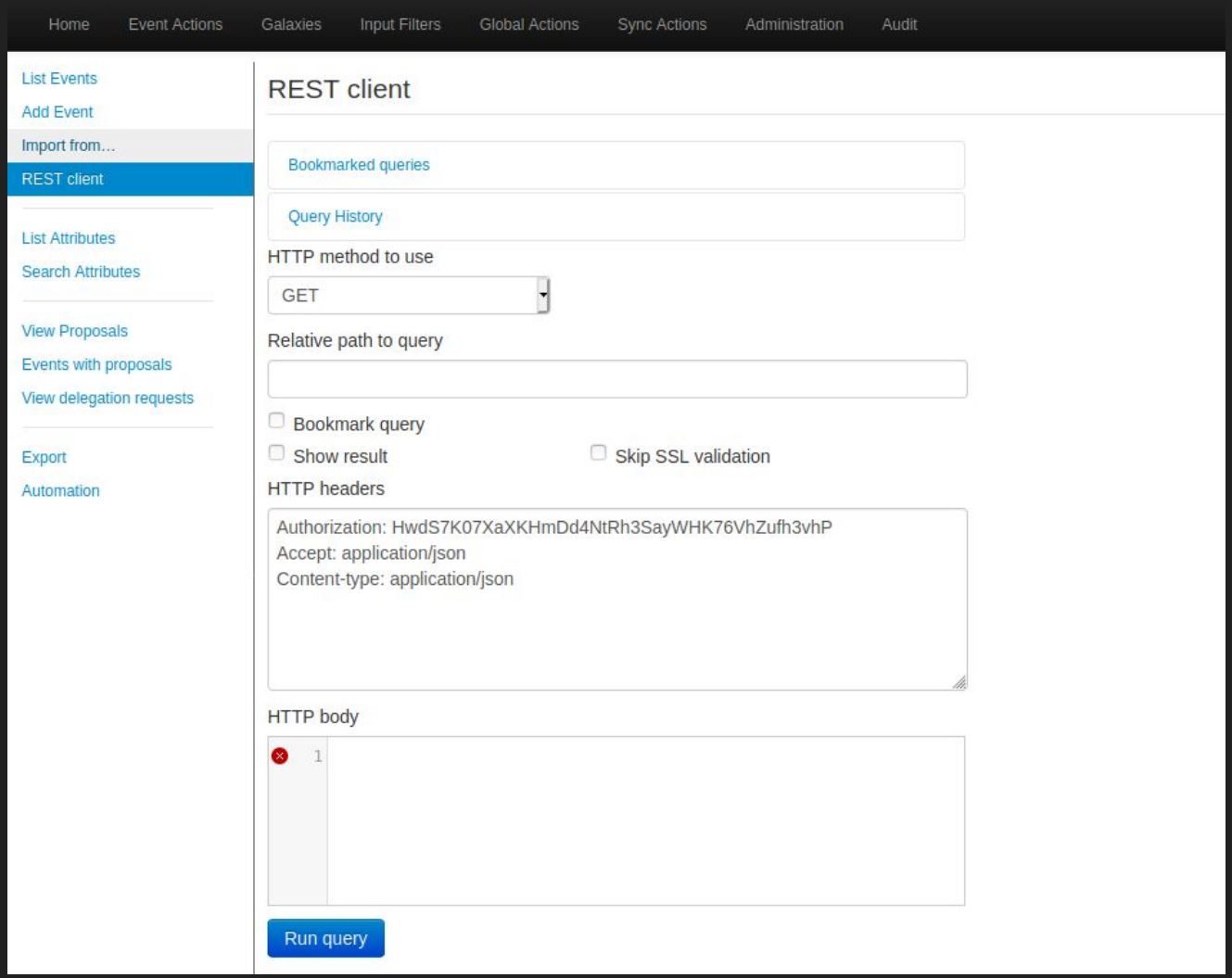
API CLIENT REST

```
curl -k \
 -d '{"returnFormat":"csv","tags":"rsit:fraud=\"phishing\""}' \
 -H "Authorization: API-KEY" \
 -H "Accept: application/json" \
 -H "Content-type: application/json" \
 -X POST https://MISP-URL/attributes/restSearch
```

```
YOUR_MISP_URL/attributes/restSearch
YOUR_MISP_URL/events/restSearch
```

```
curl -i -H "Accept: application/json" -H "content-type: application/json" -H "Authorization: YOUR
```


```
{"Event":{"date":"2015-01-01","threat_level_id":"1","info":"testevent","published":false,"analysis
```


Home
Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
List Events
Add Event
Import from…
REST client
List Attributes
Search Attributes
View Proposals
Events with proposals
View delegation requests
Export
Automation
REST client
Bookmarked queries
Query History
HTTP method to use
GET
Relative path to query
Bookmark query
Show result
Skip SSL validation
HTTP headers
Authorization: HwdS7K07XaXKHmDd4NtRh3SayWHK76VhZufh3vhP
Accept: application/json
Content-type: application/json
HTTP body
1
Run query

List Events
Add Event
Import from…
REST client

List Attributes
Search Attributes

View Proposals
Events with proposals
View delegation requests

Export
Automation

Automation

Automation functionality is designed to automatically feed other tools and systems with the data in your MISP repository. To to n
You can use the REST client to test your API queries against your MISP and export the resulting tuned queries as curl or pythor
that you normally have access to in MISP. To view the old MISP automation page, click here.

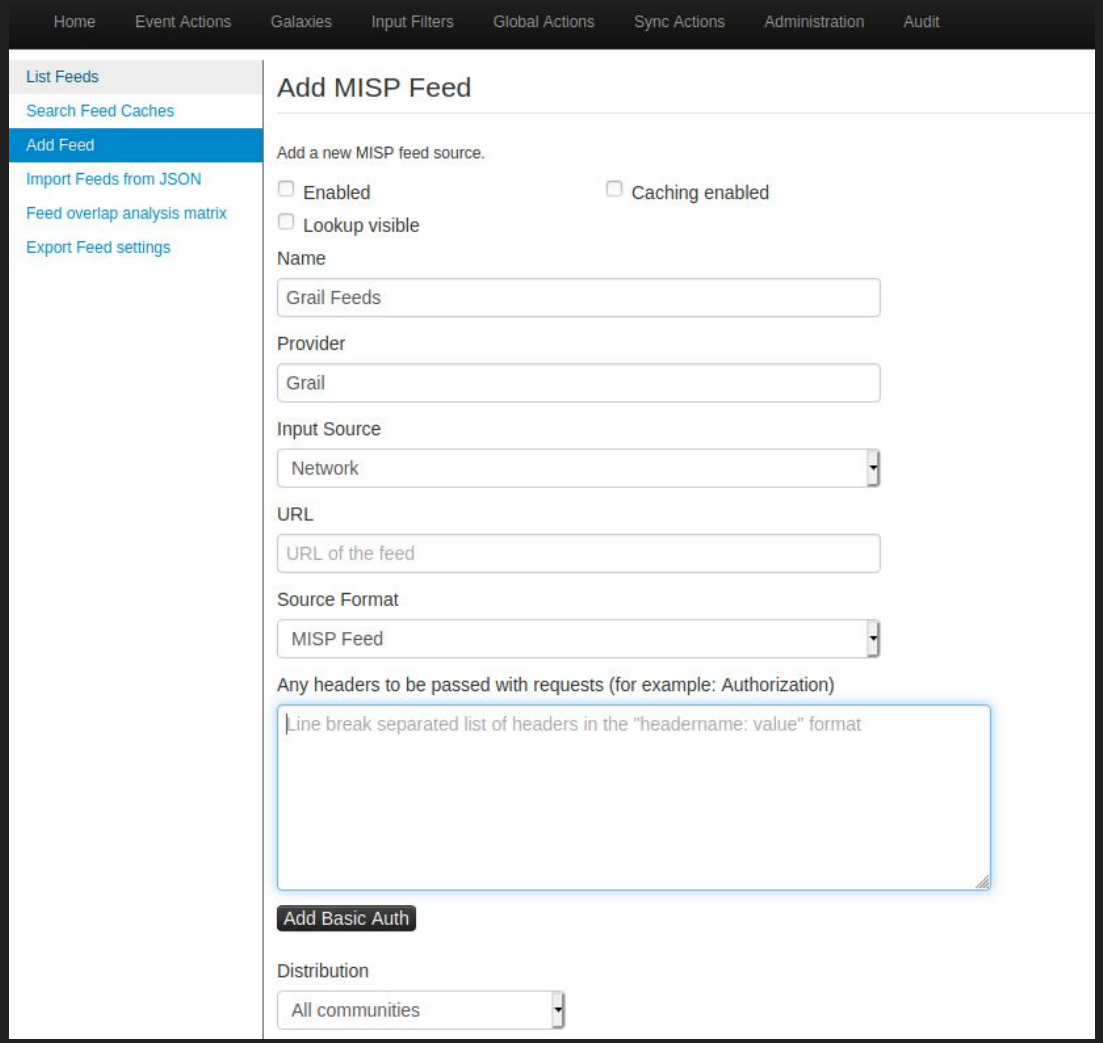
Your current key is: `HwdS7K07XaXKHmDd4NtRh3SayWHK76VhZufh3vhP`. You can reset this key.

Search

It is possible to search the database for attributes based on a list of criteria. To return an event or a list of events in a desired for
exhaustive, specific export formats could have additional parameters.

```
http://localhost/attributes/restSearch
http://localhost/events/restSearch
```

returnFormat: Set the return format of the search (Currently supported: json, xml, openioc, suricata, snort - more formats are b
passed as the first parameter after restSearch or via the JSON payload.


Home
Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
List Feeds
Search Feed Caches
Add Feed
Import Feeds from JSON
Feed overlap analysis matrix
Export Feed settings
Add MISP Feed
Add a new MISP feed source.
Enabled
Caching enabled
Lookup visible
Name
Grail Feeds
Provider
Grail
Input Source
Network
URL
URL of the feed
Source Format
MISP Feed
Any headers to be passed with requests (for example: Authorization)
Line break separated list of headers in the "headername: value" format
Add Basic Auth
Distribution
All communities

Feeds

Generate feed lookup caches or fetch feed data (enabled feeds only)

Load default feed metadata | Cache all feeds | Cache freetext/CSV feeds | Cache MISP feeds | Fetch and store all feed data

« previous | next »

Default feeds | Custom feeds | All feeds | Enabled feeds

Enter value to search | Filter

Id	Enabled	Caching	Name	Format	Provider	Org	Source	URL	Headers	Target	Publish	Delta	Override	Distribution	Tag	Visible	Caching	Actions
1	✗	✗	CIRCL OSINT Feed	misp	CIRCL		network	https://www.circl.lu/doc/misp/feed-osint		Feed not enabled	✗	✗	✗	All communities		✗	Not cached	
2	✗	✗	The Botvrij.eu Data	misp	Botvrij.eu		network	https://www.botvrij.eu/data/feed-osint		Feed not enabled	✗	✗	✗	All communities		✗	Not cached	

Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2

« previous | next »

Create Sync Config
List Servers
New Servers
List Communities

List Cerebrates

Add Server

Instance identification

Base URL

Instance name

Instance ownership and credentials

Information about the organisation that will receive the events, typically the remote instance's host organisation.

Organisation Type: Local organisation

Local Organisation: ORGNAME

Ask the owner of the remote instance for a sync account on their instance, log into their MISP using the sync user's credentials and retrieve your API key by navigating to Global actions -> My profile. This key is used to authenticate with the remote instance.

Authkey

Leave empty to use current key

Enabled synchronisation methods

- [ ] Push
- [ ] Pull
- [ ] Push Sightings
- [ ] Caching Enabled
- [ ] Push Galaxy Clusters
- [ ] Pull Galaxy Clusters

Misc settings

- [ ] Unpublish Event
- [ ] Publish Without Email

Create Sync Config
List Servers
New Servers
List Communities

List Cerebrates

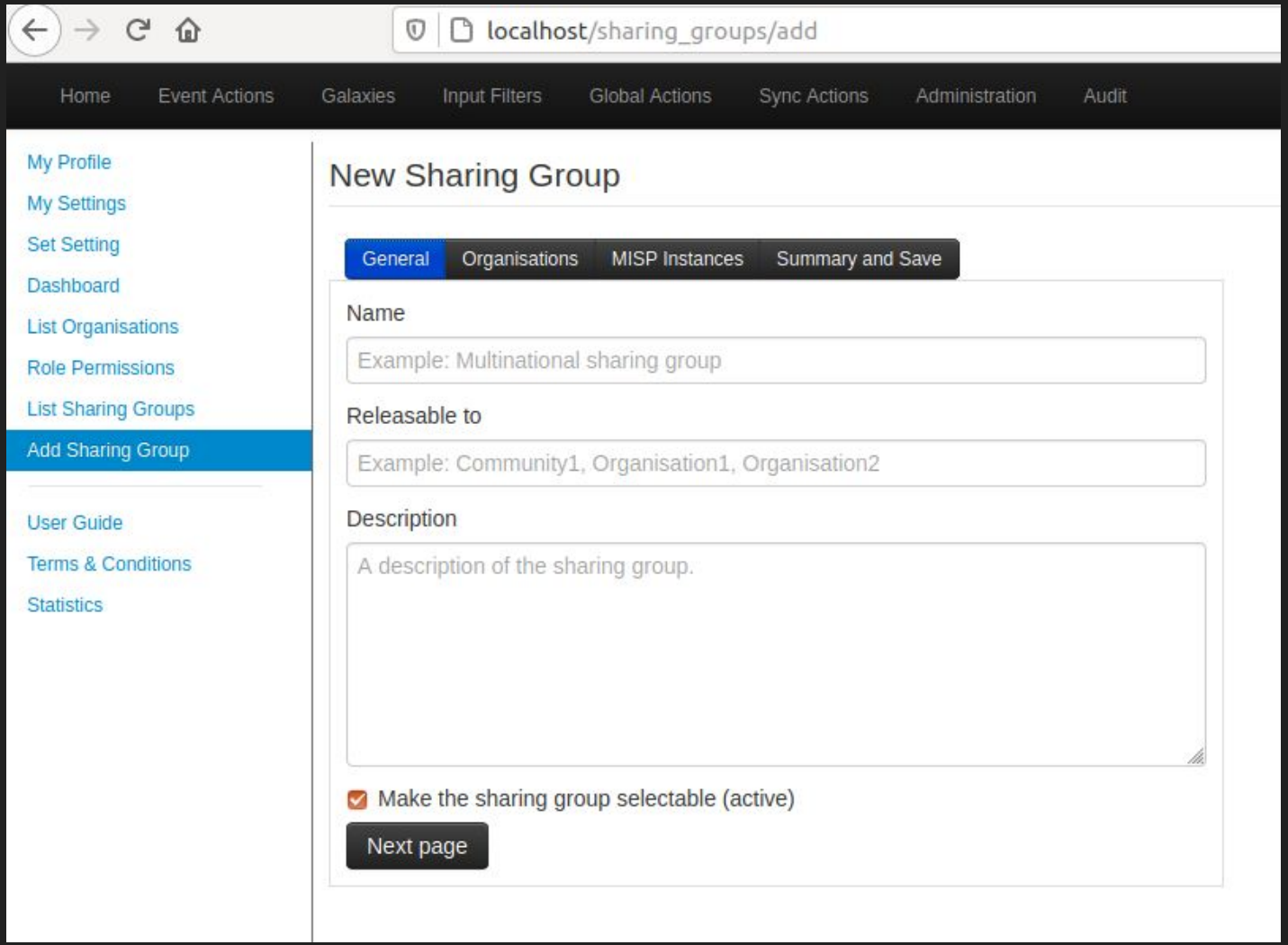
Servers

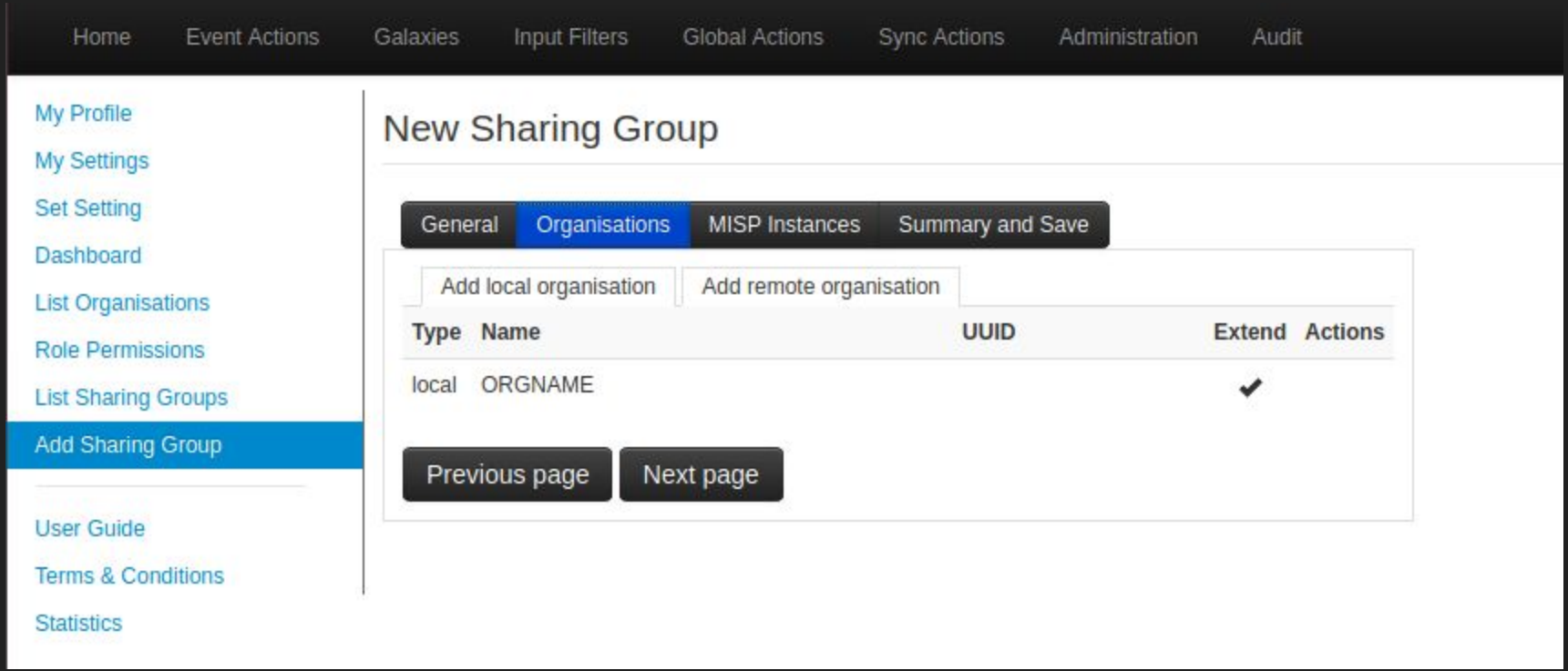
« previous next »

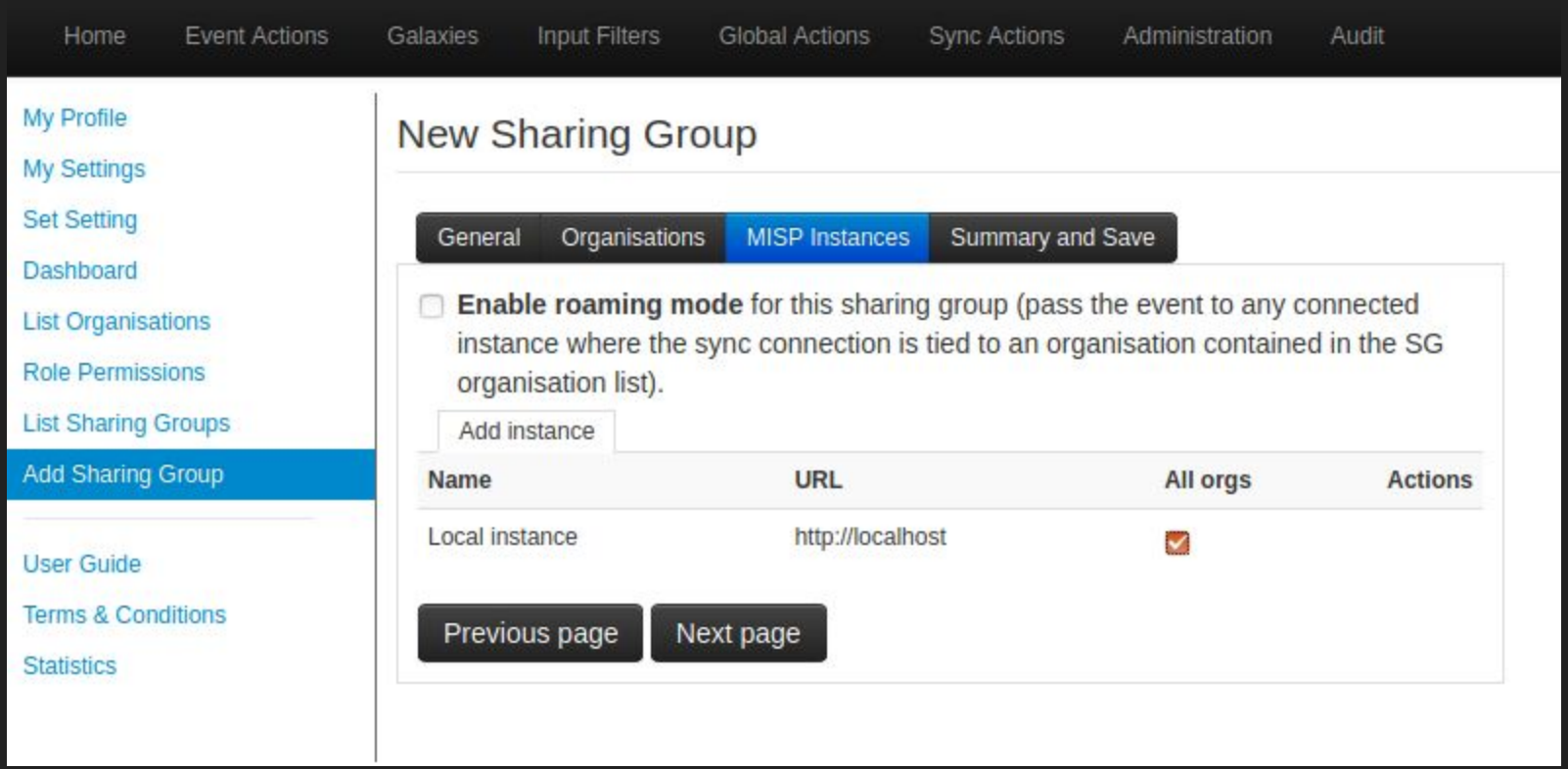
Id	Name	Prio	Connection test	Sync user	Reset API key	Internal	Push	Pull	Push Sightings	Push Clusters	Pull Clusters	Cache	Unpublish Event (push Event)	Publish Without Email (pull Event)	Url	Remote Organisation	Cert File	Client Cert File	Self Signed	Skip Proxy	Org	Actions

Page 1 of 1, showing 0 records out of 0 total, starting on record 0, ending on 0

« previous next »


localhost/sharing_groups/add
Home
Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
My Profile
My Settings
Set Setting
Dashboard
List Organisations
Role Permissions
List Sharing Groups
Add Sharing Group
User Guide
Terms & Conditions
Statistics
New Sharing Group
General
Organisations
MISP Instances
Summary and Save
Name
Example: Multinational sharing group
Releasable to
Example: Community1, Organisation1, Organisation2
Description
A description of the sharing group.
Make the sharing group selectable (active)
Next page


Home
Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
My Profile
My Settings
Set Setting
Dashboard
List Organisations
Role Permissions
List Sharing Groups
Add Sharing Group
User Guide
Terms & Conditions
Statistics
New Sharing Group
General
Organisations
MISP Instances
Summary and Save
Add local organisation
Add remote organisation
Type
Name
UUID
Extend
Actions
local
ORGNAME
Previous page
Next page


Home
Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
My Profile
My Settings
Set Setting
Dashboard
List Organisations
Role Permissions
List Sharing Groups
Add Sharing Group
User Guide
Terms & Conditions
Statistics
New Sharing Group
General
Organisations
MISP Instances
Summary and Save
Enable roaming mode for this sharing group (pass the event to any connected instance where the sync connection is tied to an organisation contained in the SG organisation list).
Add instance
Name
URL
All orgs
Actions
Local instance
http://localhost
Previous page
Next page

Create Sync Config
List Servers
New Servers
List Communities

List Cerebrates

Communities index

You can find a list of communities below that chose to advertise their existence to the general MISP user-base. Requesting access to any of those communities is of course no guarantee of being per
meant to simplify the means of finding the various communities that one may be eligible for. Get in touch with the MISP project maintainers if you would like your community to be included in the list.

« previous | next »

Vetted by the MISP-project team | Unvetted

Enter value to search

Id	Vetted	Host org	Community name	Description
1	✔		CIRCL Private Sector Information Sharing Community - aka MISPPRIV	CIRCL operates a fairly large MISP sharing community (more than 1100 international organizations are members) mainly targeting private organizations, companies, financial organizations or IT security companies. Computer Incident Response Center Luxembourg (CIRCL) operates this sharing community for the benefit of the security community at large.
2	✔		CIRCL n/g CSIRT information sharing community - aka MISP	CIRCL operates an information sharing dedicated to national/governmental CSIRTs/CERTs with national responsibilities in the EEA (European Economic Area).
3	✔		CIRCL financial information sharing community - aka Financial Sector MISP sharing groups	CIRCL operates an information sharing dedicated to the financial sector.
4	✔	X-ISAC	X-ISAC sharing community	X-ISAC (pronounced cross-ISAC) is the supporting Information Sharing and Analysis Center for other ISACs, information sharing communities or CSIRT networks which provides core software, cross-sector threat intelligence, taxonomies and open standards.
5	✔	eCrimeLabs	Danish MISP Community	The Danish MISP User group/Community operates as an informaiton sharing dedicated to Danish organisations
6	✔	Cogsec Collab	Cognitive Security Collaborative	The Cognitive Security Collaborative operates as a sharing community dedicated to information operations.
7	✔		COVID-19 MISP community	A community for tracking both health and cyber threat related information around COVID-19.
8	✔	PISAX.org	PISAX - pan-European Information Sharing and Analysis Center (ISAC) to IXPs and GRXs	The Action's overall objective is to create a common pan-

Create Sync Config
List Servers
New Servers
List Communities
Request Access
View community

List Cerebrates

Community COVID-19 MISP community

Id	7
UUID	5e59659e-8e24-4e5d-b3fa-2ba744b7dd05
Name	COVID-19 MISP community
Url	https://covid-19.iglocska.eu
Host organisation	CIRCL (55f6e5ae-2c60-40e5-964f-47a8950d210f)
Vetted by MISP-project	Yes
Type	Open topical community
Description	A community for tracking both health and cyber threat related information around COVID-19.
Email	info@circl.lu
Sector	undefined
Nationality	International
GnuPG key	▸ Detalles

Request Access

Add User
List Users
Pending registrations
User settings
Set Setting
Contact Users

Add Organisation
List Organisations

Add Role
List Roles

Server Settings & Maintenance
Update Progress

Jobs

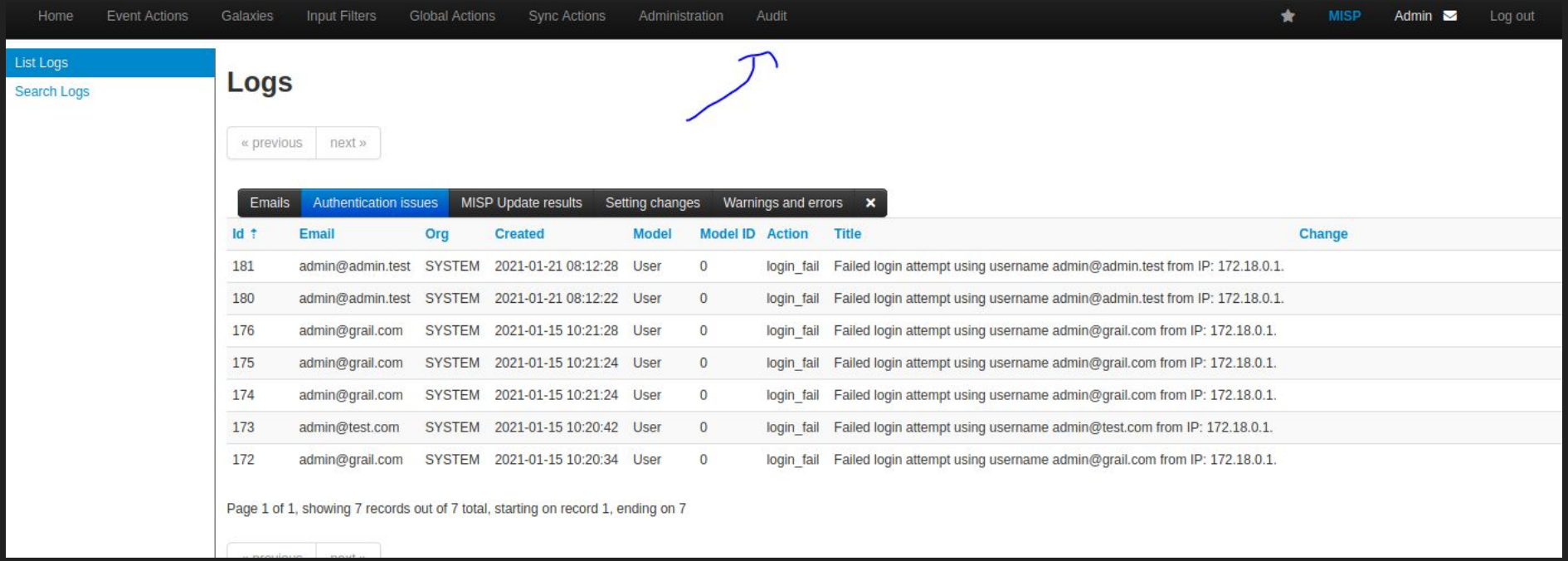
Scheduled Tasks
Event Block Rules
Blocklists Event
Manage Event Blocklists
Blocklists Organisation
Manage Org Blocklists

Server Settings & Maintenance

Overview | MISP settings (46 ⚠) | Encryption settings (8 ⚠) | Proxy settings (5) | Security settings (6 ⚠) | Plugin settings (89 ⚠) | Diagnostics | Manage files | Workers

Filter the table(s) below

Priority	Setting	Value	Description	Error Message
Critical	MISP.baseurl	http://localhost	The base url of the application (in the format https://www.mymispinstance.com or https://myserver.com/misp). Several features depend on this setting being correctly set to function.	The currenty set baseurl does not match the URL through which you have accessed the page. Disregard this if you are accessing the page via an alternate URL (for example via IP address).
Critical	MISP.external_baseurl		The base url of the application (in the format https://www.mymispinstance.com) as visible externally/by other MISPs. MISP will encode this URL in sharing groups when including itself. If this value is not set, the baseurl is used as a fallback.	Value not set.
Critical	MISP.live	true	Unless set to true, the instance will only be accessible by site admins.	
Critical	MISP.language	eng	Select the language MISP should use. The default is english.	Value not set.
Critical	MISP.enable_advanced_correlations	false	Enable some performance heavy correlations (currently CIDR correlation)	
Critical	MISP.host_org_id	No organisation selected.	The hosting organisation of this instance. If this is not selected then replication instances cannot be added.	Value not set.
Critical	MISP.uuid	11146c43-acec-46a7-ba2d-5b5fc3712713	The MISP instance UUID. This UUID is used to identify this instance.	No valid UUID set
Critical	MISP.showorg	true	Setting this setting to 'false' will hide all organisation names / logos.	
Critical	MISP.osuser	www-data	The Unix user MISP (php) is running as	


Home
Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
MISP
Admin
Log out
List Logs
Search Logs
Logs
« previous
next »
Emails
Authentication issues
MISP Update results
Setting changes
Warnings and errors
Id
Email
Org
Created
Model
Model ID
Action
Title
Change
181 admin@admin.test SYSTEM 2021-01-21 08:12:28 User 0 login_fail Failed login attempt using username admin@admin.test from IP: 172.18.0.1.
180 admin@admin.test SYSTEM 2021-01-21 08:12:22 User 0 login_fail Failed login attempt using username admin@admin.test from IP: 172.18.0.1.
176 admin@grail.com SYSTEM 2021-01-15 10:21:28 User 0 login_fail Failed login attempt using username admin@grail.com from IP: 172.18.0.1.
175 admin@grail.com SYSTEM 2021-01-15 10:21:24 User 0 login_fail Failed login attempt using username admin@grail.com from IP: 172.18.0.1.
174 admin@grail.com SYSTEM 2021-01-15 10:21:24 User 0 login_fail Failed login attempt using username admin@grail.com from IP: 172.18.0.1.
173 admin@test.com SYSTEM 2021-01-15 10:20:42 User 0 login_fail Failed login attempt using username admin@test.com from IP: 172.18.0.1.
172 admin@grail.com SYSTEM 2021-01-15 10:20:34 User 0 login_fail Failed login attempt using username admin@grail.com from IP: 172.18.0.1.
Page 1 of 1, showing 7 records out of 7 total, starting on record 1, ending on 7

Integració MISP a TheHive

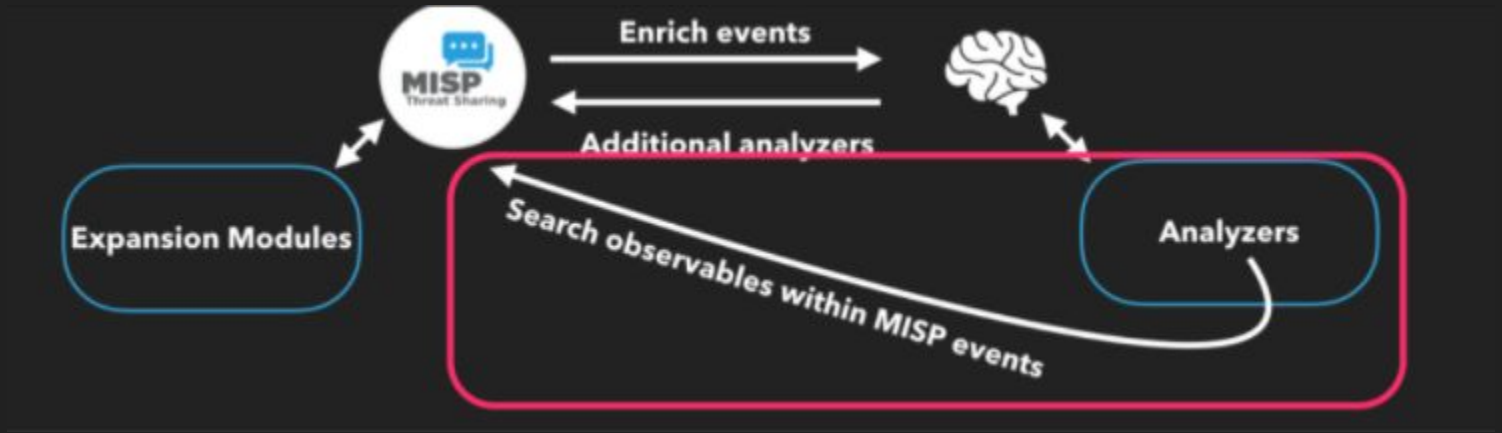
```
## Enable the MISP module (import and export)
play.modules.enabled += connectors.misp.MispConnector

misp {
  "MISP-SERVER-ID" {
    # URL of the MISP instance.
    url = "<The_URL_of_the_MISP_Server_goes_here>"

    # Authentication key.
    key = "<the_auth_key_goes_here>"

    # Name of the case template created in TheHive that shall be used to import
    # MISP events as cases by default.
    caseTemplate = "<Template_Name_goes_here>"

    # Tags to add to each observable imported from an event available on
    # this instance.
    tags = ["misp-server-id"]

    # Truststore to use to validate the X.509 certificate  of  the  MISP
    # instance if the default truststore is not sufficient.
    #ws.ssl.trustManager.stores = [
    #{
    #  type: "JKS"
    #  path: "/path/to/truststore.jks"
    #}
    #]

    # HTTP client configuration, more details in section 8
    # ws {
    #   proxy {}
    #   ssl {}
    # }

    # filters:
    max-attributes = 1000
```

Mòduls d'expansió MISP

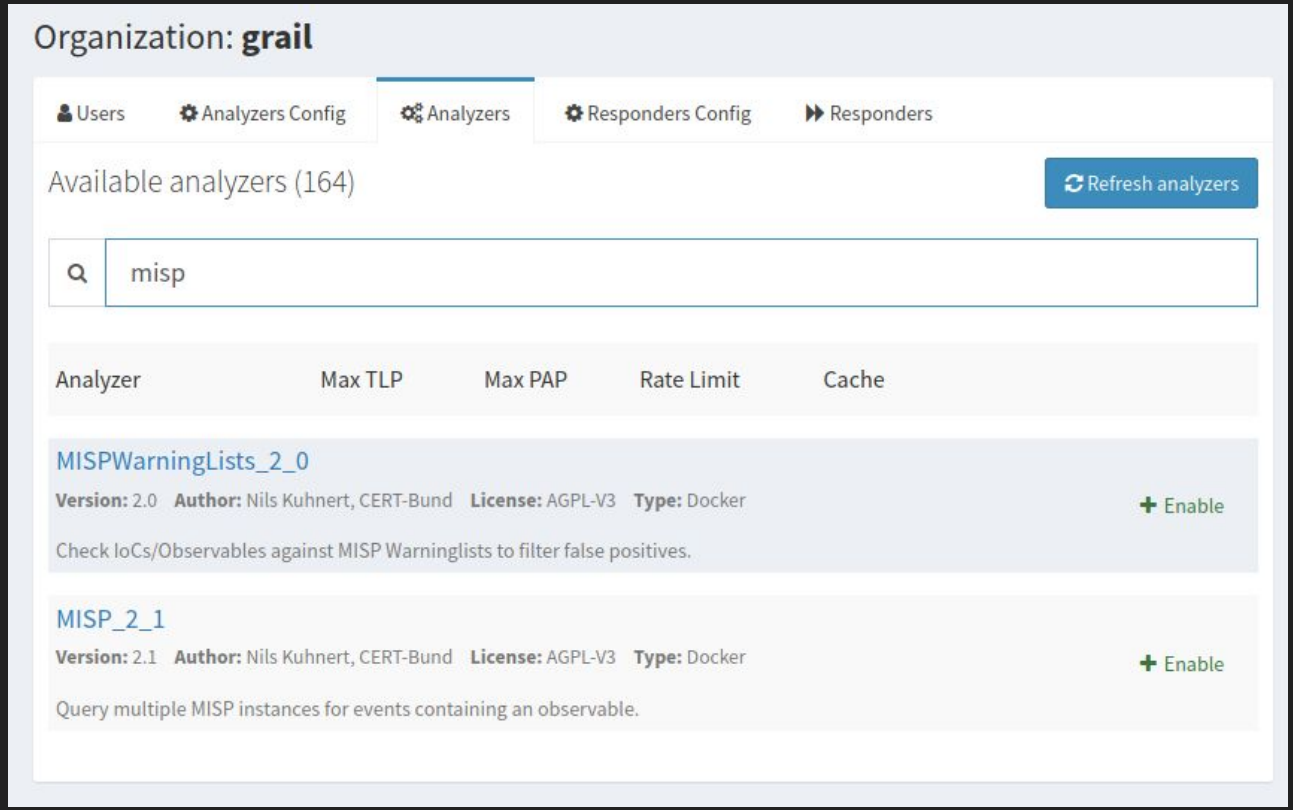
Cortex també pot invocar mòduls d'expansió MISP. MISP els fa servir normalment per enriquir els atributs dins dels esdeveniments, però Cortex també pot aprofitar-los per analitzar observables.

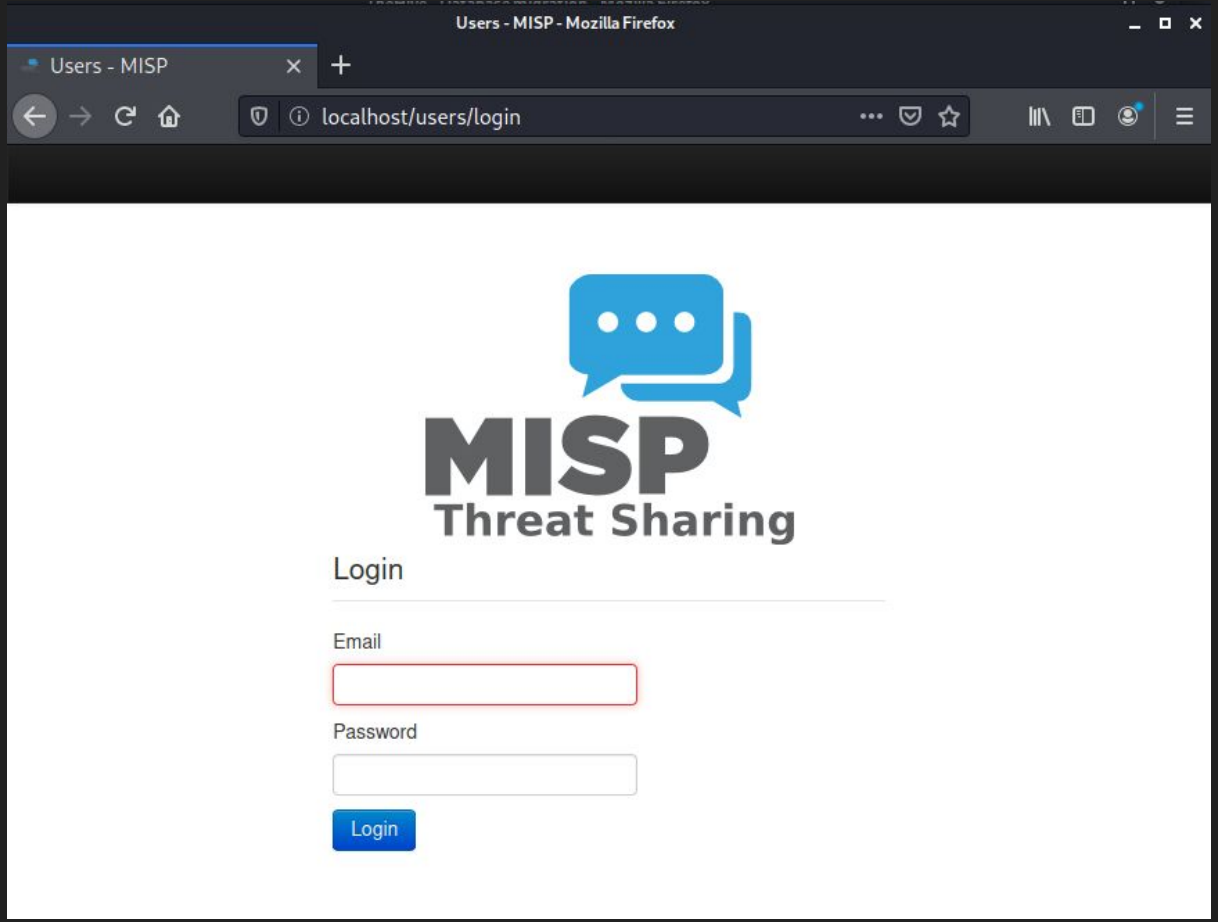
Analitzador especial de MISP

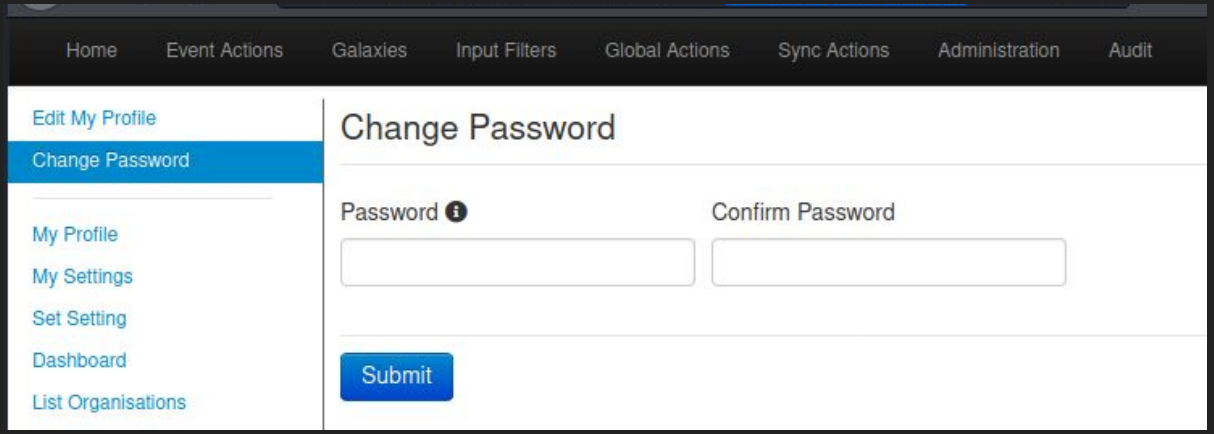
Gràcies a ell, Cortex pot cercar observables dins d'una instància de MISP.

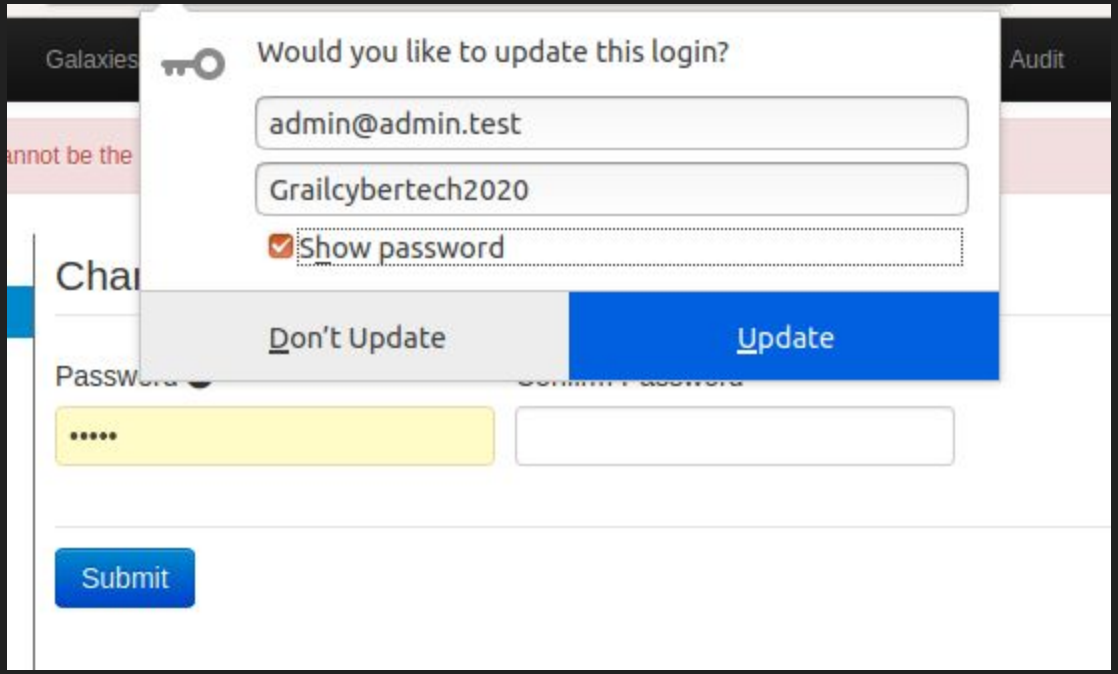


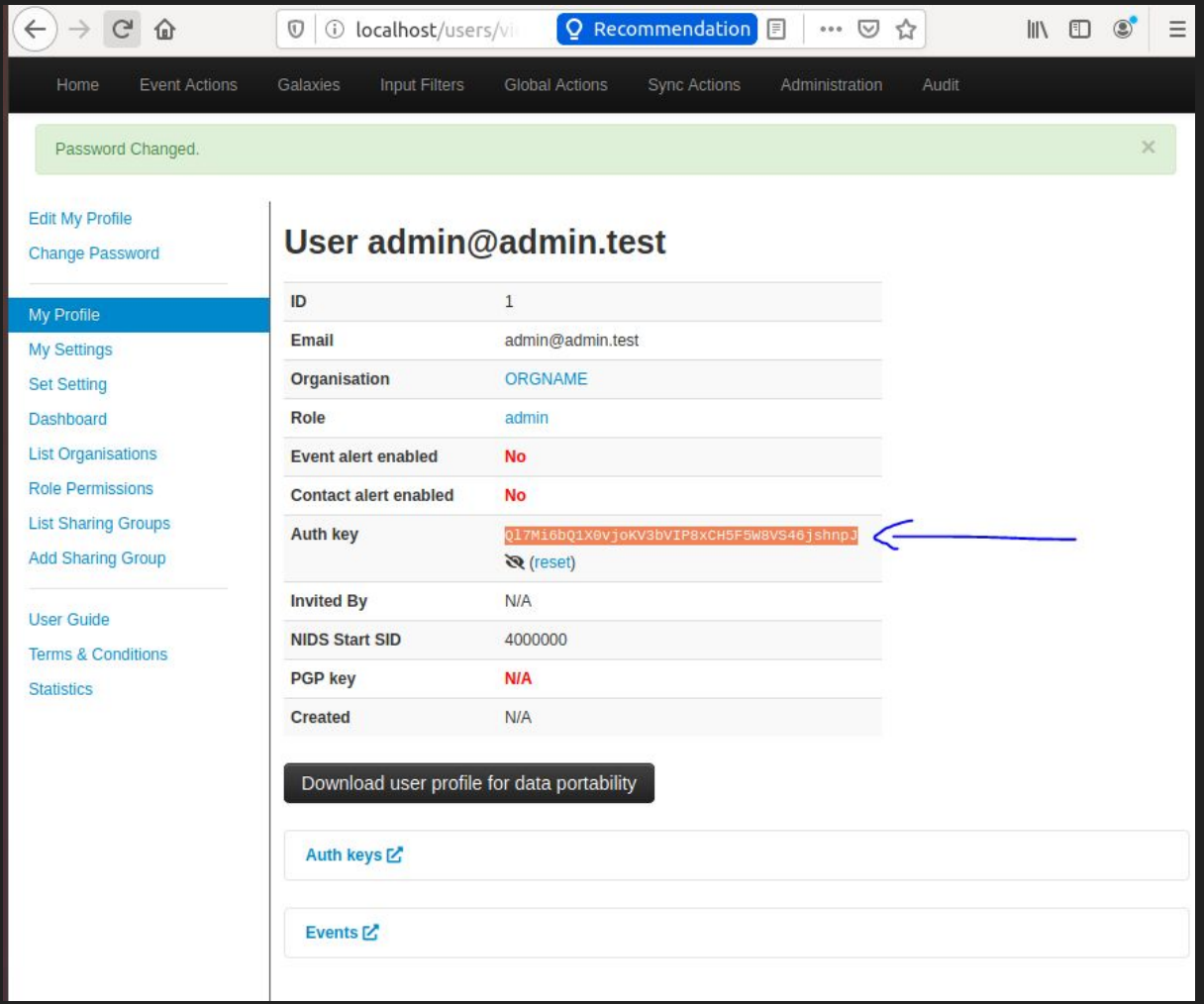
Analitzador MISP




Users - MISP - Mozilla Firefox
Users - MISP
localhost/users/login
MISP
Threat Sharing
Login
Email
Password
Login


Home
Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
Edit My Profile
Change Password
My Profile
My Settings
Set Setting
Dashboard
List Organisations
Change Password
Password
Confirm Password
Submit


Galaxies
Audit
annot be the
Would you like to update this login?
admin@admin.test
Grailcybertech2020
Show password
Don't Update
Update
Submit


localhost/users/vi
Recommendation
Home
Event Actions
Galaxies
Input Filters
Global Actions
Sync Actions
Administration
Audit
Password Changed.
Edit My Profile
Change Password
My Profile
My Settings
Set Setting
Dashboard
List Organisations
Role Permissions
List Sharing Groups
Add Sharing Group
User Guide
Terms & Conditions
Statistics
User admin@admin.test
ID 1
Email admin@admin.test
Organisation ORGNAME
Role admin
Event alert enabled No
Contact alert enabled No
Auth key Ql7Mi6bQ1X0vjoKV3bVIP8xCH5F5W8VS46jshnpJ
(reset)
Invited By N/A
NIDS Start SID 4000000
PGP key N/A
Created N/A
Download user profile for data portability
Auth keys
Events

Enable analyzer MISP_2_1

Base details

Name MISP_2_1

Configuration

Apply defaults

name

Add option

1.

Name of MISP servers

url *

Add option

1. localhost

URL of MISP servers

key *

Add option

1. [redacted]

API key for each server

cert_check *

True | False

Verify server certificate

cert_path

Add option

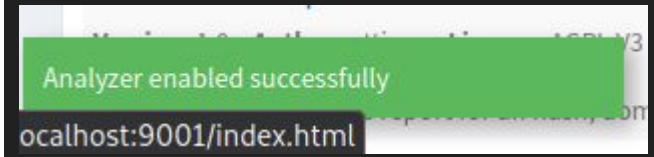
1.

Path to the CA on the system used to check server certificate

Options

Apply defaults

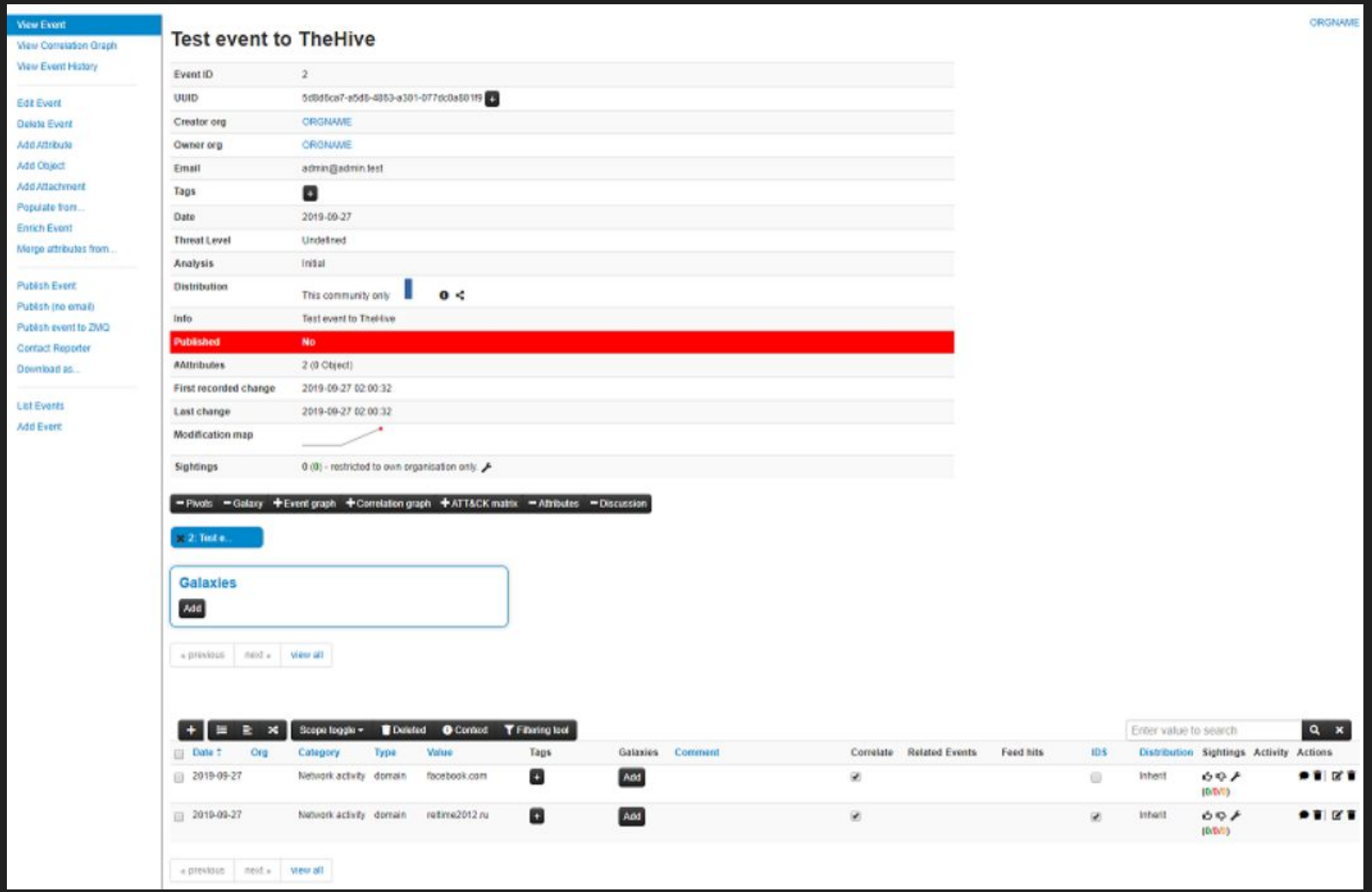
Enable TLP check True | False **Max TLP** AMBER



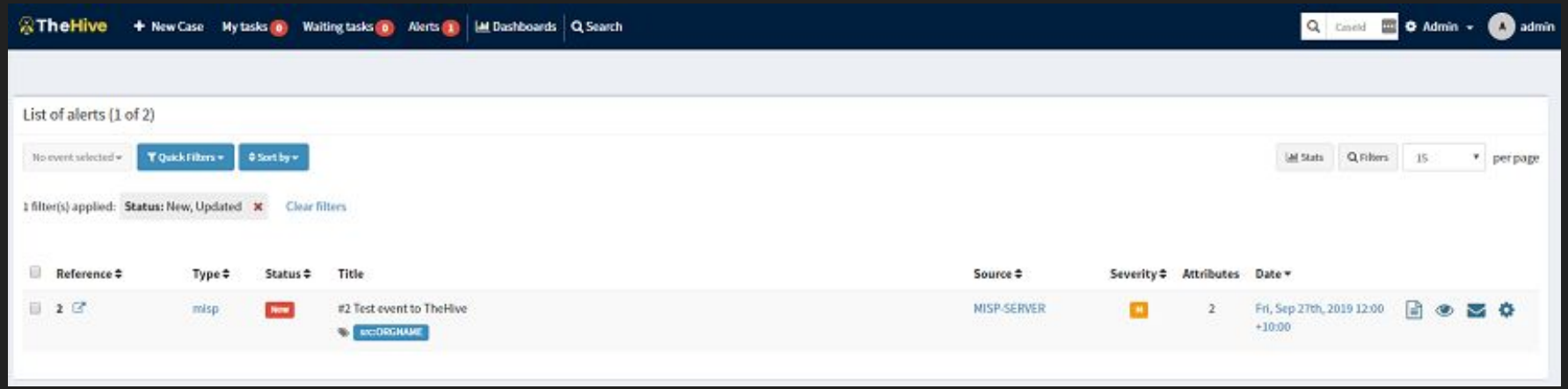
Prova d'enviament d'esdeveniments de MISP a TheHive

Donat que se tracta d'una relació bidireccional, també podem crear esdeveniments en **MISP** i enviar-los a **TheHive**. Desde **MISP** es crea un nou esdeveniment amb alguns atributs. Està marcat el domini ".ru" amb aspecte poc fiable com per Intrustion Detection System (IDS) y un altre atribut sense aquesta configuració.

Per enviar això a **TheHive**, ha de seleccionar "**Publish Event"** (no email) al tauler de l'esquerra i seleccionar "**Yes**" cuando se li demani.


View Event
View Correlation Graph
View Event History
Edit Event
Delete Event
Add Attribute
Add Object
Add Attachment
Populate from...
Enrich Event
Merge attributes from...
Publish Event
Publish (no email)
Publish event to ZMQ
Contact Reporter
Download as...
List Events
Add Event
ORGNAME
Test event to TheHive
Event ID 2
UUID 5d8d5ca7-a5d8-4853-a301-077dc0a80119
Creator org ORGNAME
Owner org ORGNAME
Email admin@admin.test
Tags
Date 2019-09-27
Threat Level Undefined
Analysis Initial
Distribution This community only
Info Test event to TheHive
Published No
#Attributes 2 (0 Object)
First recorded change 2019-09-27 02:00:32
Last change 2019-09-27 02:00:32
Modification map
Sightings 0 (0) - restricted to own organisation only
Pivots Galaxy Event graph Correlation graph ATT&CK matrix Attributes Discussion
2: Test e...
Galaxies
Add
« previous next » view all
Scope toggle Deleted Context Filtering tool
Enter value to search
Date Org Category Type Value Tags Galaxies Comment Correlate Related Events Feed hits IDS Distribution Sightings Activity Actions
2019-09-27 Network activity domain facebook.com Add Inherit
2019-09-27 Network activity domain rattime2012.ru Add Inherit
« previous next » view all

En arribar, estarà sota **Alerts**. Des d'aquí pot importar l'alerta, ignorar l'alerta o marcar-la com llegida.

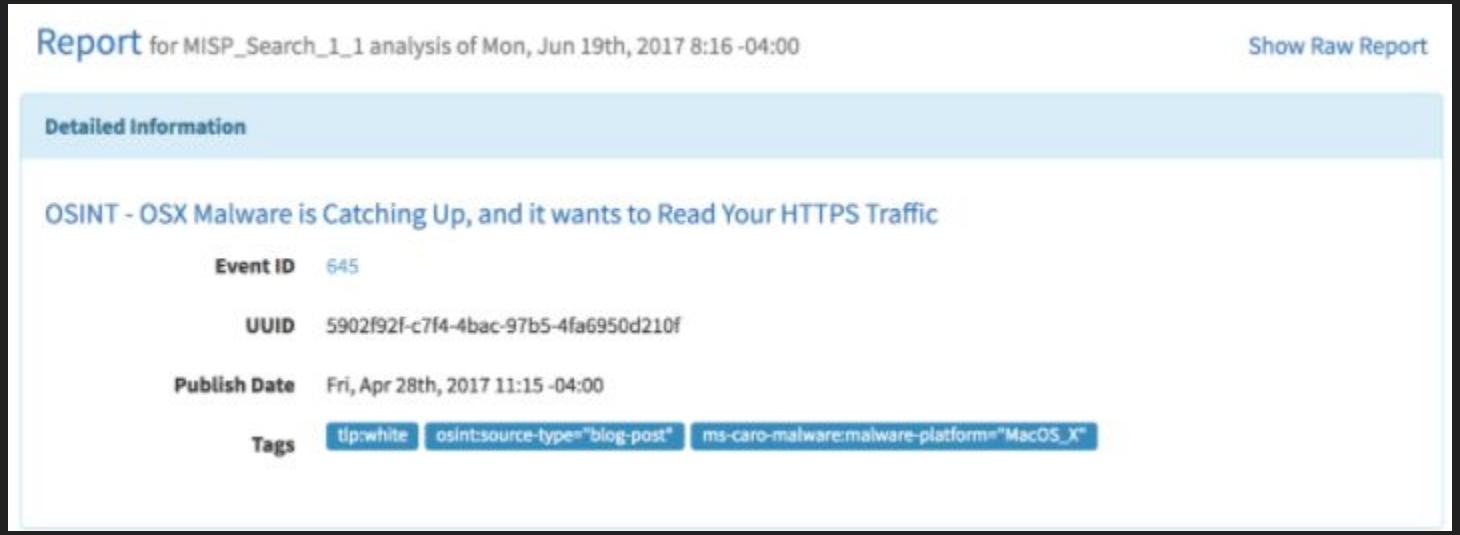


Analysis

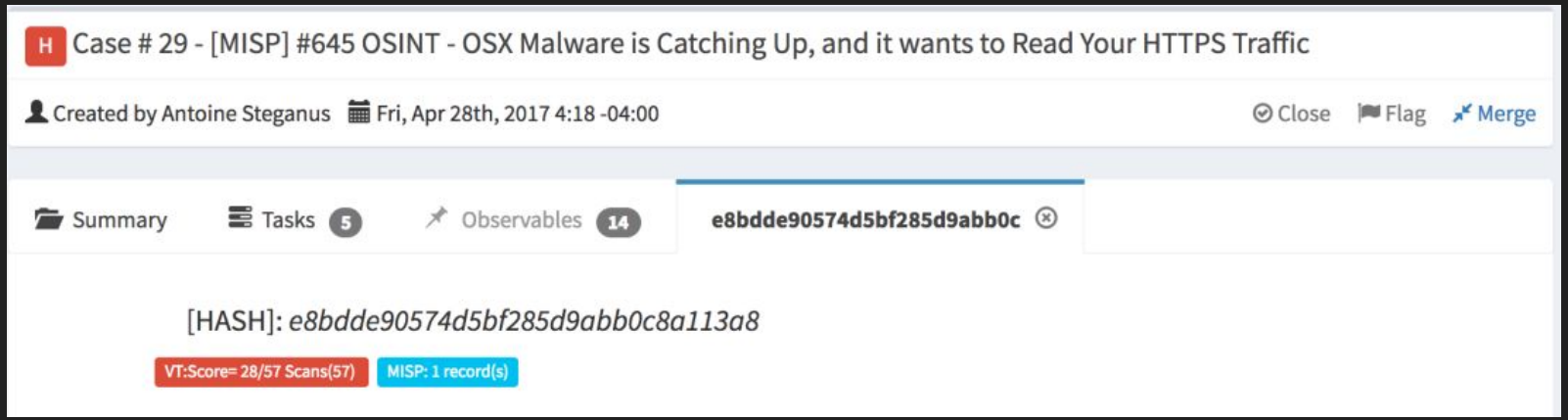
Run all

Analyzer	Last analysis	Actions
Abuse_Finder_3_0	Tue, Jan 19th, 2021 11:33 +01:00 (cortex1)	
MISP_2_1	*None*	

La mateixa recerca realitzada des TheHive: *informe extens*

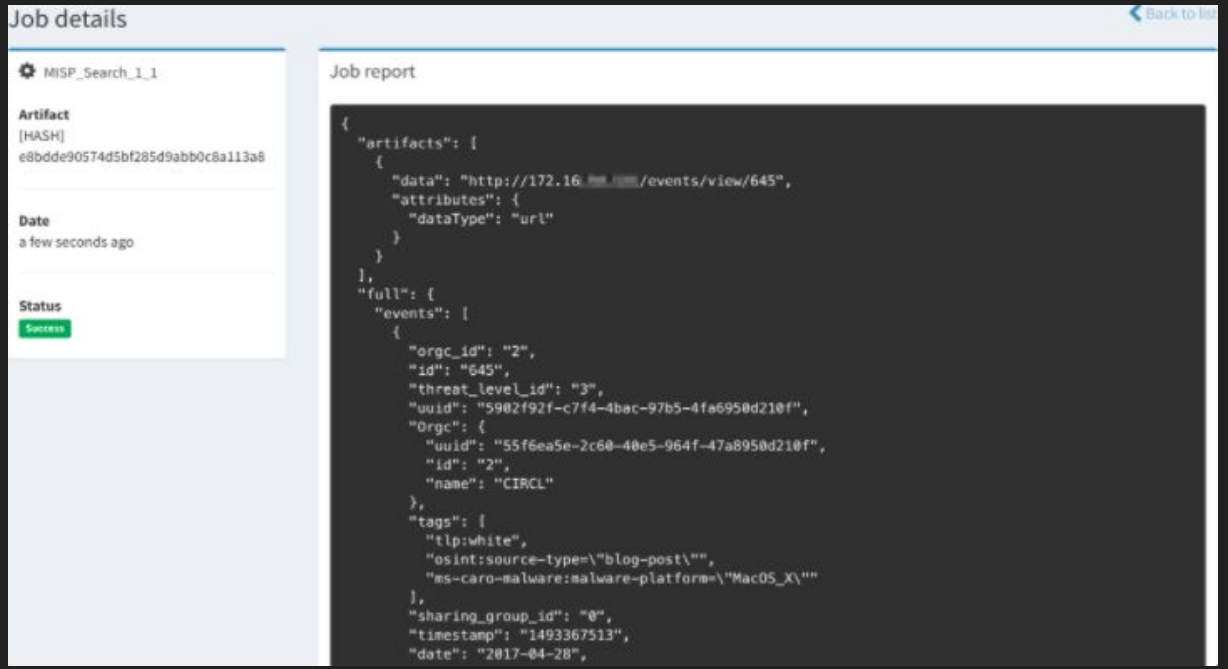


Mini informe

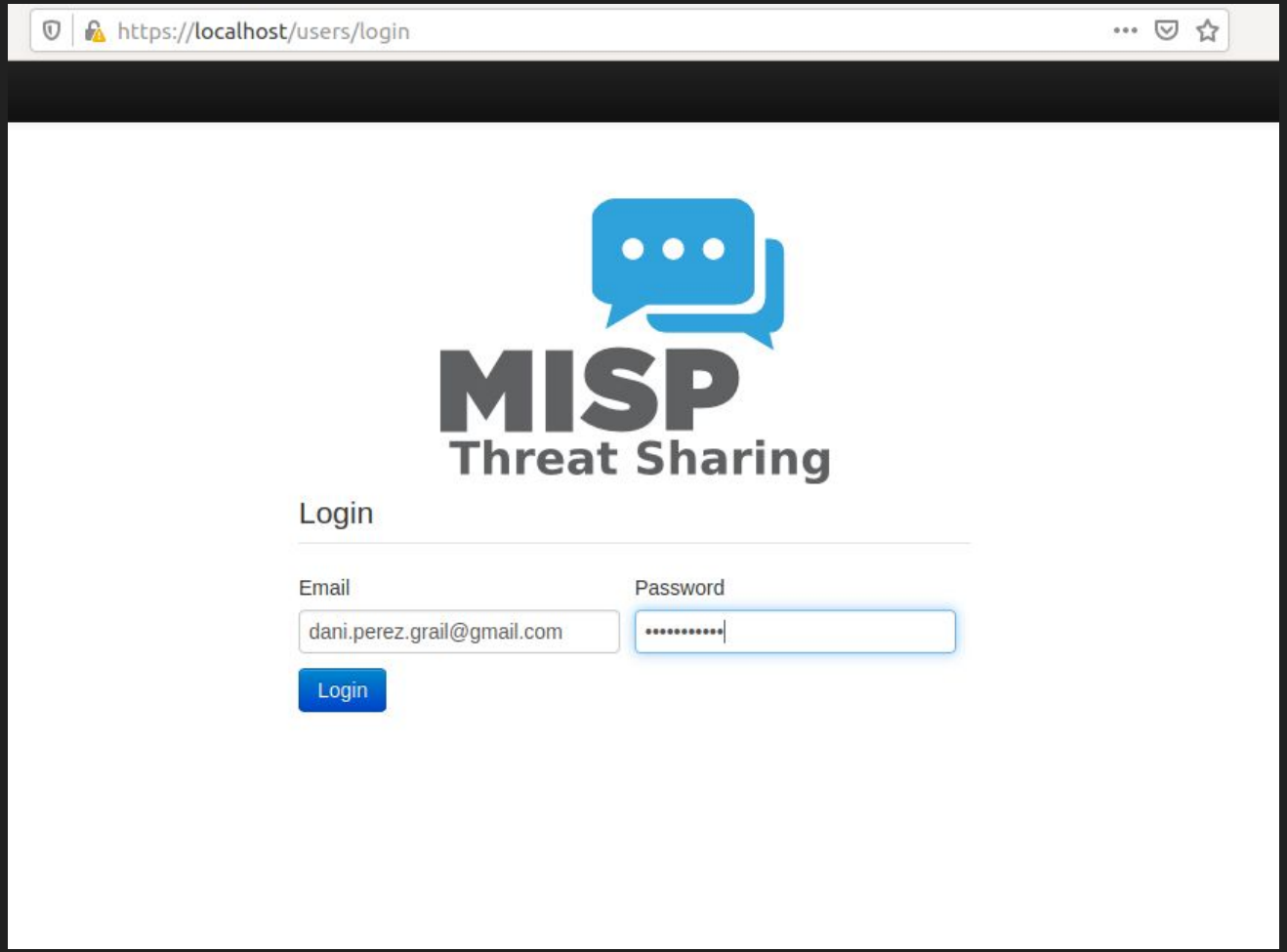


La versió actual de l'analitzador de recerca de MISP només pot buscar dins d'una única instància de MISP, però en un futur proper pot admetre diverses.

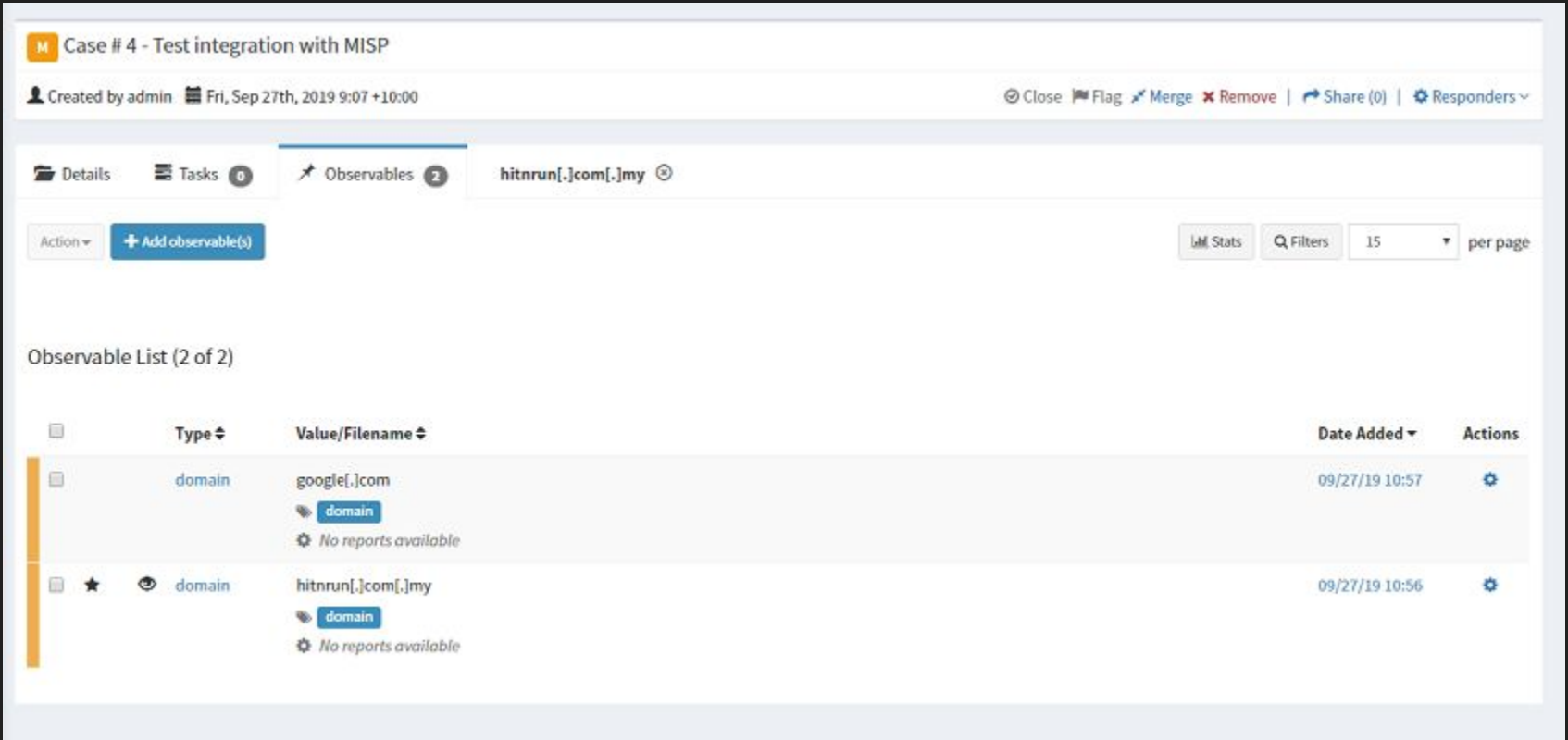
Quan es troba un observable en un esdeveniment, Cortex tornarà el nombre de registres trobats (és a dir, el nombre d'esdeveniments on s'ha trobat l'observable) i una llista d'enllaços a aquests actes amb dades addicionals.



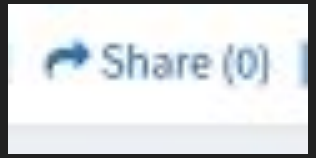
(Recerca d'un hash amb l'analitzador de recerca MISP des de la interfície d'usuari web de Cortex.)

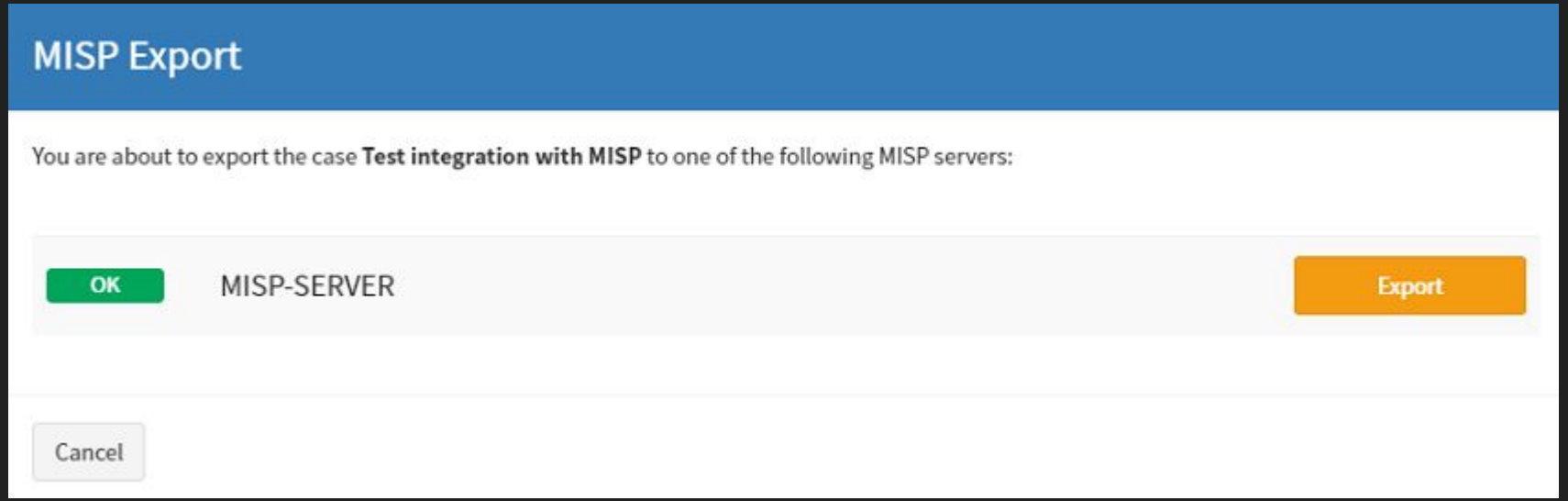

https://localhost/users/login
MISP
Threat Sharing
Login
Email
dani.perez.grail@gmail.com
Password
Login

Enviar events de TheHive a MISP

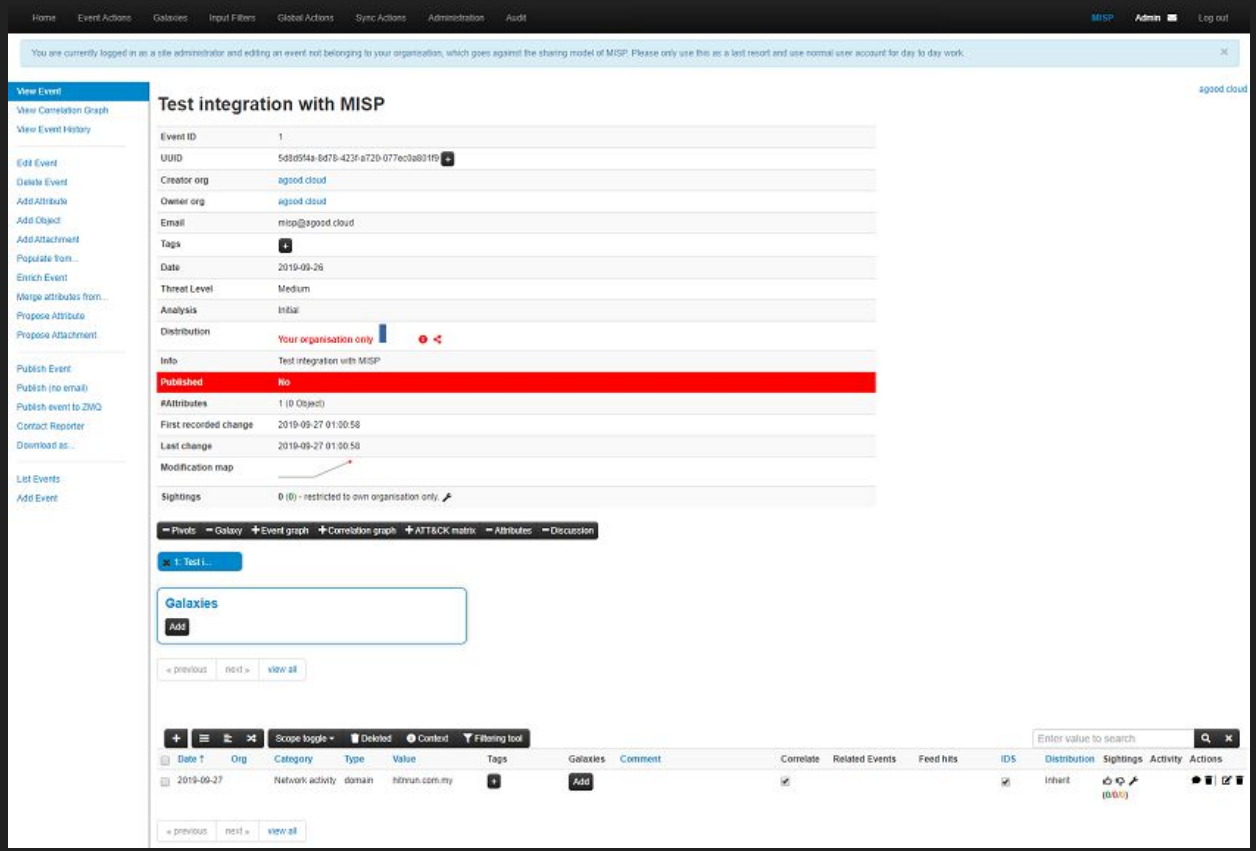


Enviant el cas a MISP

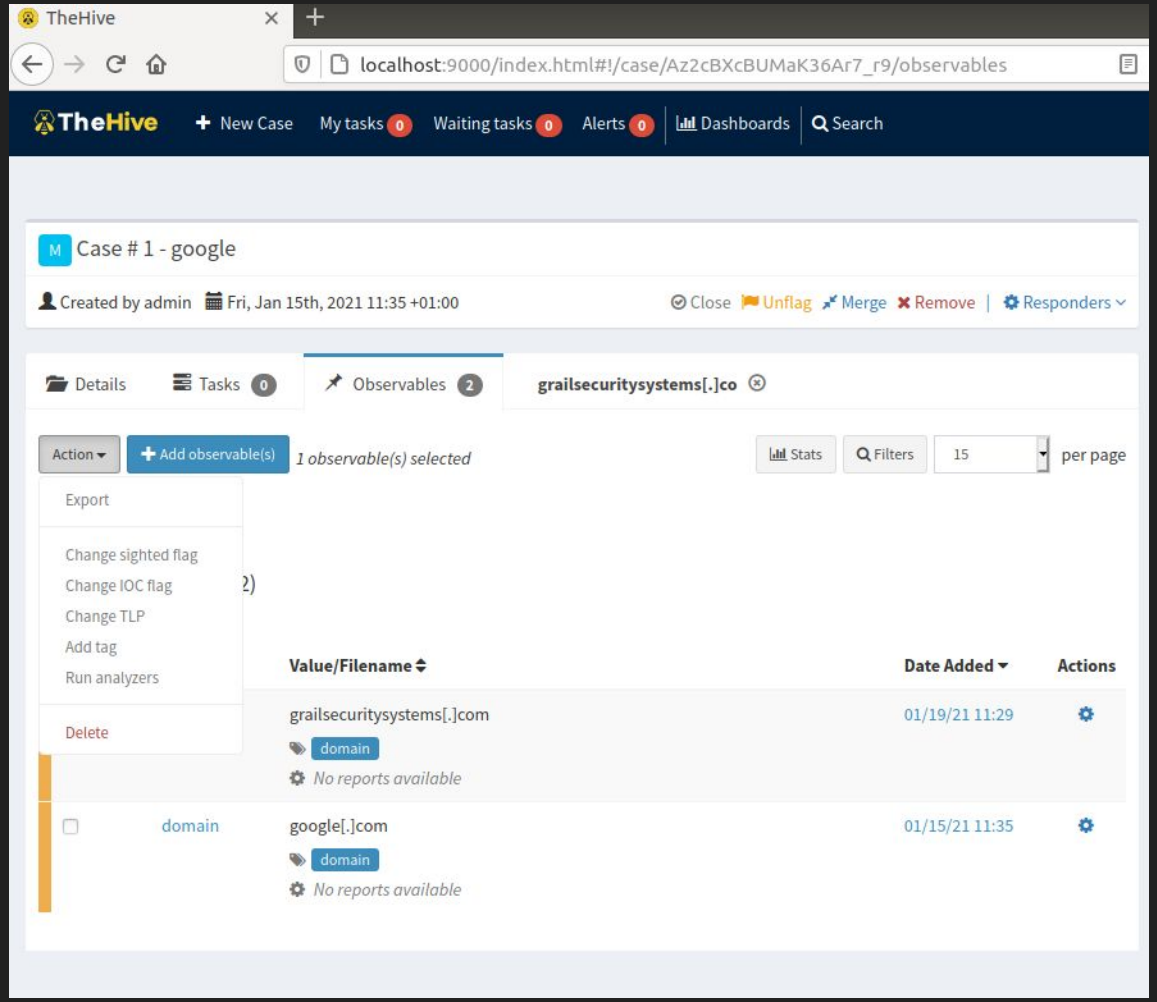


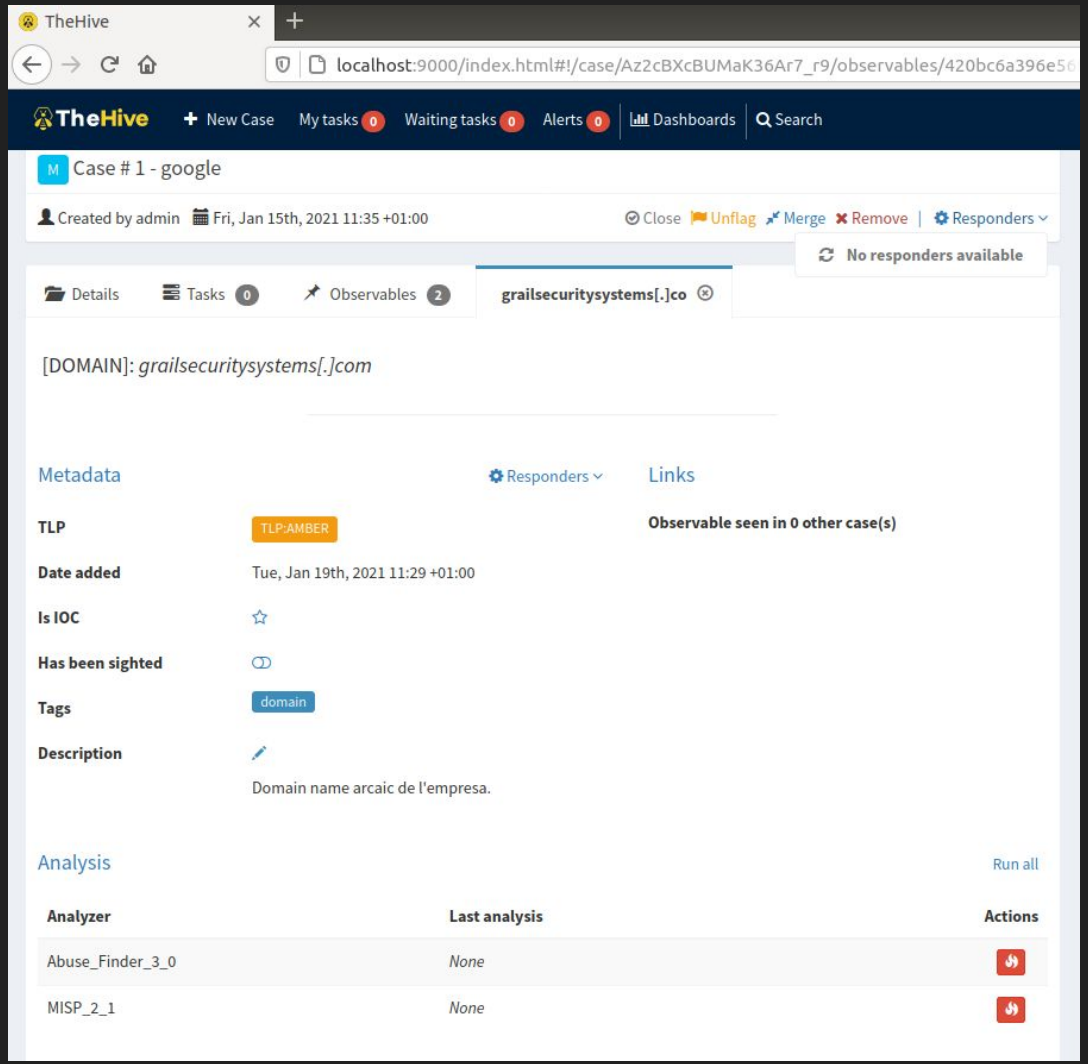


Si s'inicia sessió en la interfície de **MISP**, verà que aquest esdeveniment ha funcionat correctament. També notarà que només els esdeveniments que estan etiquetats com IOC apareixen.



Exemple cas individual


TheHive
localhost:9000/index.html#!/case/Az2cBXcBUMaK36Ar7_r9/observables
TheHive
New Case
My tasks 0
Waiting tasks 0
Alerts 0
Dashboards
Search
Case # 1 - google
Created by admin
Fri, Jan 15th, 2021 11:35 +01:00
Close
Unflag
Merge
Remove
Responders
Details
Tasks 0
Observables 2
grailsecuritysystems[.]co
Action
Add observable(s)
1 observable(s) selected
Stats
Filters
15
per page
Export
Change sighted flag
Change IOC flag
Change TLP
Add tag
Run analyzers
Delete
Value/Filename
Date Added
Actions
grailsecuritysystems[.]com
domain
No reports available
01/19/21 11:29
domain
google[.]com
domain
No reports available
01/15/21 11:35


TheHive
localhost:9000/index.html#!/case/Az2cBXcBUMaK36Ar7_r9/observables/420bc6a396e5
TheHive
New Case
My tasks 0
Waiting tasks 0
Alerts 0
Dashboards
Search
Case # 1 - google
Created by admin
Fri, Jan 15th, 2021 11:35 +01:00
Close
Unflag
Merge
Remove
Responders
No responders available
Details
Tasks 0
Observables 2
grailsecuritysystems[.]co
[DOMAIN]: grailsecuritysystems[.]com
Metadata
Responders
Links
TLP
TLP:AMBER
Observable seen in 0 other case(s)
Date added
Tue, Jan 19th, 2021 11:29 +01:00
Is IOC
Has been sighted
Tags
domain
Description
Domain name arcaic de l'empresa.
Analysis
Run all
Analyzer
Last analysis
Actions
Abuse_Finder_3_0
None
MISP_2_1
None

Analysis

Run all

Analyzer	Last analysis	Actions
Abuse_Finder_3_0	Tue, Jan 19th, 2021 11:33 +01:00 (cortex1)	
MISP_2_1	*None*	

Analyzer Abuse_Finder_3_0 has been successfully started for observable: grailsecuritysystems.com

Analysis

Run all

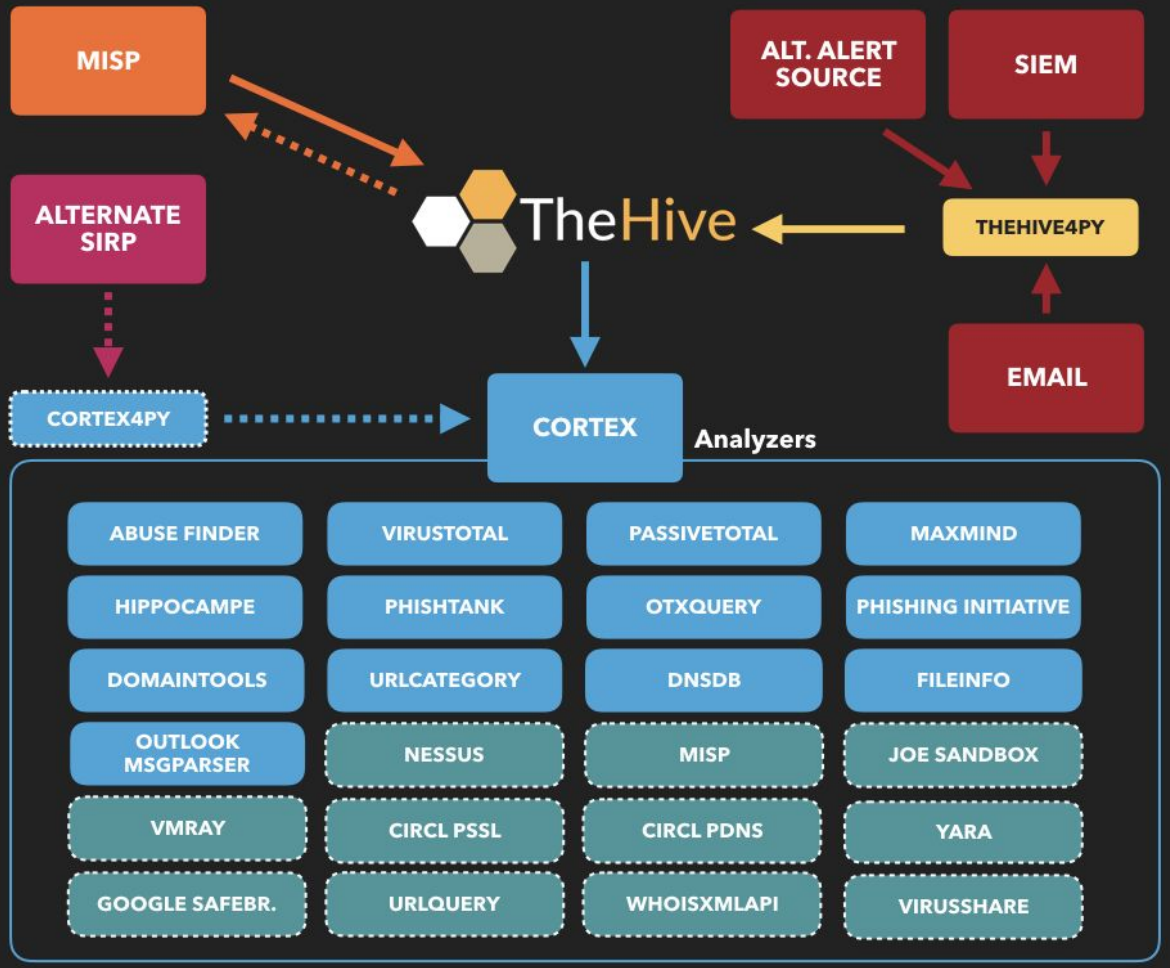
Analyzer	Last analysis	Actions
Abuse_Finder_3_0	✔ Tue, Jan 19th, 2021 11:33 +01:00 (cortex1)	
MISP_2_1	*None*	

Report for Abuse_Finder_3_0 analysis of Tue, Jan 19th, 2021 11:33 +01:00

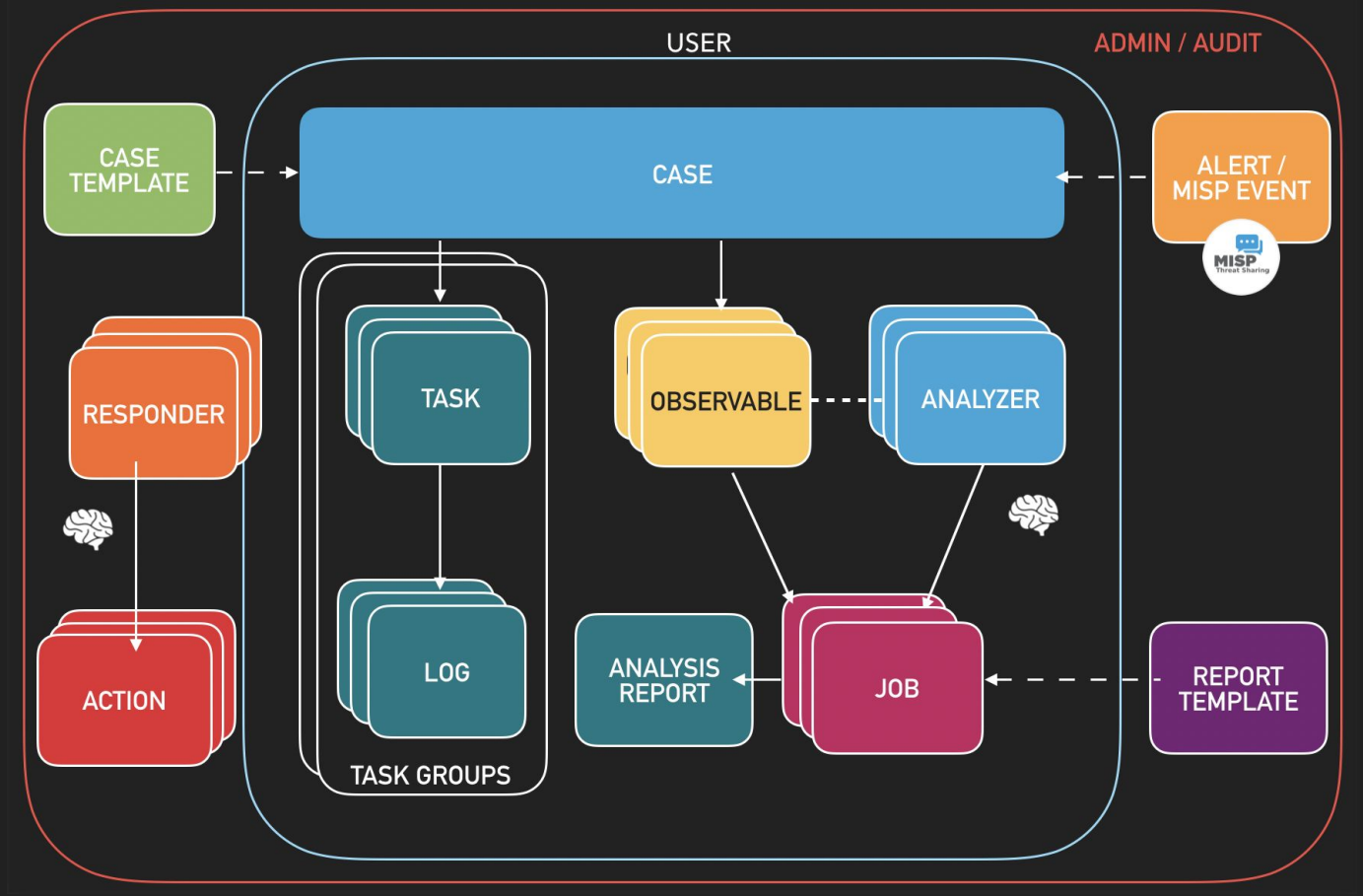
Show Raw Report | Show observables (0)

grailsecuritysystems[.]com


```
{
  "abuse_finder": {
    "value": "grailsecuritysystems.com",
    "names": [],
    "abuse": [],
    "raw": "No match for \"GRAILSECURITYSYSTEMS.COM\".\r\n>>> Last update of whois database: 2021-01-19
  }
}
```


MISP
ALT. ALERT SOURCE
SIEM
ALTERNATE SIRP
TheHive
THEHIVE4PY
EMAIL
CORTEX4PY
CORTEX
Analyzers
ABUSE FINDER
VIRUSTOTAL
PASSIVETOTAL
MAXMIND
HIPPOCAMPE
PHISHTANK
OTXQUERY
PHISHING INITIATIVE
DOMAINTOOLS
URLCATEGORY
DNSDB
FILEINFO
OUTLOOK MSGPARSER
NESSUS
MISP
JOE SANDBOX
VMRAY
CIRCL PSSL
CIRCL PDNS
YARA
GOOGLE SAFEBR.
URLQUERY
WHOISXMLAPI
VIRUSSHARE

Flux de treball



ElastAlert

És una solució per transportar les dades que s'indexen a **ES** per enviar-les arràn d'un mòdul de Python a **TheHive** per generar alertes pels analistes.

Obteniu la plantilla aquí o simplement creeu el vostre propi config.yaml i copieu només la configur*ació necessària a continuació.*

Deseu-ho com a ~elastalert/config.yaml.

```
rules_folder: /home/username/elastalert/rules
run_every:
  minutes: 1
buffer_time:
  minutes: 15
es_host: x.x.x.x
es_port: 9200
use_ssl: False
writeback_index: elastalert_status
alert_time_limit:
  days: 2
```

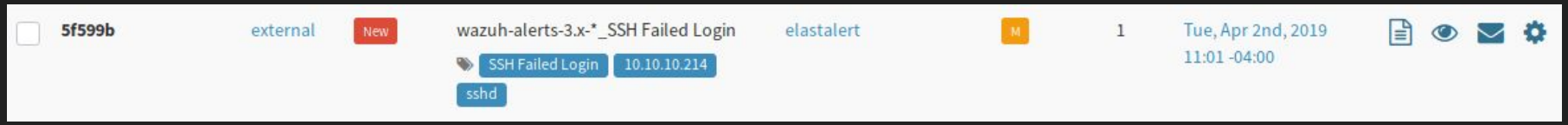
```
nano ~/elastalert/rules/failed_ssh_login.yaml
```

```
es_host: x.x.x.x
es_port: 9200
name: SSH Failed Login
type: frequency
index: wazuh-alerts-3.x-*
num_events: 2
timeframe:
    hours: 1
filter:
- term:
    rule.id: "5710"
alert: hivealerter
hive_connection:
  hive_host: http://x.x.x.x
  hive_port: 9000
  hive_apikey: <Paste API key for elastalert user here>

hive_alert_config:
  type: 'external'
  source: 'elastalert'
  description: '{rule[name]}'
  severity: 2
  tags: ['{rule[name]}', '{match[agent][ip]}', '{match[predecoder][program_name]}']
  tlp: 3
  status: 'New'
  follow: True

hive_observable_data_mapping:
    - ip: "{match[src_ip]}"
```

Hauríeu de veure les alertes que apareixen a Kibana i ElastAlert les hauria de recollir la propera vegada que s'executi.

```
INFO:elastalert:Ran SSH Failed Login from 2019-03-31 18:21 UTC to 2019-04-02 15:01 UTC: 3 query hits (0 already seen), 1 matches, 1 alerts sent
```

Això farà que es generi una nova alerta a TheHive a "Alertes".



Alert Preview New

M wazuh-alerts-3.x-*_SSH Failed Login

ID: 1a4eba6b1bdd4cfdcb3dc5cac073912b **Date:** Tue, Apr 2nd, 2019 11:01 -04:00 **Type:** external **Reference:** 5f599b **Source:** elastalert

SSH Failed Login | 10.10.10.214 | sshd

Description

SSH Failed Login Sample description

Additional fields

No aditional information have been specified

Observables (1)

All (1) | ip (1)

	Type	Data
👁	ip	10[.]10[.]10[.]25

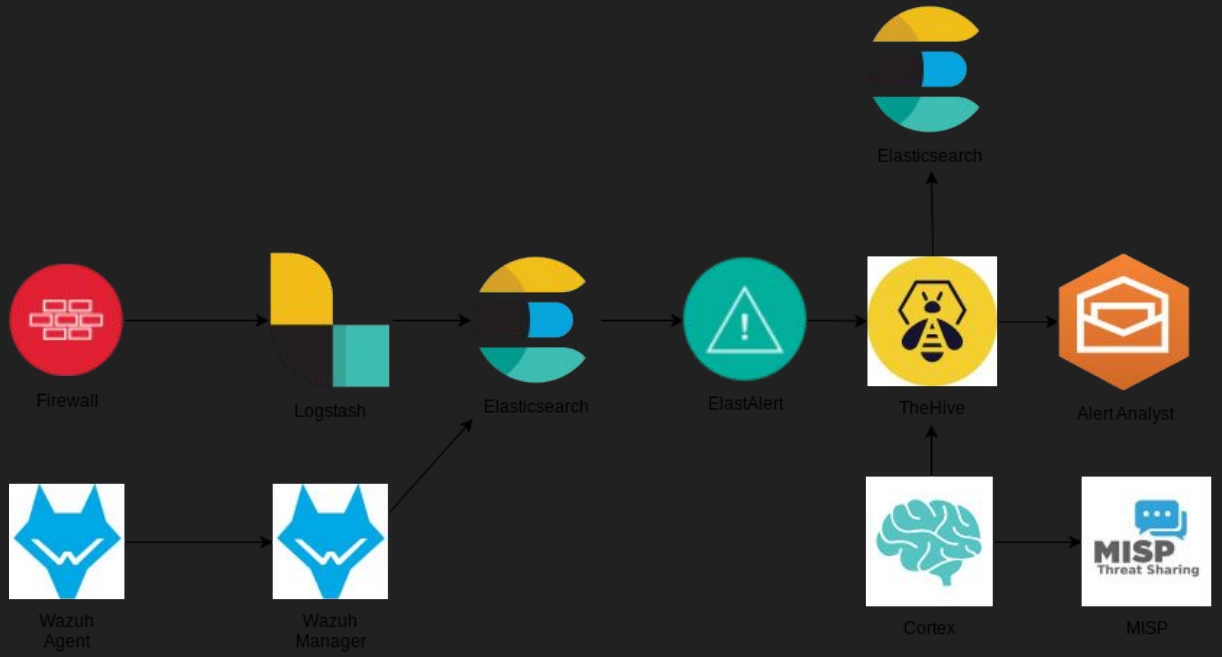
Similar cases (1)

All (1) | Open (1)

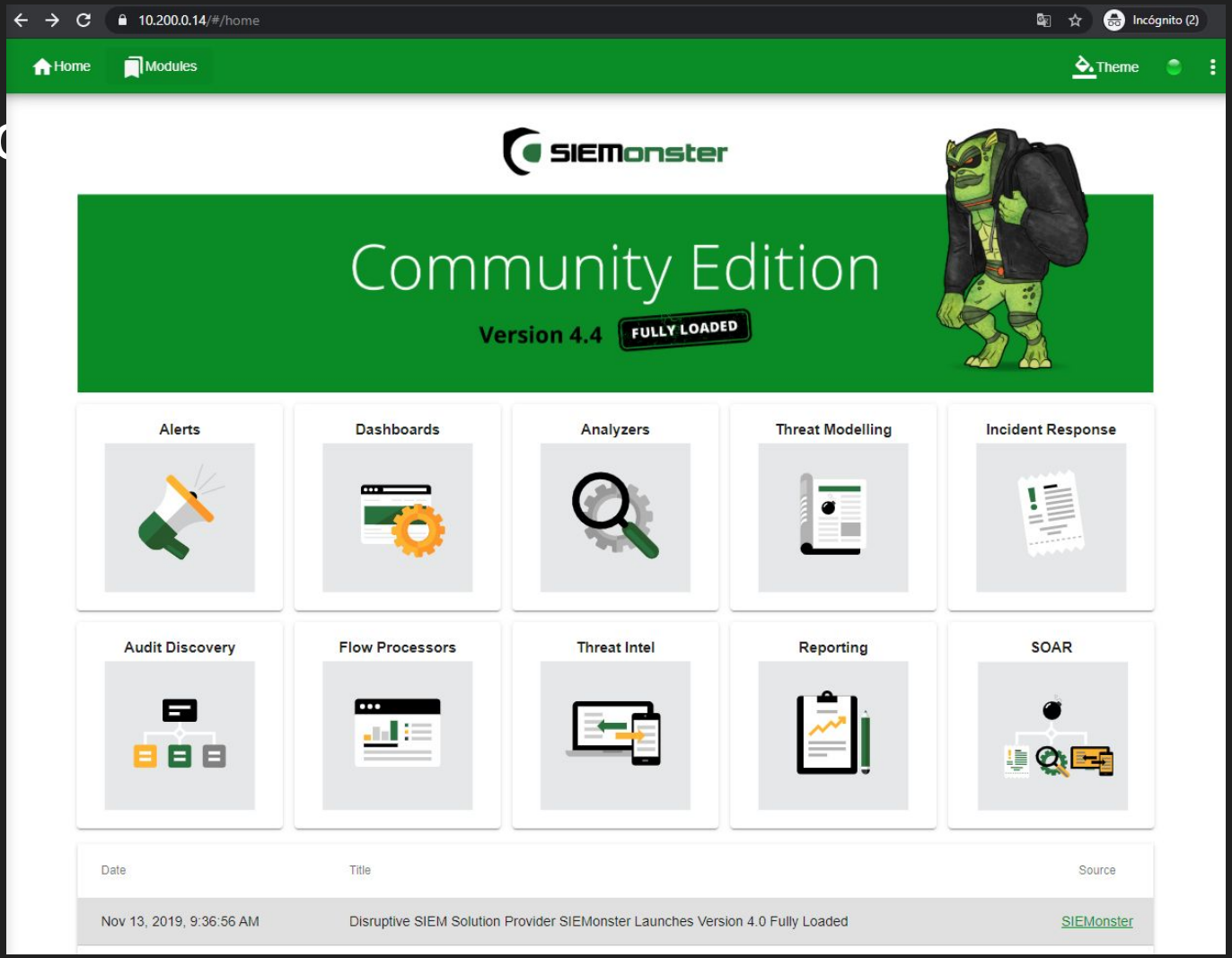
Title		Date	Observables	IOCs	Action
#6 - wazuh-alerts-3.x-*_SSH Failed Login SSH Failed Login | 10.10.10.214 | sshd	M	03/31/19 14:01	**100%** (1 / 1)	*N/A*	Merge in this case

Cancel | Mark as read | Ignore new updates | Merge into case

Import alert as SSHD Related | Yes, Import


Elasticsearch
Firewall
Logstash
Elasticsearch
ElastAlert
TheHive
Alert Analyst
Wazuh
Agent
Wazuh
Manager
Cortex
MISP
Threat Sharing
MISP

SIEMo


10.200.0.14/#/home
Incógnito (2)
Home
Modules
Theme
SIEMonster
Community Edition
Version 4.4
FULLY LOADED
Alerts
Dashboards
Analyzers
Threat Modelling
Incident Response
Audit Discovery
Flow Processors
Threat Intel
Reporting
SOAR
Date
Title
Source
Nov 13, 2019, 9:36:56 AM
Disruptive SIEM Solution Provider SIEMonster Launches Version 4.0 Fully Loaded
SIEMonster

Bibliografia

https://github.com/TheHive-Project/CortexDocs/blob/master/installation/install-guide.md#docker

https://github.com/TheHive-Project/TheHive

https://reposhub.com/javascript/misc/TheHive-Project-TheHive.html

https://www.misp-project.org/

https://blog.agood.cloud/posts/2019/09/29/integrate-misp-to-thehive/

https://github.com/TheHive-Project/TheHiveDocs/blob/master/admin/configuration.md#4-streaming-aka-the-flow

https://www.youtube.com/watch?v=S6_qM2WqY38

https://www.youtube.com/watch?v=HntocIbpzHE

https://www.youtube.com/watch?v=HMP1OcGkN4E&t=1889s

https://www.youtube.com/watch?v=K6K1fNpbf9w

https://community.rsa.com/community/products/netwitness/blog/2019/04/05/threat-intel-integration-with-misp-and-minemeld

https://www.siqure.es/traffic-light-protocol-tlp-definiciones-y-uso/

https://www.misp-project.org/taxonomies.html#_pap

https://blog.thehive-project.org/tag/pap/

Conclusions