



IMPLEMENTACIÓN Y CONFIGURACIÓN DE MISP

Cómo compartir
información de
malware

Introducción	3
MISP: Significado y desafíos	4
Características generales.....	5
Proceso de instalación.....	6
Descarga de Script de MISP	6
Ejecutar Script	7
Instalación automática	7
Confirmación de usuario	8
Credenciales.....	8
Acceso a interfaz.....	9
Cambio de contraseña.....	9
Configuración del MISP.....	10
Inicio de sesión	10
Configuración de parámetros.....	10
Modificación de parámetro de bienvenida	11
Configuración de Redis-Server	11
Configuración y reinicio de servicio	11
Script de configuración para comunicar MISP	12
Conexión del MISP.....	13
Sincronizar enviando contraseñas.....	13
Sincronizar recibiendo contraseñas.....	14
Comentarios finales.....	17
Bibliografía consultada	18

Autor: Miguel Kurte A., Analista de CSIRT
Director: Carlos Landeros C.
Edición: Katherina Canales M, Felipe Quezada V.
Diseño: Jaime Millán G.
Corrección: Patricio Quezada A. y Carolina Covarrubias
E. Correo: csirt-comunicaciones@interior.gob.cl
Santiago de Chile, Abril de 2023

Introducción

El incremento de incidentes cibernéticos a nivel global era una realidad objetiva que con la pandemia y el mayor uso extensivo e intensivo del internet se acrecentó aún más el 2020. La urgencia por implementar medidas de seguridad para enfrentar esta amenaza, especialmente en las organizaciones, demanda una mejor comunicación entre diferentes entidades con el incentivo de contrastar datos para tomar medidas preventivas o reactivas dependientes del contexto.

Hoy, contar con información de inteligencia sobre las amenazas del ciberespacio se ha convertido en un activo crítico para la toma de decisiones de los responsables de la seguridad cibernética en cada organización, pero recopilar esa información exige contar con herramientas seguras, precisas, confiables y comprensibles, además de colaboración.

Hace poco menos de una década fue creado el proyecto MISP cuyo objetivo ha sido desde un principio involucrar a más especialistas y entidades de seguridad para enfrentar los incidentes de seguridad cibernética que afectan a las organizaciones a nivel global basados en compartir indicadores de compromisos confiables y actualizados sobre las amenazas cibernéticas.

La plataforma para compartir información de malware busca que las diferentes organizaciones puedan utilizar información valiosa para tomar medidas preventivas y reactivas para proteger sus activos informáticos, incentivando de paso, la colaboración en un fin común.

El presente trabajo pretende fomentar entre sus lectores el uso de esa herramienta. Las primeras dos secciones del documento buscan definir en términos generales que es un MISP y cuáles son sus características generales, para luego enfocarse en los pasos que deben considerar los administradores para instalar, configurar, sincronizar y conectar herramientas MISP.

MISP: Significado y desafíos

MISP es un acrónimo de origen inglés que se utiliza para denominar a las plataformas para compartir información de malware (*Malware information sharing platform*). Un MISP es una plataforma libre y *open source* de inteligencia utilizada para reunir, compartir, almacenar y correlacionar indicadores de compromisos. Estos IoCs por lo general corresponden a ataques focalizados, *threat intelligence*, fraudes financieros, vulnerabilidades y en casos muy especiales, información anti-terroristas. Su principal objetivo es ayudar a establecer acciones preventivas y reactivas frente a ataques dirigidos, además de permitir la detección de amenazas mediante el intercambio colaborativo de conocimientos sobre los malware existentes.

Una condición específica del MISP es su diseño horizontal. Es lo que se conoce como plataforma *peer-to-peer*, en el que cada parte integrante del MISP puede compartir información y recibir información. Existen distintos niveles en lo que se puede compartir la información, ya sea como miembro de una organización, como parte de una comunidad o como una serie de comunidades conectadas.

La estructura de un MISP necesariamente descansa en la colaboración de las partes. Luc Dandurand y Oscar Serrano (2013), al definir las capacidades de la infraestructura de la colaboración e intercambio de datos de seguridad cibernética, sostienen que el requisito más importante para un sistema de inteligencia de amenazas exitoso es la facilidad para compartir y automatizar el intercambio de información, así como la capacidad de generar, refinar y controlar datos. Por su parte, Stuart Murdoch y Nick Leaver (2015) destacan el intercambio de información de seguridad cibernética entre organizaciones como un factor esencial para ayudar a gobiernos e industrias en la protección de la infraestructura de red crítica frente a ataques cibernéticos, y para ellos es necesario fomentar la colaboración, pero concluyen que hay barreras que deben ser superadas, especialmente en base a la confianza de las partes que integran estas comunidades, especialmente por las necesidades conflictivas de los colaboradores para proteger sus fuentes de información por razones de sensibilidad de tipo legal o de imagen pública, pero también para validar y confiar en la información compartida. A ello se suma la dependencia de este sistema colaborativo sobre la base de una comunidad activa que contribuya permanentemente en él.

Otros desafíos más prácticos que enfrenta la plataforma están relacionados con las capacidades y competencias que debe tener una organización para evaluar grandes cantidades de información que pueden ser acumuladas en los MISP. A ello se suma la forma en que las personas y entidades contribuyen en el MISP, lo que no siempre puede corresponder a un modelo estándar. Una organización puede describir un evento con la mayor cantidad de información posible, o puede disponer una información muy escueta, dificultando la búsqueda de patrones estadísticos en un incidente real. En cuanto a las competencias, la usabilidad del sistema y la experiencia de los usuarios compartiendo información representan una parte compleja de este intercambio para la veracidad e integridad de la data compartida, lo que genera la necesidad de implementar una taxonomía adecuada entre las partes.

Características generales

Debido a que el MISP es una herramienta de estructura peer-to-peer con múltiples instancias de intercambio, su protocolo de uso descansa en tres criterios: la eficiencia, la precisión y la escalabilidad. En otras palabras, los usuarios del MISP pueden definir cuál es la información que quieren compartir, a quienes se distribuye esa información, y entre qué grupos.

La información que se comparte en MISP se denomina evento, el que cuenta con una serie de atributos, incluyendo las direcciones IP de destino y los hash de los archivos. Estos atributos se identifican por categoría, tipo y valor, y otras variables de texto como la fecha, el nivel de amenaza, la descripción de la organización y galaxias sobre actores de amenazas. En un MISP, los eventos se pueden crear o cargar, almacenar, extraer, analizar y distribuir.

Adicionalmente, la interfaz de un MISP nos permite incorporar información de respaldo, como los riesgos económicos y financieros del evento, o el nivel de amenaza. En general, la forma de suministrar información, los formatos y lenguajes del MISP son sencillos gracias a su interfaz. La simplicidad del formato es uno de los objetivos de esta plataforma. El MISP cuenta con una implementación de taxonomía y etiquetas enriquecida, e incrusta directamente las etiquetas en los eventos. Si bien simplifica la tarea, también puede crear incoherencias entre versiones de la misma etiqueta.

La plataforma MISP tiene otra importante ventaja al permitir la integración con otras herramientas de Intrusión de Detección de Sistemas (IDS) y SIEM, y contiene API REST flexibles para integrar soluciones internas con la plataforma.

MISP además permite un soporte centralizado, al compartir la misma instancia entre una comunidad de confianza, y tiene soporte descentralizado, cuando varias instancias interactúan de forma peer-to-peer.

Otra de las ventajas del MISP es que permite lidiar con otros diferentes estándares, como STIX (expresión estructurada de información sobre amenazas) y TAXII (intercambio automatizado de información de inteligencia).

Proceso de instalación

La presente sección describe paso a paso la instalación de un MISP, que se realizó sobre el sistema operativo Ubuntu. En el proceso de instalación del sistema operativo se sugiere que no sea creado el usuario “misp” debido a que el script de instalación lo crea de forma automática. Este proceso dura aproximadamente 1 hora, dependiendo de las características del servidor. Las características mínimas recomendadas para el Sistema Operativo son 2CPU, 4Gb en RAM y 150Gb HDD, además de actualizar el Sistema Operativo.

Se recomienda revisar si la conexión a internet del servidor utiliza proxy, ya que el script realiza tareas de actualización y descarga de manera automática desde repositorios GIT. También es recomendable revisar la hora y la zona horaria configurada en el servidor, y de igual manera poder configurar el cliente NTP para mantener todos los log de forma ordenada y que las tareas se ejecuten en los horarios que se configuren.

Todos los comandos deben ser ejecutados con un usuario con privilegios de administrador, en nuestro caso al instalar el Sistema Operativo Ubuntu se creó un usuario “csirt” y con ese se realizó la instalación, no con el usuario root.

Descarga de Script de MISP

Desde una consola de comando ejecutar lo siguiente para poder descargar el script directo desde los repositorios de MISP:

```
wget --no-check-certificate -O /tmp/INSTALL.sh  
https://raw.githubusercontent.com/MISP/MISP/2.4/INSTALL/INSTALL.sh
```

```
csirt@misp-privado:~$  
csirt@misp-privado:~$  
csirt@misp-privado:~$ wget --no-check-certificate -O /tmp/INSTALL.sh https://raw.githubusercontent.com/MISP/MISP/2.4/INSTALL/INSTALL.sh  
--2020-06-19 20:05:40-- https://raw.githubusercontent.com/MISP/MISP/2.4/INSTALL/INSTALL.sh  
Resolving raw.githubusercontent.com [raw.githubusercontent.com]:443... 151.101.220.133  
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)[151.101.220.133]:443... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 133066 (130K) [text/plain]  
Saving to: '/tmp/INSTALL.sh'  
  
/tmp/INSTALL.sh 100%[=====] 129.95K --.-KB/s in 0.01s  
  
2020-06-19 20:05:40 (12.9 MB/s) - '/tmp/INSTALL.sh' saved [133066/133066]  
csirt@misp-privado:~$
```

Ejecutar Script

Una vez descargado, ejecutar el script. En nuestro caso, con el comando anterior se descargó en la ubicación tmp por lo que el comando será el siguiente: **bash /tmp/INSTALL.sh -c -M -D**

```
2020-06-19 20:05:40 (12.9 MB/s) - '/tmp/INSTALL.sh' saved [133066/133066]

csirt@misp-privado:~$ bash /tmp/INSTALL.sh -c -M -D
next step: Checking if we are run as the installer template
next step: Checking Linux distribution and flavour...
next step: We detected the following Linux flavour: Ubuntu 18.04
next step: Checking if we are uptodate and checksums match
sha1 matches
sha256 matches
sha384 matches
sha512 matches
-----
next step: Setting MISP variables
next step: Setting generic MISP variables shared by all flavours
groups: 'misp': no such user
The following DB Passwords were generated...
Admin (root) DB Password: 147e46          cc44ec
User (misp) DB Password: f6c901         0c1b52
next step: Checking for parameters or Unattended Kali Install
next step: Setting install options with given parameters.
core
modules
dashboard
Install on Ubuntu 18.04 LTS fully supported.
Please report bugs/issues here: https://github.com/MISP/MISP/issues
-----
Proceeding with the installation of MISP core
-----
next step: Setting Base URL
[sudo] password for csirt: █
```

Instalación automática

Avanzando en la instalación se solicitará ingresar la clave del usuario y se inicia el proceso de instalación automática.

```
[sudo] password for csirt:
next step: VMware,
##### (4h)
Checking for sudo and installing etckeeper
Hit:1 http://security.ubuntu.com/ubuntu bionic-security InRelease
Hit:2 http://archive.ubuntu.com/ubuntu bionic InRelease
Hit:3 http://archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:4 http://archive.ubuntu.com/ubuntu bionic-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  grub-pc-bin
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libpython-stdlib libpython2.7-minimal libpython2.7-stdlib python python-minimal python2.7 python2.7-minimal
Suggested packages:
  python-doc python-tk python2.7-doc binutils binfmt-support
The following NEW packages will be installed:
  etckeeper libpython-stdlib libpython2.7-minimal libpython2.7-stdlib python python-minimal python2.7 python2.7-minimal
0 upgraded, 8 newly installed, 0 to remove and 0 not upgraded.
Need to get 3,996 kB of archives.
After this operation, 17.0 MB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libpython2.7-minimal amd64 2.7.17-1-18.04ubuntu1 [335 kB]
Get:2 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 python2.7-minimal amd64 2.7.17-1-18.04ubuntu1 [1,294 kB]
Get:3 http://archive.ubuntu.com/ubuntu bionic/main amd64 python-minimal amd64 2.7.15-rc1-1 [28.1 kB]
Get:4 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libpython2.7-stdlib amd64 2.7.17-1-18.04ubuntu1 [1,915 kB]
Get:5 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 python2.7 amd64 2.7.17-1-18.04ubuntu1 [248 kB]
Get:6 http://archive.ubuntu.com/ubuntu bionic/main amd64 libpython-stdlib amd64 2.7.15-rc1-1 [7,620 B]
Get:7 http://archive.ubuntu.com/ubuntu bionic/main amd64 python amd64 2.7.15-rc1-1 [140 kB]
Get:8 http://archive.ubuntu.com/ubuntu bionic/main amd64 etckeeper all 1.18.5-1ubuntu1 [28.3 kB]
Fetched 3,996 kB in 3s (1,184 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libpython2.7-minimal:amd64.
(Reading database ... 102986 files and directories currently installed.)
Preparing to unpack .../0-libpython2.7-minimal_2.7.17-1-18.04ubuntu1_amd64.deb ...
```

Confirmación de usuario

Se preguntará si se desea crear el usuario MISP “There is NO user called 'misp' create a user 'misp' (y) or continue as csirt (n)? (y/n)”. Le diremos que sí, “(y)”.

```
Next step: Checking Locale
apt is maybe locked, waiting 3 seconds.
Reading package lists...
Building dependency tree...
Reading state information...
locales is already the newest version (2.27-3ubuntu1).
The following package was automatically installed and is no longer required:
  grub-pc-bin
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Generating locales (this might take a while)...
  en_US.UTF-8... done
Generation complete.
Next step: Upgrading system
apt is maybe locked, waiting 3 seconds.
Reading package lists...
Building dependency tree...
Reading state information...
Calculating upgrade...
The following package was automatically installed and is no longer required:
  grub-pc-bin
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
##### (12%)
Next step: Setting generic MISP variables shared by all flavours
groups: 'misp': no such user
The following DB Passwords were generated...
Admin (root) DB Password: 2d75:                1fb33b
User (misp) DB Password: 36ca:                11ed5
##### (16%)
Next step: Checking if tuih as root and misp is present
id: 'misp': no such user
There is NO user called 'misp' create a user 'misp' (y) or continue as csirt (n)? (y/n)
```

Credenciales

Al finalizar la instalación, en pantalla aparecen impreso las credenciales para conectarse al MISP, las credenciales de base de datos y las credenciales del sistema local.

```
Attempting uninstall: pymisp
Found existing installation: pymisp 2.4.123
Uninstalling pymisp-2.4.123:
Successfully uninstalled pymisp-2.4.123
Running setup.py develop for pymisp
Successfully installed pymisp validators-0.14.3
Traceback (most recent call last):
  File "tests/testLiveComprehensive.py", line 40, in <module>
    from keys import ucl, key # type: ignore
  File "/var/www/MISP/PyMISP/tests/keys.py", line 2
    key = "4yYI          1z3X3"
          ^
SyntaxError: EOF while scanning triple-quoted string literal
##### (88%)
Admin (root) DB Password: 2d75                6e4fb33b
User (misp) DB Password: 36ca                d5511ed5
Authkey: 4yYI                               4jz3X3
-----
MISP Installed, access here: ""
User: admin@admin.test
Password: admin
-----
The following files were created and need either protection or removal (shred on the CLI)
/home/misp/mysql.txt
-----
Admin (root) DB Password: 2d75                1fb33b
User (misp) DB Password: 36ca                11ed5
/home/misp/MISP-authkey.txt
-----
Authkey: 4yYI                               1z3X3
-----
The LOCAL system credentials:
User: misp
Password: e7687b933                          cc5b # Or the password you used of your custom user
OnuPG Passphrase id: 7434b095*                1f8e1d5833e
-----
To enable outgoing mails via postfix set a permissive SMTP server for the domains you want to contact:
sudo postconf -e 'relayhost = example.com'
sudo postfix reload
-----
Enjoy using MISP. For any issues see here: https://github.com/MISP/MISP/issues
-----
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
misp@misp-privado:~$
```

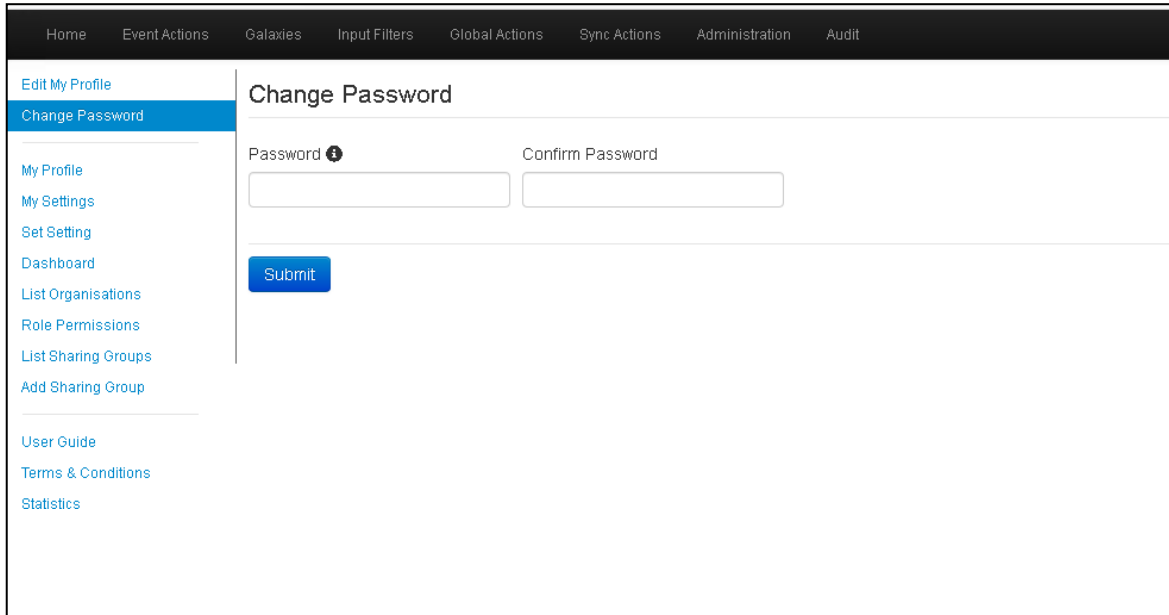

Acceso a interfaz

Una vez finalizada la instalación podemos acceder a la interfaz web https://<IP_servidor_MISP>. Utilizaremos las siguientes credenciales que vienen por defecto:

Usuario: admin@admin.test

Contraseña: admin

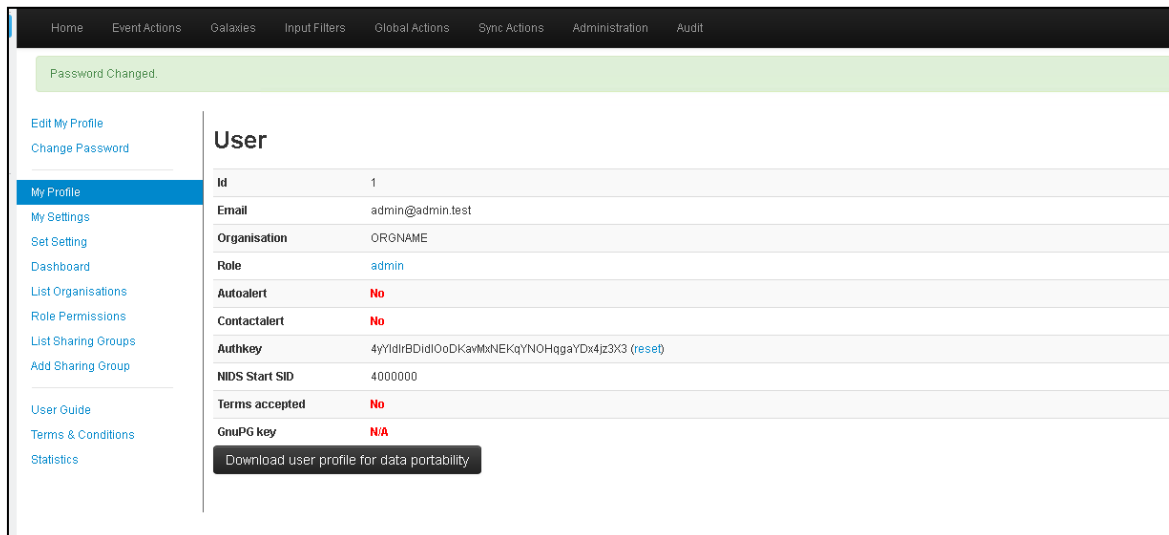
La primera vez que se ingrese se pedirá cambio de la contraseña.



The screenshot shows the MISP web interface with the 'Change Password' form. The navigation bar at the top includes: Home, Event Actions, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, and Audit. On the left, a sidebar menu lists: Edit My Profile, Change Password (highlighted), My Profile, My Settings, Set Setting, Dashboard, List Organisations, Role Permissions, List Sharing Groups, Add Sharing Group, User Guide, Terms & Conditions, and Statistics. The main content area is titled 'Change Password' and contains two input fields: 'Password' and 'Confirm Password', followed by a blue 'Submit' button.

Cambio de contraseña

Una vez cambiada la contraseña, se podrá acceder a las demás opciones y empezar a configurar el servicio.



The screenshot shows the MISP web interface after a successful password change. A green notification bar at the top reads 'Password Changed.'. The navigation bar and sidebar are the same as in the previous screenshot. The main content area is titled 'User' and displays a table of user details:

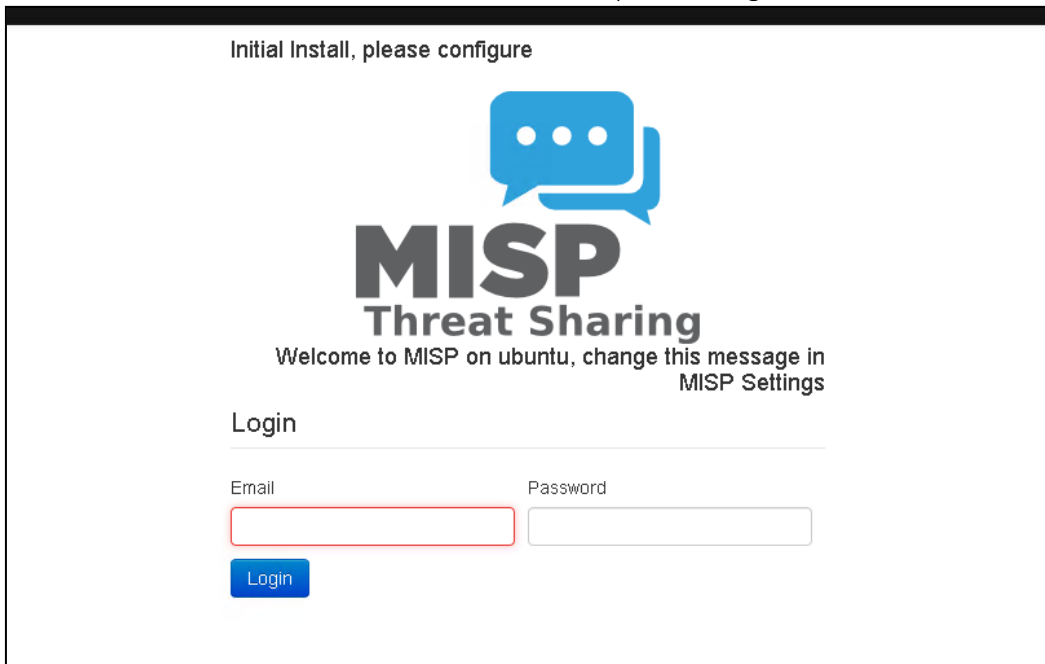
Id	1
Email	admin@admin.test
Organisation	ORGNNAME
Role	admin
Autoalert	No
Contactalert	No
Authkey	4yYldlrBDldlOoDkavMxNEKqYNOHqgaYDx4jz3X3 (reset)
NIDS Start SID	4000000
Terms accepted	No
GnuPG key	N/A

Below the table is a button labeled 'Download user profile for data portability'.

Configuración del MISP

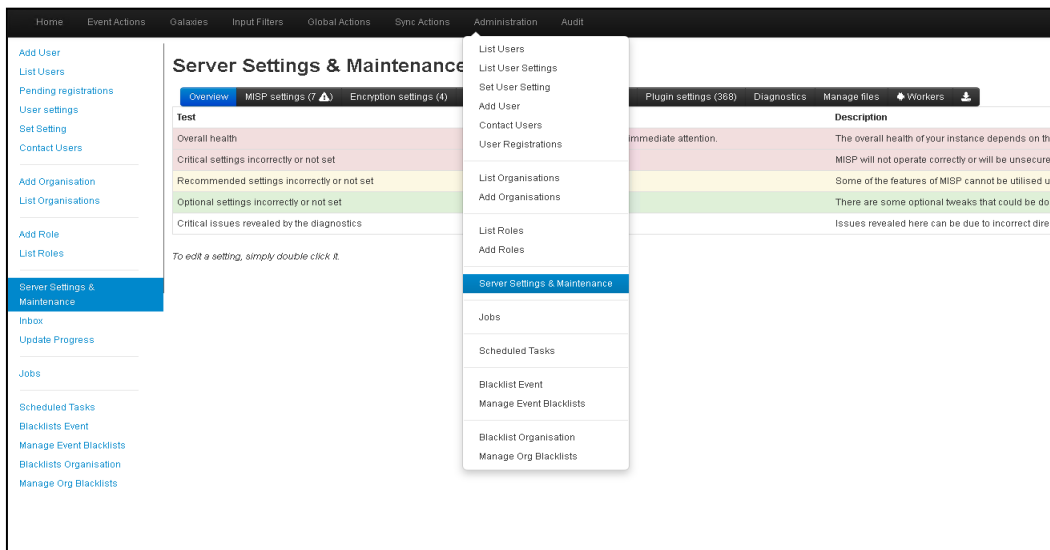
Inicio de sesión

Se debe iniciar sesión en el servidor con las credenciales que se le asignaron.



Configuración de parámetros

En el menú **Administration** seleccionar la opción **Server Settings & Maintenance** para configurar parámetros que nos ayudarán a un mejor rendimiento del equipo.



Test	Description
Overall health	The overall health of your instance depends on the immediate attention.
Critical settings incorrectly or not set	MISP will not operate correctly or will be unsecure unless you fix these issues.
Recommended settings incorrectly or not set	Some of the features of MISP cannot be utilised unless you fix these issues.
Optional settings incorrectly or not set	There are some optional tweaks that could be done to improve performance.
Critical issues revealed by the diagnostics	Issues revealed here can be due to incorrect direct

Modificación de parámetro de bienvenida

Modificar parámetro “MISP.welcome_text_top” para personalizar el mensaje de bienvenida.

Optional	MISP.full_tags_on_event_index	Full tags	Show the full tag names on the e
Optional	MISP.welcome_text_top	Initial Install, please configure	Used on the login page, before t
Optional	MISP.welcome_text_bottom	Welcome to MISP on ubuntu, change this message in MISP Settings	Used on the login page, after the

Configuración de Redis-Server

Si no tiene habilitado IPv6 en el servidor MISP, deberá configurar el servicio Redis-Server para que no utilice IPv6, esto debido a que en algunas ocasiones al reiniciar el servicio arroja un error y no levanta la aplicación.

Se realiza de la siguiente manera:

`vi /etc/redis/redis.conf`

```
# IF YOU ARE SURE YOU WANT YOUR INSTANCE TO LISTEN TO ALL THE INTERFACES
# JUST COMMENT THE FOLLOWING LINE.
# ~~~~~
bind 127.0.0.1 :::1
# Protected mode is a layer of security protection, in order to avoid that
# Redis instances left open on the internet are accessed and exploited.
#
```

Configuración y reinicio de servicio

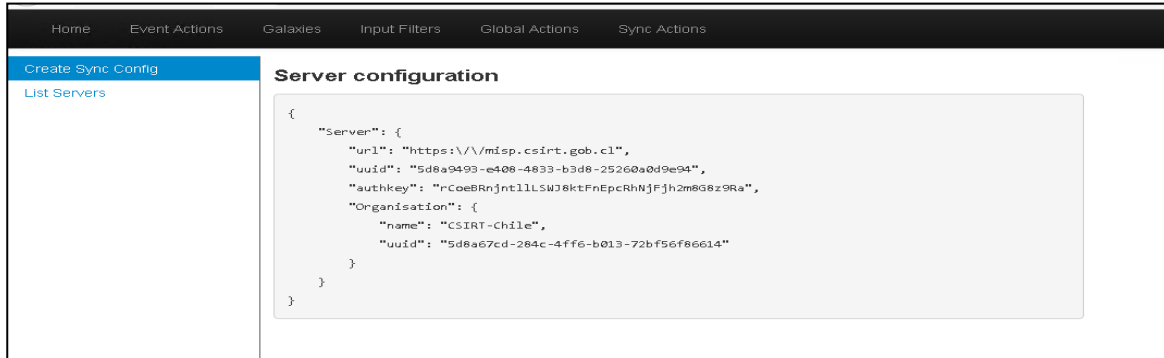
Se debe eliminar la configuración `:::1` y luego reiniciar el servicio (o servidor)
`systemctl restart redis-server`

```
root@misp-privado:~# systemctl restart redis-server
root@misp-privado:~#
root@misp-privado:~#
root@misp-privado:~#
root@misp-privado:~# systemctl status redis-server
● redis-server.service - Advanced key-value store
   Loaded: loaded (/lib/systemd/system/redis-server.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2020-06-23 15:27:39 UTC; 10s ago
     Docs: http://redis.io/documentation,
           man:redis-server(1)
   Process: 21700 ExecStop=/bin/kill -s TERM $MAINPID (code=exited, status=0/SUCCESS)
   Process: 21703 ExecStart=/usr/bin/redis-server /etc/redis/redis.conf (code=exited, status=0/SUCCESS)
  Main PID: 21721 (redis-server)
    Tasks: 4 (limit: 4915)
   CGroup: /system.slice/redis-server.service
           └─21721 /usr/bin/redis-server 127.0.0.1:6379

Jun 23 15:27:39 misp-privado systemd[1]: Starting Advanced key-value store...
Jun 23 15:27:39 misp-privado systemd[1]: redis-server.service: Can't open PID file /var/run/redis/redis-server.pid (yet)
Jun 23 15:27:39 misp-privado systemd[1]: Started Advanced key-value store.
root@misp-privado:~#
```

Script de configuración para comunicar MISP

Para obtener el script de configuración para establecer comunicación entre otros MISP se debe iniciar sesión con un usuario **SyncUser**, luego en **Sync Actions** y **Create Sync Config**.



The screenshot shows the MISP web interface. The top navigation bar includes 'Home', 'Event Actions', 'Galaxies', 'Input Filters', 'Global Actions', and 'Sync Actions'. The left sidebar has 'Create Sync Config' (highlighted) and 'List Servers'. The main content area is titled 'Server configuration' and displays a JSON configuration for a server:

```
{
  "server": {
    "url": "https://misp.csirt.gob.cl",
    "uuid": "5d8a9493-e408-4833-b3d8-25260a0d9e94",
    "authkey": "rCoeBRnjnt11LSWj0ktFnEpcRhNjFjh2m08z9Ra",
    "organisation": {
      "name": "CSIRT-Chile",
      "uuid": "5d8a67cd-284c-4ff6-b013-72bf56f86614"
    }
  }
}
```

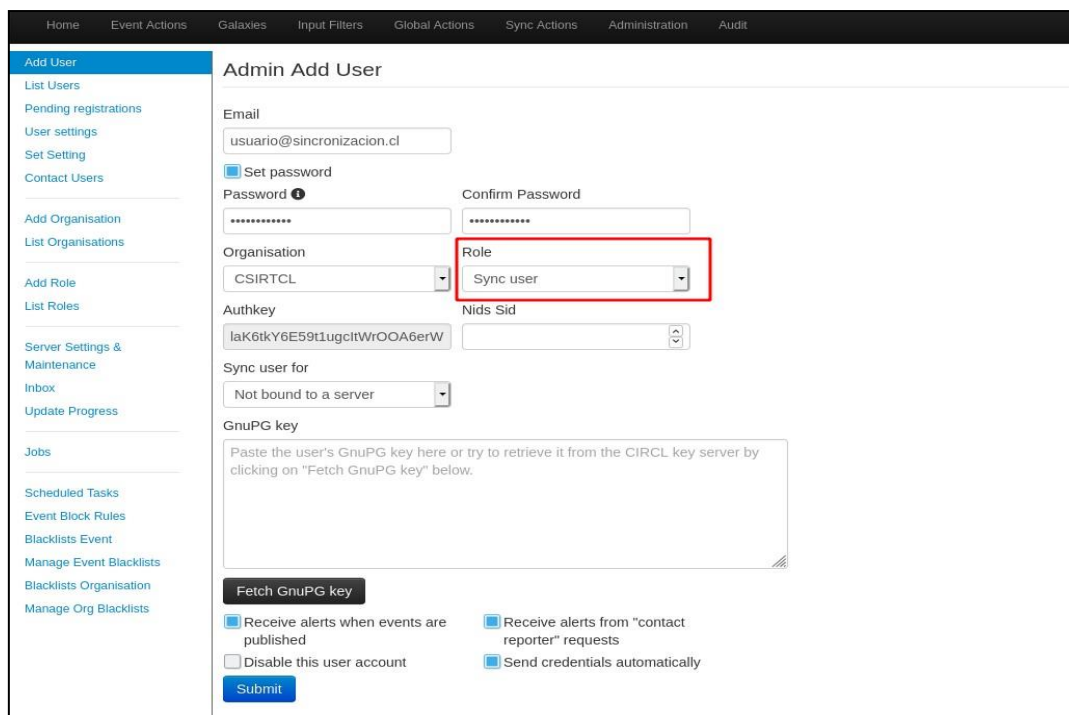
Conexión del MISP

Esta sección tiene como objetivo guiar a los usuarios y organizaciones para que puedan conectar su plataforma MISP (Plataforma para compartir información de Malware) con otras similares. Aquí se describen los pasos que deben seguir los administradores de la plataforma, ya sea en el caso de enviar la información para sincronizar los ambientes, o en el caso de recibirlo.

Sincronizar enviando contraseñas.

Para conectar 2 instancias de MISP se recomienda utilizar usuarios de sincronización. Para este primer paso, y con un usuario con rol **Org Admin**, tenemos que dirigirnos al menú **Administration** → **Add User**, dónde crearemos un usuario con el rol **Sync user**.

Luego se debe enviar al administrador de la plataforma misp a la cual nos queremos conectar la siguiente información del usuario:



The screenshot shows the 'Add User' form in the MISP administration interface. The form is titled 'Admin Add User' and includes the following fields and options:

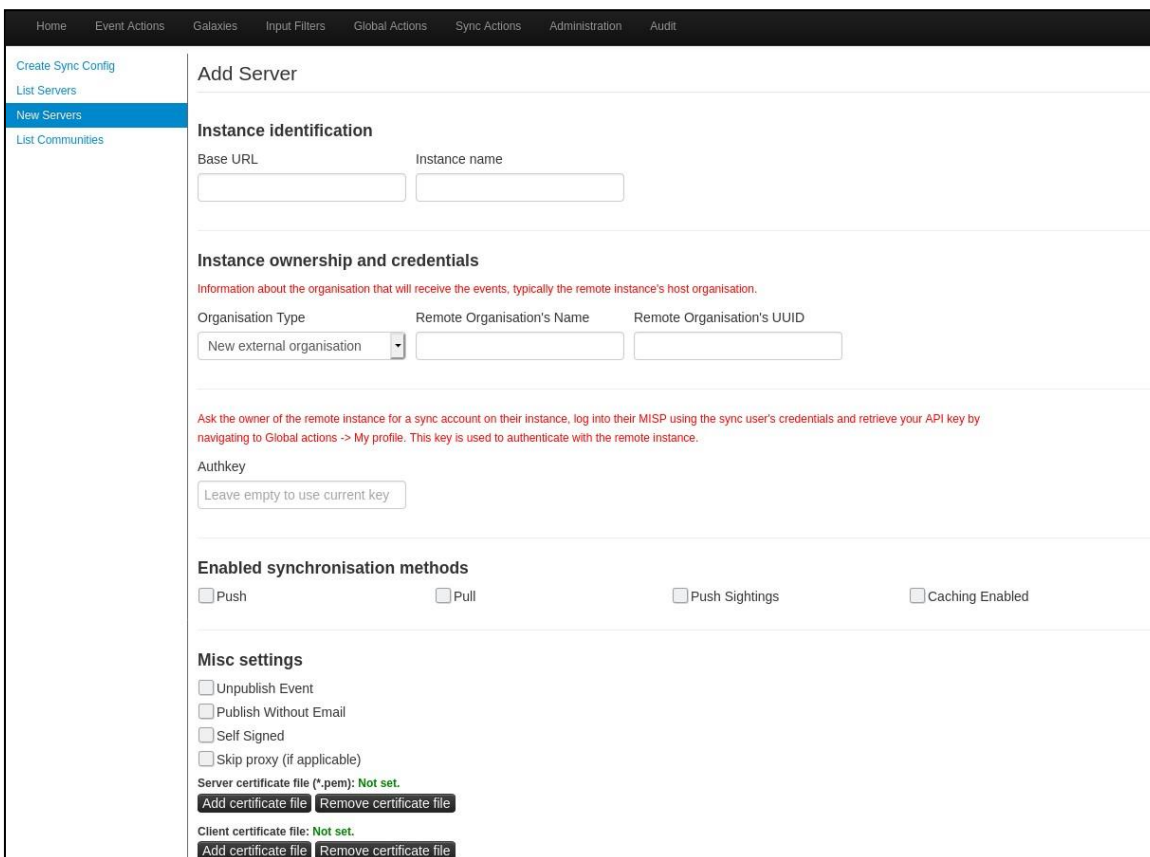
- Email:** usuario@sincronizacion.cl
- Set password:**
- Password:** [Redacted]
- Confirm Password:** [Redacted]
- Organisation:** CSIRTCL
- Role:** Sync user (highlighted with a red box)
- Authkey:** laK6tkY6E59t1ugctWroOA6erW
- Nids Sid:** [Redacted]
- Sync user for:** Not bound to a server
- GnuPG key:** [Redacted]
- Fetch GnuPG key:** [Button]
- Receive alerts when events are published:**
- Receive alerts from "contact reporter" requests:**
- Disable this user account:**
- Send credentials automatically:**
- Submit:** [Button]

- Base Url (url o IP de su instancia MISP)
- email (del Sync User creado anteriormente)
- Authkey (del Sync User creado anteriormente)
- UUID (se encuentra en el menú Administration → List Organisations, seleccionar el UUID de su instancia)

Sincronizar recibiendo contraseñas

En el caso de que reciba la información anterior, se debe configurar en el servidor MISP de la siguiente manera:

- 1) Se debe loguear con un usuario utilizando el rol **Org Admin** o **Admin**.
- 2) Luego en el menú **Sync Actions** → **Remote Server**.
- 3) Enseguida, en el menú de la izquierda, se debe seleccionar **New Servers** y rellenar los campos **Base URL** e **Instance name** (con un nombre descriptivo de la instancia a la cual se conectará).
- 4) En el combo box **Organization Type**, debe seleccionar la opción **New external organisation** y rellenar los campos **Remote Organisation's Name** y **Remote Organisation's UUID**.
- 5) De la misma manera, se debe rellenar el campo **Authkey**.



The screenshot shows the 'Add Server' configuration page in the MISP interface. The page is divided into several sections:

- Instance identification:** Contains two input fields for 'Base URL' and 'Instance name'.
- Instance ownership and credentials:** Includes a dropdown menu for 'Organisation Type' (set to 'New external organisation'), and input fields for 'Remote Organisation's Name' and 'Remote Organisation's UUID'. A red note below states: 'Information about the organisation that will receive the events, typically the remote instance's host organisation.'
- Authkey:** A text input field with a placeholder 'Leave empty to use current key'.
- Enabled synchronisation methods:** Four checkboxes: 'Push', 'Pull', 'Push Sightings', and 'Caching Enabled'.
- Misc settings:** A list of checkboxes: 'Unpublish Event', 'Publish Without Email', 'Self Signed', and 'Skip proxy (if applicable)'. Below these are two sections for certificates: 'Server certificate file (*.pem): Not set.' and 'Client certificate file: Not set.', each with 'Add certificate file' and 'Remove certificate file' buttons.

- 6) En las opciones **Enabled synchronisation methods** en un primer paso no se debe seleccionar nada, una vez se valide la comunicación entre MISP se pueden seleccionar las acciones que queremos que se ejecuten, por lo general **Push y Pull**.
- 7) En las opciones **Misc settings** seleccionar la opción **Self Signed** (esto nos asegura que se conecten las instancia aunque no tengan un certificado) y la opción **Publish Without Email** (para evitar que se envíen muchos correos en el caso de que la cantidad de eventos creados sean muchos), no se recomienda marcar **Unpublish Event** para evitar que se compartan eventos que estén en algún proceso de relleno y en el caso de la opción **Skip proxy solo si aplica**.
- 8) Finalizar esta primera etapa de configuración con el boton **Submit**. Al realizar este paso se mostrará el nuevo servidor ya configurado, para verificar que la comunicación es exitosa podemos ejecutar el test que se encuentra al lado del nombre del nuevo registro creado.

The screenshot shows the 'Servers' management interface. A table lists the server configuration for 'CSIRT-Chile'. The 'Run' button is highlighted with a red arrow.

Id	Name	Prio	Connection test	Sync user	Reset API key	Internal	Push	Pull	Push Sightings	Cache	Unpublish Event (push Event)	Publish Without Email (pull Event)
2	CSIRT-Chile				View	Reset	x	✓	x	x	x	x

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

Un resultado exitoso de este procedimiento debe visualizarse como sigue:

The screenshot shows the 'Servers' management interface with detailed configuration information for the 'CSIRT-Chile' server.

Id	Name	Prio	Connection test	Sync user	Reset API key	Internal	Push	Pull	Push Sightings	Cache	Unpublish Event (push Event)	Publish Without Email (pull Event)
2	CSIRT-Chile		Local version: 2.4.130 Remote version: 2.4.128 Status: Remote outdated, notify admin! Compatibility: Compatible POST test: Received sent package		View	Reset	x	✓	x	x	x	x

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

Continuamos la configuración de esta instancia presionando el ícono de **Edit** en el campo **Actions**. Posteriormente, habilitaremos los métodos de sincronización activando **Push** y **Pull** según corresponda.

Además se podrán configurar reglas para cada tipo de sincronización, permitiendo o denegando algún TAG y/o Organizaciones.

Id	Name	Prio	Connection test	Sync user	Reset API key	Internal	Push	Pull	Push Signings	Cache	Unpublish Event (push Event)	Publish Without Email (pull Event)	Url	Remote Organisation	Cert File	Client Cert File	Self Signed	Skip Proxy	Org	Actions
2	CSIRT-Chile		Local version: 2.4.130 Remote version: 2.4.128 Status: Remote outdated, notify admin Compatibility: Compatible POST test: Received sent package	View	Reset	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	https://misp.csirt.gob.cl	CSIRT-Chile			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	CSIRTCL	Edit

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

En el caso de las reglas de **Pull**, se recomienda agregar el siguiente parámetro para que en el caso de Conectarse con un MISP con muchos eventos solo sincronice los últimos 7 días:
“{“publish_timestamp”: “7d”}”

Set pull rules

Allowed Tags (OR)

<<
>>

Blocked Tags (AND NOT)

AND

Allowed Orgs (OR)

<<
>>

AND NOT

Blocked Orgs (AND NOT)

Additional sync parameters (based on the event index filters)

```
{“publish_timestamp”: “7d”}
```

[Update](#)

[Cancel](#)

Comentarios finales

Adoptar un MISP en una organización mejora las capacidades de seguridad cibernética y de análisis de datos, especialmente en términos de recolección, almacenamiento, correlación, procesamiento de datos y visualización de la información.

Los MISP permiten obtener indicadores de compromisos en forma oportuna que podrían evitar un incidente dentro de una entidad específica, o un sector definido.

Este trabajo busca ser un incentivo para las organizaciones, para prepararse y sumarse a un proyecto nacional que permita asociar a entidades de diferentes rubros y hasta competidores en áreas comerciales, para que configuración de un MISP.

El objetivo de fondo es tomar medidas pro-ciberseguridad sin esperar que existe un marco normativo ideal, y beneficiar a diferentes comunidades mediante una fórmula de colaboración probada y exitosa, que permita formar una cultura organizacional de ciberseguridad en nuestro ecosistema nacional.

Bibliografía consultada

- Dundarad, L.; Serrano, O. Towards Improved Cyber Security Information Sharing. 5th International Conference on Cyber Conflict (CyCon). Enero, 2013.
- Murdoch, S.; Leaver, N. Anonymity vs. Trust in Cyber-Security Collaboration. WISCS '15: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security. Octubre, 2015.
- Wagner, C.; Dulaunoy, A.; Wagener, G.; Iklody, A. MISP - The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform. 3rd ACM Workshop on Information Sharing and Collaborative Security. Octubre, 2016.
- Cornet Arbós, D. Dockerized MISP (Malware Information Sharing Platform). Escola Tècnica d'Enginyeria de Telecomunicació de Barcelona Universitat Politècnica de Catalunya, Junio, 2018.
- González-Granadillo, G.; Faiella, M.; Madeiros, I.; Azevedo R.; González-Zarzosa, S. Enhancing Information Sharing and Visualization Capabilities in Security Data Analytic Platforms. 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W). Junio, 2019.
- Bauer, S.; Fischer, D.; Sauerwein, C.; Latzel, S.; Stelzer, D; Breu, R. Towards an Evaluation Framework for Threat Intelligence Sharing Platforms. Proceedings of the 53rd Hawaii International Conference on System Sciences. 2020

