# Caso de estudio

Para mostrar el uso de la herramienta se simulo en un ambiente virtualizado la interacción y colaboración entre varios CSIRTs. Mediante esta prueba se realizo el intercambio de cyber observables entre las distintas organizaciones. Dicho intercambio se realizo utilizando los distintos servicios provistos por TAXII.

## Escenario del caso de estudio

Se desplegaron dos servidores para realizar la prueba de concepto, cada uno de estos servidores tiene instalado Linux Mint 17. En dichos equipos se instaló RTIR junto con TAXIIApp. Además en el servidor correspondiente al CSIRT2 se instalo YETI. Cada uno de esos servidores tiene incluido una base de datos con esquemas correspondientes a cada una de las aplicaciones. En la figura 1 se ve un esquema representando el despliegue realizado.

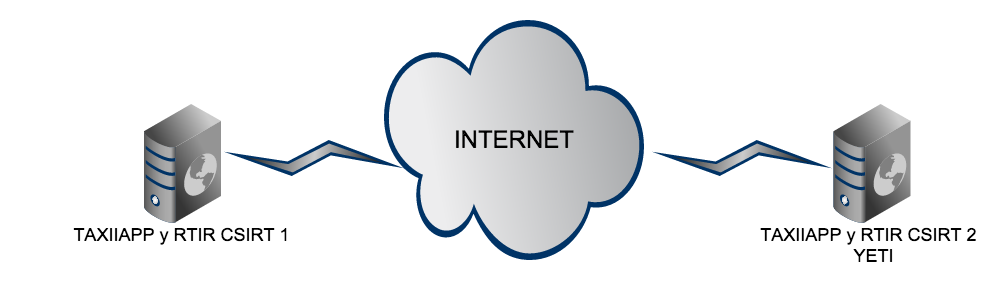


Figura 1 Despliegue realizado para el caso de estudio

La tabla que se presenta a continuación indica la información respecto al laboratorio implementado.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Equipo | Hostname | Ip | Puerto | Aplicación |
| CSIRT 1 | csirt1.com | 172.16.59.219 | 8080 | RTIR |
| CSIRT 1 | csirt1.com | 172.16.59.219 | 8001 | TAXIIApp |
| CSIRT 2 | csirt2.com | 172.16.59.218 | 8080 | RTIR |
| CSIRT 2 | csirt2.com | 172.16.59.218 | 8001 | TAXIIApp |
| CSIRT 2 | csirt2.com | 172.16.59.218 | 9080 | YETI |

En la tabla 1 se muestra las direcciones ip para cada uno de los equipos utilizados en el caso de estudio. En el CSIRT 1 se tiene instalado RTIR con el plugin implementado durante el proyecto para comunicarse con TAXIIApp. También se tiene instalado TAXIIApp para realizar los intercambios de información con el protocolo TAXII. RTIR escucha en el puerto 8080 mientras que TAXIIApp en el 8001.

Dichas aplicaciones se encuentras instaladas también en el CSIRT 2 escuchando en los mismos puertos. A su vez en el CSIRT 2 se encuentra una instalación de YETI. Dicha instalación se encuentra escuchando en el puerto 8080. YETI y TAXIIApp se encuentran corriendo ambas en el mismo equipo para no tener una maquina virtual extra.

En cada uno de los equipos se encuentra instalada una base de datos Mysql en la que se encuentran los esquemas de base de datos utilizados por cada una de las aplicaciones.

## Ejecución del caso de estudio

La figura 3 siguiente muestra cuales fueron los pasos para realizar el intercambio entre las distintas organizaciones.

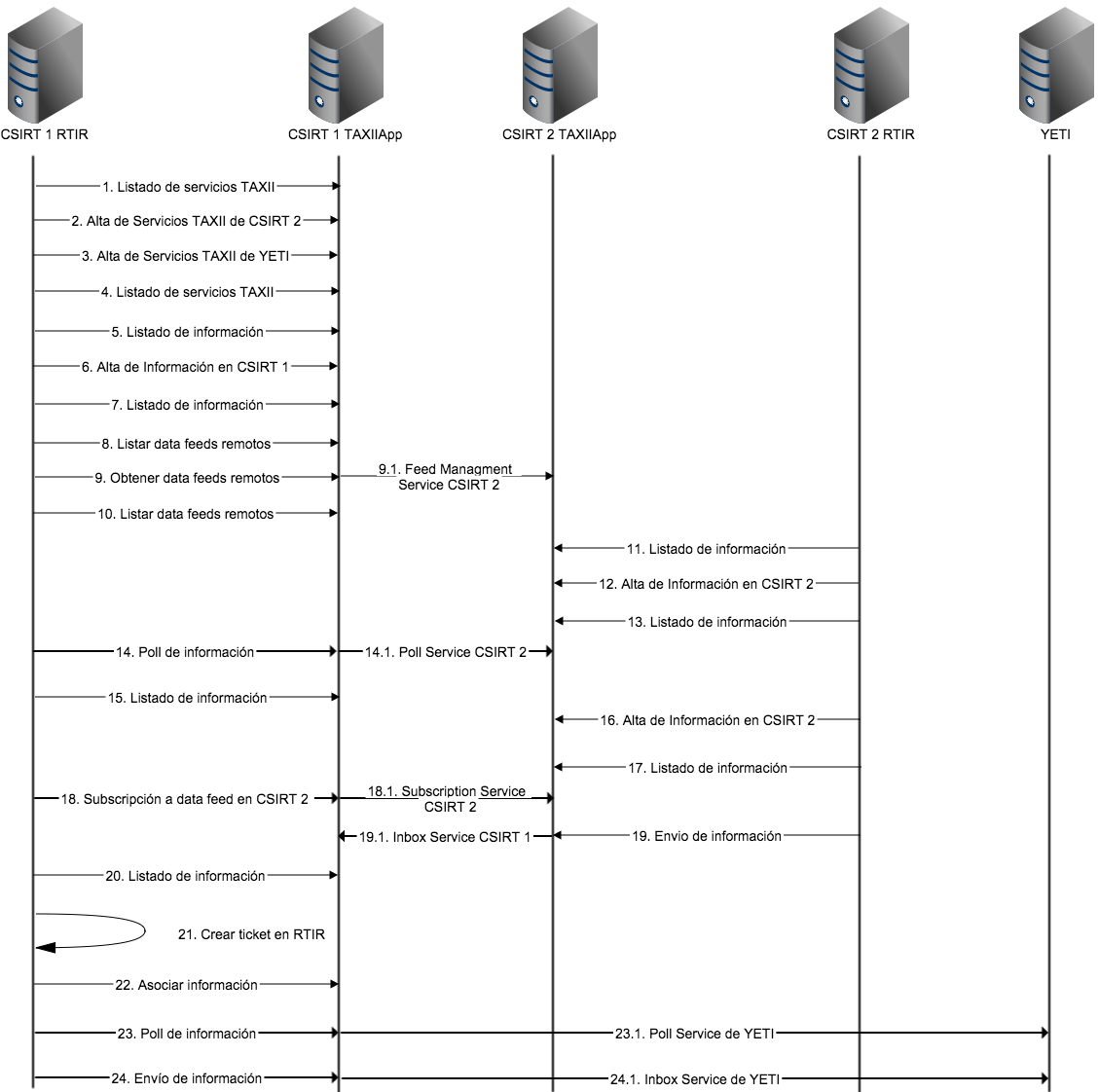


Figura 3 Flujos realizados por el caso de estudio

En los pasos 1 a 4 de la figura 3 agregamos en el CSIRT 1 los servicios TAXII correspondientes a TAXII App y a YETI, ambos ejecutándose en el CSIRT 2.

En el caso de TAXII App se agregaron todos los servicios necesarios para realizar el intercambio. Sin embargo, la implementación de YETI solo cuenta con el inbox service, poll service y discovery service, por lo tanto se agregaron inbox service y poll service como los servicios en YETI. La implementación de TAXII realizada durante el proyecto no implementó el discovery service y por ello fue necesario implementar un caso de uso para ingresar los servicios. Es necesario recordar que al realizar la implementación se pueden decidir que servicios se implementan y cuales no, de forma de que no se tiene porque contar con todos ellos.

En la figura 4 observamos el ingreso de los servicios TAXII y en la figura 5 el listado de los servicios ingresados anteriormente.

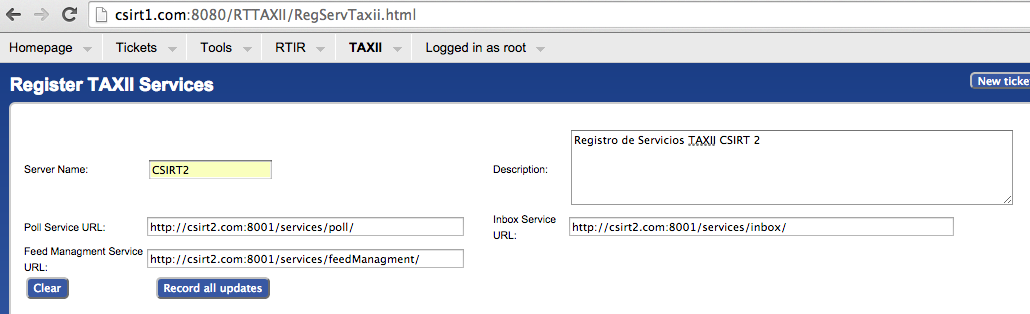


Figura 4 Registro de Servicios TAXII

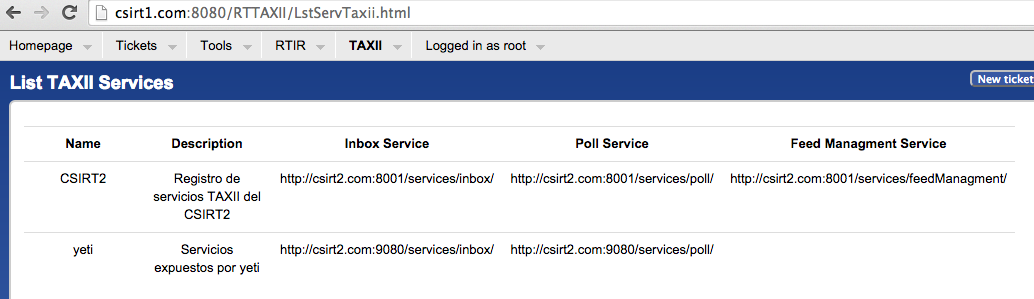


Figura 5 Listado de Servicios TAXII

En los pasos 5 a 7 de la figura 3 se ingresa nueva información en el CSIRT 1, a su vez se comprueba que la información se halla dado de alta adecuadamente en el sistema. Lo mismo se realiza en los pasos 11 a 13, 16 y 17, la diferencia que esta vez se realiza desde el CSIRT 2, dicha información será luego enviada al CSIRT 1 por medio del poll service así como del inbox service.

En la figura 6 se ve el ingreso de información, se da de alta un Cyber observable que representa un correo electrónico que podría provenir por ejemplo de un ataque de phishing. En el anexo se pueden ver los distintos cyber observables dados de alta, los cuales se obtuvieron de [MITRE](https://cybox.mitre.org/language/version2.1/#CYBOX%20samples). (Esto en realidad es una referencia al link)

En la figura 7 se observa información dada de alta en el sistema, también se ve información que fue obtenida por medio del poll service del data feed “default” del CSIRT 2.

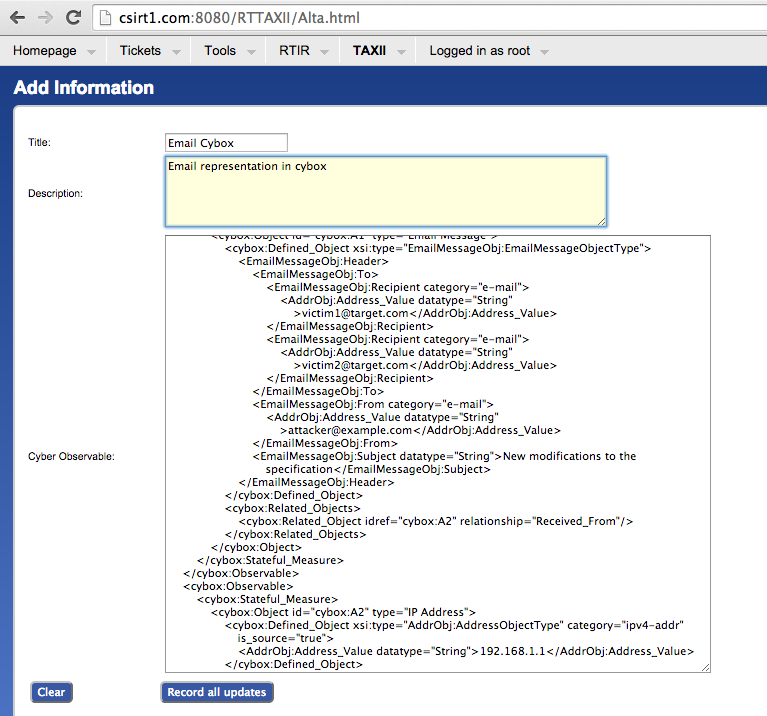


Figura 6 Alta de información de correo electrónico

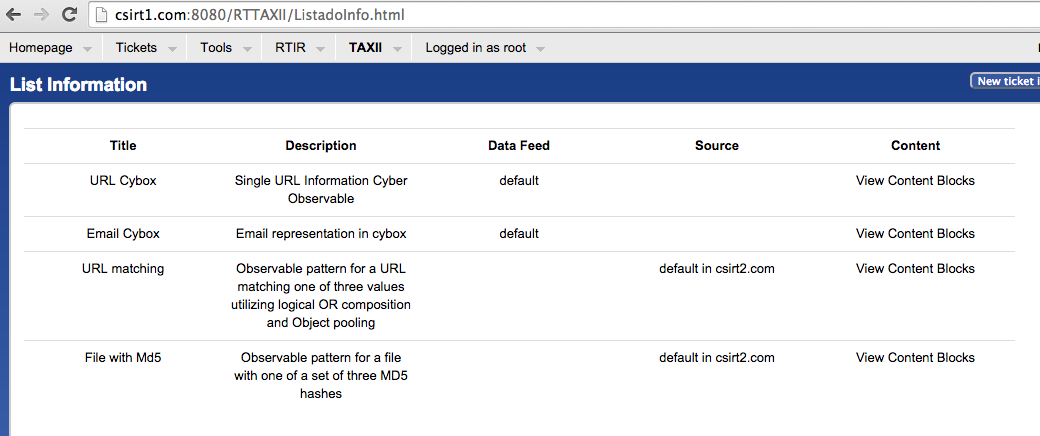


Figura 7 Listado de información en el sistema

Los pasos 8 a 10 se encargan de la obtención de los data feeds en el CSIRT 2 y a su vez se comprueba que los data feeds se hayan obtenido correctamente. Para obtener los data feeds se envía un mensaje desde TAXII App en el CSIRT 1 solicitándolos al CSIRT 2.

La figura 8 muestra la obtención de los data feeds remotos en el CSIRT 2, luego en la figura 9 se ve un listado del data feed obtenido. A su vez se ve el data feed de YETI.

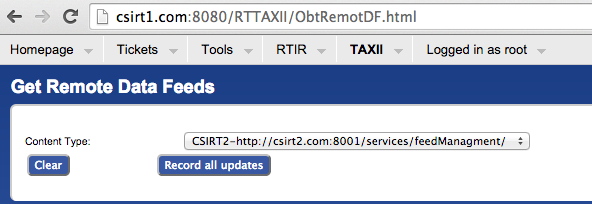


Figura 8 Obtención de data feeds remotos

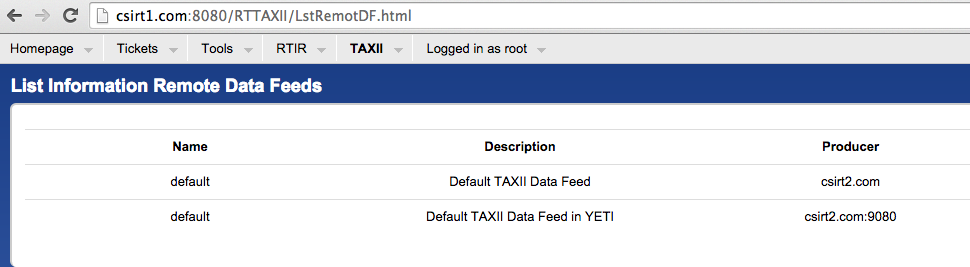


Figura 9 Data feeds en otras organizaciones

En el paso 14 se realiza el poll de información, para ello se invoca al poll service en el CSIRT 2, esto devuelve toda la información en el data feed especificado. Luego de realizado este paso, se lista nuevamente la información para ver cuales fueron los datos recibidos.

En la figura 10 se ve el polling de información. Previamente se vio el listado de información luego de hacer el poll.

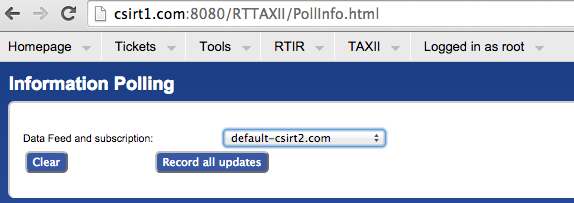


Figura 10 Poll de información

Como se dijo anteriormente, en los pasos 16 y 17 se ingresa nueva información al CSIRT 2, dicha información es agregada para luego ser enviada al inbox del CSIRT 1. Previo a ser enviada, el CSIRT 1 debe registrarse para indicar que desea recibir información al inbox service. Dicha subscripción se realiza en el paso 18 invocando al servicio de feed managment del CSIRT 2. Luego de esto, en el paso 19, se envía la información al inbox service del CSIRT 1 desde el CSIRT 2.

En el paso 20 se observan los nuevos datos obtenidos luego de que se envíe la información al inbox service del CSIRT 1.

En las figuras 11 y 12 se ve la subscripción a un data feed en otra organización, mientras que en la 13 se ve el envío de información que se realizará por medio de inbox service como se dijo anteriormente.

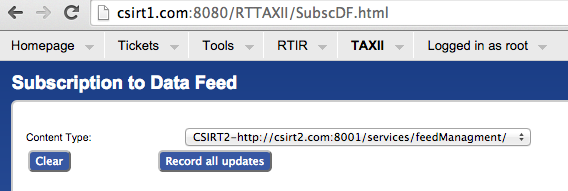


Figura 11 Primer paso de subscripción a data feeds

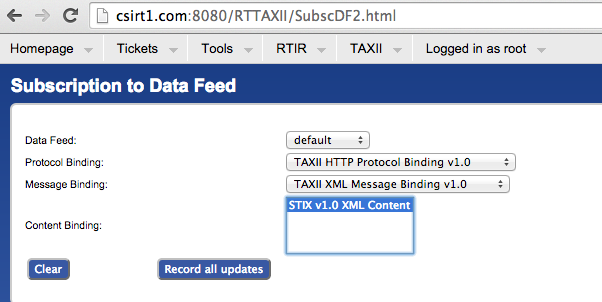


Figura 12 Segundo paso de subscripción a data feeds



Figura 13 Envio de información

En el paso 21 se crea un nuevo ticket en el RTIR, dicho ticket será asociado con información existente en TAXII App. Dicha información puede haber sido obtenida de uno de los otros CSIRTs o de ingresada por un analista localmente.

En la figura 14 se ve la asociación entre tickets del RTIR e información almacenada en TAXIIApp.



Figura 14 - Asociación entre Tickets y Content blocks

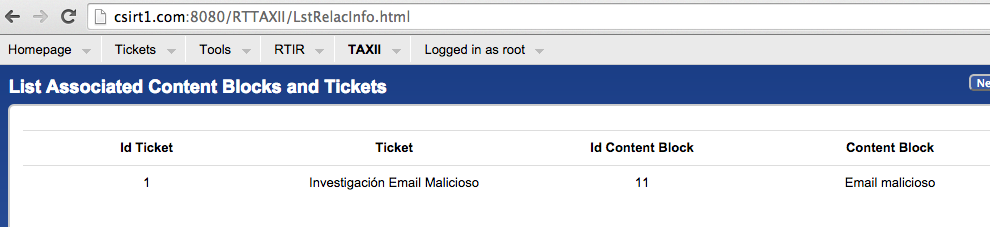


Figura 15 Listado de asociaciones existentes

Finalmente se invoca al poll service de YETI para obtener información y luego se envía información a YETI utilizando su inbox service. Como se dijo anteriormente, YETI no tiene todos los servicios implementados y además no puede iniciar el intercambio de información. Como YETI no implementa el manejo de subscripciones u obtenciones de data feeds, se ingreso previamente dicha información de YETI en el CSIRT 1.