Implementació d'una plataforma d'intercanvi d'informació de ciberamenaces

Aleix De la Rubia Campamà

Resum– Els problemes de seguretat estan augmentat molt progressivament degut al gran impacte que tenen les tecnologies en la vida quotidiana i sobretot en el món laboral. Aquests problemes poden ser d'espionatge, hacking, virus, atacs Man In the Middle, entre d'altres. Però sobretot, amb l'objectiu d'obtenir informació de tercers motiu pel qual la compartició de la informació en PIMES i grans multinacionals és un problema molt important ja que cada cop s'envia més informació i es reben més ciberamenaces, obligant a les organitzacions a tenir un pla definit per tal de contrarrestar-les. Aquest informe, intenta donar resposta a aquest problema i demostrar que mitjançant una plataforma per a la compartició de ciberamenaces pot ajudar a reduir el temps de resposta i fer que la informació sigui llegible per a tothom.

Paraules clau– Ciberinteligència, Ciberseguretat, Ciberamenaça, MISP, Grup compartit, Observable, Event, Feed, Docker.

Abstract– Security issues are increasing progressively due to the great impact of technologies on everyday life and especially on the laboral world. These issues can be espionage, hacking, viruses, Man In the Middle attacks, among others, but especially with the aim of gaining third party information which is why sharing information in SMEs and large multinationals is being a very important issue since every time more information is being sent and more cyberthreats are being processed forcing organizations to have a defined plan in order to counteract them. This report tries giving a solution to this issue and demonstrate that using a cyber threat sharing platform can help reducing response time and make information readable to everyone.

Keywords– CyberIntelligence, Cibersecurity, Cyberthreat, MISP, Sharing group, Observable, Event, Feed, Docker.

1 Introducció

A TOTA empresa i administració pública sempre existeixen riscos de patir atacs informàtics a través de la xarxa com bé pot ser el correu electrònic, plataforma web de la pròpia empresa, per medis externs en el sentit de connectar-se a altres pagines web i en les quals ens poden robar credencials [1] o fins i tot a través de dispositius de hardware físics com poden ser el router, cables, entre d'altres. En la figura 1 [2] es mostren totes les incidències que el Centre criptològic nacional localitzat dins del CNI (Centre Nacional d'intel·ligència) ha gestionat en els últims anys i s'observa un augment de quasi 6000 incidències més respecte del 2017.

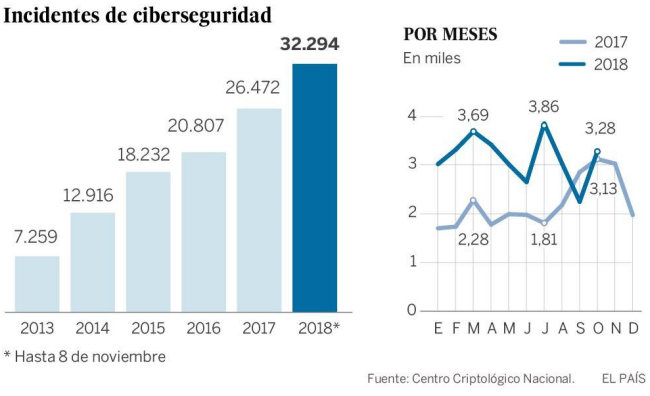

Fig. 1: Incidències de ciberseguretat.

La gestió de tot aquest tipus d'incidències que realitza l'organització de tota aquesta informació es defineix amb el terme de ciberseguretat [3]. Molts cops, els incidents d'aquest tipus no són abordats de forma òptima o bé perquè no existeix un pla concret d'acció o perquè no s'actua amb la celeritat suficient i en aquest àmbit de problemes el temps és crucial. Només un 3% de tots els atacs són descoberts en minuts i més del 68% passen dos mesos desapercebuts com

• E-mail de contacte: aleix.delarubia@e-campus.uab.cat
• Menció realitzada: Tecnologies de la Informació
• Treball tutoritzat per: Ángel Elbaz (DEIC)
• Curs 2019/2020

bé es detalla en la figura 2 [4].

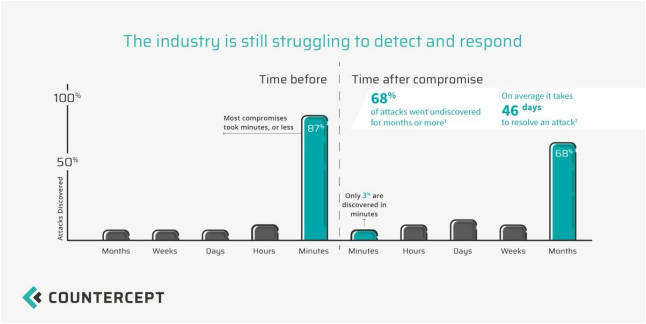

Fig. 2: Temps de resposta a les ciberamenaces.

D'altra banda, un dels principals problemes que existeix un cop l'empresa capta i coneix què ha sigut o si es troba sent atacada és la compartició [5] de tota la informació que la pròpia organització genera a partir dels seus sistemes d'informació interns així com les dades procedents de fonts externes que aquesta ha de tractar i processar en relació amb les amenaces. En aquesta última part, quan es fa referència a la informació que s'ha de processar el que es vol fer entendre és que un atac a vegades pot tenir un modus operandi similar i si més no es poden detectar respostes del sistema semblants. Amb tot això, la compartició o difusió de la informació sobre les ciberamenaces és un gran problema perquè:

- No es realitza de forma eficient, degut per exemple a la gran quantitat de dades que s'han vist afectades.
- La dificultat de fer un seguiment exhaustiu en relació a aquestes sobretot si es tracta d'amenaces avançades persistents APT (Advanced Persitent Threat), que s'executen durant un llarg període de temps i que tenen un grup d'organitzacions específic i d'interès per l'atacant.
- Pel tipus de format en el que es comparteixen les dades ja que cada font designa la seva pròpia manera d'interpretar les característiques de la ciberamenaça.
- Els possibles tipus de protocols o mecanismes utilitzats acostumen a ser diferents.
- Alhora de descriure l'amenaça la semàntica difereix i no existeixen estàndards que defineixin diferents aspectes concrets de l'incident. Per tant, tota aquesta informació s'ha de recopil·lar de forma que tingui un valor final com és el d'assegurar el benestar dels negocis i la gent relacionada amb ells així com també evitar qualsevol inconvenient que els pugui afectar, aquest concepte s'anomena ciberinteligència.

El propòsit d'aquest treball de fi de grau no és ni més ni menys que el de fer conèixer als administradors i tècnics de seguretat d'organismes tan privats com públics la importància que té l'intercanvi d'informació sobre les ciberamenaces. Molts cops quan una empresa rep una atac la gent encarregada d'eliminar els possibles danys o bé no comparteixen la informació amb altres organismes o quan ho comparteixen no segueixen cap estàndard que el seu propi, generant molta ambigüitat a altres empleats encarregats de la seguretat d'administracions diferents alhora d'interpretar la informació de l'incident en qüestió. Per això, una de les principals accions que s'haurien de dur a terme en primera instancia és dotar a tots els empleats de certs coneixements i mecanismes pràctics per tal que puguin descriure tots els incidents, ja siguin importants o no, amb un llenguatge de semàntica estàndard com pot ser per exemple STIX. Per últim, cal destacar que els responsables de seguretat han de ser conscients en tot moment del que està passant a la xarxa i que amb el mínim comportament sospitós que pugui presentar qualsevol sistema o indicador s'actuï seguint un pla de reconeixement [6].

D'altra banda, a la secció 2 s'expliquen els objectius que s'han dut a terme al llarg de tot el treball. A l'apartat 3 es presenten algunes de les mètriques que ajuden a la descripció de tots els actius relacionats amb la ciberseguretat com és el cas dels protocols Security Content Automation Protocol (SCAP) [7]. També s'estudiaran les diferències que existeixen entre marcs comuns utilitzats per a l'intercanvi d'informació de ciberamenaces tals com Cyber Observable eXpression (CYBOX), Structured Threat Information eXpression (STIX) o Trusted Automated eXchange of Indicator Information (TAXII) i després es dóna a conèixer una de les plataformes per compartir la informació . A la secció 4 s'informa de la metodologia emprada. Dins la secció 5 es detalla l'ús dels estàndards STIX i TAXII, apartats 5.1 i 5.2 i més endavant s'explica la implementació d'una plataforma d'intercanvi d'informació de ciberamenaces mitjançant una tecnologia open source d'intercanvi de ciberinteligència com Malware Information sharing Platform (MISP) [8], secció 5.3, on s'intentarà demostrar que quan es rebi un atac es pugui distribuir la informació de manera entenedora entre fonts externes, és a dir, que es pugui intercanviar informació amb altres organitzacions. A partir de la secció 5.4 fins la secció 5.10, s'exposaràn els casos pràctics demostrant que totes les organitzacions s'entenguin entre elles, establir la direcció en la que pot viatjar la transferència de la informació i determinar la visibilitat de les dades entre diferents instàncies. Finalment, a la secció 6 s'esposen les conclusions del treball.

2 OBJECTIUS

L'objectiu principal del projecte com bé s'ha explicat a la part anterior consisteix a implementar una plataforma de ciberamenaces MISP on s'intentarà demostrar que quan es rebi un atac es pugui distribuir la informació de manera entenedora entre diferents organitzacions. Per tal de poder dur a terme aquest objectiu final s'han hagut de realitzar els següents:

- Explicar algunes de les iniciatives més importants emmarcades dins la iniciativa SCAP per la protecció dels actius de la informació.
- Explicar de forma detallada els marcs comuns que han creat el DHS, US-CERT i MITRE CORPORATION com són les mètriques TAXII, STIX i CYBOX.
- Especificar casos d'ús STIX per donar una visió orientativa dels diferents perfils que entren en joc alhora d'abordar un ciberatac.

- Mostrar l'arquitectura conceptual STIX per mostrar quins són els passos d'acció davant un atac informàtic
- Compartició de la informació (perfils de STIX).
- Introducció a TAXII, explicar la seva arquitectura així com els serveis que ofereix.
- Mostrar en un taula les diferencies entre cadascuna d'elles (Estàndards de ciberseguretat).
- Crear una plataforma MISP per mostrar la compartició de la informació.

3 ESTAT DE L'ART

Les ciberamenaces en el món de les noves tecnologies són cada vegada més complexes i difícils de gestionar motiu pel qual la compartició de la informació o *information sharing* s'ha d'efectuar d'una forma ràpida, eficaç i generant el màxim coneixement comú i compartit. Degut a aquests factors tant les entitats públiques com privades requereixen de més col·laboració entre elles ja sigui en la identificació dels incidents, caracterització de certes amenaces i sobretot que la publicació de totes aquestes dades sigui el més estandarditzada per a tothom. En aquest punt és on entren en joc alguns dels estàndards per la compartició de la informació de ciberamenaces com són els Information Sharing Standards, per exemple SCAP, que engloben un gran nombre d'iniciatives que promouen i ajuden a definir diferents tipus d'incidents i a comunicar-los entre les diverses organitzacions.Els estàndards [9] per la compartició de ciberinteligència són un conjunt d'iniciatives creades entre diferents agencies del govern americà les quals intenten facilitar l'automatització i estructuració de vulnerabilitats, mètriques de dany o gravetat de les vulnerabilitats o configuracions gràcies a les quals podem fer ús de mecanismes que ens permeten fer un càlcul i anàlisis molt més precís sobre com ha afectat un atac o quin ha estat l'impacte d'aquest envers al sistema. Totes aquestes propostes es troben emmarcades dins la iniciativa Security Content Automation Protocol (SCAP) que defineix com s'han d'utilitzar tots aquests estàndards per tal d'aconseguir aquestes capacitats i que va ser promoguda pel National Institute of Standards and Technology (NIST), una agència molt important de tecnologia del departament d'administració de comerç dels Estats Units que incentiva i promou l'ús de les Tecnologies de la Informació (TIC) [10] i que col·labora amb organitzacions com MITRE Corporation [11]. Alguns dels estàndards actuals que inclou SCAP són *Common Vulnerability Scoring System (CVSS)* [12] per a calcular mètriques de les vulnerabilitats, *Common Vulnerabilities and Exposures (CVS)* un tipus de taula en la qual trobem vulnerabilitats comuns, etc

D'altra banda, quan es parla de ciberamenaces el Department of Homeland Security (DHS) [13] va crear un marc comú d'actuació per a la compartició o intercanvi de la informació sobre ciberseguretat amb l'objectiu de millorar el coneixement de les ciberamenaces i protegir les xarxes de comunicacions. Aquest marc està compost per 3 estàndards:

- Cyber Observable eXpression (CYBOX): És un tipus d'esquema estandarditzat utilitzat per l'especificació, caracterització, comunicació i gestió dels events de seguretat que succeeixen als sistemes o xarxes de comunicacions, descripció de malware, sistemes de detecció d'intrusions, resposta a incidents i anàlisi forense digital.
- Structured Threat Information eXpression (STIX): És un llenguatge estandarditzat molt flexible, extensible i llegible que pretén descriure totes les dades possibles provinents d'una ciberamenaça.
- Trusted Automated eXchange of Indicator Information (TAXII): És un conjunt de serveis i formats que permeten l'intercanvi d'informació entre organitzacions en temps real però no defineix com s'han d'intercanviar les dades sinó que facilita quin tipus d'informació compartir i amb quines altres organitzacions.

Entre les diferents plataformes open source on compartir la informació hi destaquen: MISP, Wazuh, Suricata, Postfix. Cadascuna d'elles s'ha creat amb l'objectiu de vetllar per la integritat de les dades, millorar la detecció d'amenaces i agilitzar la resposta davant d'un ciberatac. En aquest projecte s'ha emprat MISP, una eina desenvolupada pel CIRCL que és l'equip de defensa de Bèlgica i la OTAN (NCIRC) dins la qual es vol emmagatzemar i correlacionar indicadors de compromís sobre atacs dirigits, permetent d'aquesta manera a les diferents organitzacions compartir informació sobre atacs juntament amb els seus indicadors. Gràcies a això, s'aconsegueix una comunitat col·laborativa sobre ciberamenaces amb l'objectiu d'ajudar a millorar les accions en contra d'aquelles que són dirigides i establir nous plans de prevenció i detecció. De les tres iniciatives per l'information sharing s'ha escollit treballar amb STIX i TAXII ja que són les més utilitzades i compatibles amb la plataforma MISP que és una plataforma open source i fàcil de treballar en un entorn docker per a poder realitzar els casos pràctics que s'explicaràn més endavant.

4 METODOLOGIA

Aquest projecte es desenvoluparà fent servir una metodologia Critical Chain Project Management (CCPM) [14], que es defineix com una metodologia pas per pas amb una sèrie d'activitats independents que segueixen els patrons de planificació, execució i vigilància. La CCPM a més, posa èmfasis als recursos necessaris per executar cadascuna de les tasques afegint més temps del necessari en cadascuna d'elles per tal de no passar-se de la data límit i no perdre temps. Una CCPM funcionaria de la següent manera:

- S'assignen les diferents activitats amb un temps determinat.
- S'assigna més temps extra a aquelles activitats que siguin més propenses a patir més errors durant la seva etapa de vida, normalment són les etapes practiques.
- Un cop realitzada la panificació es comencen a executar les tasques i el temps ja no es pot canviar en tot el projecte. En el cas que alguna de les activitats es retrassi serà degut a que no hi ha hagut una bona planificació.

- L'etapa de vigilància consisteix a monitorejar totes aquelles tasques que o bé han arribat al màxim de temps o que s'han retrassat per tal d'aplicar les solucions corresponents.

5 RESULTATS

5.1 Introducció a STIX

5.1.1 Quin llenguatge utilita STIX

STIX com a llenguatge estandarditzat i comú ens permet compartir informació sobre les ciberamenaces podent ser empleat en qualsevol organització, sistema o base de dades per poder implementar la gran majoria de casso d'ús [15] i els que no estan contemplats. La seva estructura es basa en Extensible Markup Language (XML) per l'especificació dels atacs i tots els elements que es defineixen a la pràctica tenen un format XML Schema Definition (XSD). D'altra banda, cal destacar que XML i XSD no és el mateix i la principal diferència es que XML és el llenguatge com a tal, definint tota la base del codi mentre que XSD s'utilitza per validar i descriure l'estructura i el contingut del codi base XML, és a dir, utilitza tot els atributs que el format XML pot prendre.

5.1.2 Per què s'utilitza STIX

Per tal d'aconseguir que STIX sigui accessible des de diverses plataformes i es pugui aplicar dins múltiples organitzacions compleix els següents principis. El primer d'ells és l'expressivitat fent referencia a la quantitat d'informació que es pot extreure de les ciberamenaces i plasmarho al XML amb XSD. També, STIX permet la integració d'altres estàndards de representació que ajuden a explicar millor les dades d'un atac tals com CyBOX que ajuda a indicar parts observades d'una ciberamenaça, Malware Attribute Enumeration and Characterization (MAEC) [16] o Common Attack Pattern Enumeration and Classification(CAPEC) [17]. Una altra propietat és la flexibilitat, o sigui, el elements obligatoris que una organització ha d'utilitzar alhora de descriure qualsevol atac s'han reduït al mínim. L'extensibilitat permetent extensions customitzades de STIX, l'automatització permetent utilitzar aplicacions per a la creació del codi sens haver de picar-lo des de zero i per acabar la llegibilitat ja que el codi pot ser entès per les persones. D'altra banda, en aquest treball s'utilitzarà una plataforma que utilitza una tecnologia MISP i que es troba organitzada de forma compatible amb STIX i per tant, permet definir la gran majoria d'aspectes involucrats dins un incident amb els atributs que maneja STIX.

5.1.3 Casos d'ús STIX

Per poder descriure la gestió que es fa de les ciberamenaces s'utilitzen els casos d'ús [18] amb els quals descrivim una acció o una activitat realitzada ja sigui pel sistema o per l'usuari mateix.

1. Anàlisi de la ciberamenaça: Aquest primer cas d'ús l'implementa el rol d'analista de ciberseguretat i es basa es poder documentar les característiques de l'atac en qüestió fent servir STIX. A partir d'aquest punt si es considerés necessari s'extrapolaria tota aquesta informació ja sigui o bé a parts internes de la companyia que s'hagin vist afectades, parts externes, a altres organitzacions etc. La informació recollida per part de l'analista pot variar des de definir el comportament de la ciberamenaça, com actuen el ciberatacants o explicar les accions de resposta més òptimes com per exemple, procediments per aturar l'atac, com es poden recuperar les parts afectades etc.

2. Establir patrons del ciberatac: Aquest segon cas d'ús també l'implementa l'analista de ciberseguretat i es basa en establir certs patrons de l'amenaça amb tota la informació que s'ha observat en el pas anterior per així poder identificar-la o detectar-la.

3. Resposta a les ciberamenaces: Aquest cas d'ús l'implementen els responsables de la presa de decisions i els encarregats d'operacions dels sistemes de ciberseguretat. Els responsables usen tota la informació que prèviament els analistes han categoritzat en format STIX i avaluen totes aquelles recomanacions o possibles solucions que s'han especificat dins el document. A més, estudien les accions especifiques més adients i eficients dins l'entorn que s'ha vist afectat per l'atac. D'altra banda, els encarregats de les accions tal i com indica el nom tenen la funció d'aplicar aquells elements, definits en format STIX, que s'han seleccionat per ser implementats en els diferents sistemes de seguretat tals com la prevenció dels atacs els quals doncs s'intenta aplicar algun tipus de bloqueig, la detecció d'aquests en la qual s'intenta actuar quan es produeix l'amenaça i després es genera una alerta a l'equip d'operacions per a que actuï i finalment la resposta als incidents, on es comprova si la ciberamenaça ja és coneguda i llavors s'actua en funció d'aquesta solució o si no ho és doncs utilitzar informació d'atacs semblants.

4. Compartició de la informació: Els responsables poden definir dins del marc STIX quins continguts de l'atac poden ser comunicats i a qui se li poden enviar. Llavors, aquesta política es recollida per les TIC que permeten la comunicació i quan la informació es rebuda per part de les altres organitzacions que han acordat tenir com a format STIX ja la poden incorporar dins els seus sistemes.

   En la figura 9 s'observa el procediment que es realitza quan es rep una ciberamenaça juntament els rols que hi participen.

5.1.4 Arquitectura STIX

Entre organitzacions, la informació que es defineix sobre una ciberamenaça pot ser exactament la mateixa però pot variar si s'analitza com està descrita. Per això, al utilitzar el llenguatge STIX farà que el resultat sigui el més semblant possible. L'arquitectura conceptual STIX, és a dir, no fa referència al codi es basa amb els següents conceptes mostrats a la figura 10.

5.1.5 Perfils STIX: Què són i per què s'utilitzen?

Com bé s'ha comentat abans STIX ens permet compartir tota aquella informació que l'administració vol compartir i aquí és on entren en joc els perfils. Llavors, un perfil es pot definir com la utilització del llenguatge per a compartir informació de les ciberamenaces entre una comunitat, o dit d'una altra forma, les dades que es poden representar mitjançant STIX que una organització comparteix amb la resta de membres de la comunitat. Per aquest motiu, mitjançant l'ús dels perfils es pot indicar quin tipus de dades es vol compartir o no. En la figura 11 es pot observar un exemple sobre com funcionen els perfils. En aquest cas, ambdues organitzacions acorden les dades (variables de color verd) que compartiran com són: Indicator1, Indicator2, Indicator3, TTP1 i TTP2. La fletxa que va des de l'Org A cap a l'Org B indica que la primera és qui facilita la informació a la segona i alhora l'Org A és qui rep aquesta informació. Tanmateix, ambdues entitats es posen d'acord sobre quines variables difonen treien com es pot veure en els sharing profiles les varibles de color vermell com són: Threat Action i el Campaign.

5.2 Introducció a TAXII

TAXII com a tal no utilitza cap llenguatge propi per tal de definir la informació referent a les ciberamenaces sinó que el pretén, és establir un mecanisme de transport de missatges amb el qual es produeixi l'intercanvi d'informació entre les diferents organitzacions emprant a poder ser STIX, és a dir, aquest estàndard pot utilitzar STIX. Per això, és molt important entendre que TAXII no és cap eina ni sistema d'informació de compartició de dades en si mateixa, tot al contrari, defineix protocols per a que es puguin dur a terme aquestes accions. És així, que l'objectiu principal de TAXII és que a través dels serveis que s'especifiquin permetin a productors, s'explica en el següent apartat, i consumidors de la informació realitzar diferents models d'intercanvi de dades.

D'altra banda, alguns dels models de compartició de TAXII són:

- Missatgeria mode push [19]: Un productor facilita informació a un consumidor en forma de missatges que van cap a una safata d'entrada, o sigui, com si fos un correu normal.

- Missatgeria en mode pull: El consumidor decideix que es vol descarregar la informació sense haver d'esperar la connexió del productor guanyant temps de resposta.

- Consulta: El consumidor pot voler només rebre un cert tipus de missatges que compleixin certs criteris.

Per últim, aquests tres models es poden representar en escenaris compostos per un node [20] central per on passen totes les dades que o bé rep informació d'un productor i alhora la transmet a un consumidor, o un node que fa el paper d'ambdós rols. També tenim un productor que emet informació a tots els consumidors i finalment una xarxa P2P que implica que tots es conneten entre si.

5.2.1 Arquitectura TAXII

L'arquitectura de TAXII [21] està composta per tres unitats funcionals, TAXII Transfer Agent (TTA) que es conecta a la xarxa i envia/rep missatges TAXII al message handler d'un altre TTA. Després, el TAXII Message Handler (TMH) la unitat responsable de generar els missatges en el format escollit i que interactua amb el back-end per tal d'interpretar els missatges rebuts. Finalment , el TAXII back-end que realitza una funció diferents depenent de l'organització i per això no hi ha accions generals que realitzi.

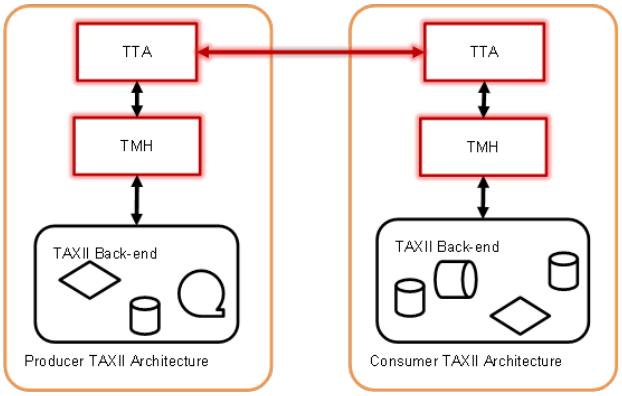

Fig. 3: Arquitectura TAXII.

D'altra banda, si es mira des del punt de vista d'una xarxa l'arquitectura de TAXII es pot descriure en dos parts. La primera, el dimoni que proporciona els serveis que ofereix aquest estàndard com pot ser l'intercanvi de missatges en el que s'utilitza un protocol determinat, el format d'aquests, etc. La segona, la part del client el qual manté contacte directe amb el dimoni remot però no té cap servei que estigui connectat directament a la xarxa, sempre ha de passar pel servidor.

A la figura 3 s'observa un client que pot publicar informació al servidor per a que aquest la pugui enviar cap a altres servidors i alhora, el dimoni remot es troba subscrit als clients en qüestió.

5.3 Implementació

5.3.1 Instal·lació de la instància MISP amb docker

Per recrear l'entorn amb el qual es desenvoluparà la part pràctica s'ha utilitzat la tecnologia Docker [22]. Aquesta eina pretén que els usuaris facin ús dels anomenats contenidors que són espais on s'emmagatzema tota la informació i una de les seves principals avantatges és que són lleugers, és a dir, no ocupen tant d'espai a la memòria com un arxiu d'una imatge virtual i portables ja que permeten executar les aplicacions de software que hi ha instal·lades en qualsevol màquina docker, sense importar el sistema operatiu que hi hagi actiu. Aquesta última qualitat ens permet centrar-nos només en el desenvolupament de codi sense preocupar-nos sobre la instal·lació de possibles requeriments que s'haurien de tenir en compte si es treballés directament des de un SO. Llavors, per tal d'instal·lar l'entorn primer de tot s'ha de procedir a descarregar-se el mecanisme que ens permetrà utilitzar docker i com la part pràctica s'ha dut a terme en un sistema operatiu Ubuntu amb versió 18.04.3 LTS s'han

executat les comandes:sudo apt-get update i sudo apt install docker.io

Amb la primera actualitzem el paquets instal·lats del sistema operatiu ubuntu sense eliminar-los del propi sistma i amb la segona, ja instal·lem el nou paquet docker que ens permetrà utilizar les comandes d'aquesta tecnología.

Arribat a aquest punt s'ha de descarregar l'arxiu docker que conté la plataforma misp per a poder-la executar en localhost, tal i com s'ha dut a terme amb les comandes següents:*git clone https://github.com/harvard-itsecurity/docker-misp.git* i *cd docker-misp.*

Amb la primera descarreguem el repositori remot on es troba l'arxiu Docker amb els arxius necessaris per instal·lar la instància de misp en localhost. En aquest cas, com no li hem indicat cap nom després de la Uniform Resource Locator (URL) se'ns descarregarà amb el nom original que té en remot, docker-misp en aquest cas i amb cd hi accedim un cop baixada.

Després, s'accedeix a la carpeta arrel, *cd .. ./build.sh*, i executem l'arxiu build.sh el qual descarregarà dues imatges i es configurarà tot internament per al seu correcte funcionament. Després, per poder utilitzar MISP s'haurà d'iniciar la base de dades i activar el contenidor harvardsecurity/misp. *docker run -it –rm -v /docker/misp-db:/var/lib/mysql harvarditsecurity/misp /init-db*,*docker run -it -d -p 443:443 -p 80:80 -p 3306:3306 -v /docker/misp-db:/var/lib/mysql harvarditsecurity/misp*.

Finalment, per comprovar si el contenidor es troba actiu executem docker ps -a i si ho està, es fa un start del servei de docker i del contenidor en qüestió amb: *service docker start* i *docker start Çontainer ID"*.

5.3.2 Configuració de l'entorn MISP en localhost

Un cop l'entorn està carregat s'han de procedir a activar certes característiques per a poder treballar. La primera d'elles és canviar el password actual (admin) per un nou de 12 caràcters i clicar la opció *Server Settings & Maintenance*, per a corregir tots els errors que hi ha per defecte a l'aplicatiu MISP. Per a corregir aquest errors, només clicant al camp de l'atribut ja es pot seleccionar el valor per defecte que ens dona i atribuir-li el nou valor fins que el camp deixi d'estar en vermell.

Ara, s'haurà d'activar la part dels anomenats feeds que són els diferents recursos que s'obtenen o bé de forma local o remota per tal de poder generar informació de tercers i que podem recollir per afegir-ho a la nostra instància MISP. Dit d'una altra forma, aquest entorn incorpora una sèrie d'Open-source intelligence (OSINT) feeds, concretament 65 per defecte, per poder ser utilitzats sense que prèviament s'hagi d'importar cap mena d'arxiu. Aquests arxius poden trobar-se en format CSV, MISP o text. Amb tots aquests passos ja podem procedir a realitzar la part pràctica del projecte i poder compartir informació.

5.4 CAS 0: Subscripció a feeds públics

Un cop s'han activat els feeds que ens proporciona MISP per defecte podem rebre informació procendent d'aquests. Tots aquests feeds als quals podem accedir provenen d'altres organitzacions que publiquen events per a totes les comunitats MISP, és a dir, qualsevol instància MISP podrà beneficiar-se de totes aquestes dades i això s'aconsegueix clicant la opció *Sync Actions - List Feeds - Cache MISP feeds*. Per exemple, en la figura 16 s'observen dos feeds provinents de dues organitzacions diferents, ID's diferents, una d'elles ens informa d'un nou BabyShark Malware provinent d'estats Units mentre que l'altre ens indica d'una activitat njRAT que és un tipus de virus Trojan d'accés remot.

5.5 CAS 1: Compartir informació dins una mateixa organització

Tots els casos pràctics es basen en la idea de crear plataformes per una Universitat que tingui diferents departaments. Per tant, el concepte d'organització s'ha d'entendre com si fos un departament o facultat de la UAB com l'Escola d'enginyeria, departament de ciències polítiques de la UAB, etc.

5.5.1 Com podem transmetre dades entre diferents organitzacions ?

Per a poder transmetre les dades s'han de crear events, que són tots els registres d'una mostra que han estat creats a partir d'un atac informàtic i en els quals figuren els seus Indicators of compromise (IOC) que s'han descobert al analitzar la ciberamenaça, s'han importat d'una base de dades o d'una altra entitat que ha patit el mateix atac, podent-los relacionar amb la llista dels nostres feeds.

- Afegim els atributs a l'event en qüestió. Aquests atributs poden ser per exemple des de les parts que ha afectat l'atac, el seu nom, descripció, el seu hash md5, etc.

- Tal i com mostra el requadre vermell de la figura 8, un cop es troba tot definit es publica l'event que serà visible només per la pròpia organització, en aquest cas ORGANISATION A.

En aquesta arquitectura base només hi ha un usuari (User 1) el qual té una relació amb l'event i l'organització A tal i com s'observa en la figura 5.

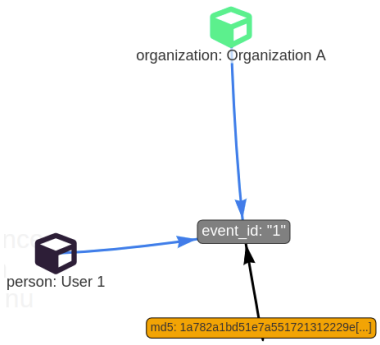

Fig. 4: Arquitectura cas 1.

5.6 CAS 2: Compartir informació entre diferents organitzacions

En aquest cas 2 només hi ha dues organitzacions dins una mateixa instància MISP en localhost. Llavors, per a poder enviar qualsevol mena d'informació sobre qualsevol possible amenaça no es pot només publicar l'event com s'ha dut

a terme en el cas base i això és així, ja que alhora de crear un event s'ha d'especificar amb qui vols compartir aquest event i per tant les dues opcions que existeixen són o bé compartir les dades dins la mateixa organització, com ja s'ha comprovat, o compartir-la a totes les organitzacions cosa que no interessa perquè pot ser que l'organització A només vulgui compartir aquest event amb certes persones d'una organització B sense que l'organització C s'enadoni. Dit això, què s'ha fet en aquest cas? Doncs per tal de poder comunicar-se entre elles s'ha procedit a la creació d'un sharing group [23] o grup compartit.

5.7 Creació d'un sharing group

Un sharing group és un conjunt d'entitats o individus que s'uneixen per tal transmetre's informació secreta o de certa privatitat de la qual no es vol compartir amb ningú més. Per a poder crear aquest grup d'organitzacions en aquest cas es realitza el següent:

1. Es clica a *Global Actions - Add sharing group* i apareixerà un requadre en el qual s'ha de desriure per a què s'utilitzarà, nom, etc.

2. Es defineix a quines organitzacions està destinat i en aquest cas com ens trobem dins la mateixa instància afegim també l'organisation B.

3. Finalment s'obté una arquitectura com la de la figura 13 on s'observa que el sharing group està compost per les dues organitzacions compartint la mateixa instància localhost. També es pot observar que l'organització B no té l'Extend seleccionat i això ha estat decidit per l'organització A ja que no vol que el receptor pugui ampliar encara més la informació recopilada sobre aquest event que s'ha compartit.

4. Com a pas opcional i per tal de comprovar que les dades s'estan enviant de forma correcte a on pertoca entrem com a usuaris de cadascuna de les organitzacions. En aquest cas UserA (organització A) UserB(organització B). No obstant, abans de continuar s'ha de destacar que aquests usuaris tenen un perfil en concret anomenat Sync user que és l'encarregat de crear els events tal i enviar-los, encara que a vegades també els pot publicar.

5.7.1 Com saber si el sharing group funciona

Primer de tot s'ha procedit a connectar-se com a UserB per tal de compatir una ciberamenaça coneguda com un Worm [24] o cuc i s'ha publicat dins la mateixa organització, és a dir, l'organització B figura 7. Després s'ha procedit a connectar-se com a UserA per comprovar que aquest event no és visible tal i com mostra la figura 8 però el que si que s'oberva en que l'usuari B té dos events procedents de l'organització A visibles. Això és degut a que els dos events que s'han compartit amb anterioritat dins el sharing group per això apareix l'opció Unpublish als quals només hi tenien accés tots aquells usuaris, en aquest cas tots, de l'entitat B.

En la figura 5, es pot contemplar l'arquitectura final d'aquest cas. Tenim les dues organitzacions, A i B, i els dos usuaris per a publicar la informació.

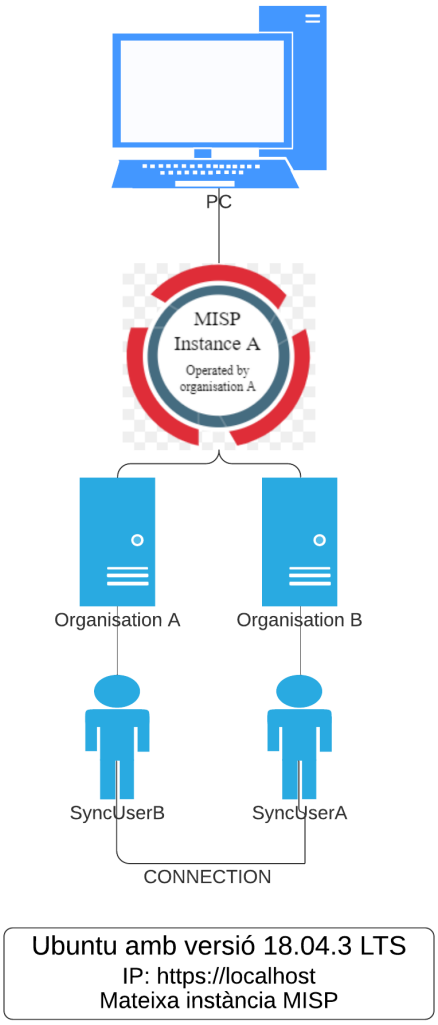

Fig. 5: Arquitectura cas 2.

5.8 CAS 3: Compartir informació entre diferents organitzacions en diferents instàncies

En aquesta cas 2 només hi ha 3 organitzacions situades en dues instàncies on s'ha instal·lat MISP en localhost. Aquestes instàncies són: Master Department que fa referència al departament central de la Universitat Autònoma (com la rectoria) i d'aqui penjarien els altres dos subdepartaments com podrien el departament d'enginyeria o Engineering Department i el departament de ciències polítiques. Llavors, per a poder enviar qualsevol mena d'informació sobre qualsevol possible amenaça no es pot només publicar l'event com s'ha dut a terme en el cas base o fent servir un sharing group com s'ha comprovat en el cas 2. Sinó que en aquest cas, cas 3, s'ha procedit a la creació d'un servidor o Sync server com a medi de transmissió de les dades i aquest mecanisme s'ha creat dins d'una de les organitzacions host [25], concretament per a cadascuna de les instàncies dels departaments com es veurà més endavant.

5.8.1 Creació del syncronisation server

S'explicarà quins passos s'han realitzat per instal·lar un servidor només en un departament ja que per tots s'ha seguit el mateix procediment.

Primer de tot s'afegeix una *Global actions - organisations - Add organisation* com a administrador amb el nom del departament i de forma local dins la instància màster per indicar que rebrà/enviarà els events cap el departament amb el que es vol sincronitzar. Encara que es diguin igual no són els mateixos departaments ja que es troben en diferents instàncies i això es pot comprovar a partir del Ids que són diferents.

Després, dins aquesta instància màster, s'afegeix un usuari de tipus SynUser al departament d'enginyeria que s'ha creat prèviament abans fent *Global actions - organisations - Add User* com a administrador. Però, alhora d'afegir aquest usuari user ens hem de guardar el seu AuthKey ja que és el que ens servirà per tal de connectar ambdós servidors.

Finalment, ara es pot procedir a crear el Sync Server dins la instància del departament d'enginyeria extern, és a dir, el que es troba a la seva pròpia instància i ara s'ha de realitzar el pas més important que és afegir la clau AuthKey de l'usuari de sincronització que s'ha creat dins la instància màster en aquest servidor. En la figura 14 es veuen diferents camps com són els d'identificació de la instància o el de les credencials. Els primers, hem de posar la base URL que té el servidor al que ens volem connectar, en aquest cas el màster o rectoria i se li assigna un nom per poder identificar-lo. Després, en quan a les credencials es selecciona Local organisation i no Remote organisation perquè en la instància del màster, en concret l'organització que fa referència a al subdepartament, s'ha agafat la UUID de la instància d'aquest i per tant automàticament encara que es seleccioni local com que té la mateixa UUID el server ho tindrà en compte alhora de fer la connexió.Per acabar amb aquest exemple, es pot observar el servidor creat dins la llista de servidors del departament d'enginyeria tal i com es mostra en la figura 15. El nom és MasterDepartment fent referència cap a quina instància es vol establir la connexió i en aquest cas, es poden publicar(publish),despublicar (unpublish) i accedir als events que s'han enviat (pull) però des d'aquesta instància per exemple no es podrà enviar res ja que la opció push es troba desactivada.

5.9 Cas 4: Implementació d'un servidor TAXII-MISP

En aquest cas molt bàsic, s'ha aconseguit crear un servidor TAXII que ha permès sincronitzar-se amb instància MISP però no s'ha pogut visualitzar la informació enviada des de TAXII. Aquest exemple implementa un dels serveis que s'han descrit a la secció 5.2, concretament el de missatgeria mode push ja que un usuari envia informació a la instància MISP com si fos un correu.

1. S'ha procedit a descarregar la carpeta amb un *git clone https://github.com/MISP/MISP-Taxii-Server*. Un cop descarregada, com MISP ja té una base de dades mysql no fa falta instal·lar-ne cap per TAXII i per tant podem procedir a configurar l'arxiu que ens permetrà sincronitzar-nos amb misp.

2. Es fa una còpia de l'arxiu de configuració original per si de cas es malmet en unj futur amb la comanda *cp config/config.default.yaml config/config.yaml*.

3. Amb l'arxiu copiat config.yaml editem el paràmetre db_connection perquè s'adapti al nostre entorn i el més important, canviem la clau auth_api i el paràmetre secret per a poder entrar a la instància local MISP.

4. Creem els usuaris amb els quals entrarem al nostre servidor TAXII *opentaxii-sync-data config/data-configuration.yaml* i executem el servidor *opentaxii-run-dev*.Per a poder publicar informació s'obre una consola a part de la que hi ha oberta pel servidor i s'executa la comanda *taxii-push –path http://localhost:9000/services/inbox -f tests/test.xml --dest my_collection –username admin –password admin* i si tot és correcte, quan s'enviï hauria d'aparèixer el missatge *Content block successfully pushed.*

Amb això, es pot dir que TAXII permet agilitzar la compartició de la informació perquè des de qualsevol dispositiu es poden enviar dades. A part, si es volgués no faria falta ni tenir instal·lada una instància MISP en el mateix ordinador ja que mitjançant mysql es pot crear una base de dades únicament per TAXII i a partir d'allà només es necessitaria saber la url del servidor misp per connectar-se i la seva auth_key.

5.10 Format de compartició dels events amb STIX

Tal i com s'ha vist a la secció 3 les principals iniciatives per a la compartició de ciberamenaces són STIX, TAXII i CybOx. Tanmateix, en aquest apartat s'explicaran algunes de la parts del format STIX d'un event en concret, exactament l'event publicat en el cas base. En primer lloc, al obrir el document es poden observar una sèrie de packages o paquets els quals s'han de declarar per a poder fer ús de certs atributs en tot el document, o sigui, es podrien definir com si fossin variables globals que es declaren a l'inici d'un programa i que es poden utilitzar al llarg d'aquest [26]. Per exemple, el id CyboxCommon que més endavant s'utilitzarà per declarar propietats com la del hash o el nom de l'organització que publica l'event.

D'altra banda, tenim propietats que es van definir en l'anterior document tals com observable. Amb aquest atribut el que s'està definint s'utilitza, entre d'altres coses, per representar qualsevol aspecte d'un sistema d'informació: tamany d'un arxiu, estat del Sistema Operatiu (SO). En aquest cas, ens està donant informació sobre l'organització que es troba connectada a l'event que s'ha publicat i això es por esbrinar ja que just a la línia següent es declara un objecte Cybox que fa referència a aquesta entitat. Recordem que CybOx és un llenguatge bastant senzill i pobre si el que es vol és donar informació molt detallada sobre la ciberamenaça en qüestió, per aquest motiu només s'utilitza per a definir objectes que facin referència als events, malware etc. En altres paraules, un cybox observable és en si mateix una sèrie de característiques que descriuen una entitat dins d'un entorn de ciberseguretat com els que es poden trobar en arxiu UNIX, libraries o en una Windows registry key.

A més, tenim propietats que es van definir en l'anterior document tals com observable. Amb aquest atribut el que s'està definint s'utilitza, entre d'altres coses, per representar qualsevol aspecte d'un sistema i en aquest cas mostra l'id de l'organització dins el document, és a dir, que no és l'id real de que té l'organització a l'entorn MISP. Aquest atribut bàsicament s'empra per tal de poder descriure una porció del codi de forma única i el cual té dos vessants, una d'elles pot ser amb el nom id o també es pot trobar de la manera idref [27], aquest segon té la mateixa funció que el primer però amb la diferència que fa referència a una part que es troba definida a un altre lloc del codi. Per últim, en aquest event compartit del cas base STIX té en compte el nivell d'amenaça que s'ha declarat a la interfície de l'entorn MISP i ens ho mostra a través de l'atribut incident, el qual ens dona més informació sobre l'event que s'ha captat per part de l'usuari en qüestió. En la nova versió de STIX, STX 2.0, els objectes per exemple es declaren d'una forma diferent a la que s'ha utilitzat en aquesta pràctica ja que es componen del llenguatge JSON [28].

6 CONCLUSIONS

Després d'haver realitzat tots els informes s'ha arribat a una sèrie de conclusions esmentades en aquest apartat. En primer lloc, la compartició de compartició de la informació sobre ciberamenaces és un dels pilars fonamentals si es vol tenir un sistema de qualitat i fiable que ajudi a les organitzacions a preveure els atacs coneguts o d'amenaces desconegudes, però millor que segueixin un modus operandi similar a alguna coneguda.
En segon lloc, per a compartir informació s'utilitzen iniciatives com CybOx, STIX i TAXII. Cal destacar, que entre elles hi ha molta relació ja que per exemple CybOx és utilitzat dins STIX aportant certs atributs que serveixen per a poder descriure parts concretes de la ciberamenaça com el sistema operatiu que s'ha vist afectat, kernel, etc. Tanmateix, STIX com a tal inclou diversos llenguatges dins la seva estructura modular però no permet l'ús d'una de les iniciatives com TAXII perquè aquesta no és un llenguatge sinó un servei molt semblant a l'intercanvi de missatges en el protocol TCP. Per aquest motiu, la plataforma MISP permet l'ús d'un mòdul extern que es pot instal·lar a la instància a fi de poder usar TAXII i establir una connexió per a transmetre informació. També, es pot dir que MISP és una plataforma de compartició d'informació de ciberintel·ligència molt completa perquè engloba molts dels estàndards inclosos en les iniciatives SCAP com són STIX, CybOx, entre d'altres. A part, et permet comunicar-te no només amb instàncies locals que tinguin el mateix entorn sinó que també et permet crear servidors de sincronització per a poder connectar diferents organitzacions d'arreu del món. Per últim, s'ha pogut comprovar que STIX és un llenguatge molt llegible i sencill degut a la bona representació que fa dels objectes que descriuen parts de la ciberamenaça incloent també possibles relacions entre ells. No obstant, ha faltat temps per a poder fer un ús més exhaustiu tant per l'anàlisi de STIX i TAXII com també de l'entorn MISP. En conclusió, MISP és una eina molt potent i molt útil dins el món de la seguretat ja que permet que tothom s'entengui entre si d'una forma molt pragmàtica i sobretot fàcil d'utilitzar.

7 TREBALL FUTUR

Després d'haver acabat aquest projecte, es podría ampliar la part pràctica afegint molts més usuaris per tal de fer-la més realista a una situació real.A més, també es podrien utilitzar altres indicadors per tal de descriure certs aspectes dels events provinents de les amenaces i en diferents llenguatges. D'aquesta forma, es podría comprobar com diferents organitzacions es comuniquen i interpreten les mateixes dades però en formats diferents. A més, una de les possibles iniciatives a prendre en treballs posteriors consistiría en poder comunicar instàncies MISP amb altres instàncies d'una altra plataforma com Suricata, Wazuh, etc.

AGRAÏMENTS

Donar gràcies a Ángel Elbaz ja que en tot moment m'ha guiat per tal d'aconseguir els objectius del projecte i sempre ha donat feedback constructiu que m'ha ajudat a reestructurar les idees del projecte de forma que quedin més clares.

REFERÈNCIES

[1] Altares, G. (2019). Cuando todo puede ser pirateado. [online] EL PAÍS. Available at: https://elpais.com/tecnologia/2016/09/28/actualidad/1475084881_284077.html

[2] González, M. (2019). Casi tres cibertataques "muy peligrosos" cada día. [online] EL PAÍS. Available at:https://elpais.com/politica/2018/11/14/actualidad/1542219228_193413.html

[3] González, R. (2019). Más de la mitad de las pymes sufren ciberataques. [online] Cinco Días. Available at: https://cincodias.elpais.com/cincodias/2018/09/28/pyme/ 1538169199_927487.html

[4] Ccn-cert.cni.es. (2019). [online] Available at: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1105-424-intercambio-informacion-ciberamenazas-stix-taxii-oct15/file.html

[5] Ccn-cert.cni.es. (2019). [online] Available at: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso- publico-ccn-stic/1105-424-intercambio-informacion-ciberamenazas-stix-taxii-oct15/file.html

[6] Minuto, A., Contra, L., Vang, B., Fan, M., Moda, D., Valenciana, C., Vasco, P., más, V., TV, P. and Micó, P. (2019). Ciberseguridad: la ignorancia nos hace menos libres. [online] La Vanguardia. Available at: https://www.lavanguardia.com/tecnologia/actualidad/20190410/461576027160/ciberserguridad-riesgos-ignoracia-libres-brl.html.

[7]] Ccn-cert.cni.es. (2019). [online] Available at: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1105-424-intercambio-informacion-ciberamenazas-stix-taxii-oct15/file.html.

[8] ”MISP: Introducción e instalación – Follow The White Rabbit”, Fwhibbit.es, 2020. [Online]. Available: https://fwhibbit.es/misp-introduccion-e-instalacion.

[9] Anon, (2019). [online] Available at: https://www.icsalabs.com/security-content-automation-protocol-scap.

[10] Business, E. (2019). ¿Qué es el Cybersecurity Framework de NIST de los Estados Unidos?. [online] Esan.edu.pe. Available at: https://www.esan.edu.pe/conexion/actualidad/2019/04/30/que-es-el-cybersecurity-framework-de-nist-de-los-estados-unidos/

[11] Mitre.org. (2019). The MITRE Corporation. [online] Available at: https://www.mitre.org/

[12] Gilligan (2019). Automating Enterprise IT Management by Leveraging Security Content Au.... [online] Slideshare.net. Available at: https://www.slideshare.net/JohnGilligan7/automating-enterprise-it-management-by-leveraging-security-content-automation-protocol-scap

[13] Ccn-cert.cni.es. (2019). [online] Available at: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1105-424-intercambio-informacion-ciberamenazas-stix-taxii-oct15/file.html.

[14] [2]”What is Critical Chain Project Management”, Simplilearn.com, 2020. [Online]. Available: https://www.simplilearn.com/what-is-critical-chain-project-management-rar68-article.

[15] First.org. (2019). [online] Available at: https://www.first.org/resources/papers/munich2016/wunder-stix-for-developers.pdf

[16] Maecproject.github.io. (2019). About MAEC — MAEC Project Documentation. [online] Available at: https://maecproject.github.io/about-maec/.

[17] Capec.mitre.org. (2019). CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC). [online] Available at: https://capec.mitre.org

[18] First.org. (2019). [online] Available at: https://www.first.org/resources/papers/munich2016/wunder-stix-for-developers.pdf

[19] Anomali.com. (2019). What are STIX/TAXII? — Anomali. [online] Available at: https://www.anomali.com/resources/what-are-stix-taxii

[20] europapress.es. (2019). Qué es una conexión P2P y por qué se utiliza para la piratería. [online] Available at: https://www.europapress.es/portaltic/internet/noticia-conexion-p2p-utiliza-pirateria-20170420085940.html

[21] Docs.oasis-open.org. (2019). TAXII Version 1.1.1. Part 1: Overview. [online] Available at: http://docs.oasis-open.org/cti/taxii/v1.1.1/csprd01/part1-overview/taxii-v1.1.1-csprd01-part1-overview.html

[22] M. Contributors, ”Get Your Instance · User guide of MISP Malware Information Sharing Platform, a Threat Sharing Platform.”, Circl.lu, 2019. [Online]. Available: https://www.circl.lu/doc/misp/get-your-instance/.

[23] Foo.be, 2020. [Online]. Available: https://www.foo.be/cours/dess-20192020/pub/0-misp-introduction-to-information-sharing.pdf.

[24] Kaspersky.es, 2019. [Online]. Available: https://www.kaspersky.es/resource-center/threats/viruses-worms.

[25] Host (Informàtica)”, Ca.wikipedia.org, 2019. [Online]. Available: https://ca.wikipedia.org/wiki/Host_(Inform%C3%A0tica).

[26] D Namespaces — python-stix 1.2.0.6 documentation”, Stix.readthedocs.io, 2019. [Online]. Available: https://stix.readthedocs.io/en/stable/overview/id_namespaces.html.

[27] Introduction to STIX”, Oasis-open.github.io, 2019. [Online]. Available: https://oasis-open.github.io/cti-documentation/stix/intro.html.

[28] CybOX Language Frequently Asked Questions (FAQs) — CybOX Project Documentation”, Cyboxproject.github.io, 2019. [Online]. Available: https://cyboxproject.github.io/faqs/.

APÈNDIX

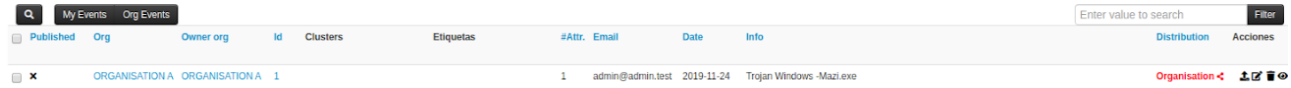

Fig. 6: Llista d'events publicats.

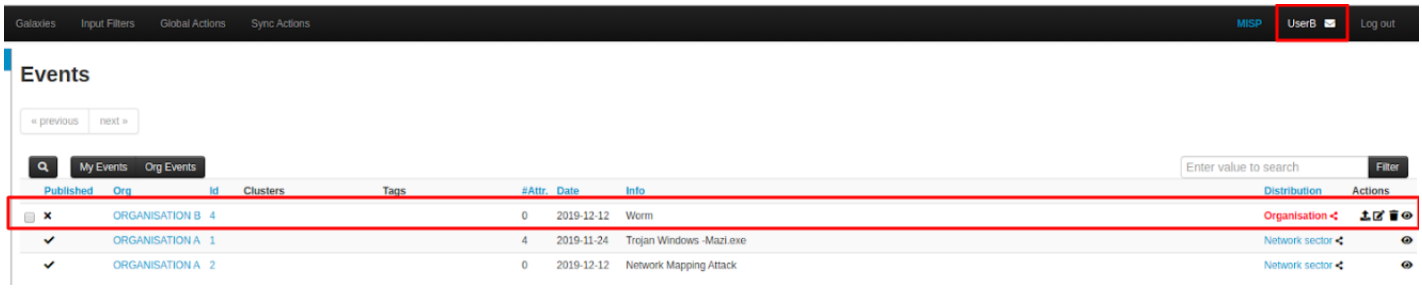

Fig. 7: Organització B.

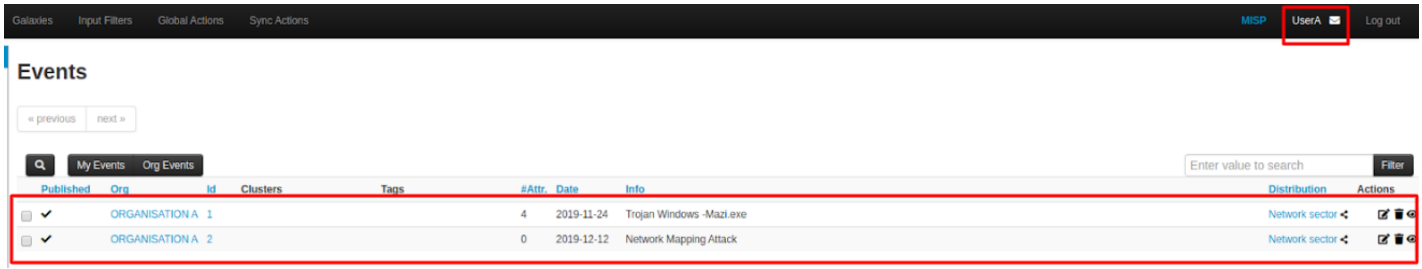

Fig. 8: Organització A.

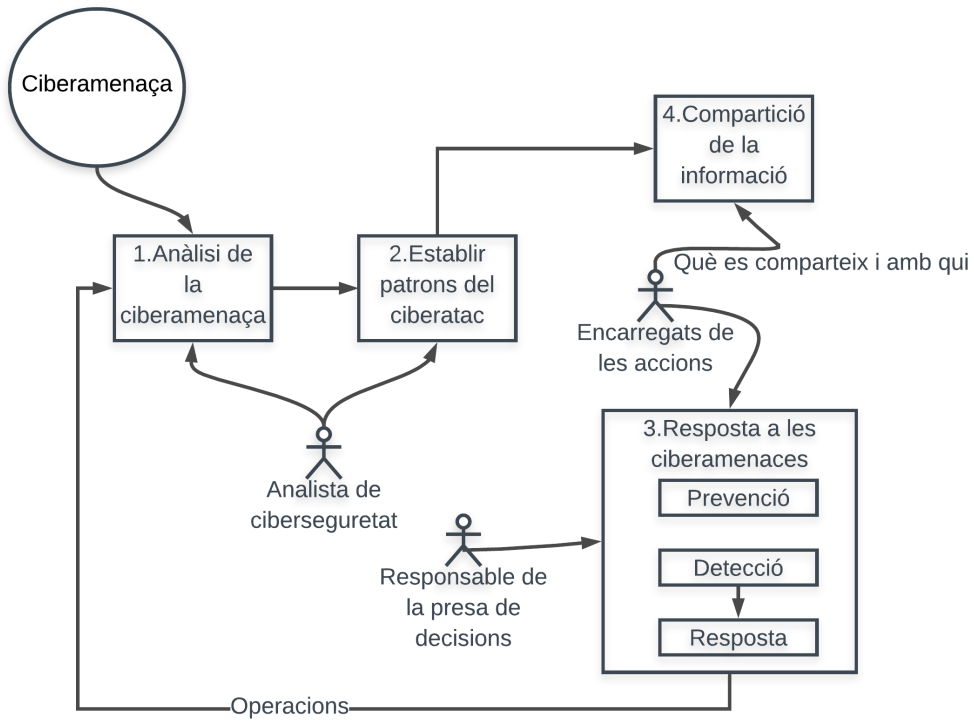

Fig. 9: Diagrama de casos d'ús.

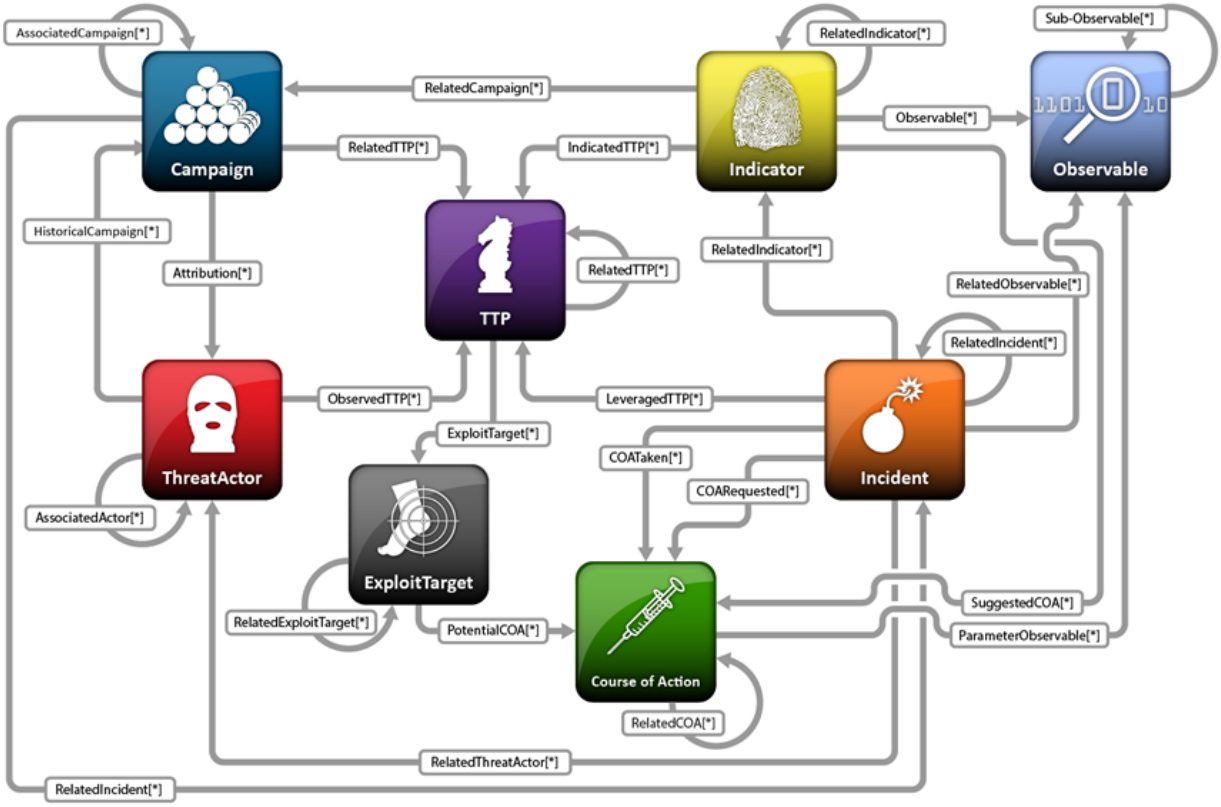

Fig. 10: Arquitectura STIX.

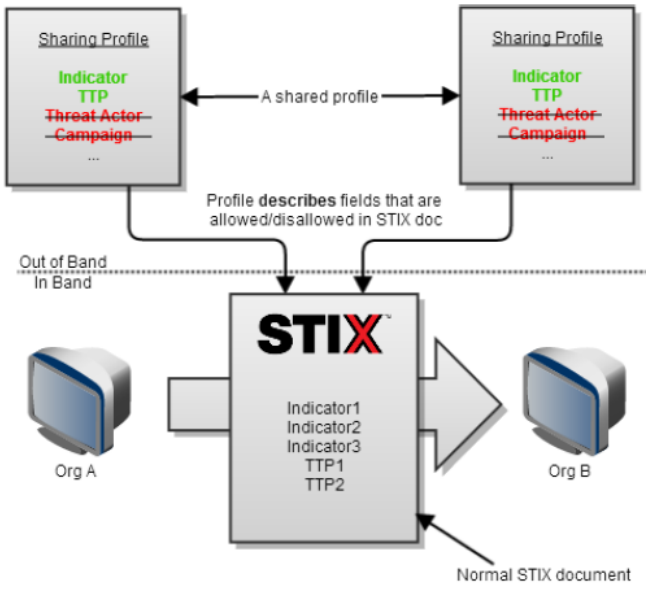

Fig. 11: Perfils STIX.

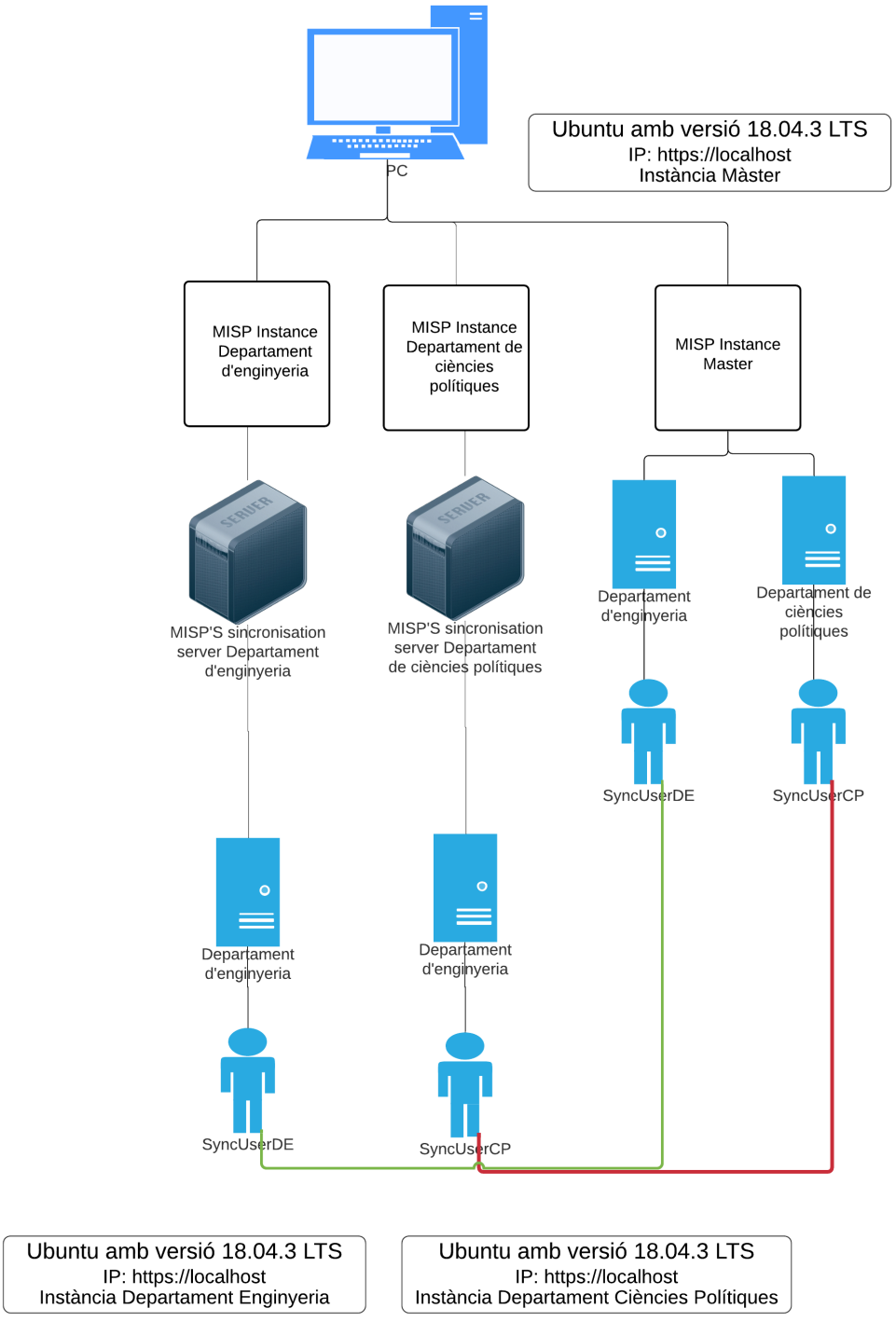

Fig. 12: Arquitectura cas 3.

Fig. 13: Sharing group.

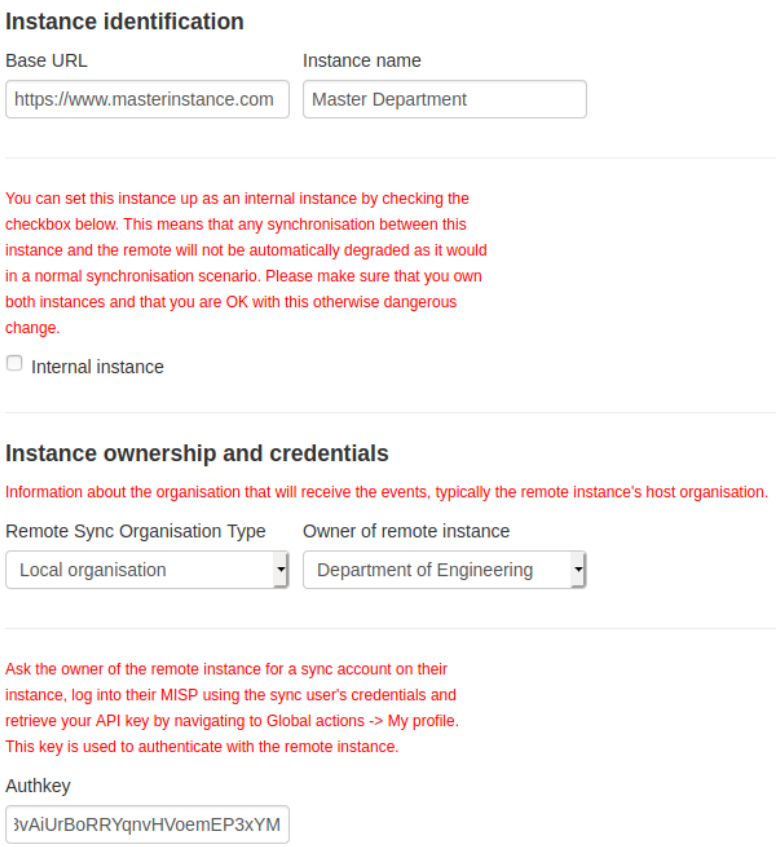

Fig. 14: Credencials.

Fig. 15: Syncserver en un dels departaments.

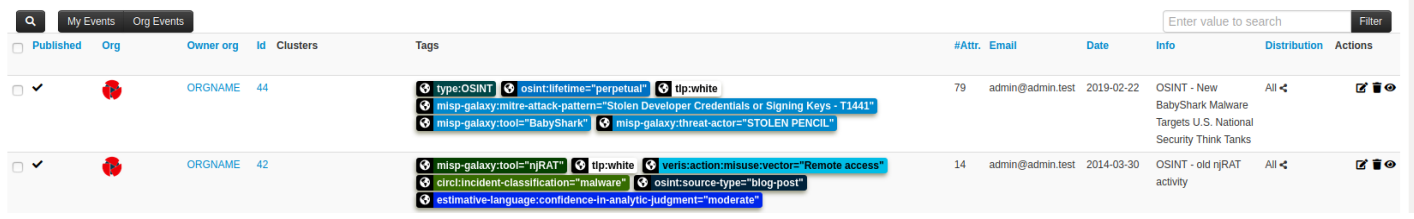

Fig. 16: Feeds públics.