GUÍA DE SEGURIDAD DE LAS TIC

(CCN-STIC-424)

INTERCAMBIO DE INFORMACIÓN DE CIBERAMENAZAS

STIX-TAXII

EMPLEO EN REYES

OCTUBRE 2015

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE LA PRESIDENCIA

NIPO: 002-15-027-0

Fecha de Edición: octubre de 2015

Wise Security (WSG TECH SOLUTIONS, S.L.) e InnoTec System han participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

Entre los elementos más característicos del actual escenario nacional e internacional figura el desarrollo alcanzado por las Tecnologías de la Información y las Comunicaciones (TIC), así como los riesgos emergentes asociados a su utilización. La Administración no es ajena a este escenario, y el desarrollo, adquisición, conservación y utilización segura de las TIC por parte de la Administración es necesario para garantizar su funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales.

Partiendo del conocimiento y la experiencia del Centro sobre amenazas y vulnerabilidades en materia de riesgos emergentes, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Una de las funciones más destacables que, asigna al mismo, el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración.

La ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 crea del Esquema Nacional de Seguridad (ENS), que establece las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.

El Real Decreto 3/2010 de 8 de enero desarrolla el Esquema Nacional de Seguridad y fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración. En su artículo 29 se autoriza que a través de la series CCN-STIC el CCN desarrolle lo establecido en el mismo.

La serie de documentos CCN-STIC se ha elaborado para dar cumplimiento a esta función y a lo reflejado en el ENS, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Octubre 2015

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

1. En la gestión de la ciberseguridad la información lo es todo. Tan pronto como los incidentes y las vulnerabilidades son detectadas se inicia un proceso de gestión en el que se genera un volumen de información muy elevado que es necesario conocer y procesar en el mínimo tiempo posible. Una información proveniente de múltiples fuentes, propias o facilitadas por otras organizaciones, públicas o privadas; con todo tipo de acciones, datos y lenguajes y expuesta a la interpretación subjetiva de la persona o grupo de gestión de incidentes que la recibe.
2. Procesar y compartir esta ingente información es, por tanto, un aspecto crítico en la gestión de la ciberseguridad y, para ello, resulta imprescindible la utilización de un lenguaje común que permita la comunicación y el intercambio sencillo y práctico. Un lenguaje basado en estándares comunes que defina claramente las características de una amenaza, dejando un estrecho margen a la interpretación, y permita el desarrollo de herramientas y procedimientos de actuación entre todos aquellos actores que deben gestionar o prevenir la misma amenaza. Teniendo en cuenta las características de una información de calidad y capaz de ser procesada: relevancia, oportunidad, exactitud, exhaustividad y posibilidad de ser digerida.

2. OBJETO

3. El objetivo de esta guía es presentar las últimas tendencias en materia de compartición de la información y de los estándares más utlizados en el sector (STIX, TAXII) así como las numerosas ventajas de su uso para la mejora de las capacidades defensivas de una organización. Teniendo en cuenta que, en estos casos, el término estándar va más allá de las especificaciones publicadas por organismos tradicionales (como puede ser la ISO[1] o ITU[2]) y abarca formatos desarrollados por otras entidades usados comúnmente en las operaciones de seguridad.
4. Todo con el fin de implementar un sistema o plataforma de intercambio de ciberinteligencia, entendiendo como tal, el resultado de valorar, analizar, integrar e interpretar la información.

3. ALCANCE

5. El Responsable de Seguridad, determinará el alcance de su aplicación, considerando la Política de Seguridad de la Organización y las amenazas a las que está expuesta la misma.

4. DEFINICIONES

6. En este apartado se dará unas nociones básicas sobre los conceptos y términos que se vayan a usan en esta guía.

[1] International Organization for Standardization
[2] International Telecommunication Union

4.1 CIBERSEGURIDAD Y CIBERINTELIGENCIA

7. Ciberseguridad es un término que, aunque se acuñó ya en los años 90[3], ha sido asociado recientemente como el término por el que se designa de manera general el proceso sistemático en una organización para la gestión de seguridad de la Información tratada mediante tecnologías de la Información y las Comunicaciones.

8. En el año 2008, la organización ITU definió en un estándar este término, la norma X.1205[4]. En este documento se define la ciberseguridad como:

9. "El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes:

   – Disponibilidad;

   – Integridad, que puede incluir la autenticidad y la trazabilidad;

   – Confidencialidad.

10. Se entiende "ciberentorno" como "usuarios, redes, dispositivos, todo el software, procesos, información almacenada o que circula, aplicaciones, servicios y sistemas que están conectados directa o indirectamente a las redes"

11. Bajo este contexto se habla entonces de ciberamenazas, o ciberatacantes como circunstancias, individuos u organizaciones que pueden poner en riesgo la ciberseguridad.

12. Igualmente, se puede hablar de ciberinteligencia que debe entenderse desde el mismo punto de vista que se entiende la Inteligencia contrapuesta a la simple Información pero aplicable al contexto de la ciberseguridad. El CNI define en su página web[5] la diferencia entre Inteligencia e Información:

13. "El término información debe diferenciarse del de inteligencia. Información equivale a noticia de un hecho en su sentido más amplio. El concepto información debe entenderse, por tanto, como el elemento de partida para la elaboración de inteligencia, considerada ésta como el resultado de valorar, analizar, integrar e interpretar la información."

14. Por lo tanto, la ciberinteligencia no se trata únicamente de la recolección de información sobre ciberseguridad, sino que tiene por objetivo comprender esta información y poder caracterizar la ciberamenaza determinado cosas como: ¿qué tipo de acciones de ataque se han producido y es probable que se produzcan?; ¿cómo pueden ser detectadas y

3 http://www.merriam-webster.com/dictionary/cybersecurity
4 http://www.itu.int/rec/T-REC-X.1205-200804-I
5 http://www.cni.es/es/preguntasfrecuentes/pregunta_010.html?pageIndex=10&faq=si&size=15

reconocidas estas acciones?; ¿cómo pueden ser mitigadas?; ¿quiénes son los actores pertinentes de las amenazas; ¿Qué están tratando de lograr?; ¿cuáles son sus capacidades, en forma de tácticas, técnicas y procedimientos que han ido desarrollando con el tiempo y es probable que repitan en el futuro?; ¿qué tipo de vulnerabilidades, errores de configuración, o debilidades que son propensos a atacar?; ¿Qué medidas para detectar y/o contener el incidente se tomó en el pasado y fueron efectivas?, y cuestiones similares.

4.2 AMENAZA AVANZADA PERSISTENTE - APT

15. Una Amenaza Avanzada Persistente (traducción del término en inglés Advanced Persistent Threat – APT) es un tipo de ataque sofisticado, que se ejecuta durante un largo periodo de tiempo y está dirigido específicamente a una Organización o conjunto de organizaciones que tienen algún aspecto en común de interés para el atacante, por ejemplo empresas de un determinado sector industrial, u organizaciones políticas de un determinado orientación ideológica, etc.

16. Tienen como objetivo extraer información confidencial o clasificada y/o reducir la capacidad operativa de la Organización u organizaciones atacadas. Habitualmente, la motivación de los atacantes no es la obtención de beneficios financieros directamente por las acciones realizadas, quizá si monetizando la información robada, pero no directamente a través de las acciones realizadas durante el compromiso de las infraestructuras. Dentro de la amenaza APT se puede incluir casos como:

    – Ciberespionaje promovido por Estados
    – Ciberespionaje industrial
    – Ciberhacktivistas[6] altamente motivados
    – rara vez ciberdelincuentes

17. La denominación APT se deriva directamente de sus tres características:

    – **Amenaza**: suponen una amenaza para la Organización, ya que el atacante está muy motivado a robar información o reducir la capacidad operativa de la Organización.
    – **Avanzada**: el atacante tiene una alta capacidad, tanto en conocimientos como en recursos, que le permite poder llevar a cabo el ataque. Esta gran capacidad le permite investigar y aprovechando las vulnerabilidades de la Organización, incluso encontrando nuevas vulnerabilidades no documentadas o utilizando varios vectores de ataque (a través de Internet, mediante ingeniería social, etc.). Es capaz de evadir los sistemas de protección tradicionales (cortafuegos, antivirus, etc.). Puede hacerse con el control absoluto del sistema comprometido.
    – **Persistente**: el ataque se produce durante un largo periodo de tiempo (se puede estar hablando de años) en el que se va consiguiendo información y acceso paulatino a los sistemas.

18. No se considera como una APT el hecho de que se detecte código dañino en un sistema sin que tenga como objetivo el robo de información sensible. Para ser calificada como

[6] Activismo digital antisocial. Sus practicantes persiguen el control de ordenadores o sitios web para promover su causa, defender su posicionamiento Político, o interrumpir servicios, impidien-do o dificultando el uso legítimo de los mismos STIC 401 Glosario 2.548 Hacktivismo

APT suele requerirse que cumpla con las 3 características anteriores y que además exista una motivación para robar información sensible.

5. GENERACIÓN Y COMPARTICIÓN DE CIBERINTELIGENCIA

19. Cuando una organización se plantea mejorar el conocimiento de la amenaza, surge una problemática común: además de procesar la información que ella misma genera (por medio de registros de funcionamiento de sus sistemas de información y de ciberseguridad), tiene que procesar información externa (pública o de terceras partes con las que exista algún tipo de acuerdo de intercambio de información) sobre las amenazas. Esta última fuente tiene unas determinadas características que plantea varios problemas:

- Los atacantes van evolucionando aunque en muchos casos se observan aspectos recurrentes: mismos modus operandi, señales que indican el mismo origen, etc. Sin embargo, existe dificultad para registrar, resaltar y comunicar estas características.
- Algunas de las propiedades de una ciberamenaza ya han sido observadas por el colectivo mundial de expertos en ciberseguridad y existen dificultades en que esa información fluya hacia interlocutores de confianza.
- La difusión de la información no se hace de manera eficiente por muchas razones
  - Exceso de fuentes de información
    - Elevado volumen
    - Dificultad para hacer el seguimiento
  - formato de la información inconexo, cada fuente elige su propia manera de expresar diversas características de la ciberamenaza.
  - Uso de diversos tipos de protocolos o mecanismos de compartición de información. Las distintas fuentes de información pueden emplear desde ficheros en texto plano publicados en sitios web, a RSS[7], cuentas automáticas en Twitter, envíos de información a listas de correo, etc.
  - Existe una gran disparidad en la manera de describir la amenaza, es decir la semántica es diferente y no existen estándares para la denominación de distintos aspectos de un incidente.

20. La conclusión es que actualmente existe una dificultad real, por no decir casi imposibilidad de procesar toda la información para convertirla en Inteligencia.

6. ESTÁNDARES PARA LA COMPARTICIÓN DE CIBERINTELIGENCIA

6.1 CONTEXTO DE CREACIÓN DE LOS ESTÁNDARES

21. Son bien conocidas las iniciativas destinadas a modelizar los activos a proteger, una de las facetas de la ciberseguridad. Se han realizado esfuerzos para facilitar la

[7] Really Simple Syndication.Formato XML para compartir contenidos en la web

automatización y estructuración referente a enumeración de tipos de plataformas, vulnerabilidades, métricas de la gravedad de las vulnerabilidades, tipos de errores, elementos de configuración, test de verificación de vulnerabilidades o de configuraciones, etc. Todas estas iniciativas están enmarcadas dentro de la iniciativa SCAP[8] (Security Content Automation Protocol) que está descrita en diversos documentos NIST[9] de la serie "Special Publication 800" (SP 800-126[10]) y en colaboración con otras organizaciones como MITRE[11] en la que ha delegado varias tareas y otras partes autónomas como FIRST[12]. De manera resumida recordemos que este conjunto está compuesto por distintos componentes que permiten describir todo lo relacionado con la protección de los activos de información:

- Security Content Automation Protocol (SCAP)
- Asset Reporting Format (ARF)
- Asset Identification (AI)
- Common Configuration Scoring System (CCSS)
- Trust Model for Security Automation Data (TMSAD)
- Open Vulnerability and Assessment Language (OVAL)
- Common Platform Enumeration (CPE)
- Extensible Configuration Checklist Description Format (XCCDF)
- Common Vulnerability Scoring System(CVSS)
- Common Vulnerability Enumeration (CVE)
- Common configuration Enumeration (CCE)

22. Por otro lado, referente al conocimiento de las ciberamenazas, el DHS (Department of Homeland Security de Estados Unidos), junto con otros organismos colaboradores (US-CERT[13] y MITRE Corporation) ha liderado la creación de un marco común para el intercambio de información sobre ciberseguridad compuesto fundamentalmente por:

- **CYBOX – Cyber Observable eXpression:** Es un esquema estandarizado para la especificación, caracterización y comunicación de eventos de seguridad o estados de un sistema de información que son observables en todas las operaciones de los sistemas y de las redes de comunicaciones. Puede ser usado en diversas situaciones: gestión de eventos de seguridad, caracterización del código dañino, sistemas de detección / prevención de intrusiones, respuesta a incidentes y análisis forense digital.
- **STIX – Structured Threat Information eXpression:** Es un lenguaje estandarizado y estructurado para describir la información sobre ciberamenazas. El marco STIX

[8] http://scap.nist.gov
[9] National Institute of Standards and Technology
[10] http://scap.nist.gov/revision/1.2/index.html
[11] MITRE Corporation es una organización estadounidense sin ánimo de lucro que provee de ingeniería de sistemas, investigación y desarrollo, y soporte sobre tecnologías de la información al gobierno de Estados Unidos. http://www.mitre.org/
[12] Forum for Incident Response and Security Terms
[13] United States -Computer Emergency Response Team

pretende tener la capacidad de expresar toda la gama de elementos de datos que están relacionados con la descripción de una ciberamenaza potencial y se esfuerza por ser tan expresiva, flexible, extensible, automatizable y legible como sea posible.

- **TAXII - Trusted Automated eXchange of Indicator Information:** Define un conjunto de servicios y formatos que permiten el intercambio de información sobre ciberamenazas entre organizaciones automáticamente y en tiempo real y servicios on-line. TAXII no es una aplicación o sistema en sí mismo y tampoco define el nivel organizativo sobre el modo en que se intercambia la información sino que simplemente facilita a las organizaciones la decisión sobre qué información compartir y con qué otras organizaciones.

23. Los tres estándares han sido creados con una orientación internacional y completamente libre para facilitar su uso apoyándose en un desarrollo dirigido por la comunidad de expertos en ciberseguridad.

24. Estos estándares deben permitir la automatización del intercambio de información sobre ciberseguridad con el objeto de mejorar el conocimiento sobre las ciberamenazas, facilitar la defensa de las redes en tiempo real y el análisis de amenazas.

6.2 ESTÁNDAR STIX

6.2.1 QUÉ ES STIX

25. De manera sencilla, STIX (Structured Threat Information eXpression, marca registrada) es un lenguaje estructurado que permite la caracterización de la información sobre ciberamenazas para poder ser compartida, almacenada y analizada de una forma consistente.

26. Su principal característica es que se trata de un lenguaje estandarizado, en formato XML[14] para la especificación y caracterización de informaciones sobre amenazas de ciberseguridad. En la práctica el estándar está definido por un conjunto de archivos XSD (XML Schema Definition) para cada uno de los elementos que se hayan definido y que se explicarán más adelante.

27. No se trata de un sistema o de las especificaciones de uno, sino únicamente de la definición de un lenguaje común que pueda ser empleado por cualquier organización, herramienta, sistema o base de datos para implementar alguna de los casos de usos previstos y posiblemente otros no contemplados.

28. Esta estructura estandarizada basada en XML permite al mismo tiempo la posibilidad de intercambiar información entre procesos automatizados y también su comprensión por parte de analistas de ciberseguridad.

6.2.2 DOCUMENTACIÓN DEL ESTÁNDAR

29. La especificación completa del lenguaje es compleja y se encuentra mantenida y actualizada por MITRE.

30. Toda la documentación oficial del estándar se puede encontrar en el siguiente enlace:

[14] eXtensible Markup Language

http://stix.mitre.org/language/index.html

31. A la fecha de edición de esta guía la versión publicada corresponde a la 1.1.1 accesible en:

http://stix.mitre.org/language/version1.1.1/

32. Por su complejidad y al tratarse únicamente de un conjunto de archivos XSD, es necesario que exista una documentación anexa que describa el significado y uso de cada uno de los distintos elementos del estándar. Para consultar en detalle la sintaxis del lenguaje de cada uno de los componentes se recomienda acudir a los sitios webs de documentación siguientes:

   – Documentación e información de soporte

   http://stixproject.github.io/

   – Herramientas oficiales facilitadas por MITRE (se ha de destacar que pueden existir otras herramientas o sistemas tal y como se comentará más adelante en esta guía)

   https://github.com/STIXProject/

33. Esta documentación es accesible desde el anterior enlace y permite acceder a una amplia documentación de cada uno de los elementos que componen STIX y otros lenguajes estándares que lo amplían.

6.2.3 PRINCIPIOS DE DISEÑO APLICADOS A STIX

34. Para conseguir la máxima eficacia del nuevo lenguaje y su potencial aplicación en múltiples organizaciones, su diseño se ha realizado buscando cumplir con los siguientes principios:

- **Expresividad:** La diversidad de situaciones que pueden concurrir en un incidente de ciberseguridad es enorme por no decir infinita y, por lo tanto, el lenguaje debe ser capaz de expresar toda la riqueza de matices que la realidad de las ciberamenazas representan.
- **Integración de otros estándares:** La problemática de compartición de ciberinteligencia no es nueva y ya existen otras iniciativas que lo han afrontado y que han desarrollado sus propios estándares que cubren total o parcialmente algún aspecto del estándar STIX. Por esta razón, STIX facilita mecanismos para incorporar estos esquemas de representación dentro de su propia arquitectura. Así por ejemplo, por defecto en la propia definición de STIX se incorpora CyBOX para la definición de los componentes denominados “Indicios Observables”, y permite incorporar otros estándares como MAEC (Malware Attribute Enumeration and Chracterization), CAPEC (Common Attack Pattern Enumeration and Classification) u otros más para la definición más precisa de algún aspecto concreto.
- **Flexibilidad:** Las casuísticas de las ciberamenazas que STIX ha de representar, así como de las organizaciones que lo deseen usar, es tal que el estándar ha buscado la flexibilidad, de manera que el conjunto de elementos que deben ser obligatorios está reducido al mínimo posible.
- **Extensibilidad / Ampliación:** Para permitir el refinamiento por parte de las organizaciones que empleen STIX, éste se ha construido de modo modular y permite la ampliación del mismo mediante extensiones particulares.

- **Automatización:** Al tratarse de un lenguaje XML definido por distintos archivos XSD, es completamente utilizable por herramientas que automaticen su creación, procesado o análisis.
- **Legibilidad:** El uso del formato XML para la descripción de informaciones sobre ciberseguridad permite su tratamiento automatizado, pero al mismo tiempo el diseño realizado sobre los distintos componentes y su denominación permite su legibilidad también por seres humanos.

6.2.4 CASOS DE USOS DE STIX

35. Aunque STIX ha sido diseñado teniendo en cuenta un determinado conjunto de casos de uso, permite incrementar un gran número de casos adicionales.
36. Los casos de uso de STIX más habituales están orientados a la generación de ciberinteligencia directamente utilizable en las operaciones de ciberseguridad o compartir con otras organizaciones.
37. Asimismo, los casos de uso planteados están relacionados entre ellos. A continuación se muestra un diagrama que refleja la interrelación entre ellos

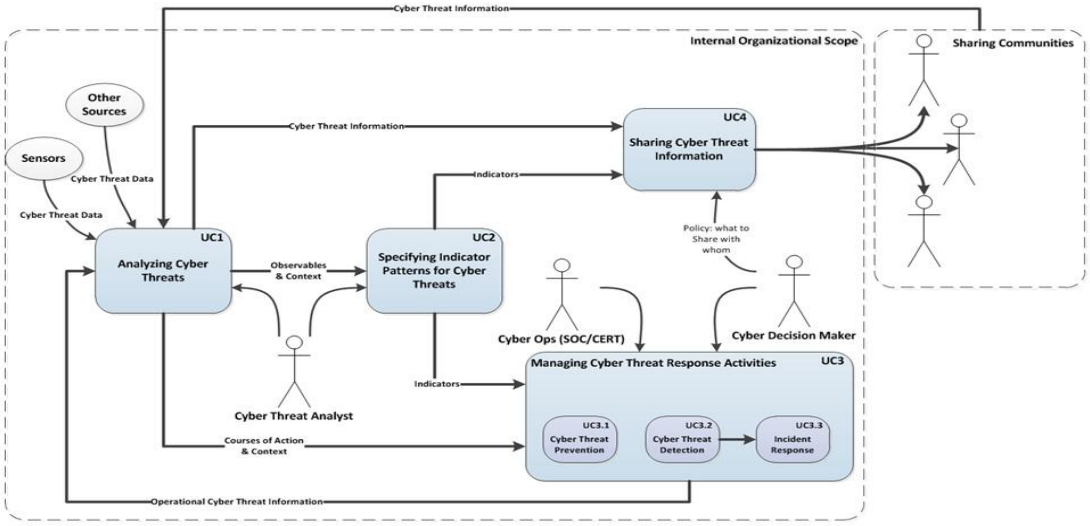


Figura 1 Visión general de la relación entre distintos casos de uso de STIX
(Fuente: http://stix.mitre.org)

38. A continuación se presentarán los casos de uso inicialmente contemplados en el diseño de STIX.

6.2.4.1 LCU1- ANÁLISIS DE CIBERAMENAZAS

39. El rol del usuario de este caso es el analista de ciberseguridad.
40. En este caso de uso, un analista revisa fuentes de información estructurada empleando STIX y otras sin estructurar con el objeto de generar inteligencia sobre determinadas ciberamenazas. Su origen puede ser manual o automatico. Mediante este análisis intenta comprender y recoger las características de la ciberamenaza, mantener este conocimiento a lo largo del tiempo, y si fuera necesario comunicarla a las partes interesadas, internas o externas. El conocimiento generado puede ser tanto intrínseco a la información recogida (por ejemplo: formas de actuar de los ciberatacantes, indicadores de su actividad, etc.) o bien generado por el propio analista: selección de

indicadores más relevantes, acciones de respuesta más eficaces (de detección, contención o recuperación), etc.

41. Ejemplo: Un analista puede estar encargado de estudiar la información recibida sobre mensajes de phishing[15] que se reciben en la organización (mediante un buzón de correo trampa que reciba correo no solicitado, también denominado en ocasiones "spam trap") y al mismo tiempo tener acceso a los registros de correo electrónico recibido. De este modo puede analizar, quién fue víctima de una campaña de phishing, de qué tipo se trataba, qué URL[16] o adjuntos contenía, determinar si se trata de explotar alguna vulnerabilidad, qué código dañino emplea, o qué tipo de respuesta a la ciberamenaza se puede realizar, tanto desde el punto de vista preventivo como reactivo. Todo este análisis puede mantenerse registrado de manera estructurada en un documento en lenguaje STIX.

6.2.4.2 CU2 – ESPECIFICACIÓN DE PATRONES INDICADORES DE CIBERAMENAZAS

42. El rol del usuario de este caso es el analista de ciberseguridad.

43. El analista realiza sus investigaciones sobre distintos aspectos observables de una ciberamenaza con el objeto de generar indicadores con los que se pueda identificar la presencia de la misma. Esto puede realizarse de manera manual o automatico por alguna herramienta. Asimismo, puede emplear estos indicadores para generar distintas reglas (para un IDS[17], generar un IOC[18], reglas YARA[19], verificaciones de sistemas mediante el lenguaje OVAL, etc.) que puedan ser incorporadas en sistemas de ciberseguridad de detección de señales de presencia de la ciberamenaza.

44. Ejemplo: En el caso que el analista haya identificado una campaña de phishing que emplee algún tipo de código dañino, puede realizar un análisis del mismo. Este análisis proporcionaría todo tipo de indicadores medibles en un sistema que puedan permitir identificar que éste ha sido afectado (hash de ficheros que intervienen en la infección como el binario original o cualquier otro que se descargue o genere posteriormente, hostname resueltos, conexiones realizadas, cambios producidos en el sistema como claves de registros en sistemas Windows, archivos leídos, etc.). La siguiente tarea de este analista consistiría en identificar todos los indicadores de la campaña de phishing, como por ejemplo: asunto de los mensajes, contenido (o parte del mismo), URL empleadas, aspectos de las cabeceras del correo (remitente, servidores empleados para el envío, etc.). Toda esta información puede ser recogida, estructurada y empaquetada en un documento STIX.

[15] Método de ataque que busca obtener información personal o confidencial de los usuarios por medio del engaño o la picaresca, recurriendo a la suplantación de la identidad digital de una enti-dad de confianza en el ciberespacio STIC 401 Glosario 2.748.1 Phishing.
[16] Uniform Resource Locator
[17] Intrusion Detection System
[18] Indicator of Compromise (Indicador de Compromiso), o fichero que contiene la definición de indicadores de compromiso mediante XML
[19] Herramienta de clasificación e identificación de código dañino

6.2.4.3 CU3 – GESTIÓN DE LAS ACTIVIDADES DE RESPUESTA A CIBERAMENAZAS

45. Dentro del área de operaciones de ciberseguridad en una organización existen distintos roles, entre ellos el de responsable de la toma de decisiones y los encargados directos de la operación de dichos sistemas de ciberseguridad (COS o Centros de Operaciones de Seguridad y/o CERT o Equipos de Respuesta ante Incidentes). Al tener el conocimiento exacto sobre el entorno a proteger y los distintos sistemas de ciberseguridad desplegados son las personas más adecuadas para trabajar conjuntamente, tomar y ejecutar las decisiones operativas más eficientes (en coste y resultados) y de este modo, prevenir, detectar o dar la respuesta en caso de materialización del incidente.

46. Estas áreas son principalmente consumidoras de ciberinteligencia generada por los analistas pero a su vez también facilitan información para que estos últimos puedan realizar su trabajo.

47. Los responsables de la toma de decisiones sobre los sistemas de la ciberseguridad emplean la ciberinteligencia generada por los analistas en formato STIX y evalúan las recomendaciones que se han realizado en esa información de ciberinteligencia y que acciones concretas son las más adecuadas y eficientes en el entorno concreto. Los responsables de la operación son los encargados de tomar los elementos de la ciberinteligencia en formato STIX que se han seleccionado para implementarlos en los distintos sistemas de ciberseguridad de la organización.

48. Las acciones que se pueden plantear pueden ser de prevención, detección o bien de respuesta, y por lo tanto existirán tres posibles casos de uso:

    CU3.1 – Prevención de ciberamenazas. En esta situación, las acciones seleccionadas y desplegadas provenientes del formato STIX son preventivas, por ejemplo: corregir vulnerabilidades, o implementar una regla de bloqueo en algún sistema de cibervigilancia, etc.

    Ejemplo: en el caso de la campaña de phishing comentada en anteriores ejemplos, los responsables de la toma de decisión evaluarán las acciones propuestas por los analistas y seleccionarán aquellas que se adecuen al entorno, como implementar un filtro específico en la pasarela de correo electrónico entrante y un filtro en el sistema de control de contenido de navegación. Esta decisión se facilita al equipo de operaciones para su despliegue.

    - **CU 3.2 – Detección de ciberamenazas**: Las acciones seleccionadas y desplegadas son de detección proactiva, y pueden ser implementadas por sistemas automáticos o manuales, con objeto de actuar en el momento que se produce la ciberamenaza.Es este caso se encuentra el tema de la implantación de reglas (de IDS o de correlación) la búsqueda en un SIEM[20] que generen una alerta hacia el equipo de operaciones del SOC[21] o CERT, o la investigación en el histórico de registros activados (por ejemplo los flujos de comunicaciones IP[22] en los registros IPFIX[23], registros del cortafuegos, sistemas de control de navegación, etc.

[20] Security Information and Event Management
[21] Security Operations Center
[22] Internet Protocol
[23] Internet Protocol Flow Information Export

Ejemplo: en el caso de la campaña de phishing comentada, se realiza una investigación para detectar posibles casos ocurridos en el pasado (el marco temporal en que buscar sería una de las informaciones de ciberinteligencia facilitada) mediante la verificación de los registros de funcionamiento de las pasarelas y servidores de correo electrónico, y los registros del sistema de control de contenido de navegación.

- **CU3.3 – Respuesta a incidentes:** Estas áreas son las encargadas de dar respuesta a los incidentes de seguridad que se detecten o notifiquen. Se hace uso de la ciberinteligencia facilitada para identificar si se trata de ataques realizados por ciberamenazas conocidas y en ese caso revisar las acciones propuestas. Igualmente, el uso de esta información permitirá identificar patrones comunes de ataques que pueden ser facilitados a los analistas para enriquezcan el conocimiento que se tiene de las ciberamenazas.

  Ejemplo: el equipo de respuesta a incidentes recibe notificaciones de infección de equipos de usuarios. El análisis de estos les permite identificar elementos que son comunes a infecciones comunicadas por el grupo de ciberanalistas. Podría tratarse, por ejemplo, de indicadores del código dañino de este ataque que coincide con otros códigos dañinos empleados en otras ocasiones (claves de registro utilizadas como Mutex[24], nombres de ficheros, resumen criptográfico o hash de binarios, estructura interna de binarios, comentarios en texto en los ficheros empleados, etc.), o sistemas de Mando y Control de una botnet[25] que han sido contactados por los equipos infectados, conocidos por haber sido empleados en otros ataques. Este intercambio de información permite el enriquecimiento mutuo sobre una ciberamenaza que pueda estar evolucionando o empleando nuevos métodos de ataque.

6.2.4.4 CU 4- COMPARTICIÓN DE INFORMACIÓN SOBRE CIBERAMENAZAS

49. Uno de los casos de uso más interesantes de STIX es el de compartición de información sobre ciberamenazas. Con el fin de garantizar la confidencialidad de la información sobre incidentes y el entorno TIC de la organización, los responsables pueden definir dentro del marco STIX qué contenidos pueden ser comunicados y a quién. Esta política de intercambio de información puede ser incorporada a los sistemas de información que facilitan el intercambio. Puesto que todas las partes involucradas han acordado el formato STIX como el de descripción de información de ciberseguridad, las organizaciones receptoras de información saben cómo interpretarla e incorporarla a sus sistemas de información.

50. Ejemplo: Tomando el caso comentado, los responsables pueden limitar las características de la información a comunicar excluyendo los aspectos referentes a datos de la víctima (cuentas de correos, servidores, direccionamientos IP internos) o motivaciones de la ciberamenaza (por ejemplo, tipo de información robada) y facilitar el resto a otras partes con las que se haya establecido acuerdos de intercambio.

[24] MUTual EXclusion object, mecanismo de programación para garantizar que sólo un proceso accede a un determinado recurso.

[25] Red de equipos infectados por un atacante remoto. Los equipos quedan a su merced cuando desee lanzar un ataque masivo, tal como envío de spam o denegación [distribuida] de servicio. STIC 401 Glosario 2.151.1 Botnet

6.2.5 ARQUITECTURA DEL STIX

51. En el siguiente apartado se muestran los distintos elementos que componen el lenguaje estándar STIX con los que se describe los aspectos de una ciberamenaza.

52. Se ha de tener en cuenta que la forma en que dos organizaciones pueden entender o podrían explicar una misma ciberamenaza puede ser distinta. Sin embargo, si se descompone la información disponible de acuerdo a la estructura ofrecida por STIX, finalmente ambas organizaciones llegarán a una descripción de la situación muy similar.

53. En la siguiente figura presentamos la arquitectura general de STIX identificado los distintos conceptos que se definen alrededor de una ciberamenaza y las interrelaciones entre ellos.

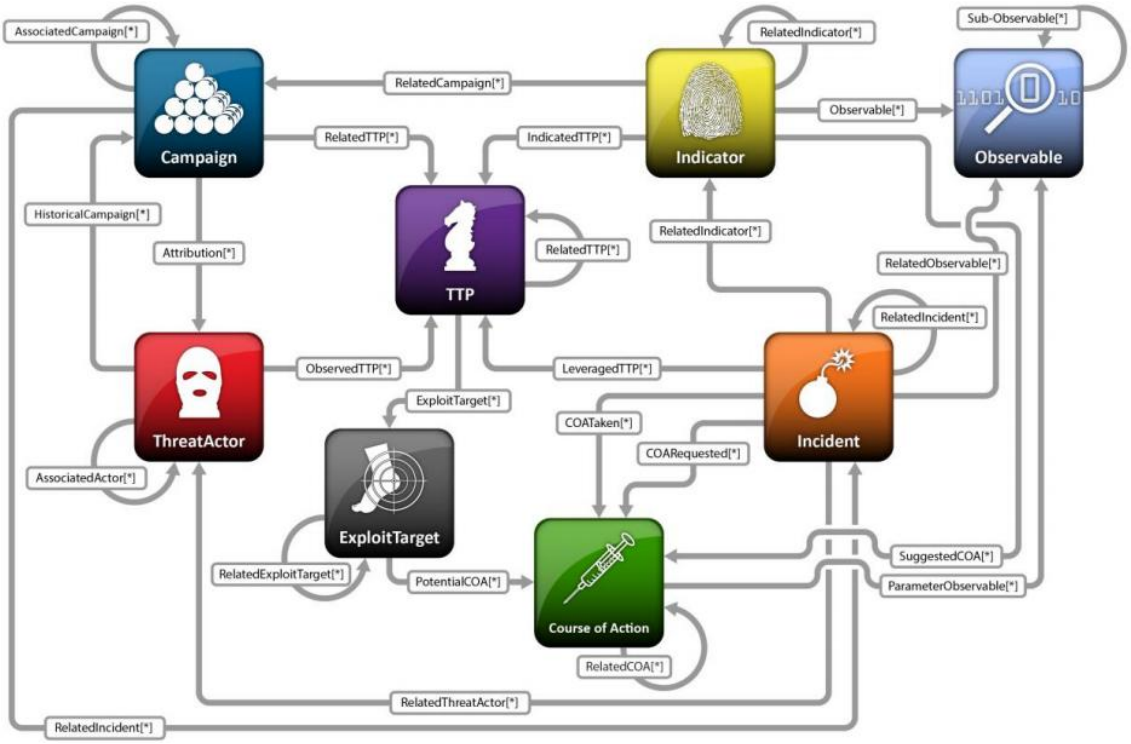


Figura 2 Arquitectura conceptual del lenguaje STIX
(fuente: http://stix.mitre.org)

1. **Observable**: describe qué ha sido o podría haber sido el ciberincidente
2. **Indicator**: describe los patrones que podrían haber sido y el significado en el caso de que lo sean
3. **Incident**: describe los casos de acciones específicas del adversario
4. **TTP** (Procedimientos, Técnicas y Tácticas del adversario): describe los patrones de ataque, código dañino, herramientas de infección, fases del ataque (kill chain), infraestructura, víctima y otros métodos usados por el atacante.
5. **Exploit target**: aborda las vulnerabilidades, debilidades o configuraciones que podrían ser explotadas.

6. **Course of action**: describe la respuesta que podría ser adoptada ante el ataque o las medidas preventivas a realizar
7. **Campaign**: trata sobre una familia de incidentes y/o TTPs con un intento compartido
8. **Threat Actors**: describe la identifiación y/o caracterización del atacante
9. **Report:** recoge el contenido STIX relacionado y ofrece la información para compartir

54. La estructuración de STIX se realiza en base a los distintos componentes en que se descompone una ciberamenaza y la interrelación que se puede construir entre ellos. Las flechas reflejan las posibles relaciones que pueden existir entre los componentes, y el asterisco representa que la relación puede presentarse varias veces.
55. A la hora de describir una ciberamenaza, se expondrán todos los componentes que se conozcan, y se establecerán las relaciones que puedan existir entre ellas. Si se está empleando algún sistema de información para gestionar toda la información de ciberinteligencia, el analista podría reutilizar algún elemento ya existente, ya sea porque se ha introducido anteriormente o bien porque una tercera parte con la que se comparte información la ha facilitado.
56. A continuación se explicará los distintos componentes del lenguaje y su relación con la descripción de una ciberamenaza.

6.2.5.1 VISIÓN GENERAL DE LOS DISTINTOS TIPOS DE OBJETOS STIX

57. Tal y como se mostrará a continuación, STIX dispone de distintos tipos de objetos que se emplean para describir diversos aspectos. Cada uno de ellos ofrece la posibilidad de describir alguno de los puntos que intervienen en una ciberamenaza y desde perspectivas diferentes, desde el nivel más bajo o detallado hasta el enfoque estratégico de la ciberamenaza que da una visión de conjunto de la situación.
58. El siguiente diagrama presenta los distintos tipos de niveles establecidos desde el punto de vista operativo de la ciberseguridad:

Nivel	Objetos STIX
Detalle operativo	 Qué actividad concreta de la ciberamenaza se está observando
Visión Táctica	 Qué amenazas se han de buscar en las redes y sistemas y porqué razón
Visión Operacional	 Dónde se ha visto la amenaza  Qué acciones se pueden realizadar para gestionar el incidente

Nivel	Objetos STIX			
				
Visión Estratégica	Quién es el responsable de esta amenaza	Porqué razón se realizan los ataques	Cómo actúan	Qué debilidades y objetivos tienen

Tabla 1 Relación entre niveles operativos de la ciberinteligencia vs. los tipos de objetos STIX (Fuente: http://stix.mitre.org)

6.2.5.2 PAQUETE STIX

59. Un documento XML conforme al lenguaje STIX es el que define una ciberamenaza.
60. El estándar STIX introduce un concepto denominado "paquete" para permitir agrupar en un contenedor común un determinado conjunto de objetos STIX. Este concepto facilita tanto el intercambio como la estructuración de la información. Asimismo, los paquetes permiten ser interrelacionados entre iguales o bien jerárquicamente.
61. La razón subyacente de agrupar en un determinado paquete varios objetos STIX puede ser muy variada. La más habitual por proceder de un mismo informe, aunque también podría ser simplemente por provenir de un determinado origen y en un determinado momento.

6.2.5.3 INDICIOS OBSERVABLES 

62. Los indicios observables son el elemento más básico dentro de la arquitectura STIX. Representan cualquier aspecto de un sistema de información o red de comunicaciones que puede ser observado y verificado.
63. Puede tratarse, sin ser exhaustivos:

- Aspectos relacionados con las **características de un fichero** en un sistema de ficheros.

  Ejemplos: tamaño, nombre, resumen criptográfico o hash, un determinado contenido total o parcial, etc.

- **Estado de un sistema operativo**.

  Ejemplos: contenido particular (total o parcial) de un fichero de configuración, un determinado servicio de sistema operativo en ejecución o detenido, en un sistema Windows claves de registro accedidas, creadas, modificadas o borradas etc.

- Comunicaciones observadas en una **red**

  Ejemplos: nombres de dominios que se intentan resolver y el estado de la consulta, tráfico HTTP u otros protocolos (por ejemplo IRC), determinados patrones de comportamiento de tráfico, etc.

  STIX aprovecha otro estándar creados con este mismo fin, CyBOX que es un lenguaje para la descripción de aspectos observables en un entorno TIC.

También se tiene que destacar que pueden existir mecanismos y herramientas[26] que de manera automática conviertan artefactos (binarios, trazas de tráfico, certificados, correos electrónicos, ficheros de logs, etc.) en objetos en formato STIX, igualmente para indicadores de compromiso en formato openIOC.

6.2.5.4 INDICADORES

64. Este componente combina o agrupa información de uno o varios "indicios observables" junto con información de contexto con el objeto de reflejar comportamientos más precisos sobre códigos dañinos o comportamientos observados.

65. La información de contexto que se añade puede tratarse del nivel de fiabilidad de la información, indicaciones sobre el manejo de posibles muestras de código dañino que cumplan los indicios observables, rangos temporales que sean relevantes (como podría ser las comunicaciones observadas o la activación de un código dañino), posibles impactos de determinados indicios observables, etc.

66. Este tipo de componente estará muy relacionado con otros como Tácticas, Técnicas y Procedimientos (TTP)[27]", u otros como "Desarrollos de las acciones" en los que se describan mecanismos de detección o de bloqueo de los indicios observables.

6.2.5.5 INCIDENTES

67. Esta componente tiene por finalidad recopilar la información concreta sobre un determinado incidente ocurrido en el ámbito TIC de una organización. Por lo tanto, contiene la información sobre lo sucedido (sistemas afectados e impacto, personas involucradas, descripción de eventos, líneas de tiempo de los sucesos confirmados), puntos de contactos de las partes involucradas en la gestión del incidente, y en general cualquier otra información relevante para el incidente.

68. Además de las informaciones propias del entorno atacado y la gestión realizada, este elemento relaciona esas circunstancias con aspectos propios de la ciberamenaza como las tácticas, técnicas y procedimientos (TTP) empleadas, los posibles actores de la amenaza, e indicadores e indicios observables. Por medio la constatación reiterada de la presencia de estos últimos es como se puede generar conocimiento sobre posibles TTP o actores de la ciberamenaza.

6.2.5.6 TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS (TTP)

69. Las TTP pretenden caracterizar maneras de actuar de los ciberatacantes, y representan comportamientos o modus operandi observados en uno o varios incidentes, como por ejemplo el tipo de activos atacados o el código dañino que emplean habitualmente. Las TTP son uno de los puntos claves de STIX a la hora de describir una ciberamenaza y es el nexo de unión entre indicadores, incidentes, campañas y actores de la amenaza. Esta información puede ser muy variada, y contener aspectos como:

[26] https://github.com/CybOXProject
[27] Tactics, Technics and Procedures. Tácticas, Técnicas y Procedimientos

- **Comportamiento observado** (patrones en el ataque, tipo de código dañino empleado, sistemas explotados) que estará recogido como relaciones a otros componentes de tipo "Indicadores" y/o "indicios observables" relacionados.
- **Objetivos atacados** habitualmente reflejando por tanto una relación con determinados componentes de tipo "objetivos de la explotación"
- **Atacantes o campañas** de ciberataques en las que se ha observado ue suelen utilizar estas TTP en su forma de opera. Se reflejará como una relación hacia una componente de tipo "actores de la amenaza" o "campaña".
- **Información no recogida en otros componentes STIX** como un conjunto de recursos que han sido empleados (herramientas o infraestructuras, personas o identidades utilizadas), información sobre las víctimas escogidas (quiénes eran, puntos en común como sector o localización).

70. En el propio desarrollo de STIX se tiene en cuenta que pueden existir otros mecanismos ya estandarizados para describir partes de este concepto. Por esta razón, STIX permite el uso de otros estándares para extender la descripción de alguna particularidad de las TTP como por ejemplo:

- MAEC (*Malware Attribute Enumeration and Characterization*, lenguaje estandarizado por MITRE para la descripción y comunicación de información sobre código dañino basado en sus atributos como comportamiento, artefactos, y patrones de ataque)
- CAPEC (*Common Attack Pattern Enumeration and Classification*, amplio diccionario y taxonomia para la clasificación de ataques conocidos que sirve para caracterizar patrones de ataques
- CyBOX para caracterizar herramientas e infraestructuras empleadas en un ataque.

6.2.5.7 CAMPAÑAS (*CAMPAIGN*)

71. En STIX, se entiende campaña como el conjunto de TTPs, incidentes y/o actores de la amenaza que de manera conjunta expresan una intencionalidad u objetivo común. Por ejemplo, un determinado adversario que focaliza su actividad contra un determinado sector industrial y emplea unos determinados TTPs constituye lo que en STIX se considera una "campaña".
72. A la hora de describir este componente, además de las relaciones con otros, también se determina aspectos como el nivel de confianza en la atribución de una determinada campaña a un actor de la amenaza, así como las posibles intenciones.

6.2.5.8 ACTOR DE LA AMENAZA (*THREAT ACTOR*)

73. Este componente recoge la información que caracteriza a los atacantes responsables de la existencia de una ciberamenaza. El termino actor se ha de interpretar en un sentido amplio, como una entidad que tiene un papel en una determinada ciberamenaza y puede tratarse de personas, grupos de personas u organizaciones, estructuradas o no.

74. La caracterización consiste en informaciones que describan aspectos (con el nivel de fiabilidad que se indique, así como la fuente de información que lo ha revelado) como su identidad (o aspectos que permitan identificarlo), motivaciones y efectos que busca, campañas en las que ha participado, TTP habitualmente empleados.

6.2.5.9 OBJETIVO DE LA EXPLOTACIÓN (*EXPLOIT TARGET*)

75. Este componente recoge la información concerniente a los aspectos técnicos aprovechados o que son objetivo durante un ciberataque. Por lo tanto, puede incluir información sobre vulnerabilidades técnicas, debilidades o errores en las configuraciones de sistemas de información o de comunicaciones.

76. En el propio desarrollo de STIX se tiene en cuenta que pueden existir otros mecanismos ya estandarizados para describir partes de este concepto. Por esta razón, STIX permite el uso de otros estándares para extender la descripción de estos aspectos técnicos:

- CVE (*Common Vulnerabilitaty Enumeration),* es un diccionario o base de datos de vulnerabilidades públicas
- OSVDB *(Open Source Vulnerability DataBase)* para la identificación de vulnerabilidades públicas
- CVRF (*Common Vulnerability Reporting Framework*) para la descripción estructurada de vulnerabilidades, incluidas potenciales vulnerabilidades no públicas (también conocidas como "vulnerabilidad 0-day[28]")
- CWE (*Common weakness enumeration*) para describir posibles debilidades en el software
- CCE (*Common Configuration Enumeration*) para describir aspectos de configuración involucrados en una ciberamenaza

6.2.5.10 DESARROLLO DE LAS ACCIONES (*COURSE OF ACTION*)

77. Este componente de STIX está relacionado con las acciones que pueden ser tomadas de cara a dar una respuesta a la ciberamenaza. Pueden ser tanto preventivas (de corrección o de detección) para dar respuesta a un determinado "objetivo de explotación", o reactivas para contener o mitigar el impacto del incidente. Este componente describe por tanto, la fase en que afecta la acción (preventiva o reactiva), indicios observables con los que está relacionado, objetivo, descripción estructurada de la acción en sí misma (puede tratarse de una regla de IPS[29], o un parche a ser instalado), el potencial impacto y coste de aplicar la acción, así como su eficacia, etc.

6.2.5.11 MARCADORES DE DATOS

78. Para permitir una expresividad máxima al lenguaje, se permite enriquecer la caracterización de alguno de los anteriores conceptos específicos de STIX con información o datos adicionales. Este concepto es definido como "marcadores de datos".

[28] Son aquellos programas dañinos que explotan o aprovechan una vulnerabilidad que todavía no se ha publicado y por tanto no dispone de soluciones de seguridad que la eviten
[29] Intrusion Prevention System

79. No existe un consenso sobre qué información deben contener y tampoco sobre el modo exacto en que se ha de emplear (por ejemplo qué partes pueden ser marcadas o si existen marcas globales) por lo que están definidos de manera muy flexible.

80. La flexibilidad de uso viene por dos aspectos. Por un lado, la definición del marcador no está incluida en los propios elementos que se han de señalar, sino por el lugar en que se inserta y por su contenido (uno de sus atributos), que indica a qué parte del documento XML en formato STIX aplica. Pueden definirse marcadores que apliquen globalmente a todo el documento o a atributos muy concretos dentro del documento. Por otro no se define una estructura propia del marcador, sino que al crearse se definirá el tipo como una particularización de un tipo básico definido en el estándar. Esto permite emplear otros esquemas ya existentes, por ejemplo TLP (*Traffic Light Protocol*) para establecer las condiciones en que una determinada parte del documento puede ser comunicada.

- **TLP – Traffic Light Protocol**

81. El TLP es casi un estándar de facto empleado por la comunidad internacional de Equipos de Respuesta a Incidentes (CSIRTs[30] o CERTs, y agrupados en la organización FIRST[31]) para clasificar que información se puede compartir.

82. El protocolo es muy simple y se basa en la definición de 4 niveles de caracterización de la información con la que se indica cuándo y quién la puede. Por lo tanto, cuando una organización o individuo genera una información y la desea comunicar a unas determinas partes, la marcará con un determinado nivel, indicando a las partes receptoras como pueden a su vez emplear y/o diseminar dicha información. Es un código que puede utilizarse en un entorno en que distintas organizaciones comparten información.

83. Los 4 niveles y su significado son los siguientes:

Nivel	Cuándo debe emplearse	Con quién se puede compartir la información
TLP:RED	Las fuentes lo emplearán cuando el mal uso de la información pueda impactar en la privacidad, reputación u operaciones	Los receptores no pueden divulgar la información con otras partes fuera del ámbito en que se divulgó la información.
TLP:AMBER	Las fuentes lo emplearán cuando es necesario divulgar una información para dar respuesta a ella pero implica riesgos para la privacidad, reputación u operaciones si se divulga fuera de las partes involucradas en la divulgación.	Los recetores sólo pueden compartir la información con miembros de su propia organización que necesiten conocer la información y sólo hasta el límite de lo que sea necesario para dar respuesta a esa información.

[30] Computer Security Incident Response Team
[31] http://www.first.org

Nivel	Cuándo debe emplearse	Con quién se puede compartir la información
TLP:GREEN	Las fuentes lo emplearán cuando la información es útil para concienciar o formar a las partes participantes del grupo de intercambio de información así como para otros interesados dentro de las organizaciones participantes o del sector en el que desarrollan su actividad.	Los receptores pueden divulgar la información en el ámbito interno de sus organizaciones o sector en el que desarrollen su actividad aunque no abiertamente por canales públicos.
TLP:WHITE	Las fuentes lo emplearán cuando la información conlleva un riesgo de mal uso mínimo o despreciable, de acuerdo con las prácticas y procedimientos propios del a organización referentes a la publicación de información	La información puede ser redistribuida sin limitaciones, siempre sujeto a restricciones legales (privacidad y/o derechos de propiedad intelectual).

Tabla 2 Estados del TLP – Traffic Light Protocol

6.2.5.12 EJEMPLO DE DOCUMENTOS STIX

84. Un documento STIX es un archivo en formato XML que cumple los requerimientos del lenguaje definidos en los distintos archivos XSD que definen los distintos componentes del lenguaje.

85. A continuación se muestra lo que sería un posible documento en formato STIX que define un indicio observable. En concreto define como indicio el que se observe cualquiera de tres (3) nombres FQDN[32] de tres (3) hosts maliciosos:

malicious1.example.com

malicious2.example.com

malicious3.example.com

[32] Fully Qualified Domain Name

```
<stix:STIX_Package
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:indicator="http://stix.mitre.org/Indicator-2"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:DomainNameObj="http://cybox.mitre.org/objects#DomainNameObject-1"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
    xmlns:example="http://example.com/"
    xsi:schemaLocation=
    "http://stix.mitre.org/stix-1 ../stix_core.xsd
    http://stix.mitre.org/Indicator-2 ../indicator.xsd
    http://cybox.mitre.org/default_vocabularies-2 ../cybox/cybox_default_vocabularies.xsd
    http://stix.mitre.org/default_vocabularies-1 ../stix_default_vocabularies.xsd
    http://cybox.mitre.org/objects#DomainNameObject-1 ../cybox/objects/Domain_Name_Object.xsd"
    id="example:STIXPackage-f61cd874-494d-4194-a3e6-6b487dbb6d6e"
    timestamp="2014-05-08T09:00:00.000000Z"
    version="1.1.1"
    >
    <stix:STIX_Header>
        <stix:Title>Example watchlist that contains domain information.</stix:Title>
        <stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicators -
Watchlist</stix:Package_Intent>
    </stix:STIX_Header>
    <stix:Indicators>
        <stix:Indicator xsi:type="indicator:IndicatorType" id="example:Indicator-2e20c5b2-
56fa-46cd-9662-8f199c69d2c9" timestamp="2014-05-08T09:00:00.000000Z">
            <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">Domain
Watchlist</indicator:Type>
            <indicator:Description>Sample domain Indicator for this
watchlist</indicator:Description>
            <indicator:Observable id="example:Observable-87c9a5bb-d005-4b3e-8081-
99f720fad62b">
                <cybox:Object id="example:Object-12c760ba-cd2c-4f5d-a37d-18212eac7928">
                    <cybox:Properties xsi:type="DomainNameObj:DomainNameObjectType"
type="FQDN">
                        <DomainNameObj:Value condition="Equals"
apply_condition="ANY">malicious1.example.com##comma##malicious2.example.com##comma##malicious3
.example.com</DomainNameObj:Value>
                    </cybox:Properties>
                </cybox:Object>
            </indicator:Observable>
        </stix:Indicator>
    </stix:Indicators>
</stix:STIX_Package>
```

86. Se pueden obtener más ejemplos en el sitio web[33] de MITRE, todos ellos conformes con la última versión de STIX.

87. Es interesante comprobar como para mostrar el poder expresivo de STIX, MITRE pone a la disposición de la comunidad toda la información correspondientes a dos incidentes ampliamente documentados por dos compañías de seguridad norteamericanas:

    – El informe de Mandiant[34] sobre el incidente denominado APT1

[33] https://stix.mitre.org/language/version1.1.1/samples.html
[34] http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

– El informe de FireEye[35], sobre el uso de una herramienta de administración remota (RAT – Remote Administration Tool) denominada Poison Ivy en diversos incidentes de seguridad y campañas de APT

6.2.6 PERFILES STIX

88. Tal y como se ha comentado, uno de los objetivos de STIX es facilitar la compartición de información sobre ciberamenazas. Sin embargo, una organización puede internamente generar mucha ciberinteligencia sobre una determinada ciberamenaza, y a la hora de compartirla con otras organizaciones, no toda esa información es conveniente que sea comunicada. En este contexto, en la definición de STIX se ha añadido el concepto de perfil que hace referencia al modo en que una determinada comunidad de organizaciones emplean STIX, es decir que subconjunto de datos representables mediante STIX una organización comparte con el resto de miembros de la comunidad. La definición de un perfil indica que subconjunto se puede emplear y de qué modo:

– **Presencia**: se especifica si un determinado componente debe estar presente, es recomendable, es opcional o no debe de estar presente en absoluto.

– **Implementación**: especifica reglas para la implementación de algún punto

– **Valores**: especifica campos que deben tener algún determinado conjunto de valores

6.2.6.1 USO DE PERFILES STIX

89. En el seno una determinada comunidad creada para el intercambio de información, sus miembros emplearán los perfiles STIX para acordar qué partes del estándar STIX se empleará en el intercambio de información y de qué modo, de forma que quede claro el alcance de la compartición de información.

[35] https://www.fireeye.com/content/dam/legacy/resources/pdfs/fireeye-poison-ivy-report.pdf

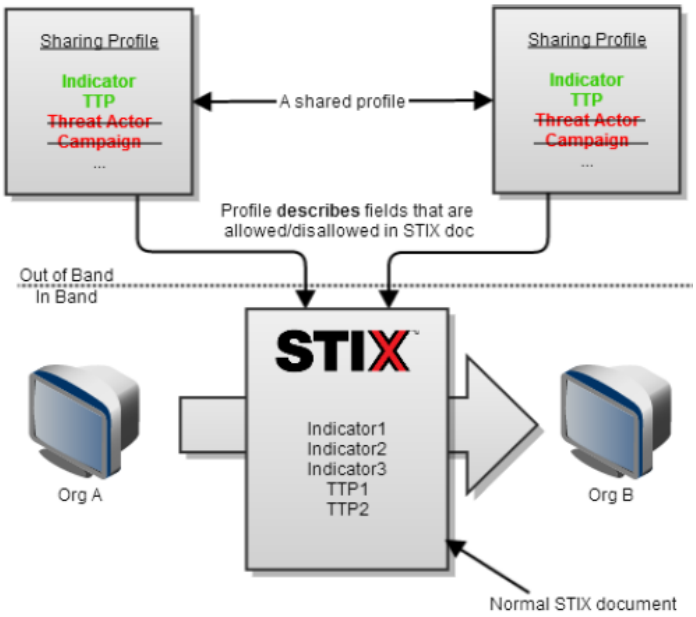


Figura 3 Aplicación de un perfil STIX
(Fuente:https://stix.mitre.org)

90. El anterior diagrama muestra un ejemplo de uso de los perfiles. Las dos organizaciones acuerdan mediante un perfil STIX compartido qué información de ciberseguridad se compartirá.

91. De este modo pueden existir distintos casos de uso:

    – Una organización que sea consumidora de información especificará en su perfil qué espera recibir como información.

    – Una organización que sea generadora de información especificará en su perfil qué información se facilita y en qué formato.

    – Pueden darse casos de comunidades muy organizadas en las que se pacte un determinado perfil común a todas las partes.

92. El uso de los perfiles también es interesante para los desarrolladores de sistemas de información que tenga que consumir o generar información sobre ciberamenazas puesto que delimita muy precisamente el alcance de la implementación de STIX que se tiene que realizar.

6.3 ESTÁNDAR TAXII

6.3.1 QUÉ ES TAXII

93. TAXII acrónimo de Trusted Automated eXchange of Indicator Information (es una marca registrada), es una iniciativa que tiene como fin dar las especificaciones de un mecanismo de transporte de mensajes que, al ser implementado permita el intercambio de información sobre ciberamenazas entre organizaciones y/o sistemas de información. Esta información debe ser descrita, preferiblemente empleando el estándar STIX. Se tiene que entender claramente que TAXII no es por tanto ni una herramienta o sistema de información, ni

tampoco una iniciativa en sí misma de compartición de información. Define mecanismos para que las organizaciones pongan en marcha servicios de compartición de información.

6.3.2 DOCUMENTACIÓN DEL ESTÁNDAR

94. Toda la documentación oficial del estándar es mantenida por MITRE que la pone a disposición pública en los siguientes enlaces:

    – Documentación oficial de las especificaciones: http://taxii.mitre.org/

    – Documentación e información de soporte: http://taxiiproject.github.io/

    – Herramientas oficiales facilitadas por MITRE (se ha de destacar que pueden existir otras herramientas o sistemas tal y como se comentará más adelante en esta guía)

    https://github.com/TAXIIProject/

95. El estándar está organizado en distintos documentos para facilitar la evolución de los aspectos de manera independiente sin afectar a la totalidad. Los documentos más relevantes son:

    – "*TAXII Services Specifications*": Especificaciones de los servicios TAXII, sobre la información que transportan los mensajes TAXII y el protocolo de intercambio de mensajes para cada uno de los servicios especificados.

    http://taxii.mitre.org/specifications/version1.1/TAXII_Services_Specification.pdf

    – "*TAXII XML Message Binding Specifications*": Especificaciones de los requerimientos sobre el modo de representar los mensajes TAXII en formato XML. Por el momento sólo existen estas especificaciones al respecto pero en el futuro, es posible que se desarrollen otras especificaciones similares para contemplar otros posibles formatos.

    http://taxii.mitre.org/specifications/version1.1/TAXII_XMLMessageBinding_Specification.pdf

    – "*TAXII HTTP Protocol binding specifications*": Especificaciones de los requerimientos del modo de transportar los mensajes TAXII con el protocolo HTTP[36] o HTTPS[37]. Por el momento sólo existen estas especificaciones al respecto del modo de transporte de los mensajes pero en el futuro, es posible que se desarrollen otras especificaciones similares para contemplar otros posibles si emergen nuevos protocolos.

    Es interesante destacar que TAXII delega en la implementación del transporte todo lo referente a autenticación de las partes que se intercambian información.

    http://taxii.mitre.org/specifications/version1.0/http1.0/TAXII_HTTPProtocolBinding_Specification.pdf

    – *"TAXII Default Query Specification"*: Para algunos de los servicios definidos para TAXII es posible realizar consultas, y este documento especifica el funcionamiento de este servicio, mensajes que se intercambian y protocolos de funcionamiento.

    http://taxii.mitre.org/specifications/version1.1/TAXII_Default_Query_Specification.pdf

96. En Anexo A se amplia la información disponible sobre el estándar TAXII.

[36] HyperText Transfer Protocol
[37] Hyper Text Transfer Protocol Secure

7. REYES

7.1 DESCRIPCIÓN

97. REYES (REpositorio común Y EStructurado de amenazas y código dañino) está basado en la tecnología MISP (Malware Information Sharing Platform)[38].

98. MISP es un sistema ya funcional y utilizable por las organizaciones para implementar una plataforma para intercambio de ciberinteligencia. Puesto que su principal caso de uso es el de intercambio de información, la herramienta está especialmente ideada para ofrecer un modo de intercambio para distintas organizaciones que internamente generan ciberinteligencia. Los usuarios del sistema tienen por tanto la oportunidad de facilitar y consumir elementos de ciberinteligencia.

99. Inicialmente fue desarrollada en el marco de las fuerzas armadas belgas (www.mil.be) pero desde 2012 se ha facilitado abiertamente a la comunidad con una licencia de código abierto y participan diversos equipos de respuesta a incidentes como NATO NCIRC[39], CIRCL[40], y CERT-EU[41].

100. Este sistema está adquiriendo bastante popularidad entre distintos equipo de respuesta a incidente que tienen relación con el NATO NCIRC y actualmente el CIRCL (CSIRT nacional de Luxemburgo) ha implementado una plataforma de intercambio de ciberinteligencia[42] con MISP en la que participan varios CSIRT[43] nacionales europeos y algunos privados.

101. El sistema ofrece una base de datos centralizada de eventos de ciberseguridad en un formato estructurado compatible con iniciativas como OpenIOC[44] o STIX, y con funcionalidades como correlación de eventos en base a sus atributos, importación y exportación de estos eventos en distintos formatos (XML, texto plano, OpenIOC, YARA, STIX, CSV, etc.).

102. Como plataforma de intercambio, el sistema está diseñado focalizando en ofrecer distintas capacidades de interrelación entre las distintas entidades que colaborarían en una instancia REYES/MISP y también entre distintas instancias REYES/MISP.

- En una instancia de REYES/MISP, una organización colaboradora puede disponer de múltiples usuarios con distintos niveles de privilegios de visibilidad de la información y con registro de sus actividades. Igualmente a nivel de organizaciones también se pueden implementar distintos niveles de visibilidad.
- Entre distintas instancias de REYES/MISP (distintas comunidades) es posible establecer relaciones en las que se establezcan limitaciones como distintos niveles de visibilidad de información, dirección en que se puede realizar la transferencia de información.

[38] http://www.misp-project.org/
[39] Nato Computer Incident Response Capability
[40] Computer Incident Response Center Luxemburg
[41] Computer Emergency Response Team. European Union
[42] http://www.circl.lu/services/misp-malware-information-sharing-platform/
[43] Computer Security Incident Response Team
[44] Open Indicator of Compromise. Indicadores de Compromiso de código abierto

103. A fecha de realización de esta guía, la última versión disponible de REYES/MISP permite la integración con otros sistemas (otras instancias de REYES/MISP u otros) pero no empleando TAXII como medio de transporte.

7.1.1 REPRESENTACIÓN DE LA INFORMACIÓN DE CIBERSEGURIDAD

104. La estructura interna de los datos almacenados en una instancia de REYES/MISP está organizada de una manera fácilmente compatible con STIX:

- Los eventos de ciberseguridad son entidades que se describen mediante uno o más atributos de distintos tipos, pudiendo incluirse varios del mismo tipo.
- Un mismo atributo puede ser empleado por varios eventos, creándose de este modo relaciones implícitas entre eventos.
- Asimismo, pueden definirse relaciones entre eventos no en base a los atributos.
- Los atributos de un evento pueden ser de distintos tipos. Aunque no permiten la gran expresividad que ofrece STIX, sí que permite describir la gran mayoría de aspectos involucrados en un incidente de seguridad, y está alineados con los conceptos manejados por STIX.

105. Para describir los eventos se definen distintas categorías de atributos y dentro de ellos distintos tipos.

106. Las categorías disponibles son:

Categoría	Descripción
Internal reference	Identificador de referencia interno utilizado por la organización que aporta la información (por ejemplo, número de identificación de incidente)
Targeting data	Información sobre los objetivos correo electrónico del destinatario, las máquinas infectadas, departamento, y/o ubicación.
Antivirus detection	Lista de proveedores de antivirus que detectan el malware o información sobre el rendimiento de detección (por ejemplo, 13/43 o 67%). Adjunto con la lista de detección o enlace URL podría ser colocado aquí también.
Payload delivery	Información sobre la forma en que la "carga útil" del código dañino es entregada inicialmente, por ejemplo, información sobre el correo electrónico o página web, la vulnerabilidad utilizada, IPs origen, etc. La muestra del código dañino debería adjuntarse aquí.
Artifacts dropped	Cualquier artefacto (archivos, claves de registro, registros de actividad, herramientas, etc.) generado por la actividad del código dañino u otras modificaciones al sistema.

Categoría	Descripción
Payload installation	Ubicación y mecanismos empleados por el código dañino para colocar la "carga útil" en el sistema comprometido. Por ejemplo, se podría añadir un atributo de tipo filename|md5 como "c:\\windows\\system32\\malicious.exe|42d8cd98f00b204e9800998ecf8423a.
Persistence mechanism	Mecanismos utilizados por el código dañino para iniciarse en el arranque del sistema comprometido. Esto podría ser una clave de registro, modificación Ilegítima de un driver, archivo de tipo LNK en el arranque del sistema, etc.
Network Activity	Información sobre el tráfico de red generado por el código dañino.
Payload activity	Información sobre la "carga útil" final empleada por el código dañino. Puede contener una funcionalidad de ésta, por ejemplo, *keylogger*, RAT, o un nombre más identificativo de alguna carga útil como las APT,s ya conocidas como *Poison Ivy* o *Darkomet*, etc.
Attribution	Identificación del grupo, organización o país detrás del ataque.
External analysis	Cualquier otro resultado de un análisis adicional del código malicioso como ejemplos salidas de herramientas (Salida de analizador de documentos pdf, de entornos de análisis dinámico de código dañino, informes de ingeniería inversa del código dañino, etc.)
Other	Atributos que no son parte de cualquier otra categoría

Tabla 3 Categorías de atributos aplicables a un evento en REYES/MISP

107. Cada una de esas categorías permite definir atributos de diferentes tipos. La siguiente tabla muestra que tipos se relacionan con cada categoría:

Categoría	Tipos de atributos relacionados en la categoría
Internal reference	*'link', 'comment', 'text', 'other'*
Targeting data	*'target-user', 'target-email', 'target-machine', 'target-org', 'target-location', 'target-external', 'comment'*
Antivirus detection	*'link', 'comment', 'text', 'attachment', 'other'*

Categoría	Tipos de atributos relacionados en la categoría
Payload delivery	*'md5', 'sha1', 'sha256', 'filename', 'filename|md5', 'filename|sha1', 'filename|sha256', 'ip-src', 'ip-dst', 'hostname', 'domain', 'email-src', 'email-dst', 'email-subject', 'email-attachment', 'url', 'ip-dst', 'user-agent', 'http-method', 'AS', 'pattern-in-file', 'pattern-in-traffic', 'yara', 'attachment', 'malware-sample', 'link', 'comment', 'text', 'vulnerability', 'other'*
Artifacts dropped	*'md5', 'sha1', 'sha256', 'filename', 'filename|md5', 'filename|sha256', 'filename|sha1', 'regkey', 'regkey|value', 'pattern-in-file', 'pattern-in-memory', 'yara', 'attachment', 'malware-sample', 'comment', 'text', 'other', 'named pipe' : 'named pipe', 'mutex'*
Payload installation	*'md5', 'sha1', 'sha256', 'filename', 'filename|md5', 'filename|sha1', 'filename|sha256', 'pattern-in-file', 'pattern-in-traffic', 'pattern-in-memory', 'yara', 'vulnerability', 'attachment', 'malware-sample', 'comment', 'text', 'other'*
Persistence mechanism	*'filename', 'regkey', 'regkey|value', 'comment', 'text', 'other'*
Network activity	*'ip-src', 'ip-dst', 'hostname', 'domain', 'email-dst', 'url', 'user-agent', 'http-method', 'AS', 'snort', 'pattern-in-file', 'pattern-in-traffic', 'attachment', 'comment', 'text', 'other'*
Payload type	*'comment', 'text', 'other'*
Attribution	*'comment', 'text', 'other'*
External analysis	*'md5', 'sha1', 'sha256', 'filename', 'filename|md5', 'filename|sha1', 'filename|sha256', 'ip-src', 'ip-dst', 'hostname', 'domain', 'url', 'user-agent', 'http-method', 'regkey', 'regkey|value', 'AS', 'snort', 'pattern-in-file', 'pattern-in-traffic', 'pattern-in-memory', 'vulnerability', 'attachment', 'malware-sample', 'link', 'comment', 'text', 'other'*
Other	*'comment', 'text', 'other'*

Tabla 4 Tipos de atributos utilizables por categorías aplicables a un evento en REYES/MISP

108. Estos distintos tipos permiten una descripción muy rica de las distintas características del evento.

Tipo de atributo	Descripción
md5	Es recomendable utilizar el “filename|md5” siempre que sea posible.
sha1	Es recomendable utilizar el “filename|sha1” siempre que sea posible.
sha256	Es recomendable utilizar el “filename|sha256” siempre que sea posible.
filename	Nombre de archivo observado
filename|md5	Un nombre de archivo y un resumen criptográfico MD5 separados por una | (sin espacios)
filename|sha1	Un nombre de archivo y un resumen criptográfico SHA1 separados por una | (sin espacios)
ip-src	Una dirección IP de origen del atacante
dst-ip	Una dirección IP de destino del atacante o servidor C&C (*command and control*).
Hostname	Nombre completo (FQDN – *Fully Qualified domain name*) de una máquina empleada por un atacante.
Domain	Nombre de dominio utilizado en el código dañino. Se debe emplear este tipo, además de *hostname*, cuando el nombre de dominio es importante o relevante, o puede ser usado para crear vínculos entre eventos.
email-src	Dirección de correo electrónico (o nombre de dominio) que se utiliza para enviar el código dañino.
email-dst	Dirección de correo electrónico del destinatario.
email-subject	El asunto del correo electrónico
email-attachment	Nombre del archivo adjunto de correo electrónico.
url	URL
http-method	Método HTTP utilizado por el malware (por ejemplo POST, GET, ...).
user-agent	El *user-agent* utilizado por el código dañino si realiza peticiones HTTP.
Regkey	Clave de registro de Windows (nombre)

Tipo de atributo	Descripción
regkey|Value	Clave de registro de Windows y valor separados por |
AS	Número de sistema autónomo (ASN)
Snort	Regla de IDS en formato snort[45]. Esta regla se reescribirá automáticamente en las exportaciones de NIDS.
pattern-in-file	Patrón en archivo que identifica o relaciona con el código dañino.
pattern-in-traffic	Patrón en el tráfico de red que identifica o relaciona con el código dañino.
pattern-in-memory	Patrón en un volcado de memoria que identifica o relaciona con el código dañino.
Yara	Firma YARA[46] de un código dañino
Vulnerability	Una referencia a la vulnerabilidad utilizada en la explotación. Es recomendar si existe el identificador CVE.
attachment	Archivo relevante que se desee adjuntar al evento que no es una muestra del código dañino.
malware-sample	Muestra del código dañino relevante.
link	Enlace a una información externa.
Coment	Comentario o descripción en un lenguaje humano. Esto no se correlaciona con otros atributos.
text	Nombre, ID o una referencia
named pipe	"*named pipe*" empleada por el código dañino para comunicación inter-procesos en el sistema comprometido.
mutex	*"mutex"*, empleada por el código dañino para garantizar la ejecución exclusiva en el sistema comprometido.
Other	Otro atributo no recogido en otros.
target-user	Nombres de ususarios de sistema atacados.

[45] https://www.snort.org/
[46] http://plusvic.github.io/yara/

Tipo de atributo	Descripción
target-email	Direcciones de correo electrónico atacados.
target-machine	Nombre de la máquina o sistema atacado.
target-org	Nombre de la organización atacada.
target-location	Ubicación de la organización atacada.
target-external	Otras organizaciones objetivo externas afectadas por este ataque.

Tabla 5 Tipos de atributos utilizables en REYES/MISP

7.1.2 FUNCIONALIDADES

109. Las funcionalidades básicas que ofrece son:

- Crear y editar eventos
- Añadir y editar atributos
- Buscar en los atributos por un valor interesante
- Correlación automática de eventos basándose en atributos que son comunes
- Exportación de datos. En especial es importante destacar que la posibilidad de exportar eventos en formato STIX.

110. Estas funcionalidades son accesibles tanto a través del interfaz web (caso de uso de un analista de ciberseguridad que accede a la aplicación) y también mediante interfaz REST[47] para permitir la consulta y/o actualización automática par parte de otros sistemas, incluso otras instancias de REYES/MISP.

7.1.3 CAPTURAS DE PANTALLAS

111. La siguiente imagen representa la página principal de REYES/MISP en la que se puede observar los últimos eventos recogidos en el sistema.

[47] http://en.wikipedia.org/wiki/Representational_state_transfer

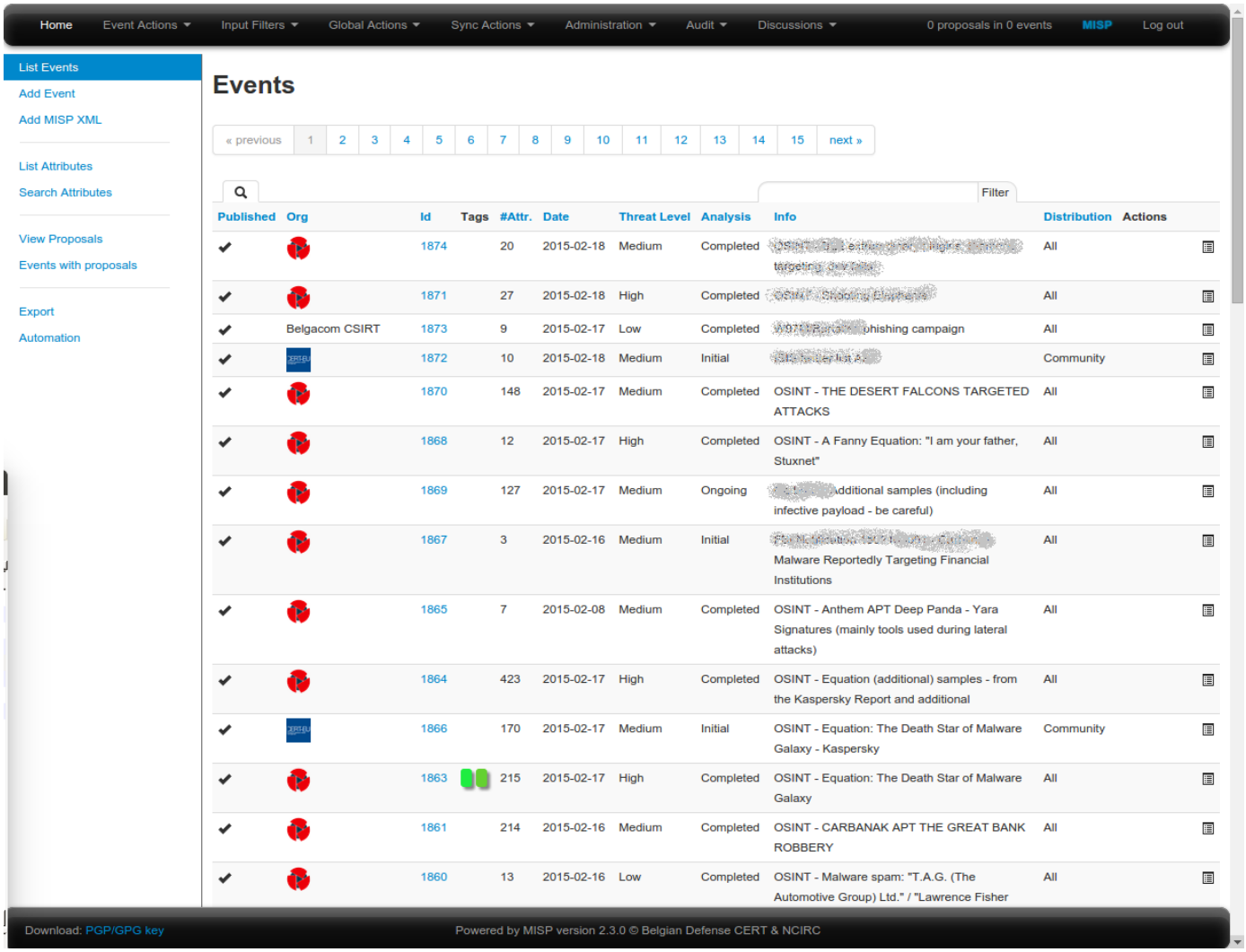


Figura 4 Página principal

112. Al visualizar un evento concreto podemos observar tanto los atributos como los metadatos del evento que pueden incluir aspectos como por ejemplo criterios sobre cómo puede ser compartida la información.

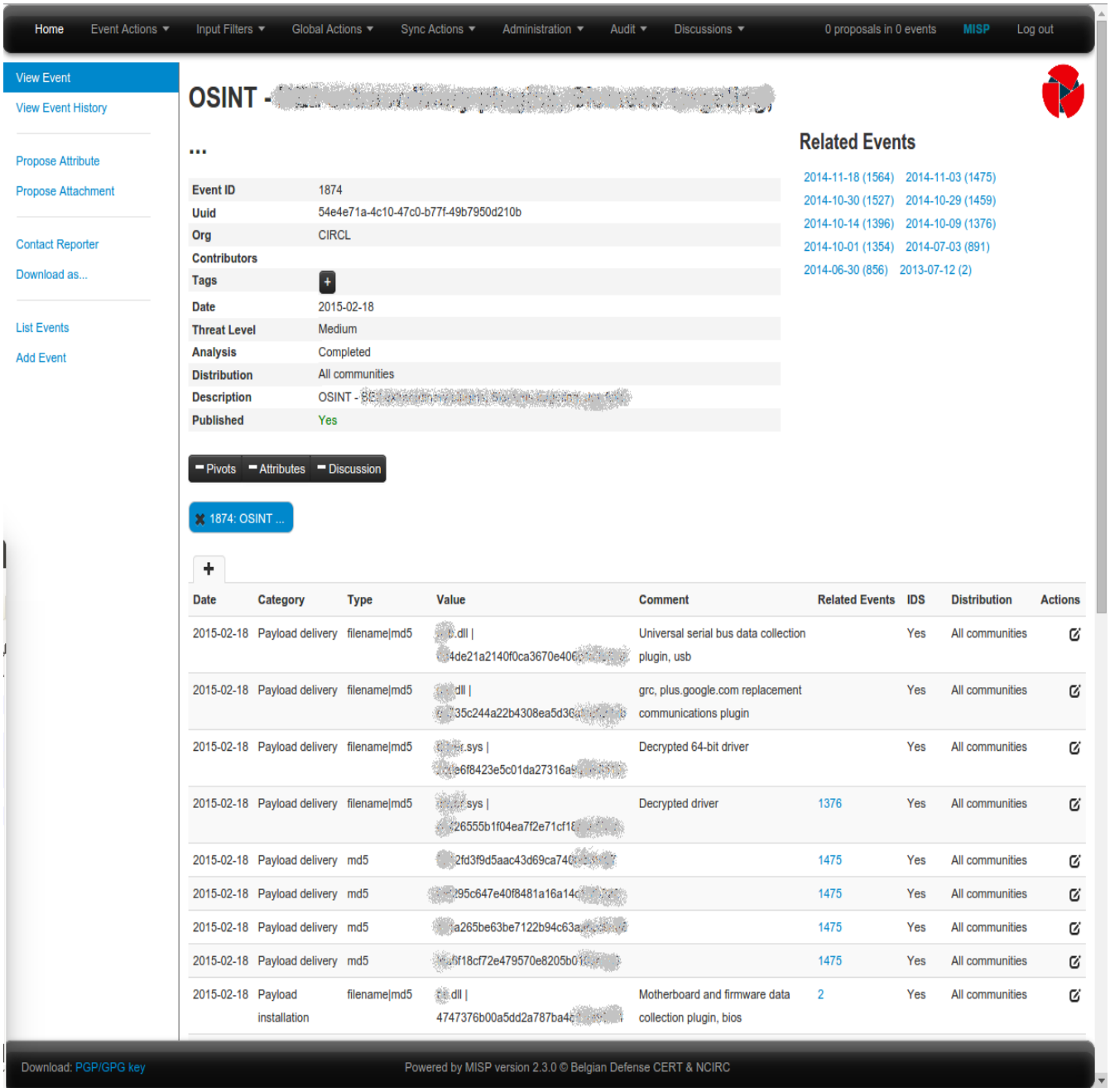
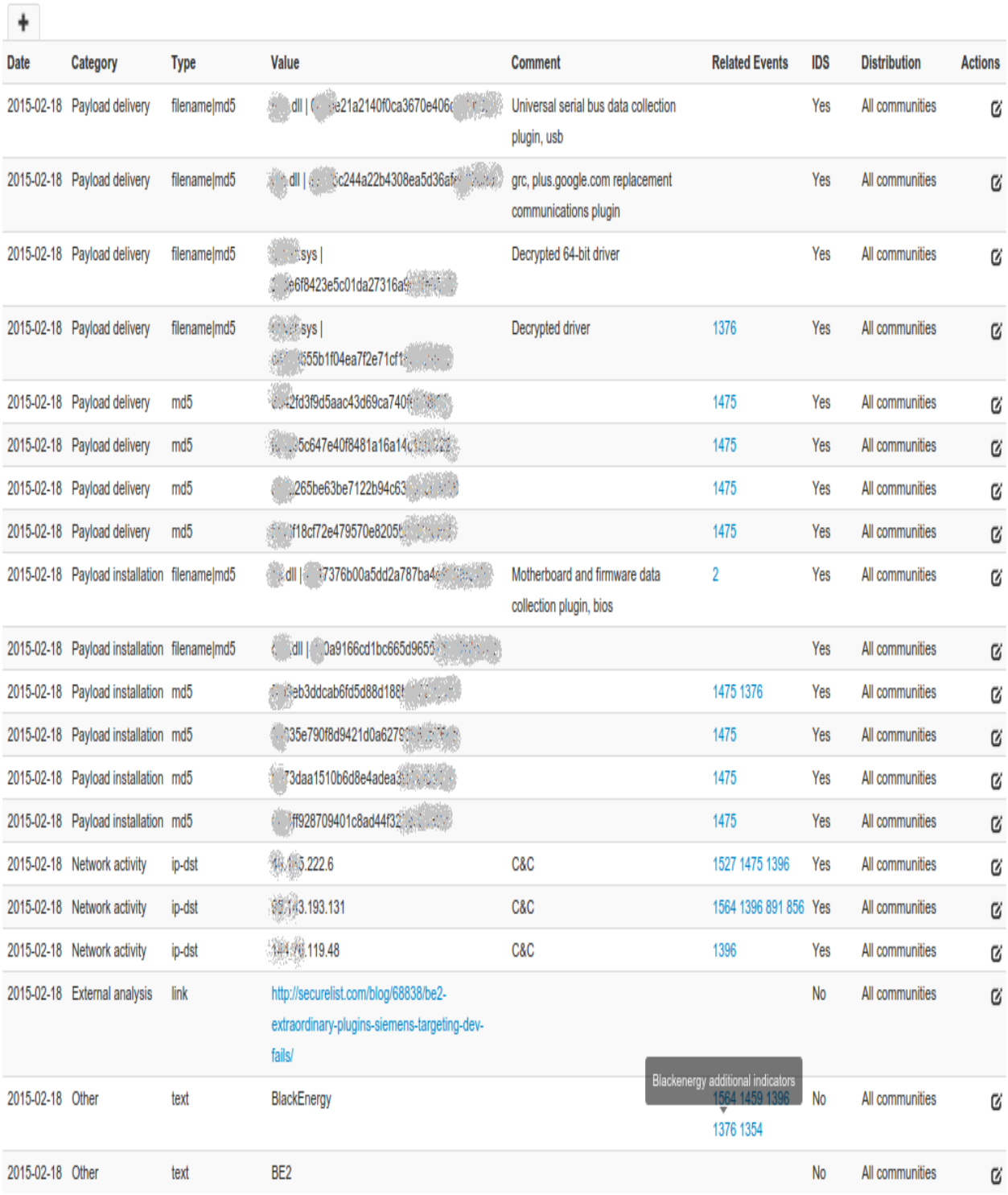


Figura 5 Vista de un evento

113. También es interesante comprobar como el sistema ha relacionado determinados atributos con otros eventos que también lo presentan, y la información aparece destacada puesto que es de gran ayuda al ciberanalista a la hora de valorar y ampliar su conocimiento sobre una determinada ciberamenaza.

114. En la siguiente captura de pantalla podemos observar todos los atributos relacionados con un evento. A medida que los distintos ciberanalistas dispongan de más información y del nivel de permisos que tengan asignados, podrán enriquecer la información.



Date	Category	Type	Value	Comment	Related Events	IDS	Distribution	Actions
2015-02-18	Payload delivery	filename|md5	[redacted].dll | [redacted]e21a2140f0ca3670e406c[redacted]	Universal serial bus data collection plugin, usb		Yes	All communities	
2015-02-18	Payload delivery	filename|md5	[redacted].dll | [redacted]5c244a22b4308ea5d36af[redacted]	grc, plus.google.com replacement communications plugin		Yes	All communities	
2015-02-18	Payload delivery	filename|md5	[redacted]sys | [redacted]e6f8423e5c01da27316a9[redacted]	Decrypted 64-bit driver		Yes	All communities	
2015-02-18	Payload delivery	filename|md5	[redacted]sys | [redacted]655b1f04ea7f2e71cf1[redacted]	Decrypted driver	1376	Yes	All communities	
2015-02-18	Payload delivery	md5	[redacted]2fd3f9d5aac43d69ca740f[redacted]		1475	Yes	All communities	
2015-02-18	Payload delivery	md5	[redacted]5c647e40f8481a16a14c[redacted]		1475	Yes	All communities	
2015-02-18	Payload delivery	md5	[redacted]265be63be7122b94c63[redacted]		1475	Yes	All communities	
2015-02-18	Payload delivery	md5	[redacted]f18cf72e479570e8205[redacted]		1475	Yes	All communities	
2015-02-18	Payload installation	filename|md5	[redacted].dll | [redacted]7376b00a5dd2a787ba4[redacted]	Motherboard and firmware data collection plugin, bios	2	Yes	All communities	
2015-02-18	Payload installation	filename|md5	[redacted].dll | [redacted]0a9166cd1bc665d9655[redacted]			Yes	All communities	
2015-02-18	Payload installation	md5	[redacted]eb3ddcab6fd5d88d188[redacted]		1475 1376	Yes	All communities	
2015-02-18	Payload installation	md5	[redacted]35e790f8d9421d0a6279[redacted]		1475	Yes	All communities	
2015-02-18	Payload installation	md5	[redacted]73daa1510b6d8e4adea3[redacted]		1475	Yes	All communities	
2015-02-18	Payload installation	md5	[redacted]ff928709401c8ad44f32[redacted]		1475	Yes	All communities	
2015-02-18	Network activity	ip-dst	[redacted]5.222.6	C&C	1527 1475 1396	Yes	All communities	
2015-02-18	Network activity	ip-dst	[redacted]3.193.131	C&C	1564 1396 891 856	Yes	All communities	
2015-02-18	Network activity	ip-dst	[redacted].119.48	C&C	1396	Yes	All communities	
2015-02-18	External analysis	link	http://securelist.com/blog/68838/be2-extraordinary-plugins-siemens-targeting-dev-fails/			No	All communities	
2015-02-18	Other	text	BlackEnergy		Blackenergy additional indicators 1564 1459 1396 1376 1354	No	All communities	
2015-02-18	Other	text	BE2			No	All communities	

Figura 6 Atributos de un evento

115. Finalmente, en la siguiente captura de pantalla podemos observar los distintos en que es posible exportar la información sobre un evento, y concretamente como está disponible el formato STIX.

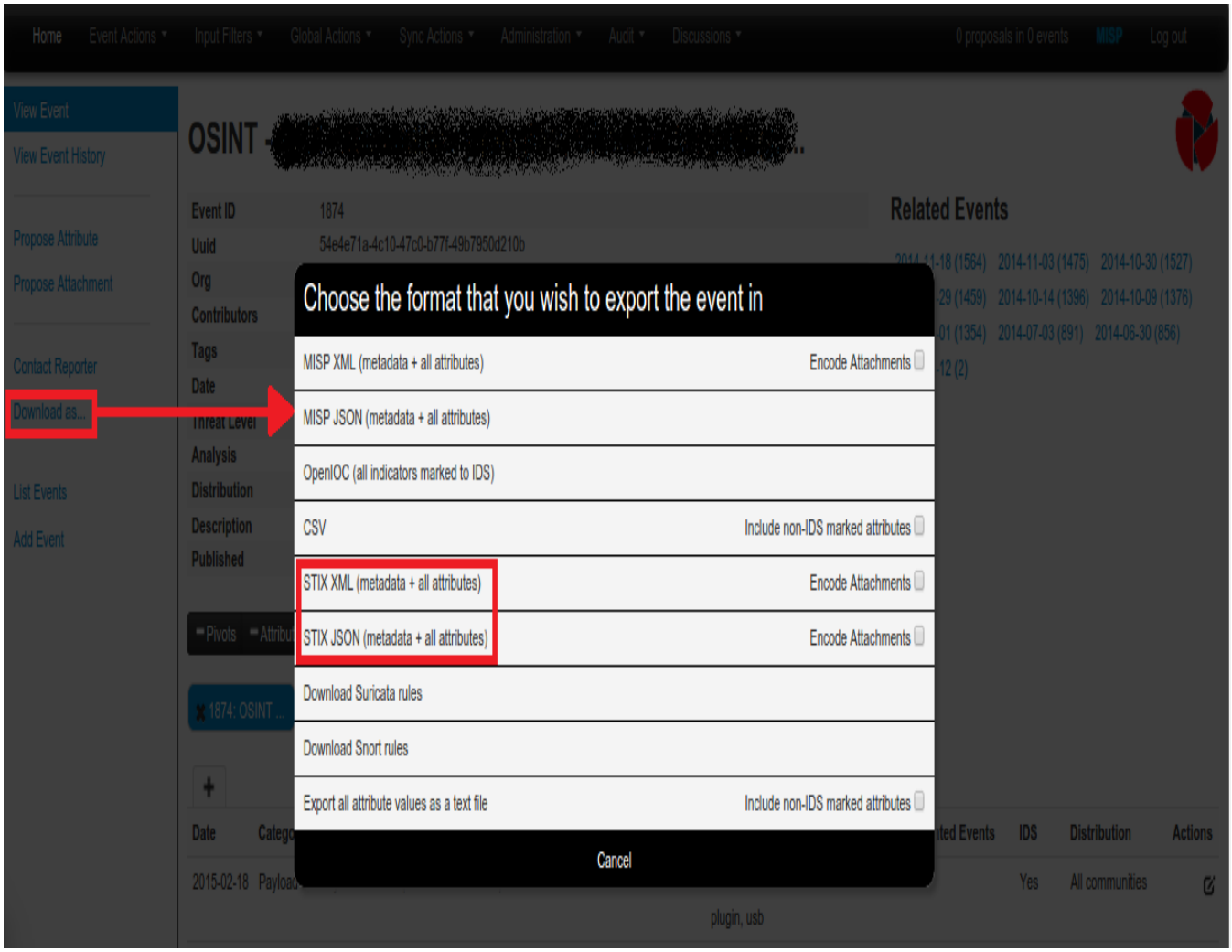


Figura 7 Formatos disponibles para descargar un evento

116. La herramienta MISP está desarrollada con una licencia de código libre y se puede conseguir gratuitamente. Su máxima utilidad no se obtiene empleándola en el contexto de una única organización sino cuando distintas organizaciones lo emplean para crear una comunidad de intercambio de información de ciberseguridad.

117. Pese a no implementar TAXII como mecanismo de transporte de la información de ciberseguridad, sí que permite crear distintos tipos de comunidades como las que TAXII contempla.

ANEXO A.ESTÁNDAR TAXII

1. MODELIZACIÓN DE COMUNIDADES DE INTERCAMBIO EN TAXII

Se pueden dar muchos tipos de comunidades donde distintas entidades (persona o grupo de personas independientes u organizaciones privadas o públicas) intercambian información de ciberseguridad. Los distintos escenarios que son soportados por TAXII son muy diversos siendo lo suficientemente flexible para poder soportarlos. Sin embargo, hay un conjunto de escenarios, por otro lado muy comunes, sobre los que TAXII ha estado especialmente interesado en poder cubrir.

1.1 ROLES

TAXII define distintos roles a la hora de actuar en estos escenarios:

- **Productor**: se trata de una entidad que es fuente de información estructurada que ofrece a través de servicios conformes con TAXII
- **Consumidor**: se trata de una entidad que es receptora de información estructurada facilitada por un productor empleando para ello servicios conforme a TAXII.

Estos roles no son excluyentes, una entidad puede actuar simultáneamente en los dos. En base al papel que juegan y como se interrelacionan se pueden plantear distintos modelos de comunidades de intercambio de información.

1.2 CAPACIDADES DE INTERCAMBIO DE INFORMACIÓN EN TAXII

El objetivo de TAXII es que a través de los servicios que se especifican, sea posible implementar un conjunto de capacidades que permitan a productores y consumidores de información realizar distintos modos de intercambio de información.

Por tanto, TAXII da la especificación de diversos servicios que permiten implementar las siguientes capacidades:

- **Mensajería en modo “push”**

  El productor de información facilita al consumidor información siguiendo lo establecido en un acuerdo previo o no, que contemple exactamente el modo en que se realizará. Según si este acuerdo existe estamos ante un modelo de intercambio en el que un consumidor se suscribe a un determinado servicio que ofrece un productor, o bien, si no existe dicho acuerdo ante un consumidor que está actuando como repositorio público de información al que cualquier productor puede aportar de manera libre.

  Es interesante destacar que en este modelo de intercambio, TAXII define el concepto de “buzón” que es donde el consumidor va a recibir la información en forma de mensajes con contenido TAXII.

- **Mensajería en modo “pull”**

  El consumidor puede desear ser él quien descargue la información del productor. Esto le permite controlar el momento y también elimina la necesidad de que el consumidor deba de estar esperando conexiones entrantes desde el productor. Al igual que en el

modelo anterior, los acuerdos pueden existir o no y ello dará lugar a modelos muy diferentes, básicamente fuentes de información pública o no.

– **Consultas**

Además de las capacidades de mensajería en modo "push" o modo "pull", el consumidor puede necesitar recibir únicamente la información que cumpla unos determinados criterios, por lo que TAXII también permite añadir a las capacidades de mensajería descritas anteriormente la capacidad de realizarse bajo unos criterios de consulta que el consumidor establezca.

– **Descubrimiento de servicios**

Puesto que TAXII permite distintas modalidades de servicio que pueden ser variadas (modo "push" y modo "pull", y modo consulta), así como el uso de distintos protocolos de transporte de mensajes (actualmente sólo HTTP o HTTPS), y distintos formatos de representación de los mensajes (actualmente está especificado el uso de XML), es necesario que TAXII ofrezca la capacidad de descubrir qué tipo de capacidades ofrece un determinado productor de información.

1.3 TIPOS BÁSICOS DE COMUNIDADES:

Considerando los distintos roles presentados y las distintas capacidades que se ofrece, TAXII contempla los siguientes escenarios principales de compartición de información. No son únicos ni tampoco se excluye que TAXII pueda ser empleado en otros modelos de comunidades.

– **Nodo central coordinador de intercambio**

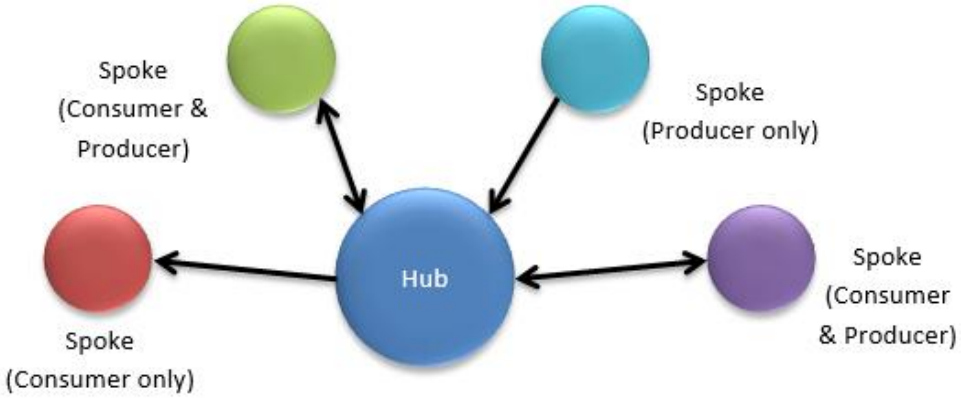


Figura 8 Comunidad colaborativa de intercambio con nodo central coordinador

En este modelo existe una organización que actúa de centralizador de la información y es a la vez productora y consumidora. Además otro conjunto de organizaciones hacen uso del rol centralizador de la anterior organización para actuar como productora o consumidora, o ambos roles a la vez. En este escenario, la organización centralizadora puede que no genere por si misma información y que la que se ofrece como productora únicamente sea la que otras organizaciones están facilitando.

– **Nodo centralizado de distribución**

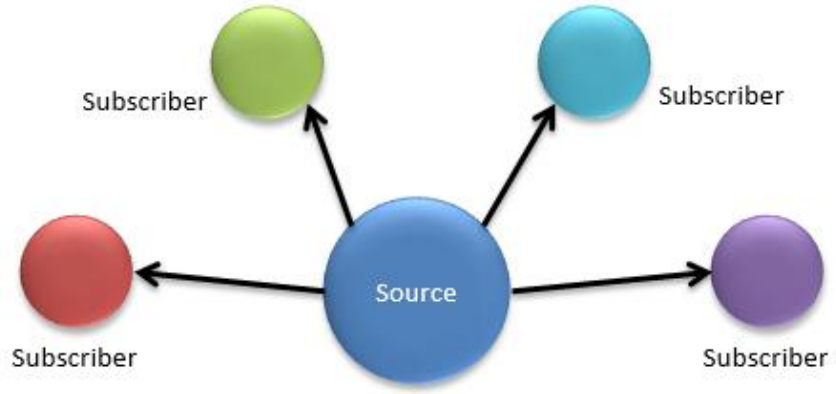


Figura 9 Comunidad de consumidores de información con nodo central distribuido

Existe un nodo único central que actúa como productor y que facilita la información de ciberseguridad al resto de organizaciones que actúan únicamente como consumidoras. Es un clásico modelo de servicio de suscripción, en el que una organización ofrece a sus suscriptores (libre o previo pago) información acorde a los acuerdos que se hayan establecido.

– **Redes P2P[48] o entre iguales**

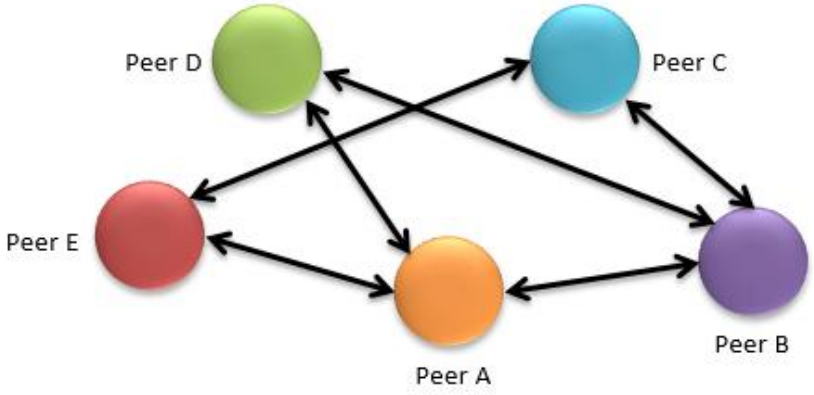


Figura 10 Comunidad de intercambio entre iguales

En este modelo, no existe ninguna jerarquización y las organizaciones actúan ya sea como productora y/o consumidora y estableciendo las relaciones de intercambio con otras organizaciones de manera no coordinada o planificada, y quizá de manera temporal. De esta manera se establece una red mallada entre los distintos participantes de la red a medida que las necesidades lo indican.

En realidad estos modelos no son excluyentes entre sí a la hora de implementar un servicio de intercambio de información con TAXII y es posible diseñar escenarios de uso diferentes siempre y cuando se base en la definición de TAXII de servicios y roles.

[48] Peer To Peer.Red de ordenadores sin un servidor central

1.4 ARQUITECTURA DE TAXII

1.4.1 ARQUITECTURA FUNCIONAL TAXII

A nivel funcional, una implementación de TAXII define unas unidades funcionales necesarias para implementar un sistema conforme a TAXII.

– **TTA - TAXII Transfer Agent**

Unidad funcional que conecta con la red y que envía y recibe los mensajes TAXII a otros TTA. Debe seguir las especificaciones de empaquetamiento de mensajes TAXII en el protocolo escogido. Así mismo, ofrece al TMH la abstracción de la implementación del transporte.

– **TMH - TAXII Message Handler**

Esta unidad es la responsable de recibir y generar los mensajes TAXII en el formato que se haya escogido en la implementación y de acuerdo a las especificaciones (actualmente solo para XML) e interactúa con el TAXII back-end facilitándole o recibiendo información extraída o a ser incluida en los mensajes TAXII.

– **TAXII back-end**

En realidad TAXII no define ningún requerimiento para esta unidad funcional salvo que debe interactuar con el TMH.

1.4.2 ARQUITECTURA TAXII – COMPONENTES DE RED

A nivel de modelo o arquitectura de red, TAXII contempla un modelo cliente-servidor.

– **Demonio TAXII**

Es la parte de la implementación de TAXI que facilita uno más servicios TAXII que se detallan en el siguiente apartado.

– **Cliente TAXII**

Es la parte de la implementación de TAXII que inicia un intercambio de mensajes con el demonio remoto TAXII. El cliente no mantiene un servicio escuchando en la red.

Es importante entender que no existe un mapeo entre el rol TAXII y el componente de red y cualquier combinación es posible y da lugar a modelos de intercambio distintos. Por ejemplo, en un modelo con un nodo central de intercambio de información, el nodo central implementará al mismo tiempo la parte cliente y la parte servidora para poder ofrecer todas las capacidades TAXII previstas. Igualmente, en un modelo de mensajería en modo "push", el consumidor de información está funcionando como demonio TAXII.

1.5 ESPECIFICACIONES DE TAXII

El estándar TAXII especifica principalmente:

– **Servicios TAXII:** Se trata de los mecanismos necesarios para poder ofrecer las capacidades anteriormente descritas.

- **Intercambio de mensajes TAXII:** Se trata del protocolo de intercambio de mensajes TAXII que se debe producir en cada uno de los servicios TAXII que se deben realizar para poder ofrecer el servicio que se ha especificado.
- **Mensajes TAXII:** el estándar define las distintas partes que deben contener los diferentes mensajes necesarios. El formato del mensaje no se especifica en el documento principal de TAXII para ofrecer la flexibilidad de que se pueda definir mediante distintas soluciones. Actualmente está definido en otro documento del estándar para emplear XML.

1.6 MENSAJES TAXII

La especificación de los distintos mecanismos de intercambio de mensajes que deben soportar los servicios TAXII emplean el siguiente conjunto de mensajes TAXII.

- **TAXII Status Message:** Se utiliza para indicar una condición de error o, en algunos intercambios, un acuse de recepción del mensaje.
- **TAXII Discovery Request:** Una solicitud de información sobre los servicios TAXII soportados por el demonio TAXII consultado**.**
- **TAXII Discovery Response:** Una respuesta a un mensaje TAXII Discovery Request que contiene información sobre los servicios TAXII soportados.
- **TAXII Collection Information Request:** Una solicitud de información sobre la Colecciones de datos TAXII soportadas o facilidades desde el demonio TAXII consultado.

Las "Colecciones de datos TAXII" son conjuntos estructurados de información sobre ciberseguridad que pueden ser intercambiados empleando servicios TAXII. En el contexto de una entidad que ofrece servicios TAXII, cada colección ofrecida tiene un nombre único que la identifica. Existen dos tipos en forma de conjuntos de información ordenados (denominados TAXII data feeds) o bien en forma de conjunto no ordenado (TAXII data sets).

- **TAXII Collection Information Response:** Una respuesta a una solicitud TAXII Collection Information Request que contiene información sobre las colecciones de datos TAXII ofrecidas desde el servidor TAXII consultado. Esta solicitud puede contener criterios de consulta para los casos en que el cliente no esté interesado en la totalidad de la colección y sólo desee suscribirse a un subconjunto que cumpla unos determinados criterios.
- **TAXII Manage Collection Subscription Request:** Una petición para establecer una nueva suscripción o gestionar una suscripción existente.
- **TAXII Manage Collection Subscription Response:** Una respuesta a una solicitud de suscripción que indica el nuevo estado de las suscripciones a una colección de datos TAXII dada.
- **TAXII Poll Request:** Una solicitud de contenido asociado a una colección de datos TAXII.
- **TAXII Poll Response:** Una respuesta a una solicitud de contenido de información de ciberseguridad asociada a una colección de datos TAXII. Esta respuesta contiene en sí

la información de ciberseguridad y el modo preferido para estructurar esa información que se facilita sería STIX, aunque el estándar TAXII no lo impone. En ocasiones la respuesta a enviar al cliente puede contenerse en un único mensaje o bien se descompondrá en varios mensajes de respuesta.

– **TAXII Poll Fullfillment Request:** Se utiliza para que el cliente TAXII solicite un resultado que, o bien había sido retrasado (si el servidor contestó a una petición con mensaje de estado de tipo "pendiente"), o bien se corresponde a otra porción del resultado cuando la respuesta total a la petición se indicó en la primera respuesta que se descomponía en varias partes.

– **TAXII Inbox Message:** Se utiliza para que el servidor TAXII envíe contenido de información de ciberseguridad asociada a una colección de datos TAXII a un consumidor de información TAXII que la recibirá en un "buzón" o "TAXII inbox".

1.7 SERVICIOS TAXII

El funcionamiento de TAXII está completamente basado en servicios que productores y consumidores emplean para establecer sus modelos de relación. El estándar no obliga a la implementación de ninguno de ellos, es decir las entidades pueden o no implementar los servicios según sea su necesidad. Es decir es posible realizar una implementación de TAXII en la que no se ofrezca ningún servicio, por ejemplo en el caso de un sistema que implementa un consumidor de información que utiliza la capacidad de mensajería en modo "pull".

A continuación presentaremos los servicios que es posible implementar y el intercambio de mensajes TAXII que debe realizarse.

– **Discovery Service:** Es el mecanismo para que el demonio TAXII comunique al cliente información sobre disponibilidad de otros servicios, como acceder a ellos (dirección: un servicio podría encontrarse otro demonio TAXII en otra dirección, formato del mensaje TAXII). Para este servicio sólo se contempla un posible intercambio de mensajes TAXII:

  - *"Discovery Exchange"*

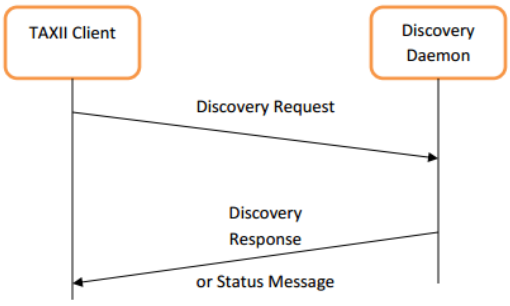


Figura 11 Intercambio de mensajes "*Discovery Exchange*"

– **Collection Management Service:** Es el mecanismo para que un consumidor de información consulte a un productor las colecciones de datos disponibles, y solicite y gestione una suscripción a alguna de las colecciones disponibles. Para este servicio, el servidor ha de soportar alguno (o ambos) de los intercambios de mensajes siguientes:

- *"Collection Information Exchange"*

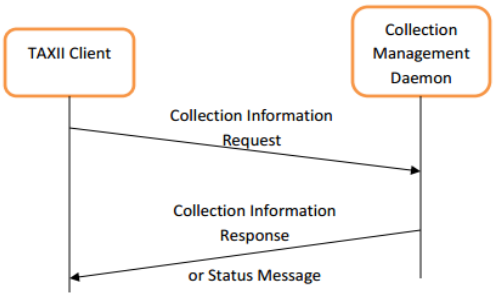


Figura 12 Intercambio de mensajes "*Collection Information Exchange*"

- *"Subscription Management Exchange"*

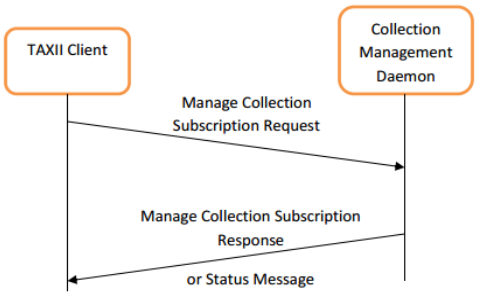


Figura 13 Intercambio de mensajes "*Subscription Management Exchange*"

La solicitud de suscripción puede contener una consulta con el fin de establecer una suscripción a un subconjunto de la totalidad de información contenida en la colección

– **Inbox Service:** Es el mecanismo por el cual un consumidor de información recibe por parte de un productor el contenido TAXII sin iniciar él la conexión. Es importante destacar que la especificación de TAXII no implica que deba existir una suscripción previa, es decir que es posible que un consumidor reciba, si así lo decide, información no solicitada. Esta es una decisión de implementación y de posibles acuerdos entre entidades de la comunidad de intercambio de información. Para este servicio sólo se contempla un posible intercambio de mensajes.

- *"Inbox Exchange"*

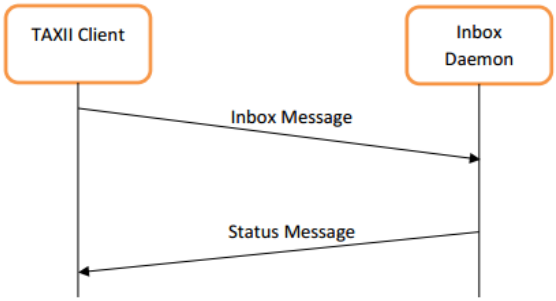


Figura 14 Intercambio de mensajes "*Inbox Exchange*"

En el mensaje "Inbox Message" está el contenido de información TAXII en que la parte de información de ciberseguridad no está definida por TAXII. Es decisión de las entidades

establecer que estructura tendrá, sin embargo es recomendable que esta información de ciberseguridad venga expresada mediante STIX. Es importante destacar que en este servicio, el productor de información está actuando como cliente TAXII y el consumidor como servidor.

– **Poll Service:** Es el mecanismo por el que un productor de información permite al consumidor iniciar la conexión para descargar contenido de una colección de datos. Al iniciar la conexión, el consumidor puede especificar una consulta para recuperar únicamente un subconjunto de los datos de la colección. Para este servicio se contemplan dos posibles intercambios de mensajes, el primero de ellos es de obligada implementación si se ofrece el servicio.

  - *"Poll Exchange"*

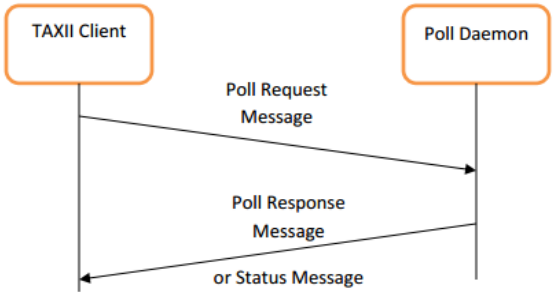


Figura 15 Intercambio de mensajes "*Poll Exchange*"

En el mensaje "Poll Response Message" está el contenido de información TAXII en que la parte de información de ciberseguridad no está definida por TAXII. Es decisión de las entidades establecer que estructura tendrá, sin embargo es recomendable que esta información de ciberseguridad venga expresada mediante STIX.

  - *"Multi-part Poll Exchange"*

Cuando la respuesta es muy grande y no es práctico el incluirla en único mensaje TAXII, el demonio puede tomar la decisión de dividirla en varios mensajes. Empleará entonces este esquema de intercambio de mensajes.

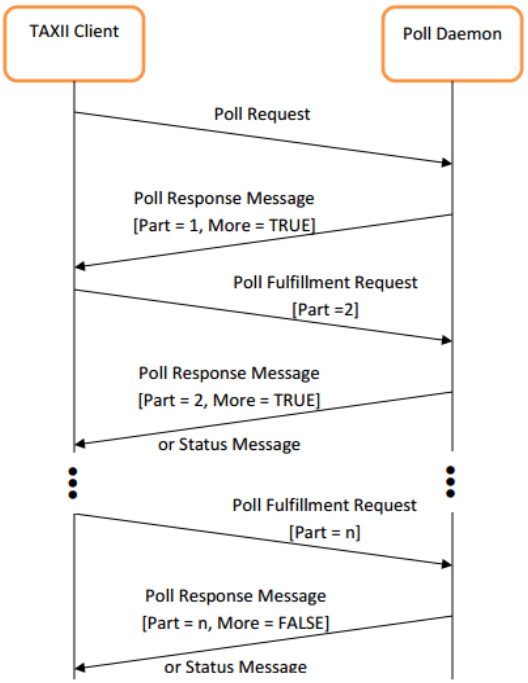


Figura 16 Intercambio de mensajes "*Poll Exchange*"

En el mensaje "Poll Response Message" está el contenido de información TAXII en que la parte de información de ciberseguridad no está definido por TAXII. Es decisión de las entidades establecer que estructura tendrá, sin embargo es recomendable que esta información de ciberseguridad venga expresada mediante STIX.

- *Intercambios asíncronos en el servicio "Poll Service"*

No se trata propiamente dicho de un servicio, sino de un modo de funcionamiento del "Poll Service". Tal y como se ha mostrado el modo de funcionamiento sería completamente síncrono, las respuestas se envían a continuación de recibir la solicitud. TAXII da la posibilidad de que este servicio funcione en modo asíncrono para permitir que la respuesta se pueda demorar. Pueden existir diversas razones para ello (por ejemplo, la información solicitada puede requerir la ejecución de tareas costosas en el back-end TAXII y es preferible indicar la demora al cliente), pero TAXII no las especifica.

Para permitir este funcionamiento, previamente en la solicitud del cliente se debe indicar que se soporta este modo de funcionamiento. Si la parte servidora lo estima necesario, se enviará un mensaje TAXII de estado indicando el estado "pendiente". Junto con este valor de estado también le informa del momento en que se espera que esté el resultado, un identificador con el que se hará referencia a los resultados que están pendientes (por si hubieran en paralelo varias consultas en estado pendiente) y también el modo en que se entregarán los resultados. La entrega de los resultados pendientes puede realizarse de dos formas.

- *Modo "pull"*

Es el modo más sencillo y preferible de funcionamiento. En cualquier momento posterior a la recepción del mensaje de estado de "pendiente", el cliente vuelve a solicitar las partes restantes. Él iniciará la conexión de nuevo y enviará un mensaje "Poll Fulfillment Request" con el identificador de la respuesta que está esperando.

El servidor responderá bien con el contenido (puede iniciar un intercambio en varias partes si es necesario); indicando con un mensaje de estado que ha habido un error en el mensaje "Poll Fulfillment Request" y entonces el cliente puede volver a enviarlo corregido (el error vendrá indicado en un valor del mensaje de estado recibido); que ha habido un error y que ambas partes cancelan la consulta (responderá con un mensaje de estado con el estado "Asynchronous Poll Error"); o bien iniciará el envío de la respuesta que puede ser en múltiples partes o no.

- *Modo "push"*

Este modo es más complicado puesto que requiere que el cliente soporte el servicio "Inbox Service" para permitir la recepción de la respuesta con una conexión iniciada por el servicio "Poll Service". Por lo tanto TAXII lo marca como opcional a la hora de implementarse el servicio "Poll Service" y sólo se empleará si ambas partes lo acuerdan. En la solicitud el cliente indicará que soporta este mecanismo asíncrono y dará las indicaciones necesarias del servicio "Inbox Service" que tenga implementado.

1.8 CONSIDERACIONES SOBRE EL CONTROL DE ACCESO A LA INFORMACIÓN EN TAXII

A pesar que TAXII no contiene ninguna especificación sobre mecanismos de identificación, autenticación y control de acceso a las colecciones de datos que un Productor de información de ciberseguridad ofrece, sí que hace unas ciertas consideraciones.

1.9 SOPORTE DE LOS PROTOCOLOS DE TRANSPORTE DE MENSAJES TAXII

No se indica explícitamente en el estándar TAXII pero está especificado que HTTPS es uno de los protocolos de transporte y este permite implementar mecanismos fuertes de identificación y autenticación de las partes involucradas. El implementador de un sistema conforme con el estándar TAXII deberá tomar las decisiones de diseño que le permitan emplear esta identificación de la entidad con la que se intercambia la información para determinar el nivel de autorización que se le da.

1.10 CONTROL DEL PRODUCTOR SOBRE LA INFORMACIÓN

La especificación de TAXII determina que el productor de la información tiene todos los derechos sobre la información y por lo tanto es libre de aplicar los criterios de control de acceso a la misma, y no sólo a los propios contenidos de las colecciones de datos sino también a los propios componentes TAXII, es decir, colecciones de datos disponibles, servicios ofrecidos, e incluso no existe obligación ninguna por parte del productor de informar al consumidor que existen limitaciones en el acceso a la información.

ANEXO B.SISTEMAS DE GESTIÓN DE CIBERINTELIGENCIA

1. SISTEMAS CONFORMES A TAXII

En la actualidad existen múltiples esfuerzos de la comunidad internacional de especialistas en ciberseguridad para la compartición de ciberinteligencia. A continuación presentaremos algunas iniciativas que hacen uso de TAXII para el transporte de la misma.

2. FUENTES DE CIBERINTELIGENCIA ABIERTA

Tradicionalmente, la comunidad de especialistas en ciberseguridad ofrece distintas fuentes de información actualizada sobre ciberamenazas. Sin embargo, el modo en que se han ofrecido ha sido muy heterogéneo y ha dificultado su integración en plataformas que buscan automatizar tareas de los ciberanalistas.

La compañía SOLTRA, organización creada por el FS-ISAC – Financial Services Information Sharing and Analysis Center y el DTCC - The Depository Trust & Clearing Corporation, con el objeto de facilitar al sector financiero estadounidense de mecanismos para mejorar su resiliencia frente a ciberamanazas.

Desde Soltran se ha promocionado el sitio web http://hailataxii.com que centraliza algunas de estas fuentes actuales de ciberinteligencia más populares y más reputadas, la transforma a objetos STIX y ofrece la información mediante servicios TAXII.

Actualmente transforma las siguientes fuentes de información:

http://www.abuse.ch: ofrece hilos referentes al seguimiento de las amenazas correspondientes a código dañino de las familias ZeuS, Palevo, SpyEye y Feodo.

http://Cybercrime-tracker.net: seguimiento de paneles de control de distintos tipos de botnets.

http://www.emergingthreats.net/: proveedor comercial de ciberinteligencia que ofrece asimismo de modo libre información de ciberseguridad que, sin ser tan completa como la versión comercial, es de utilidad para complementar otras fuentes de información pública.

http://malwaredomains.lehigh.edu/: iniciativa promovida por la universidad norteamericana Lehigh por la que se ofrece un hilo de información en el que se publican dominios relacionados con la publicación o uso de código dañino para ser empleado como lista negra de dominio.

http://www.malwaredomainlist.com: iniciativa no comercial que facilita listas de dominios relacionados con código dañino.

https://torstatus.blutmagie.de/: listado de nodos de salida de la red anónima TOR.

http://www.dshield.org: también conocido como “Internet Storm Center”, es una iniciativa de la organización SANS (www.sans.org) dedicada a la detección temprana de incidentes de seguridad. En el marco de esta iniciativa facilitan una lista de las 20 subredes de clase C que han identificado como generadoras de más ataques.

http://www.phishtank.com: iniciativa abierta para el reporte de URL de sitios de phishing.

Este servicio puede ser empleado tanto para comprobar y realizar pruebas con plataformas que hayan de emplear TAXII para recibir ciberinteligencia, como en un entorno más productivo, con información práctica y operativa. Sin embargo, existe riesgo de errores de funcionamiento al tratarse de un servicio ofrecido sin ningún tipo de garantía de servicio.

3. SOLTRA EDGE

La compañía SOLTRA ha creado una plataforma, denominada Soltra Edge (es una marca registrada) para implementar una comunidad de compartición de ciberinteligencia en el que de una plataforma para la compartición.

Sotra Edge (anteriormente fue conocida como "avalanche") es un sistema para la implementación de una comunidad para generación y compartición de ciberinteligencia que hace uso de STIX como lenguaje para estructura la información y de TAXII como mecanismo para transportarla a otras organizaciones con las que se haya establecido un acuerdo y sean productoras o consumidoras de ciberinteligencia en una instancia concreta de Soltra Edge.

Permite construir todos los modelos de relaciones definidos por TAXII y la información se estructura con STIX, y puede ser utilizada por una organización para albergar un punto común de intercambio de información para grupos internos u otras organizaciones con las que establezca acuerdos de intercambio.

Sin embargo, sus actuales términos de uso tienen ciertas limitaciones pero implementa un sistema completo conforme a STIX y TAXII. Ofrece funcionalidades como las siguientes:

– **Crear relaciones con otros sistemas automáticos que ofrezcan servicios o reciban en modo "pull" información vía TAXII:** El sistema permite crear relaciones con otros sistemas que ofrecen servicios TAXII en modo "*pull*" como se puede observar en la siguiente captura de pantalla en la que se puede ver como para un sitio se han seleccionado diversos hilos de información o colecciones de datos TAXII a la que el sistema se ha suscrito.

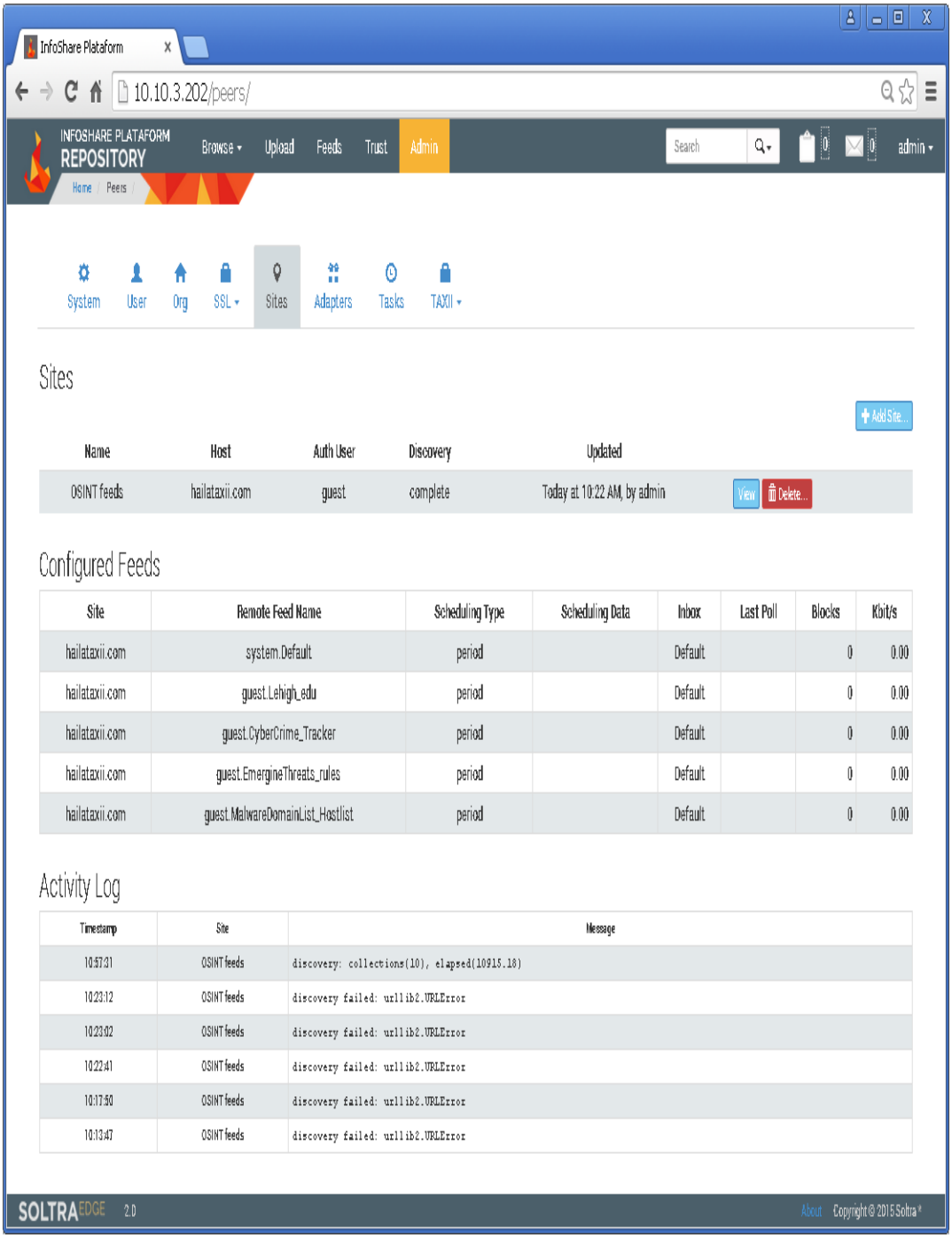


Figura 17 Creación de sitios con los que se va a relacionar la instancia para obtener información vía TAXII

La siguiente captura de pantalla muestra las distintas colecciones de datos TAXII que ofrece un sitio y las que están configuradas para ser recogidas periódicas.

Las consultas pueden ser programadas.

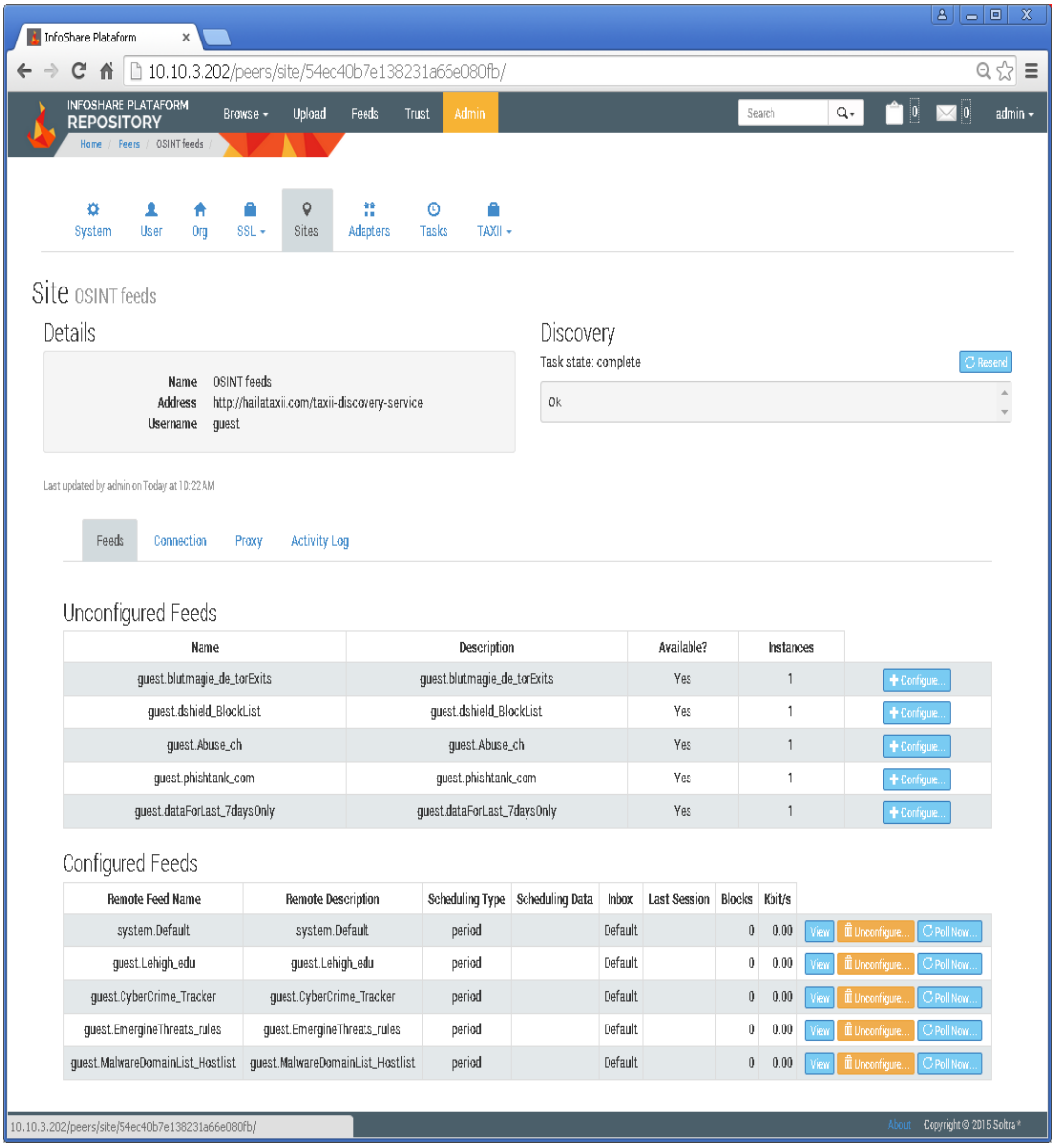


Figura 18 Hilos de colecciones de datos TAXII ofrecidos por otro host mediante TAXII

– **Crear publicar hilos de información filtrada para que sea consumida por usuarios en modo “pull” (por ejemplo otros sistemas Soltra Edge)**

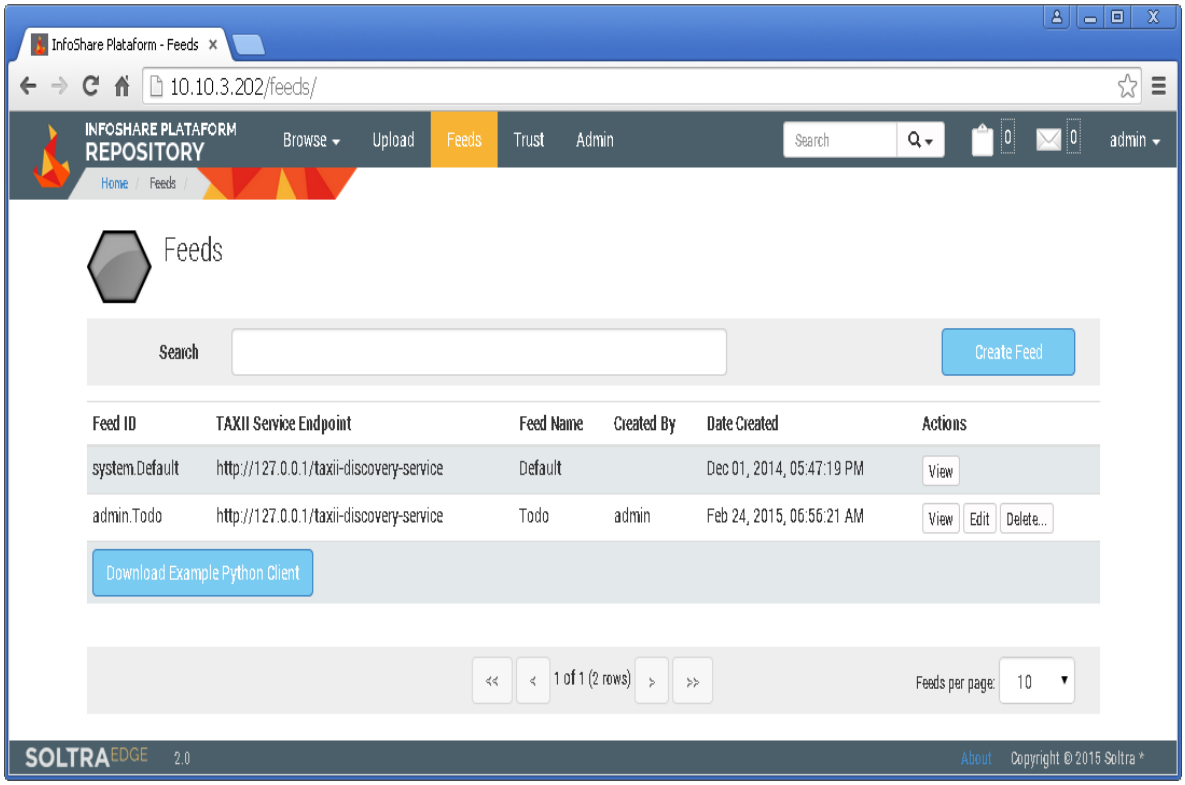


Figura 19 Colecciones de datos TAXII que publica el sistema, ofrecidos a través de servicios TAXII

El sistema permite crear hilos de información y filtrar con bastante detalle el tipo de información que se desea publicar así como las organizaciones con las que se puede compartir y el nivel de TLP que se publicará.

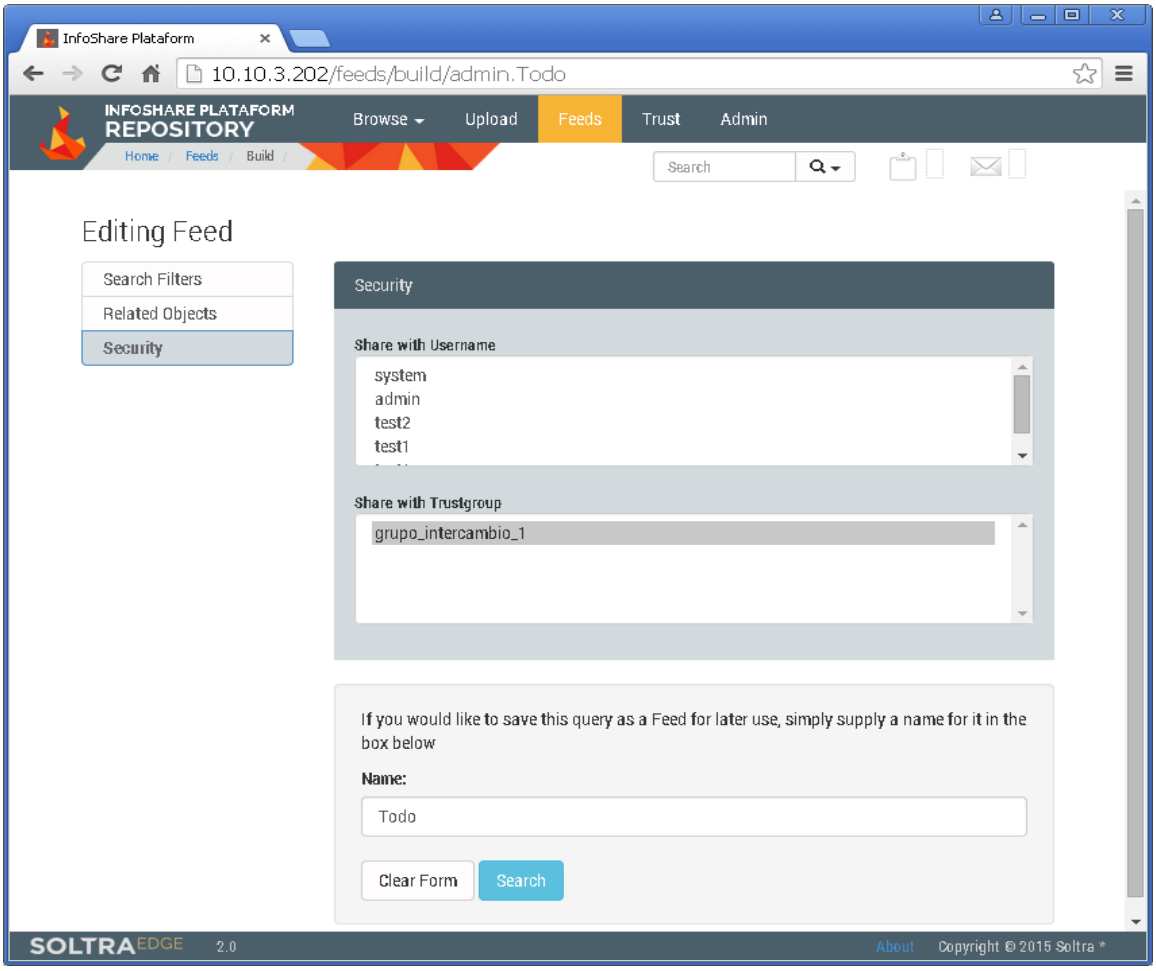


Figura 20 Configuración de los permisos para acceder a una colección de datos TAXII publicada por el sistema

Es posible controlar la información que se publica en una determina colección de datos TAXII mediante la configuración de criterios de filtrado.

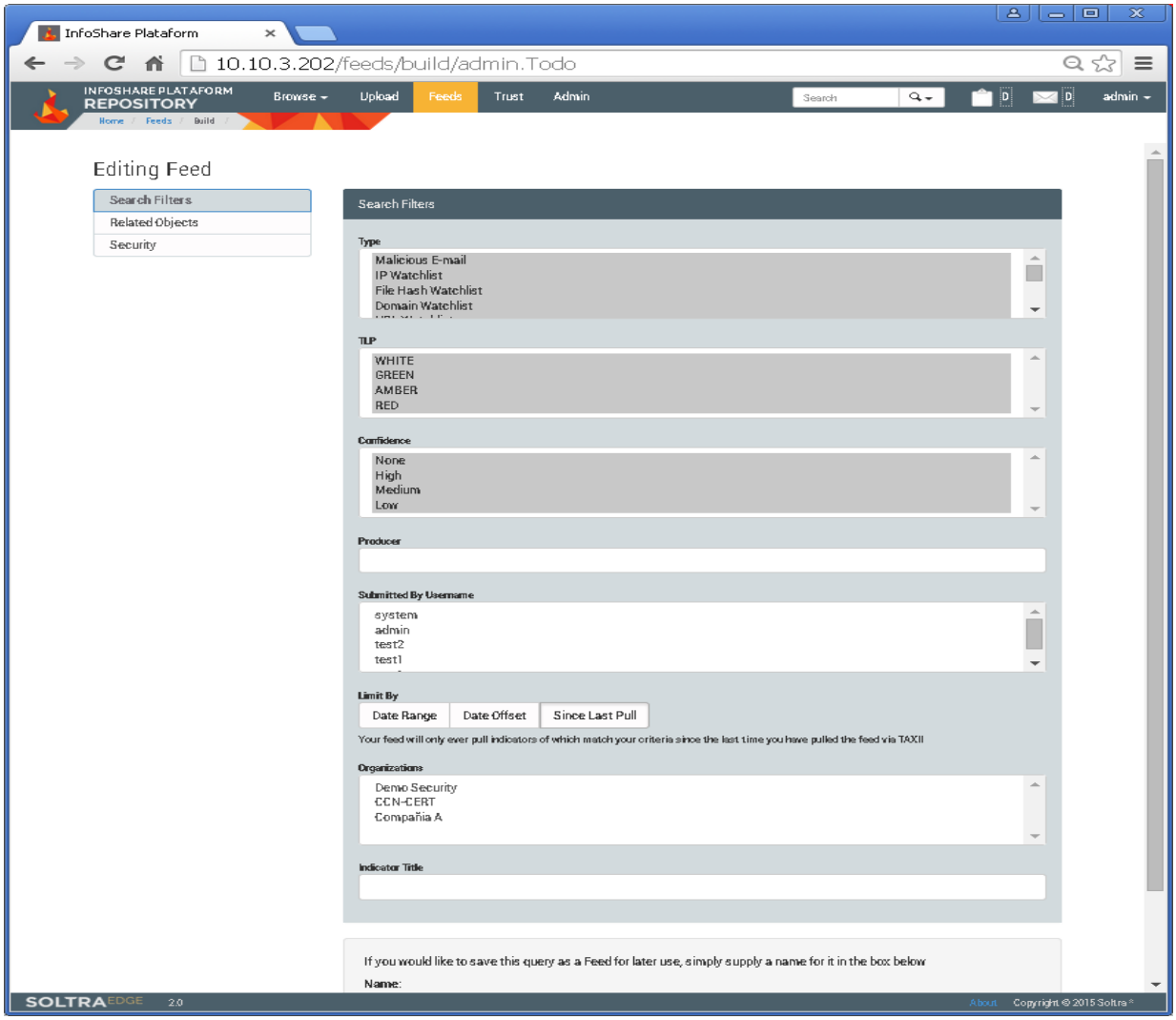


Figura 21 Configuración de los criterios de selección de objetos a publicar en el hilo

– **Crear, usuarios y organizaciones usuarias del sistema así como grupos de confianza más específicos.**

Esta granularidad permite refinar las comunidades o grupos de confianza dentro de la propia aplicación para crear distintos niveles de visibilidad de la información.

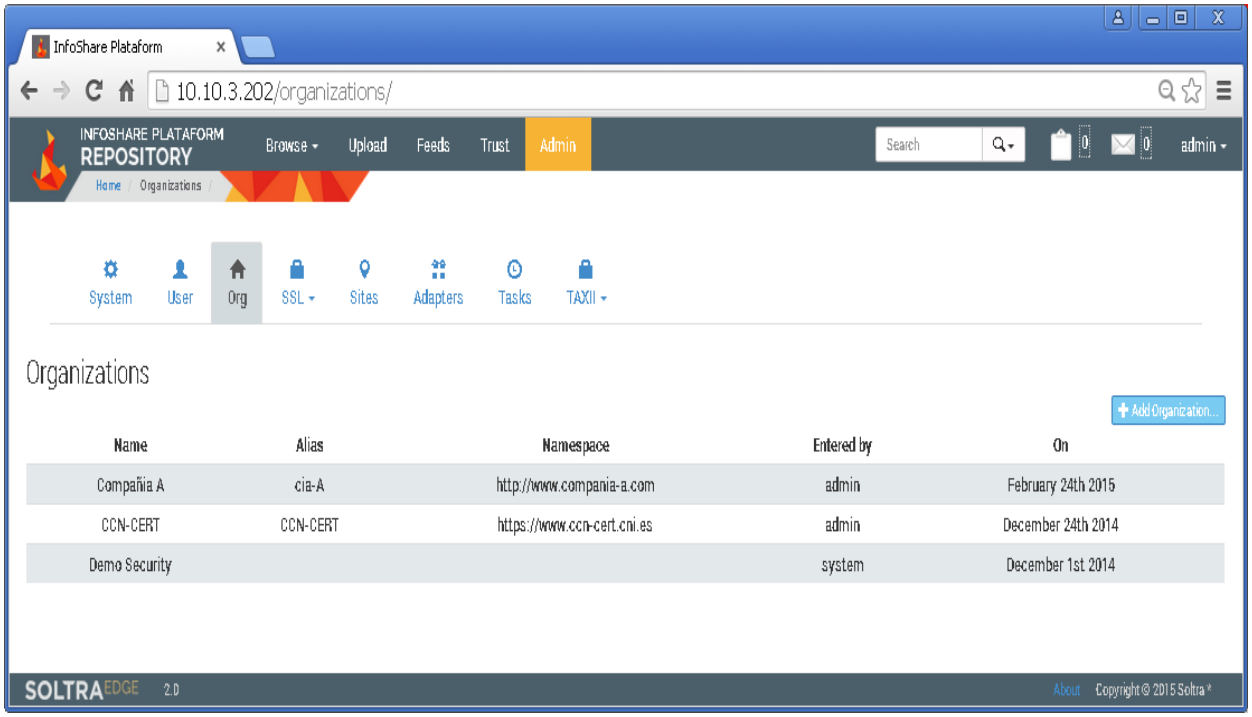


Figura 22 Administración de las organizaciones registradas en el sistema

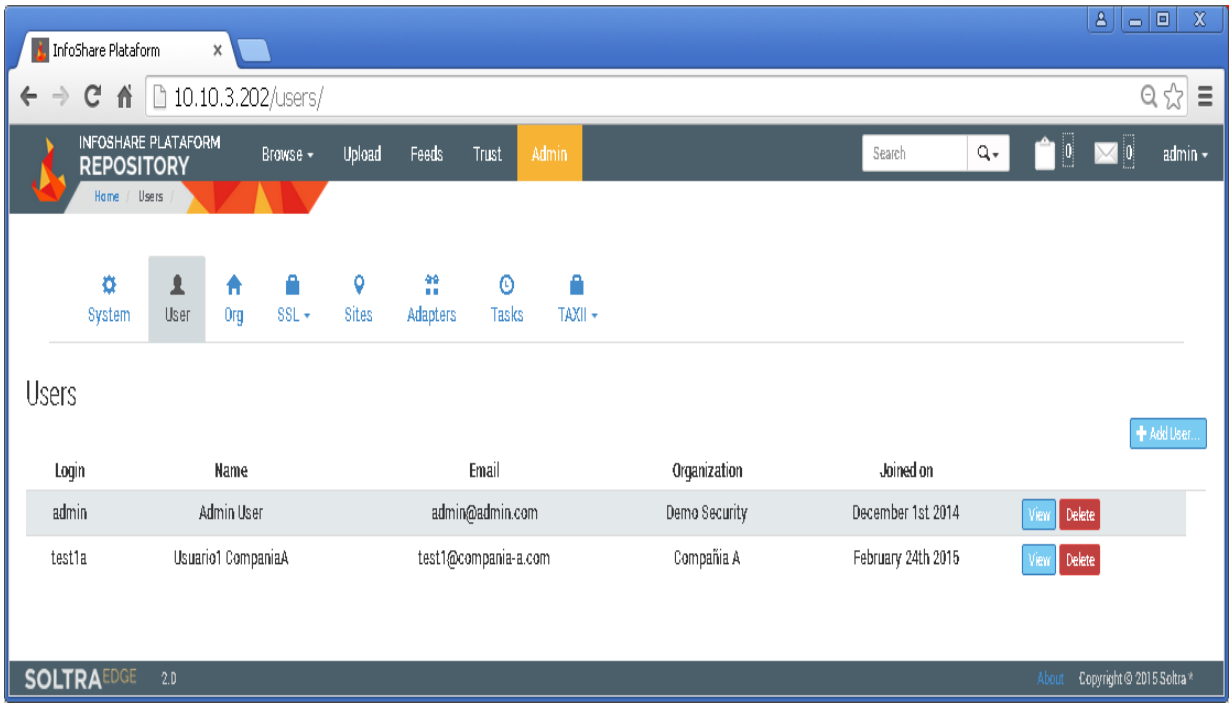


Figura 23 Administración de los usuarios del sistema (adscritos a una organización)

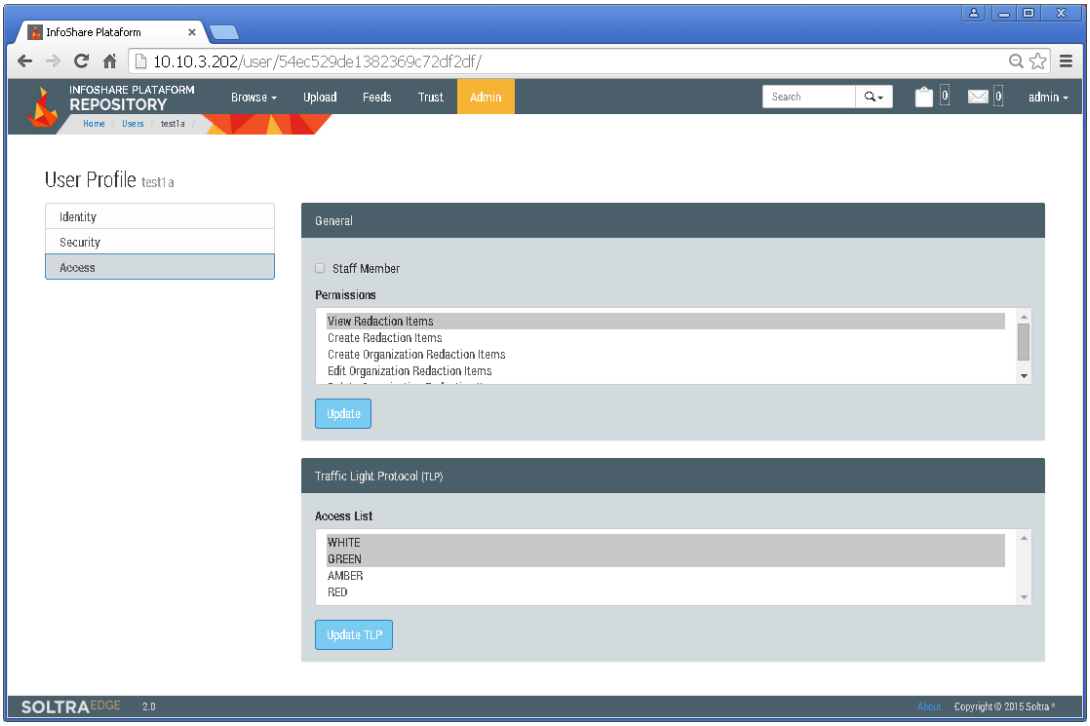


Figura 24 Configuración de permisos para un usuario

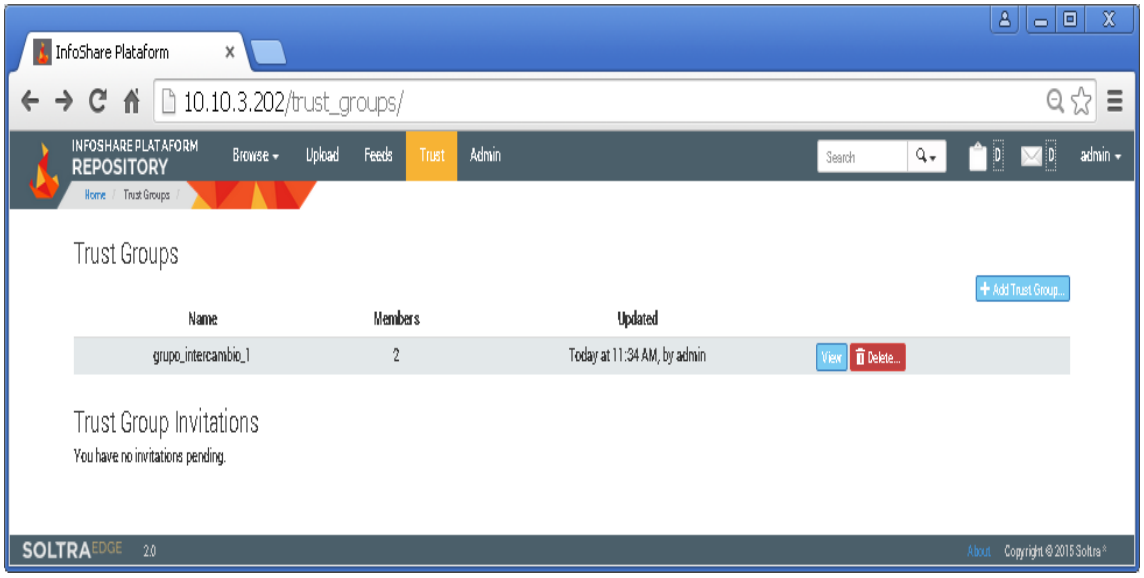


Figura 25 Creación de un grupo de confianza

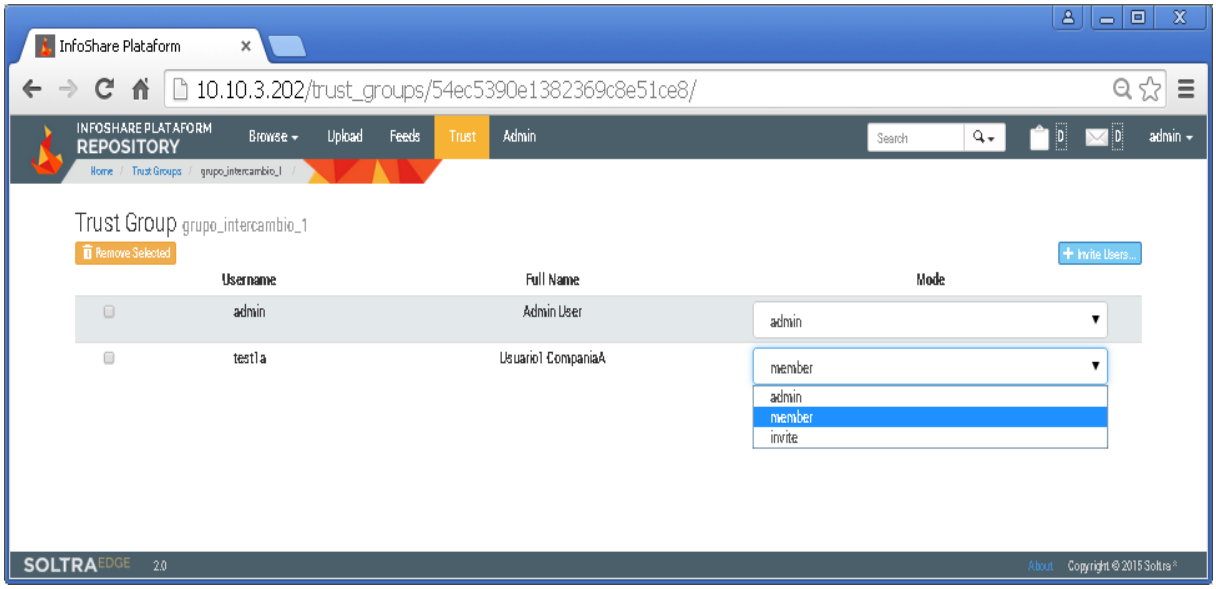


Figura 26 Administración del grupo de confianza
(se puede emplear invitaciones o asignar directamente la pertenencia)

– **Un repositorio centralizado de elementos de ciberinteligencia organizados y descritos empleando los conceptos y el lenguaje STIX así como un editor de los mismos.**

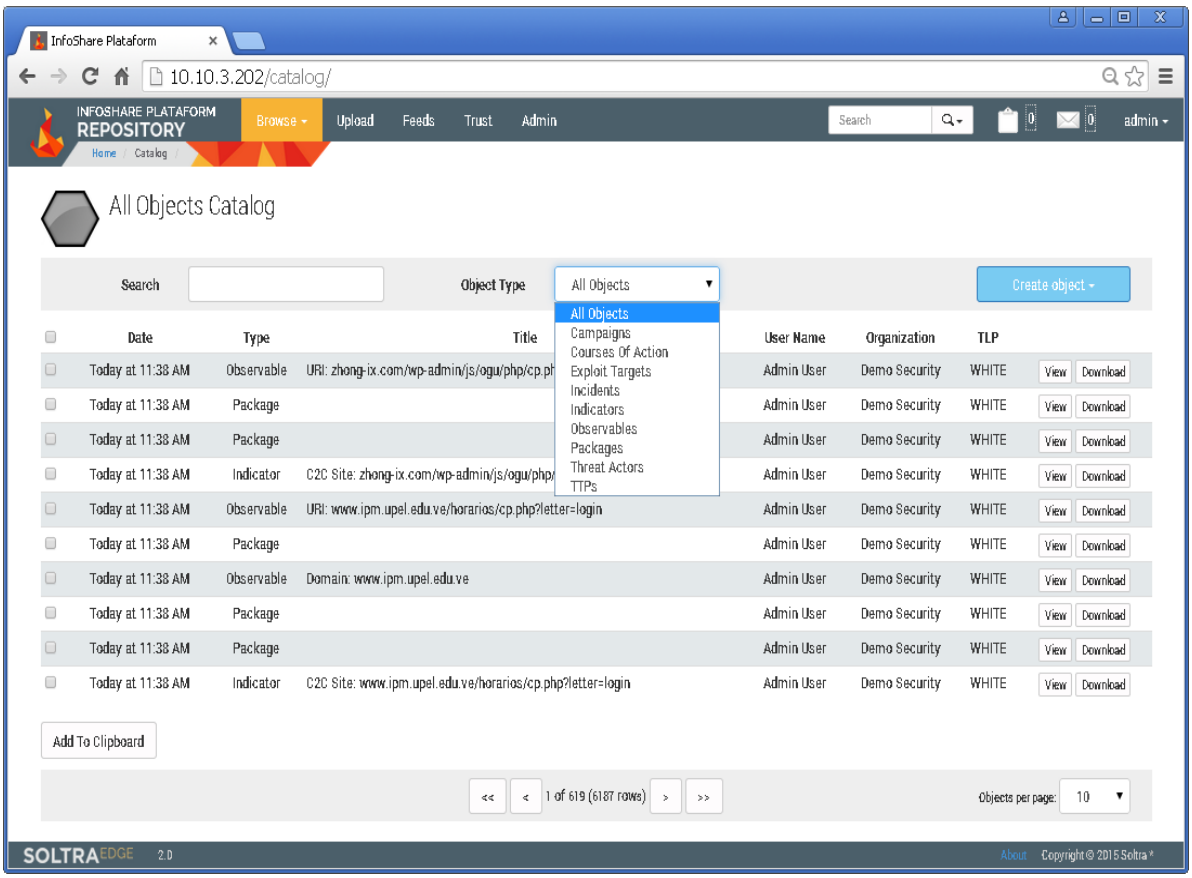


Figura 27 Vista general de los distintos tipos de objetos disponibles y el listado de objetos en el sistema

Figura 28 Detalle de un objeto disponible en el sistema de tipo “Indicador” y obtenido de una fuente externa

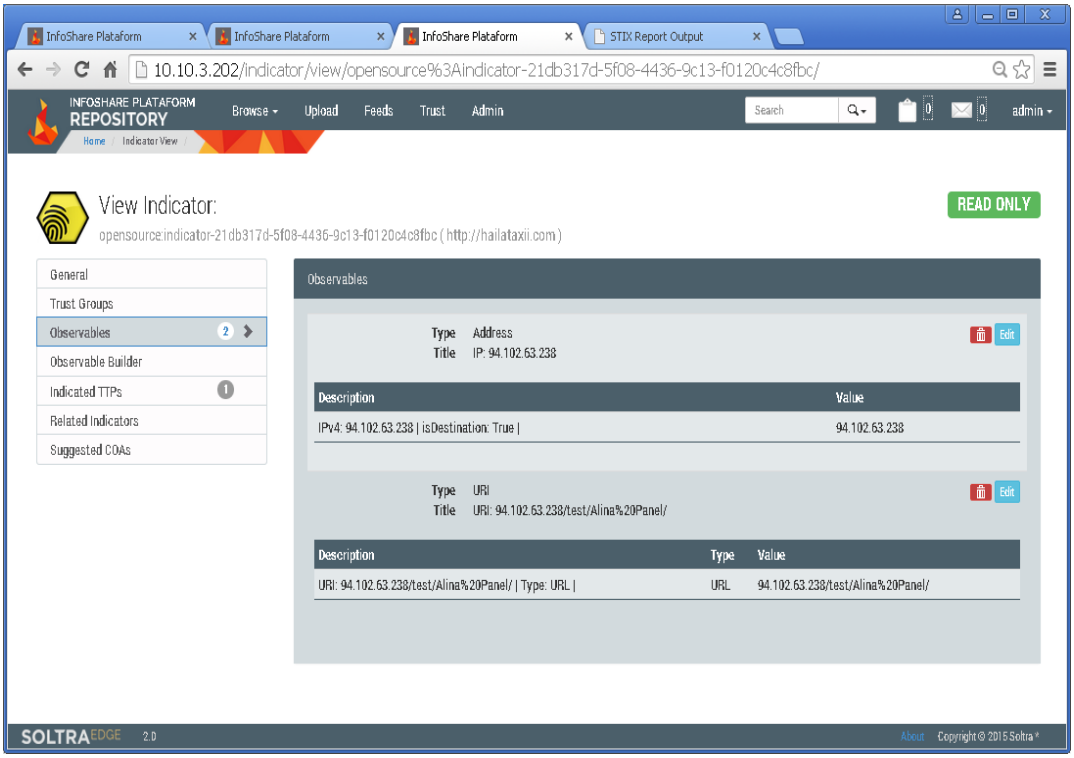


Figura 29 Vista del objeto en el editor (sólo lectura)

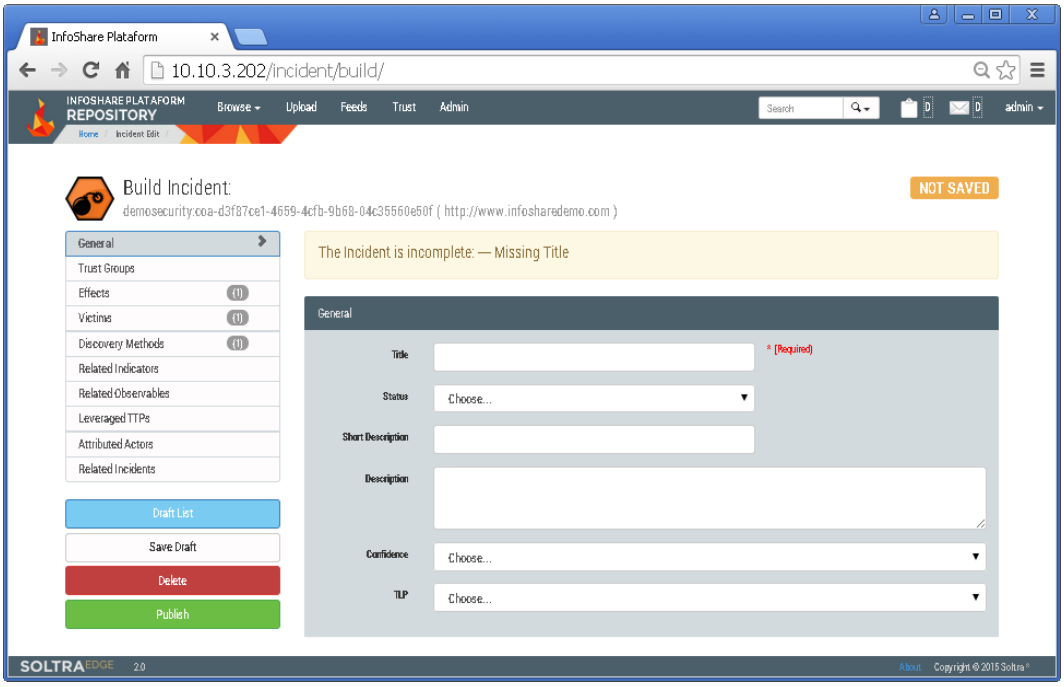


Figura 30 Editor de objetos. En este ejemplo de tipo “Incidente”
Se puede relacionar con otros objetos según el tipo que se edita

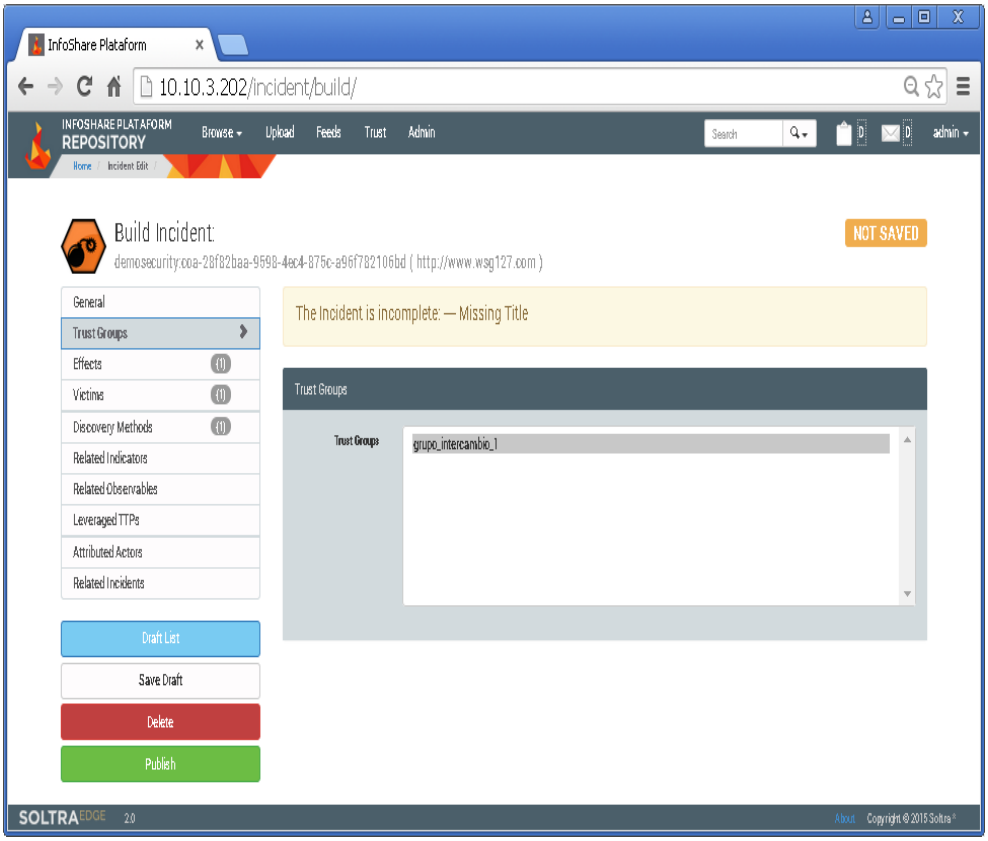


Figura 31 Editor de objetos.
Limitación de visibilidad a un determinado grupo de confianza

4. OTROS SISTEMAS PARA LA GESTIÓN DE CIBERINTELIGENCIA

Adicionalmente a los sistemas MISP y Soltra Edge presentados anteriormente, la comunidad internacional de ciberseguridad está desarrollando distintas herramientas relacionadas con generación, manejo y compartición de ciberinteligencia.

Algunas iniciativas recientes, a fecha de realización de esta guía, han contemplado la modelización de la ciberinteligencia empleando STIX como modelo de objetos y/o formatos de importación y exportación de la información.

4.1 CRITS

MITRE ha promocionado el desarrollo de una plataforma para el manejo de información de ciberseguridad denominada CRITS (Collective Research Into ThreatS)[49].

El sistema permite importar y exportar ciberinteligencia en formato STIX, sin embargo no es un sistema conforme con TAXII puesto que no de manera nativa no lo soporte y se requiere una modificación e incorporación de otros componentes de software.

[49] https://crits.github.io/

4.2 MANTIS

La compañía Siemens ha promovido la creación de MANTIS (Model-based Analysis of Threat Intelligence Sources)[50] que es un simple prototipo o prueba de concepto de una herramienta para el manejo información sobre ciberamenazas conforme con distintos estándares, principalmente STIX, CyBOX y IODEF (RFC 5050).

No es un sistema utilizable en un entorno operativo, y en lo relativo al objeto de esta guía únicamente implementa la descripción de la ciberinteligencia en un formato que permite la importación y exportación a paquetes STIX.

[50] http://django-mantis.readthedocs.org/en/latest/

ANEXO C CASO DE USO CON REYES

En este anexo se mostrará un caso práctico de uso con la herramienta REYES (REpositorio común Y EStructurado de amenazas y código dañino). En él, el lector podrá seguir las operaciones básicas – como importar y exportar inteligencia -, todo ello basado en un ataque conocido.

Para la realización de este ejemplo se ha utilizado un incidente real, llamado APT 28, descubierto por la empresa FireEye.

1. CREAR UN EVENTO

A la hora de poder trabajar con este incidente, lo primero que se ha de crear es un evento asociado al mismo. REYES soporta actualmente la importación de datos basados en OpenIOC, o a través del portal ThreatConnect. Este caso de uso se basará en la importación de datos a través de OpenIOC.

Para poder importar un fichero de tipo IOC, es necesario generar un evento en la plataforma REYES. Para hacerlo, tan solo es necesario pulsar en el botón **Add Event**, tal y como se muestra en la siguiente figura:

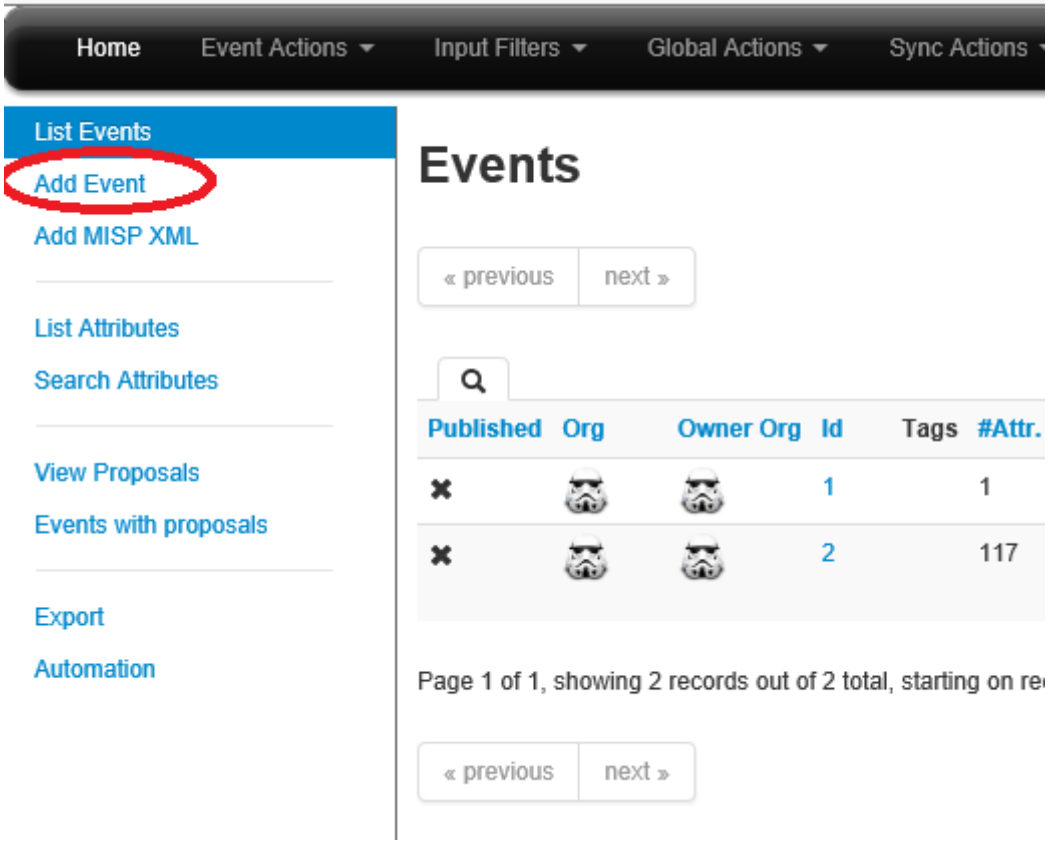


Figura 32. Creación de evento en REYES

Una vez generado el evento en REYES, tan sólo hay que rellenar el mismo con información de valor, como por ejemplo el nivel de amenaza o el tipo de análisis.

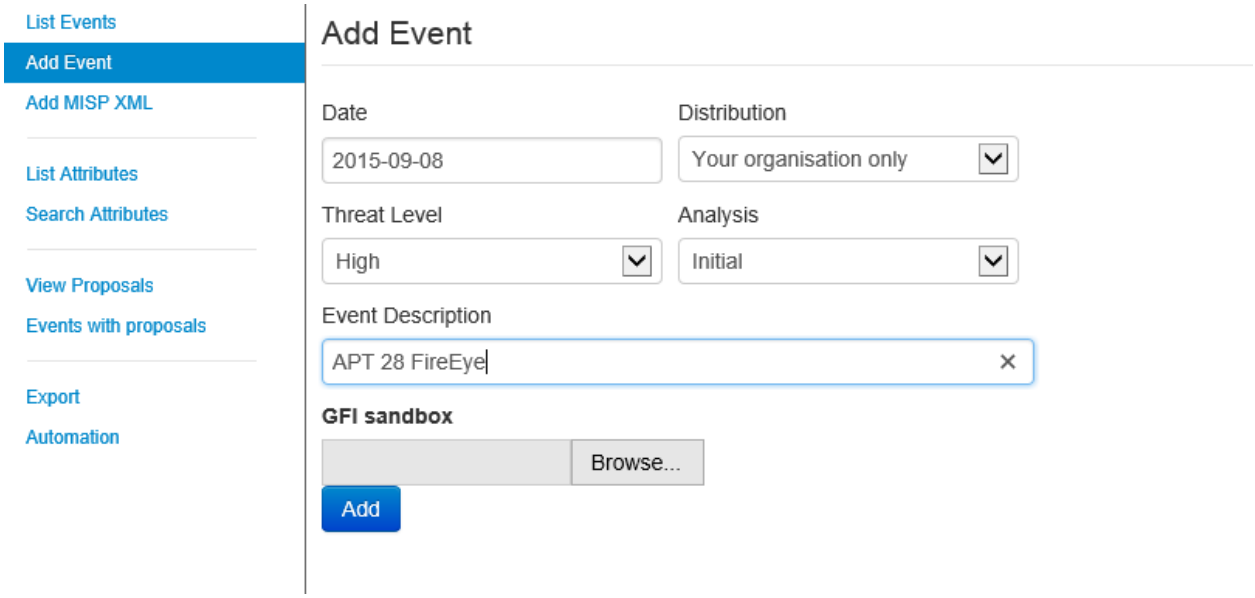


Figura 33. Creación de evento en REYES

2. IMPORTAR INFORMACIÓN

Una vez generado el evento, se hace necesario alimentar el mismo con información sobre el incidente. Esta información puede venir en forma de OpenIOC o a través del portal de ThreatConnect. Debido a que en la información existente sobre el incidente APT 28 vienen generados ya los **ficheros IOC**, se utilizarán estos para alimentar el evento en REYES. Para importar ficheros de tipo IOC, se deberá hacer pulsando en el enlace con leyenda **Populate from OpenIOC**, tal y como se muestra en la siguiente figura:

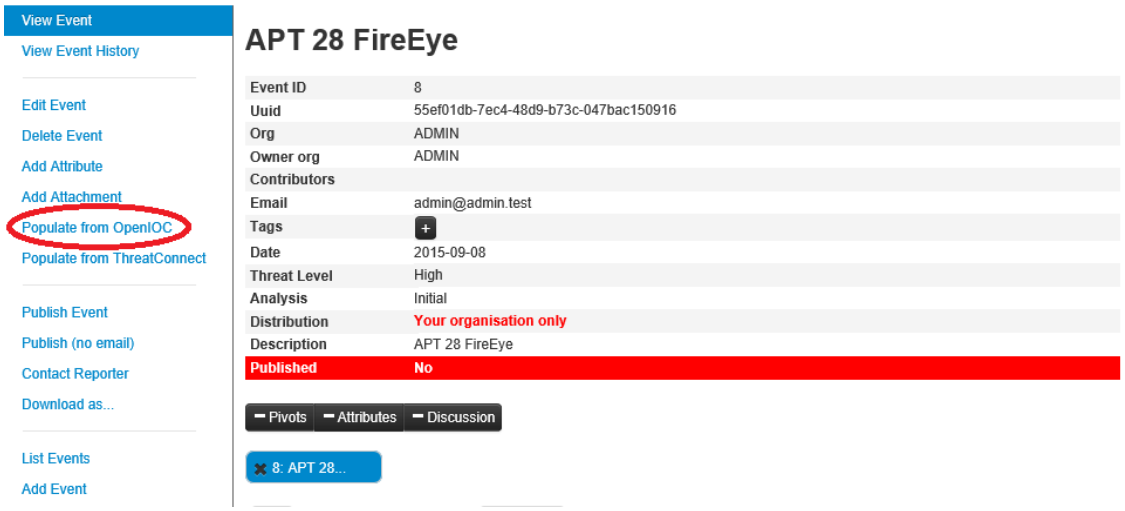


Figura 34. Importación de OpenIOC en REYES

Una vez subido el fichero de tipo IOC, y si todo ha ido correctamente, se mostrará una pantalla a modo resumen, indicando aquellos indicadores que se han subido correctamente.

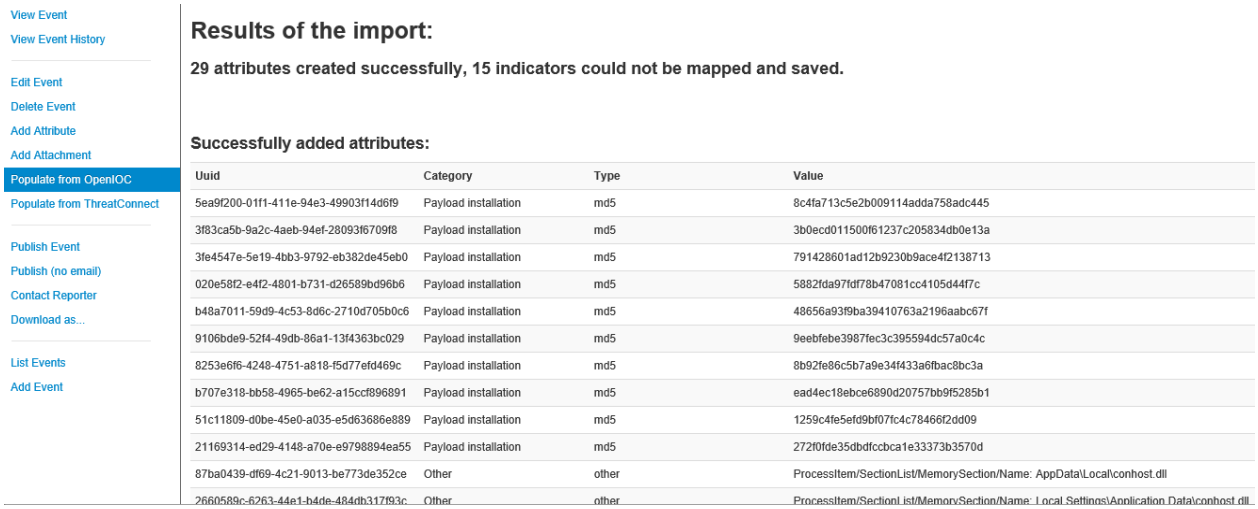


Figura 35. Resultados de la importación

3. PUBLICAR Y EXPORTAR UN EVENTO

En el momento en que estos eventos se encuentren con información relativa al caso – como **nombres de dominio o direcciones ip maliciosas** – se hace posible el poder trabajar con ellos mediante la exportación en múltiples formatos de uso. Algunos de ellos son los siguientes:

- Exportación de resultados en reglas SNORT
- Exportación de resultados en reglas de SURICATA
- Exportación de eventos en XML o JSON
- Exportación de dominios o direcciones IP en múltiples formatos

No obstante, para poder trabajar con la exportación es necesario publicar el evento. **La publicación de un evento activará las opciones de exportación en múltiples formatos.**

En función de los cambios realizados en el evento, es posible publicar el mismo y enviar un mensaje de alerta, o publicar el evento sin enviar el mensaje. Una vez decidido este paso se procederá a publicar el evento pulsando el botón Publish, tal y como aparece en la siguiente figura:

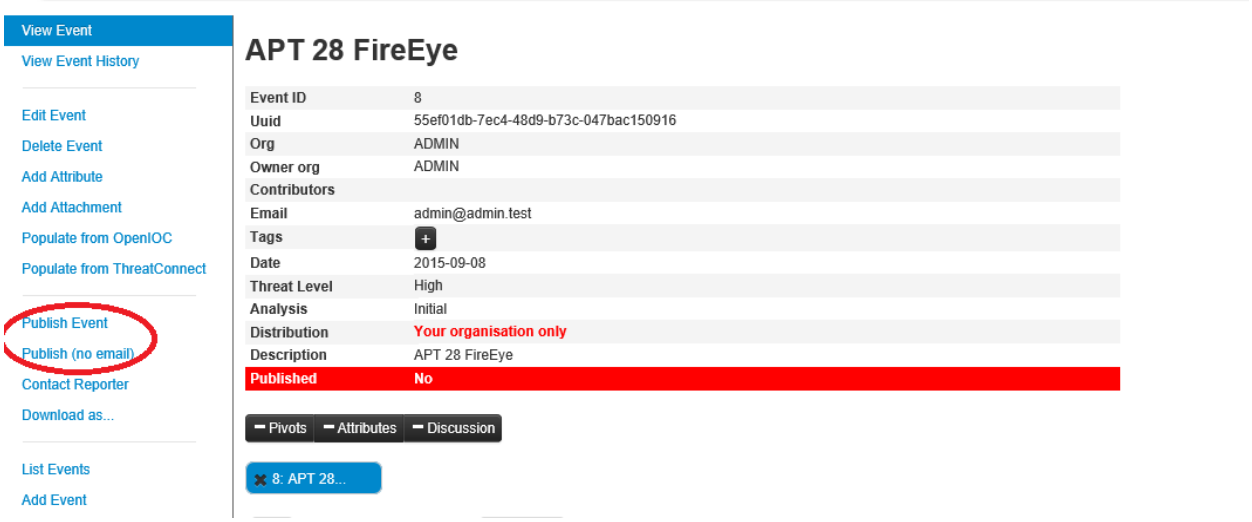


Figura 36. Publicación de evento en REYES

Si el evento se ha publicado correctamente, en la información general del mismo aparecerá como publicado, tal y como se muestra en la siguiente figura:

Figura 37. Evento publicado con éxito en REYES

4. FORMATOS DE EXPORTACIÓN

En el momento de publicación del mismo, REYES faculta al usuario la posibilidad de poder exportarlo en numerosos formatos.

Por ejemplo, si el usuario necesitase **exportar los nombres de dominio y direcciones IP a una zona de tipo RPZ (Response Policy Zone)**, con REYES puede realizarlo mediante el botón **Download as**, seguido del **formato RPZ**, tal y como se muestra en la siguiente figura:

Figura 38. Descarga de inteligencia en formato RPZ

Una vez seleccionado el formato RPZ, REYES transformará la inteligencia del evento en un formato compatible para poder ser introducido como una zona en un servidor DNS.

```
$TTL 1w;
@               SOA localhost. root.localhost (2015090800 2h 30m 30d 1h)
                NS localhost.

; The following list of IP addresses will timeout.
32.10.221.85.70.rpz-ip CNAME rpz-drop.

; The following hostnames will timeout.
adawareblock.com CNAME rpz-drop.
baltichost.org CNAME rpz-drop.
checkmalware.org CNAME rpz-drop.
kavkazcentr.info CNAME rpz-drop.
login-osce.org CNAME rpz-drop.
mail.g0v.pl CNAME rpz-drop.
malwarecheck.info CNAME rpz-drop.
n0vinite.com CNAME rpz-drop.
nato.nshq.in CNAME rpz-drop.
natoexhibitionff14.com CNAME rpz-drop.
novinitie.com CNAME rpz-drop.
poczta.mon.q0v.pl CNAME rpz-drop.
q0v.pl CNAME rpz-drop.
qov.hu.com CNAME rpz-drop.
rnil.am CNAME rpz-drop.
scanmalware.info CNAME rpz-drop.
smigroup-online.co.uk CNAME rpz-drop.
standartnevvs.com CNAME rpz-drop.
```

Figura 39. Transformación de inteligencia en formato RPZ

5. TRANSFORMACIÓN A FICHEROS DE TEXTO

Esta inteligencia puede ser también transformada en ficheros de texto plano y totalmente adaptable por el usuario, gracias a que REYES utiliza campos y atributos de tipo **NOMBRE: VALOR**. Este diseño permite que un usuario pueda descargarse sólo los campos que le interesen, obviando el resto.

Un ejemplo claro se obtiene por ejemplo a la hora de **alimentar una lista negra de un dispositivo cortafuegos o Firewall**, por ejemplo. Por regla general, este tipo de reglas trabajan con ficheros en texto plano que **sólo contienen direcciones IP o nombres de dominio.**

6. PETICIONES DE FICHEROS DE CAMPO ÚNICO

El formato que sigue REYES a la hora de realizar peticiones de campos únicos es el siguiente:

http://SERVIDORREYES/events/TIPO_FICHERO/download/<ID_EVENTO>/1/TAG/<CAMPO_RELACIÓN>/CAMPO

Si por ejemplo se desea descargar del evento 8 un fichero de tipo CSV sólo con direcciones IP, la URL resultante sería la siguiente:

http://SERVIDORREYES/events/csv/download/8/1/false/Network%20activity/ip-src

Si por el contrario también se desea descargar un fichero de tipo CSV sólo con los nombres de dominio descubiertos, se podría utilizar la siguiente URL:

http://SERVIDORREYES/events/csv/download/8/1/false/Network%20activity/hostname

ANEXO D. GLOSARIO

Término	Significado
AI	Asset Identification
APT	Advanced Persistent Threat (Amenaza Avanzada Persistente)
ARF	Asset Reporting Format
CAPEC	Common Attack Pattern Enumeration and Classification
CCE	Common configuration Enumeration
CCE	Common Configuration Enumeration
CCSS	Common Configuration Scoring System
CERT-EU	Computer Emergency Response Team. European Union
CIRCL	Computer Incident Response Center Luxemburg
COS	Centro de Operaciones de Seguridad
CPE	Common Platform Enumeration
CRITS	Collective Research Into ThreatS
CSIRT	Computer Security Incident Response Team
CSV	Comma Separated Values
CVE	Common Vulnerability Enumeration
CVRF	Common Vulnerability Reporting Framework
CVSS	Common Vulnerability Scoring System
CWE	Common weakness enumeration
CyBOX	Cyber Observable eXpression
DHS	Department of Homeland Security
DLL	Dynamic Link Library
DTCC	The Depository Trust & Clearing Corporation
FAT	File Allocation Table
FIRST	Forum for Incident Response and Security Terms
FQDN	Fully Qualified Domain Name
FS-ISAC	Financial Services Information Sharing and Analysis Center
HASH	Función resumen
HTML	Hyper Text Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IDS	Intrusion Detection System
IDT	Interrupt Description Table
IOC	Indicator of Compromise (Indicador de Compromiso), o fichero que contiene la definición de indicadores de compromiso mediante XML
IP	Internet Protocol
IPFIX	Internet Protocol Flow Information Export
IRP	Input/Output Request Packets
ISO	International Organization for Standardization
ITU	International Telecommunication Union
JSON	Java Script Object Notation

MAEC	Malware Attribute Enumeration and Chracterization
MANTIS	Model-based Analysis of Threat Intelligence Sources
MIR	Mandiant Incident Response
MISP	Malware Information Sharing Platform
MRI	Malware Risk Index (Indicador de Riesgo de Código dañino)
MUTEX	MUTual EXclusion object, mecanismo de programación para garantizar que sólo un proceso accede a un determinado recurso.
NCIRC	Nato Computer Incident Response Capability
NDIS	Network Driver Interface Specification
NIST	National Institute of Standards and Technology
NTFS	New Technology File System
OpenIOC	Open Indicator of Compromise. Indicadores de Compromiso de código abierto
OSVDB	Open Source Vulnerability DataBase
OVAL	Open Vulnerability and Assessment Language
P2P	Peer To Peer
RAT	Remote Administration Tool
REST	Representational State Transfer
REYES	REpositorio común Y EStructurado de amenazas y código dañino
RPZ	Response Policy Zone
RSS	Really Simple Syndication.Formato XML para compartir contenidos en la web
SCAP	Security Content Automation Protocol
SCAP	Security Content Automation Protocol
SIEM	Security Information and Event Management
Snort	Es un sistema de prevención de intrusiones (IPS) de código libre
SOC	Security Operations Center
SSDT	System Service Descriptor Table
STIX	Structured Threat Information eXpresion
TAXII	Trusted Automated eXchange of Indicator Information
TCPIP	Transmision Control Protocol Internet Protocol
TLP	Traffic Light Protocol
TMH	TAXII Message Handler
TMSAD	Trust Model for Security Automation Data
TTA	TAXII Transfer Agent
TTP	Tactics, Technics and Procedures. Tácticas, Técnicas y Procedimientos
URL	Uniform Resource Locator
US-CERT	United States -Computer Emergency Response Team
XCCDF	Extensible Configuration Checklist Description Format
XML	eXtensible Markup Language
XSD	XML Schema Definition
YARA	Herramienta de clasificación e identificación de código dañino