Tilsor S.A.

Universidad de la República

Facultad de Ingeniería

Tesis de grado

---

# Advanced Threats Information Sharing and Collaboration

---

*Autor:*
Julio Saráchaga

*Supervisor:*
Dr. Gustavo Betarte

*Contraparte del cliente:*
Ing. Fernanda Molina

*Supervisor alterno:*
Ing. Marcelo Rodríguez

2 de junio de 2013

# Índice general

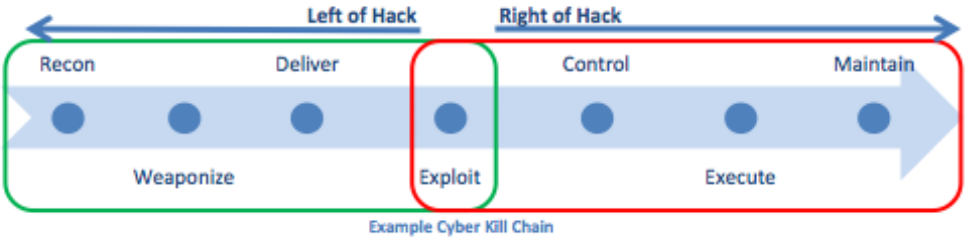
# Capítulo 1

# Introducción

## 1.1. Introducción

Históricamente, se ha visto un aumento en la sofisticación, velocidad, impacto y cantidad de los ataques informáticos. Se ha vuelto necesario que las estrategias de defensa se adapten a los nuevos actores y ataques. Para responder a esto, las organizaciones han tenido que recurrir al intercambio de información referente a las amenazas con el fin de tener una visión más amplia de las actividades de los adversarios y así ayudar a administrar sus recursos de forma de obtener el mejor resultado posible de sus defensas. Hoy en día el compartir información es realizado de forma manual lo cual es una tarea que consume una cantidad de tiempo considerable o por medio de procesos automatizados con grandes limitaciones los cuales se realizan dentro de comunidades especificas. La capacidad de compartir información completa de forma automática con un gran número de comunidades no existe en la actualidad. Hay múltiples métodos para el intercambio de información y estos juegan un rol significante en los tipos, volúmenes y naturaleza de la información compartida con la comunidad. Algunos de estos medios de intercambio limitan el tipo de contenido que es compartido de forma sencilla mientras que otros promueven ciertos tipos de intercambio. De todas formas, la mayoría de estos métodos no permiten el consumo de información de amenazas de forma automática, esto hace que rutinariamente las organizaciones deban tomar dicha información y sintetizarla en sus bases de datos locales. Si bien los métodos utilizados en la actualidad han ayudado a mejorar las capacidades defensivas de numerosas organizaciones, estas no han logrado explotar su máximo potencial. Por ello es que actualmente existen varios esfuerzos para generar arquitecturas abiertas, estándar basadas en indicadores e información de incidentes. La realidad es que ninguno de estos ha podido convertirse en un estándar para el intercambio entre comunidades. Las aproximaciones tradicionales de seguridad se

focalizan en entender y registrar vulnerabilidades, debilidades y configuraciones necesarias pero insuficientes. Para defenderse las organizaciones tienen estrategias de defensa que buscan predominantemente bloquear los ataques y arreglar las vulnerabilidades, esta estrategia se basa en alertas. Si bien puede ser efectiva contra algunas amenazas no logra detener ataques avanzados o proveer información sobre las actividades de un atacante luego de que la red fue penetrada. Una estrategia mas adecuada es basarse en *cyber kill-chain*, en esta estrategia se busca descomponer las fases de un ataque con la finalidad de obtener una mejor comprensión del ataque y el atacante así como mejorar las posibilidades de defensa.



Example Cyber Kill Chain

Los primeros pasos de esta estrategia representan una oportunidad para detectar y mitigar las amenazas de forma proactiva antes de que el adversario realice un acceso no autorizado en los sistemas de la organización. En los pasos posteriores es donde se realiza la detección, respuesta y aseguramiento de los activos más importantes. Al entender al adversario los defensores tienen una mejor oportunidad para descubrir y responder al ataque. Un entendimiento de la amenaza permite la realización de decisiones mas efectivas, priorizando los recursos para así lograr tener una ventaja ante el adversario. El efecto de las defensas en base a inteligencia es una mejor postura respecto respecto a las respuestas dado que los atacantes ajustan sus operaciones basandose en el éxito o falla de sus intentos. En un modelo como el presentado los intentos que realiza un adversario pueden ser reconocidos, logrando que los defensores tengan la posibilidad de ajustar sus tácticas para una mejor respuesta que genere que el adversario le sea mas difícil alcanzar sus objetivos. Compartir información sobre amenazas con socios y comunidades de confianza le permite a las organizaciones tener un conjunto de información relevante para tener una identificación precisa de una amenaza. Por el medio de este intercambio, cada ente puede alcanzar un nivel mas alto de entendimiento del panorama de las amenazas, no solamente de forma abstracta sino que también de evidencias especificas que indiquen la presencia del atacante. Actualmente se busca que las defensas anticipen y mitiguen las amenazas antes de que sean más difíciles de encontrar y erradicar utilizando los métodos tradicionales de detección y respuesta. Para poder realizar esto es necesario que se realice una actividad de cyber inteligencia recolectando información referente a ataques. Con

esta información los analistas pueden agrupar patrones de actividades similares, atribuir actividades a ciertos actores, identificar e implementar estrategias de mitigación de forma rápida y anticiparse al lanzamiento de ataques similares en el futuro. Para aprovechar de forma más adecuada los beneficios de la cyber inteligencia, las organizaciones deben compartir la información recolectada (incluyendo sus estrategias de defensa) con socios de su confianza. De esta forma se obtiene una imagen más completa de las actividades del adversario y de las acciones defensivas que se deben realizar. Por medio del análisis del comportamiento de los adversarios en distintos objetivos y en un periodo de tiempo adecuado, los defensores son capaces de identificar un conjunto importante de indicadores, tácticas, técnicas y procedimientos (TTPs). De esta forma se obtiene información de los objetivos y las estrategias lo cual permite al defensor predecir el comportamiento del ataque y generar defensas dinámicas. Dada la forma y complejidad con la que evoluciona el panorama de las amenazas, la velocidad con la cual ocurren los eventos, y la basta cantidad de datos que se deberian intercambiar, es necesario establecer una forma automática para ayudar a los analistas y tomadores de decisión a tomar acciones defensivas para que esta aproximación sea efectiva. La automatización requiere de información de calidad, dado que las arquitecturas son heterogéneas con distintos productos y sistemas, es necesario la estandarización con representaciones estructuradas de información y un mejor aprovechamiento de la información sin saber de antemano quien va a proveer que información. Dicha información debe ser leíble por un humano y pareseable por una máquina. Estos requerimientos tienen varias justificaciones, primer que nada, un analista podría realizar un análisis que es inapropiado para ser automatizado o que sea focalizados en tomas de decisiones por parte de personas. También podría ser de interés que un analista tenga conocimiento de la situación actual. Además podría ser un buen medio para evaluar la fidelidad de las fuentes y los métodos utilizados para producir la información. Dados todos los factores presentados anteriormente, es necesaria la existencia de representaciones estructuradas de la información y que esta sea expresiva, flexible, extensible, automatisable y legible. Además se deben contar con medios para permitir el intercambio seguro y confiable de información entre distintas organizaciones.

# Capítulo 2

# IDMEF e IODEF

IDMEF e IODEF

## 2.1. IDMEF

IDMEF fue especificado como un protocolo experimental que no especifica ningún estándar. Sin embargo IODEF se basa en las especificaciones de las clases definidas en IDMEF. El propósito de IDMEF es definir formatos de datos y procedimientos de intercambio para compartir información de interés con sistemas de detección de intrusos y sistemas de respuesta con los sistemas de administración que podrían necesitar interactuar con estos. El RFC de IDMEF describe el modelo de datos para representar información tomada de los sistemas de intrusión y explica la razón de usar este modelo. IDMEF busca ser un formato que pueda ser utilizado por los IDSs para reportar alertas sobre eventos que parecen sospechosos. Se puede proveer interoperabilidad entre sistemas comerciales, open source y sistemas de investigación, permitir a los usuarios esta mezcla de sistemas ayuda a obtener una implementación óptima de sus sistemas. Se utiliza XML digital signature para proveer integridad, autenticación de los mensajes y autenticación de los servicios del firmante para datos de cualquier tipo, estos sean localizados en el XML que incluye la firma o en otro lugar. La responsabilidad para la integridad y autenticación de los mensajes es responsabilidad del protocolo de comunicación y no del formato de mensaje. Sin embargo en situaciones en que los mensajes IDMEF son intercambiados sobre protocolos poco seguros, o en casos en que las firmas digitales deben ser archivadas para uso posterior, la inclusión de firmas digitales en mensajes IDMEF debería ser realizada.

### 2.1.1. Modelo de datos de IDMEF

El modelo de datos de IDMEF es una representación orientada a objetos de los datos del alerta enviados a los administradores de los sistemas de intrusión. El modelo de datos presenta varios problemas referentes a la representación de los datos:

- La información de alertas es mayormente heterogénea. Algunas alertas son definidas con muy poca información, como orígenes, destinos, nombre u hora del evento. Otras alertas proveen mucha mas información, como puertos de servicios, procesos, información de usuarios, etc. El modelo de datos que debe representar dicha información debe ser flexible para adaptarse a las distintas necesidades. Un modelo orientado a objetos es extensible por medio de agregación y sub clases. Si una implementación del modelo de datos extiende con una nueva clase, por medio de agregación o subclases, una implementación que no entienda estas extensiones podrá seguir entendiendo el subconjunto de información que esta definido en el modelo. Estas dos formas de extender el modelo permiten que se mantenga la consistencia del modelo.

- Los IDS son diferentes, algunos analizadores detectan ataques analizando el trafico en la red, otros utilizando los logs de sistemas operativos o aplicaciones que auditan información. Alertas para el mismo ataque enviadas por analizadores con diferentes fuentes de información, no contendran los mismos datos. El modelo de datos define clases que soportan las diferencias en las fuentes de los datos. En particular, las nociones de fuente y objetivo para el alerta son representadas por una combinación de nodo, procesos, servicio y clase de usuario.

- Las capacidades de los analizadores son diferentes. Por ello el modelo de datos debe permitir la conversión de formatos utilizados por herramientas distintas a IDSs con el propósito de mayor procesamiento de la información.

- Los ambientes operacionales son diferentes. Dependiendo en el tipo de red o sistemas operativos utilizados, los ataques serán observados y reportados con diferentes características. El modelo de datos se adapta a estas diferencias.

- Los instrumentos comerciales persiguen objetivos diferentes. Por varias razones, estos desean entregar mas o menos información sobre ciertos tipos de ataques. El modelo orientado a objetos permite la flexibilidad necesaria preservando la integridad del modelo.

### 2.1.2. El diseño del modelo de datos

El modelo de datos fue diseñado para proveer una representación estándar de las alertas de una manera que la información no se ambigua. Además busca permitir describir la relación entre alertas simples y complejas.

#### 2.1.2.1. Representación de eventos

El objetivo del modelo de datos es proveer una representación estándar de la información que el analizador de un sistema de intrusión reporta cuando detecta la ocurrencia de eventos inusuales. Estas alertas pueden ser simples o complejas dependiendo de las capacidades del analizador que la creo.

#### 2.1.2.2. Enfocada al contenido

El diseño del modelo de datos es enfocado al contenido. Lo cual significa que los nuevos objetos son introducidos para referenciar a contenido adicional. Esto es importante debido a que la tarea de clasificar y nombrar vulnerabilidades en computados es difícil y sumamente subjetiva. El modelo de datos no debe ser ambiguo, esto significa que mientras se permite que los analizadores sean mas o menos precisos entre ellos, no se debe permitir que estos produzcan información contradictoria en dos alertas describiendo el mismo evento. De todas formas, siempre es posible insertar toda la información ïnteresante"de un evento en campos de extensión de la alerta en lugar de a los campos a los que estos pertenecen, sin embargo, dichas practicas reducen la interoperabilidad y deberian ser evitadas en lo posible.

#### 2.1.2.3. Relación entre alertas

IDMEF busca cubrir todo el rango de alertas posibles, desde las simples a las más complejas. Para esto el modelo de datos debe proveer una forma de representar alertas complejas que agregan muchas alertas simples y que se permitan identificar dichas alertas simples en el contenido de la alerta compleja.

## 2.2. IODEF

Las organizaciones deben colaborar entre ellas para mitigar las actividades maliciosas que atacan sus redes así como para ganar conocimiento de posibles amenazas. Esta coordinación puede requerir coordinación con ISPs, sitios remotos o intercambiar datos con socios. IODEF son las siglas para Incident Object Description Exchange Format, este define una representación de datos que provee un framework para el intercambio de información entre CSIRTs, dicho tipo de información es intercambiado comúnmente por CSIRTs y es referente a incidentes de seguridad. IODEF provee una representación en XML para transportar información de incidentes entre dominios administrativos entre pares que tienen una responsabilidad operacional de remediar o de analizar y establecer advertencias en un dominio definido. El modelo de datos provisto en IODEF codifica la información referente a hosts, redes y servicios corriendo en estos sistemas; metedologia de ataques y evidencia forense asociada; impacto de la actividad realizada; aproximaciones limitadas para documentar el flujo. El objetivo primordial de IODEF es mejorar las capacidades operacionales de los CSIRTs. La adopción por parte de la comunidad provee una habilidad mejorada para resolver los incidentes y transmitir el contexto simplificando la colaboración e intercambio de datos. El formato estructurado provisto por IODEF permite:

- Incrementar la automatización en el procesamiento de los datos, ya que los recursos de los analistas de seguridad de parsear documentos se verá reducido.
- Bajar el esfuerzo necesario para normalizar datos similares de diferentes fuentes.
- Un formato común con el cual construir herramientas interoperables para el manejo de incidentes y análisis subsecuente, específicamente cuando los datos provienen de dominios distintos.

La coordinación entre CSIRTs no es un problema estrictamente técnico. Hay muchas consideraciones: procedimientos, confianza, legales, las cuales pueden ocasionar que las organizaciones intercambien información. IODEF no busca evadir dichas consideraciones, sin embargo, las implementaciones operacionales de IODEF deben considerar este contexto.

### 2.2.1. Modelo de datos de IODEF

A la hora de diseñar IODEF se realizaron ciertas consideraciones de diseño

- El modelo de datos sirve como formato de transporte. Por ello, su representación especifica no es optima para almacenamiento en disco, archivamiento a largo plazo o procesamiento en memoria.
- Por medio de la implementación no se busca establecer un consenso respecto a la definición de un incidente. Se busca en su lugar un entendimiento amplio que sea lo suficientemente flexible como para abarcar la mayoría de las operaciones.
- Describir un incidente para todas las definiciones requeriría un modelo de datos extremadamente complejo. Por ello, IODEF solo busca dar un marco para transmitir información de incidentes comúnmente intercambiada. Se asegura un mecanismo amplio para ser extendido para soportar información propia de la organización, y técnicas para referenciar información mantenida por fuera del modelo de datos.
- El dominio del análisis de seguridad no esta totalmente estandarizado y debe basarse en descripciones textuales libres. IODEF busca conseguir un balance entre el contenido libre, pero permitiendo el procesamiento automático de la información de los incidentes.
- IODEF es solo una de las representaciones que han sido estandarizadas. El modelo de datos de IDMEF influencio el diseño de IODEF.

### 2.2.2. Implementaciones de IODEF

Las implementaciones del protocolo se especifican como un esquema XML. Implementar IODEF en XML provee varias ventajas. Que sea extensible lo hace ideal para especificar codificación de datos que soporta varias codificaciones de caracteres. Es mas simple la manipulación debido a la presencia de varias tecnologías para ello. Aunque fundamentalmente XML es una representación de texto, lo cual lo hace ineficiente cuando se deben embeber datos binarios o grandes volúmenes de datos deben ser intercambiados.

### 2.2.3. Internacionalización

Internacionalización y localización son de interés para IODEF, dado que solo por medio de colaboración (a menudo con barreras idiomáticas) son resueltos ciertos incidentes. IODEF soporta esto dependiendo de las construcciones de XML, y por medio de diseño explícito en el modelo de datos. Como IODEF es implementado como un esquema XML, este soporta las diferentes codificaciones de caracteres. Además, los documentos IODEF deben especificar el lenguaje en el cual sus contenidos son codificados.

### 2.2.4. Consideraciones de Seguridad

El modelo de datos de IODEF no introduce problemas de seguridad. Este solo define una representación simple para información de incidentes. Como los datos codificados por IODEF pueden ser considerados sensibles por las partes que los intercambian o por los descritos por los datos, se deben tomar precauciones para asegurar la confidencialidad durante el intercambio y el subsecuente procesamiento. El primero debe ser resguardado por un formato de mensaje, pero luego se deben tener consideraciones de seguridad por el sistema que procesa los datos, los almacena y archiva la documentación y la información derivada de estos. El contenido de un documento IODEF puede incluir un pedido de acción o un parser puede independientemente tener lógica para realizar cierta acción basandose en información que encuentra. Por esta razón, se debe tener cuidado de autenticar apropiadamente el beneficiario del documento y atribuir un nivel de confidencialidad apropiado a los datos antes de realizar la acción. El formato de mensaje subyacente y el protocolo utilizado para intercambiar datos provee una garantía de confidencialidad, integridad y autenticidad. El uso de protocolos de seguridad estandarizados es recomendado. Por ejemplo el uso de IODEF/RID. Con el fin de sugerir buenas practicas en el procesamiento y manejo de los datos codificados, IODEF permite a un emisor de documentos transmitir una política de privacidad utilizando un atributo de restricción. Las distintas instancias de este atributo permite a los distintos elementos del documento tener las mismas políticas. Esto sirve como una guía para el receptor, pero este podría decidir ignorarlo, este problema no es un reto técnico.

## 2.3. Protocolo RID

Real-time Inter-Network Defense (RID) es un método de comunicación entre redes para facilitar el intercambio de datos de incidentes y a su vez integrando mecanismos existentes de detección, seguimiento, identificación de fuentes y mitigación que aporta una solución al manejo de incidentes. Combinar estas capacidad en un sistema de comunicación provee una forma de alcanzar un nivel de seguridad en la red. Las políticas para manejar incidentes son recomendadas y pueden ser acordadas por un consorcio utilizando recomendaciones y consideraciones de seguridad. RID ha sido ampliamente utilizado en comunidades de investigación, pero no ha sido muy adoptado en otros sectores. RID fue desarrollado como un mecanismo de comunicación para facilitar la transferencia de información entre distintos proveedores de servicios de internet para trazar precisa y eficientemente el flujo que llevan paquetes nocivos a lo largo de la red. RID considera la información que necesitan varias implementaciones para seguir paquetes dentro de una red y los requerimientos de los proveedores de servicios de decidir si se permite trazar

el recorrido de un paquete o no. Los datos en RID son representados como documentos XML utilizando el formato de IODEF. De esta forma se simplifica la integración con otros aspectos del manejo de incidentes. RID busca proveer un método para comunicar la información relevante entre CSIRTs manteniendo la compatibilidad con varios sistemas de rastreo y respuesta. Para conservar la privacidad y tener un buen nivel de seguridad, los mensajes RID toman ventaja de los mecanismos provistos por XML. El esquema RID funciona como un mecanismo de transporte para soportar la comunicación de documentos IODEF para intercambiar y realizar un seguimiento de incidentes de seguridad. Los mensajes RID son encapsulados para el transporte, este procedimiento se define en el RFC 6046. La autenticación, integridad y autorización son el resultado de las capacidades de cada capa y son utilizadas para alcanzar un buen nivel de aseguramiento. Los mensajes RID tienen la intención de ser usados en el manejo coordinado de incidentes para localizar la fuente de un ataque y detener o mitigar sus efectos. Los tipos de ataque incluyen redes o sistemas que se vieron comprometidos, denegaciones de servicio o cualquier otro tipo de trafico malicioso en una red. RID es esencialmente un sistemas de mensaje para coordinar la detección de ataques, los mecanismos de rastreo, y el manejo de incidentes. Los CSIRTs tienen la posibilidad de reportar ataques que estén ocurriendo a otros CSIRTs o pedir información a estos de si también detectaron el ataque. Para esto se utiliza el *Report message* para indicar que un reporte a sucedido. Con un mensaje de *IncidentQuery* se le puede preguntar a otro CSIRT si este ha detectado el ataque. Los sistemas comprometidos pueden resultar de otros incidentes de seguridad como worms, troyanos o virus. Puede suceder que un incidente no sea reportado incluso cuando la dirección de origen del ataque sea valida y este disponible debido a que sea difícil realizar una acción para mitigar o detener un ataque. El manejar incidentes es una tarea difícil para un proveedor de internet o en algunos clientes debido al tamaño de la red o los recursos disponibles. RID provee el framework necesario para realizar la comunicación entre redes involucradas en el manejo, seguimiento y mitigación de incidentes de seguridad. Distintos tipos de mensajes son necesarios para facilitar el manejo de incidentes. Los mensajes que se incluyen son *Report*, *Incident Query TraceRequest*, *RequestAuthorization*, *Result* e *Investigation Request message*. El mensaje de *Report* es utilizado cuando se ingresa un incidente en un sistema RID y no se deben realizar más acciones. Un mensaje *Incident Request* es utilizado para pedir información de un incidente en particular. Un mensaje *Trace Request* es utilizado cuando la fuente del trafico puede estar oculta. En ese caso, cada proveedor de red que reciba uno de estos mensajes enviara uno a la red anterior en el camino del mensaje para obtener la fuente del trafico. Los mensajes *Request Authorization* y *Result* son utilizados para comunicar el estado y resultado de un mensaje *Trace Request* o *Investigation Request*. El mensaje *Investigation Request* solo considera los sistemas RID en el camino a la fuente del trafico y no el uso de las redes de los sistemas de seguimiento. Un mensaje enviado entre sistemas RID

para *Trace Request* o *Investigation Request* para detener trafico en una fuente por fuera de una red debería requerir la siguiente información:

- Suficiente información para permitir a los administradores de la red tomar una decisión sobre la importancia de seguir el seguimiento.
- El incidente o información del paquete IP necesarias para realizar el seguimiento.
- Información de contacto o el origen de la comunicación RID.
- Información del camino de la red para prevenir loops en el rutado a través de la red. Si un sistema RID recibe un mensaje de *Trace Request* conteniendo su propia información en el camino el sistema RID debería emitir una alerta.
- Un identificador único para cada ataque. Este identificador debería ser utilizado para correlacionar los seguimiento en múltiples fuentes en un ataque DDoS.

Es responsabilidad de cada participante adherirse a las reglas establecidas el las políticas globales de uso para este sistema y las establecidas en cada acuerdo para los acuerdos bilaterales o acordes a las reglas del consorcio. El objetivo de dichas políticas es evitar el abuso del sistema. En RID se pueden diseñar topologias que permitan el intercambio de información facilitando la comunicación entre socios. La topología más básica para comunicar sistemas RID es una comunicación directa. En una organización se pueden establecer y utilizar varias topologías. Una podría fortalecer las relaciones bilaterales con socios. Los socios podrían enrutar los mensajes RID entre ellos. Este enfoque permite un rastreo iterativo en donde la fuente es desconocida. La comunicación entre los sistemas RID debe ser protegida. RID tiene muchas consideraciones de seguridad incluidas en el diseño del protocolo. Al considerar el transporte de mensajes RID, una red fuera de banda, ya sea física o lógica, puede prevenir ataques externos contra las comunicaciones RID. Se deben utilizar conexiones autenticadas y encriptadas entre sistemas RID para proveer confidencialidad, integridad, autenticidad y privacidad de los datos. Las relaciones de confianza son realizados por socios y establecen relaciones de confianza por medio de infraestructuras de PKI. El protocolo de transporte utilizado debe proveer encriptación para dar un nivel de seguridad e integridad adicional, mientras se provee autenticación por medio de certificados. De todas formas los mensajes RID no confían únicamente en la seguridad provista por el protocolo de transporte. La infraestructura PKI provee la base para la autenticación, autorización, encriptación y firmas digitales necesarias para establecer una relación de confianza entre los miembros de una comunidad RID. Problemas de privacidad pueden ser de preocupación cuando se habla de compartir información y se deben considerar a la hora de alcanzar la meta de detener o mitigar los efectos de un incidente de seguridad. Para ello hay clases especificas

para automatizar las políticas de privacidad. Como se explico anteriormente, IODEF describe un formato de documentos XML con la finalidad de intercambiar información de seguridad entre CSIRTs u otras organizaciones. El formato establecido le permite a los CSIRTs intercambiar información que sea facilmente parseable. IODEF define un formato de mensaje, no un protocolo de transporte, esto se realiza para permitir a los CSIRTs intercambiar y almacenar los datos de la forma que más le conviene a cada una de las organizaciones. Sin embargo, RID requiere una especificación de un protocolo de transporte para asegurar la interoperabilidad entre las organizaciones socias. En el RFC6046, se especifica el transporte de mensajes RID sobre HTTP/TLS. En esta especificación, cada servidor RID funciona como servidor y cliente. Todos los sistemas RID deben estar preparados para aceptar conexiones HTTP/TLS de cualquier socio con la finalidad de soportar llamadas en respuesta tardías a pedidos que se realizaron.

# Capítulo 3

# STIX

Chapter 3. *STIX*

## 3.1. Background

STIX busca dar una representación estructurada de la información y que a su vez está sea expresiva, flexible, extensible, automatizable y legible. Esto se presenta como un desafío ya que la información intercambiada debe ser estructurada para que pueda ser parseada por una maquina pero no se debe perder la posibilidad de que una persona la pueda leer y entender así de esta forma no se pierde el juicio y control que esta puede tener. También se busca que STIX se transforme en un estándar para la comunidad para obtener información de calidad que de un aprovechamiento mejor de esta y sin saber de antemano la fuente de los datos provistos. El desarrollo de una herramienta de este tipo se ha vuelto urgente dado la velocidad y complejidad con la cual evolucionan las amenazas también teniendo consideración de la basta cantidad de datos que se deben intercambiar. Por ello es necesario establecer una forma automática para ayudar a los analistas a ejecutar acciones defensivas con un conjunto de datos mas grande del que podrían obtener si trabajaran aisladamente.

## 3.2. Aproximaciones de la actualidad

La información que se intercambia y utiliza hoy en día es atómica, inconsistente y muy limitada en sofisticación y expresividad. En donde se utilizan estructuras estandarizadas, estas son tipicamente focalizadas en una porción del problema. Además no se integran de

forma adecuada entre si o carecen de flexibildiad. Las actividades de intercambio de indicadores son entre humanos, siendo los indicadores desestructurados o semi-estructurados intercambiados por portales web o encriptados via email. Más recientemente se ha visto el surgimiento de transferencias entre maquinas de conjutnso de indicadores simples de modelos de ataques bien conocidos. STIX busca extender los indicadores para permitir el manejo e intercambio de indicadores de forma más expresiva así como de un espectro más amplio de información. Actualmente, el intercambio y manejo de información de forma automatica de información es visto tipicamente en lineas de productos, servicios ofrecidos o soluciones especificas de una comunidad. STIX busca permitir el intercambio de información de forma comprensiva, rica, de alta fidelidad entre organizaciones, comunidades, productos y servicios ofrecidos. STIX es un lenguaje para la especificación, captura, caracterización y comunicación de información de seguridad estandar. Lo hace de forma estructurada para soportar un mejor manejo de la información y la aplicación de automatización. Una variedad de casos de uso para dicha información son realizados.

- Analisis de las amenazas
- Especificación de patrones de indicadores para la amenaza.
- Manejo de las actividades de respuesta
- Intercambiar información

STIX provee un mecanismo común para hacer frente a estos casos de uso dando consistencia, eficiencia, interoperabildiad y conciencia global de la situación.

STIX provee una arquitectura unificada juntando un conjunto amplio de información incluyendo:

- Cyber Observables
- Indicadores
- Incidentes
- Tacticas, tecnicas y procedimientos de los adversarios
- Objetivos de exploits
- Cursos de acción
- Capañas de ataques
- Actores de ataques

Para permitir que dicha solución sea practica para cualquier caso de uso, lenguajes existentes y estandarizados son utilizados.

## 3.3. Casos de uso

### 3.3.1. Analisis de amenazas

Un analista revisa información estructurada y no estructurada respecto a actividades de amenazas de una variedad de fuentes de entrada manuales o automaticas. El analista buscan entender la naturaleza de las amenazas relevantes, identificarlas y caracterizarlas totalmente para que todo el conocimiento relevante de la amenaza sea totalmente expresado y evolucionado a traves del tiempo. Este conocimiento relevante incluye acciones relacionadas con la amenaza, comportamientos, capacidades, intenciones, actores atribuidos, etc. Por medio del entendimiento y la caracterización, el analista puede especificar patrones de indicadores relevantes, sugerir acciones para las actividades de respuesta y compartir la información con miembros de la comunidad.

### 3.3.2. Especificación de patrones de indicadores

Un analista especifica patrones medibles representando las características observables de una amenaza junto con su contexto y metadata para ser interpretadas, manejadas y aplicar el patrón y sus resultados. Esto puede ser realizado de forma manual o con la asistencia de una herramienta automatizada.

### 3.3.3. Manejo de las actividades de respuesta

Los tomadores de decision y el personal de operaciones trabajan en conjunto para prevenir o detectar actividades amenasantes y responder a los incidentes detectados que sean realizados por dichas amenazas. Las acciones preventivas pueden mitigar vulnerabilidades, debilidades, o malas configuraciones que sean que sean objetivos de los exploits. Luego de la detección e investigación de incidentes específicos, acciones reactivas pueden ser realizadas. *Prevención de amenazas* //REPASAR ESTO Los tomadores de decisiones evaluan acciones preventivas para amenazas relevantes que sean identificadas y seleccionan acciones apropiadas para su implementación. El personal de operaciones implementa las acciones seleccionadas para prevenir la ocurrencia de amenazas especificas aplicando mitigaciones amplias o con objetivos especificos iniciados por intepretación de los indicadores. *Detección de amenazas* //REPASAR ESTO El personal de operaciones

aplica mecanismos (automaticos y manuales) para monitorear y asistir las operaciones con la finalidad de detectar la ocurrencia de amenazas especificas basandose en la evidencia historica, analisis del contexto actual, interpretación de los indicadores que se presentan. Esta detección se realiza generalmente por medio de patrones de indicadores.

*Respuesta a incidentes* El personal de operaciones responde a amenazas detectadas, investiga que ha ocurrido o esta ocurriendo, trata de identificar y caracterizar la naturaleza de las amenazas y lleva a cabo la mitigación o lleva a cabo cursos de acción preventivos. Una vez que los efectos son entendidos, el personal de operaciones puede implementar mitigaciones acordes o llevar a cabo cursos de acción correctivos.

### 3.3.4. Compartir información de amenazas

Los tomadores de decisión establecen políticas respecto a que tipo de información será compartida, además toman decisiones respecto a con quienes se comparte y como debería ser manejada basandose en frameworks de confianza de forma de mantener niveles adecuados de consistencia, contexto y control. Esta politica es luego implementada para compartir los indicadores de amenazas apropiados y otra información de amenazas.

## 3.4. Principios de guia

En el enfoque dado a STIX se ha buscado implementar un conjunto de principios con el consenso de la comunidad. Esos principios son los siguientes:

### 3.4.1. Expresividad

Con el fin de soportar la diversidad de casos de uso relevantes, STIX apunta a proveer una cobertura expresiva en todos sus casos de uso especificos en lugar de dirigirse especificamente a alguno de ellos.

### 3.4.2. Integración en lugar de duplicación

Cuando STIX abarca conceptos de información estructurada para los cuales ya existen representaciones estandarizadas con el consenso adecuado y que se encuentran disponibles, se busca integrar estas representaciones a la arquitectura STIX en lugar de duplicar esta información innecesariamente.

### 3.4.3. Flexibildiad

Con el fin de soportar un amplio rango de casos e información variable con varios niveles de fidelidad, STIX esta diseñado para ofrecer tanta flexibilidad como sea posible. STIX se adhiere a una politica de permitir a los usuarios utilizar cualquier porcion de representaciones estandar que sean relevantes para un contexto dado y evita elementos obligatorios siempre que sea posible.

### 3.4.4. Extensibildiad

//REVISAR Con la finalidad de soportar un amplio rango de casos de uso con un potencial diferente de representación y para asegurar la facilitar el perfeccionamiento impulsado por la comunidad, se ha diseñado STIX para construir mecanismos de extensión para uso específicos, para usos localizados, para refinamientos del usuario y evolución y para facilidad de refinamiento y evolución centralizada.

### 3.4.5. Automatización

El diseño realizado en STIX busca maximizar la estructura y la consistencia para soportar metodos de procesamiento automatico por maquinas.

### 3.4.6. Lectura

El diseño de STIX busca estructuras del contenido para que nos ea únicamente consumible o procesable por maquinas sino que también sea leíble por humanos. Esto es necesario para claridad y comprensibilidad durante las primeras etapas de desarrollo y adopción y para el uso sostenido en diversos ambientes,

## 3.5. Implementacion

La implementación inicial de STIX utiliza XML como un mecanismo portable, estructurado y que se puede encontrar en cualquier parte para la discusión, colaboración y refinamiento entre las comunidades involucradas. Esta pensado para el desarrollo colaborativo de un lenguaje estructurado sobre información de amenazas entre expertos de la comunidad. Se ha pensado que el uso del lenguaje es incentivado y soportado por medio del desarrollo de varias herramientas como APIs. Solo por medio de niveles adecuados

de colaboración entre miembros de la comunidad y con la utilización de datos reales se puede llegar a que la solución evolucione.

# Capítulo 4

# TAXII

## 4.1. Background

El intercambio de información se ha tornado critico contra los adversarios actuales. Actualmente un número creciente de organizaciones comparten información de amenazas con el fin de tener un visión más amplia de las actividades de los adversarios y así ayudar a administrar los recursos de las organizaciones para obtener el mejor resultado posible de sus defensas. La capacidad de compartir información de forma automática con un gran número de comunidades y que dicha información sea completa no existe en la actualidad. El objetivo que plantea TAXII es extender la capacidad de compartir indicadores permitiendo intercambios robustos, seguros y de gran volumen de datos los cuales deben poseer información mas expresiva de amenazas informáticas. TAXII es un conjunto de especificaciones técnicas y de documentación para permitir el intercambio de información procesable entre organizaciones. Para ello se definen protocolos y formatos de datos para intercambiar información de forma segura la cual ayude a detectar, prevenir y mitigar amenazas informáticas en tiempo real. No se buscan definir acuerdos para el intercambio de información, gobierno o aspectos técnicos del intercambio de información. En su lugar, permite a las organizaciones alcanzar una mejora en su situación respecto a las nuevas amenazas y además compartir información que ellos elijan con quien elijan de forma simple y rápida aprovechando las relaciones y sistemas existentes. En el desarrollo de TAXII se busco consenso y participación de la comunidad. TAXII permite intercambio de información sobre amenazas de forma eficiente y comprensiva por medio de *automatización* y *articulación* de un modelo detallado de información. Para lograr esto, se utiliza una representación estándar de información de amenazas y un framework para soportar el intercambio de datos. El modelo permite el envío y recepción de un conjunto amplio de información de seguridad para soportar un amplio

número de necesidades referentes al intercambio de información. TAXII cubre un amplio número de casos de uso, tecnologías, especificaciones e implementaciones. Los casos de uso son desarrollados de manera secuencial, permitiendo un conjunto inicial de casos de usos que permite el intercambio e información. TAXII utiliza protocolos y especificaciones existentes siempre que es posible y se integra con mecanismos de intercambio de información existentes para reducir los costos de implementación y permitir la adopción rápida por parte de organizaciones ya establecidas que ya intercambian información.

### 4.1.1. Fundamentos

Las estrategias de defensa se deben adaptar al creciente número, frecuencia y complejidad de los ataques que se llevan a cabo. Actualmente la estrategia predominante se refiere a bloquear los ataques y arreglar las vulnerabilidades, esta estrategia se basa en alertas. Si bien puede ser efectiva contra algunas amenazas no logra detener ataques avanzados o proveer información sobre las actividades de un atacante luego de que la red fue penetrada. Una estrategia más adecuada es *çyber kill-chain"* la cual se representa a continuación.

ACA va la figura 1 de White paper de taxii

La estrategia presentada busca descomponer las fases de un ataque con la finalidad de obtener una amplia comprensión del ataque y el atacante así como mejorar las posibilidades de defensa.

Aca pongo la tabla 1 del White paper

Los primeros pasos de esta estrategia representan una oportunidad para detectar y mitigar las amenazas de forma proactiva antes de que el adversario realice un acceso no autorizado en los sistemas de la organización. En los pasos posteriores es donde se realiza la detección, respuesta y aseguramiento de los activos más importantes. Al entender al adversario los defensores tienen un mejor oportunidad para descubrir y responder al ataque. Actualmente se busca que las defensas anticipen y mitiguen las amenazas antes de que sean mas difíciles de encontrar y erradicar utilizando los métodos tradicionales de detección y respuesta. Para poder realizar esto es necesario que se realice una actividad de cyber inteligencia, recolecte información referente a ataques, con esta información analistas pueden agrupar patrones de actividades similares, atribuir actividades a ciertos actores, identificar e implementar estrategias de mitigación de forma rápida y anticiparse al lanzamiento de ataques similares en el futuro. Para aprovechar de forma más adecuada los beneficios de la cyber inteligencia, las organizaciones deben compartir la información recolectada (incluyendo las estrategias de defensa entre otras) con socios

de su confianza. De esta forma se obtiene una imagen mas completa de las actividades del adversario y de las acciones defensivas que se deben realizar. [1] Por medio del análisis del comportamiento de los adversarios en distintos objetivos y en un periodo de tiempo, los defensores son capaces de identificar un conjunto importante de indicadores y tácticas, técnicas y procedimientos (TTPs). De esta forma se obtiene información de los objetivos y las estrategias lo cual permite al defensor predecir el comportamiento del ataque y generar defensas dinámicas.

### 4.1.2. Comunidades

Hoy en día un número creciente de organizaciones buscan compartir información de las amenazas. Con esto ha crecido el número y tipo de las comunidades que buscan compartir información. Se pueden encontrar tres tipos de comunidades :

- Peer
- Comerciales
- Gobierno

La necesidad primordial entre dichas organizaciones es la confianza dado que compartir información sensible podría exponer a una organización a un daño en su reputación, demandas o advertir a un adversario con lo cual el trabajo realizado fuera inútil. Se deben definir medidas para la protección de los datos como restricciones en el manejo de los datos, sanitización de los datos y el establecimiento de confianza entre las dos partes. Esto es particularmente importante cuando las organizaciones forman parte de varias comunidades para el intercambio de amenazas de seguridad. Se puede ver que lo que es compartido con una comunidad no necesariamente debería ser compartido con otra. Las comunidades entre peers son las más comunes, en estas organizaciones o individuos con un propósito común se unen para mejorar las defensas colectivas contra adversarios comunes o conjuntos de adversarios. Las comunidades comerciales se basan en membresias por parte de los miembros y son altamente anónimas. La organización comercial maneja de forma centralizada la información y la distribuye entre los miembros de la organización. Estas organizaciones proveen una forma rápida de obtener información, además puede ser más amplia que la información especializada que es compartida por pares y puede que no siempre sea aplicable a las necesidades de una organización. Las comunidades gubernamentales son establecidas y manejadas por el gobierno, son voluntarias u obligatorias e incluyen participantes tanto del gobierno como de la industria privada. En ellas el gobierno controla la información y la diseminación de esta, cabe

señalar que así como en las comunidades comerciales la información y los participantes son altamente confidenciales.

### 4.1.3. Modelos

Hay tres modelos principales para el intercambio de información entre organizaciones:

- hub and spoke
- peer to peer
- source/subscriber

En el método hub and spoke, una entidad controla la recepción y la diseminación de los datos. La entidad hub usualmente realiza una anonimiza los datos recolectado de las amenazas y provee una análisis adicional a los participantes. Este modelo es comúnmente visto en comunidades de gobierno o comerciales. En el modelo peer to peer, los participantes intercambian y reciben información directamente de los otros participantes. La información es compartida entre todos los miembros de la comunidad por igual y la fuente esta claramente identificada. El modelo faltante es el de source/suscriber, este modelo es utilizado por las comunidades comerciales que proveen de información. El proveedor de información envía regularmente información a todos los suscriptores y estos podrían eventualmente enviarle información a la fuente. Usualmente, en este modelo la información esta codificada de una manera propietaria y puede faltar información esencial sobre algunas intentos de irrupción. Presenta la ventaja de que se tiene acceso rápido a un conjunto de datos amplio y es útil para organizaciones con recursos limitados.

### 4.1.4. Métodos para el intercambio de información

Hay múltiples métodos para el intercambio de información. Usualmente, el método juega un rol significante en los tipos, volúmenes y naturaleza de la información compartida con la comunidad. Algunos medios de intercambio limitan el tipo de contenido que es compartido de forma sencilla mientras que otros promueven ciertos tipos de intercambio. Algunos métodos comunes son:

- Email lista de servidores
- Foros de discusión
- wikis

- repositorios de datos

La mayoría de estos métodos no permiten el consumo de información de amenazas de forma automática. La mayoría de los consumidores rutinariamente toman esta información y la sintetizan en sus bases de datos locales. Existen varios esfuerzos para generar arquitecturas abiertas, estándar basados en indicadores e información de incidentes. La realidad es que ninguno de estos a podido convertirse en un estándar para el intercambio entre comunidades.

### 4.1.5. Información compartida

Actualmente los indicadores que se comparten son sistemas malignos o actividades de red o cyber observables de interes como las direcciones de IP, nombres de dominio, nombres de archivos o direcciones de email. En algunos casos, la información compartida esta enfocada en una amenaza en particular, como las botnets. En otros casos se incluye malware en uso u otros TTP. La información compartida esta establecida generalmente por la comunidad o por el grado de confianza entre las partes.

Limitaciones Compartir información ha ayudado a mejorar las capacidades defensivas de numerosas organizaciones. Sin embargo, las aproximaciones actuales no han logrado que se llegue al máximo potencial. Los procesos para compartir información son manuales, llevan mucho tiempo, son repetitivos y en muchos casos requieren que las organizaciones re escriban o traduzcan la información a una amplia variedad de formatos. La información es además compartida por medios inseguros. Debido a la variedad de formatos y los protocolos en uso, así como los procesos manuales involucrados, esta técnica se lleva a cabo entre pocas organizaciones en las que se confía. Otro factor que hace que hace ineficiente el intercambio de información ineficiente, menos escalable y que consuma mucho tiempo es el uso de tecnologías y/o formatos propietarios, presentandose la necesidad de desarrollar un amplio número de scripts y módulos para permitir compartir información por fuera de las comunidades. Para aquellas comunidades con algún grado de automatización, sus modelos son generalmente bajos en prestaciones y usan soluciones propietarias, comerciales o adaptadas a su comunidad. Otra limitación se presenta en la naturaleza atómica de la mayoría de los indicadores. Por ejemplo, cuando una IP en particular es identificada como sospechosa el esfuerzo que debe realizar el adversario para cambiar la IP es prácticamente cero. Confiar únicamente en indicadores atómicos sin contexto puede proveer un gran número de falsos positivos llevando a un desperdicio en tiempo de análisis.

Motivación Una mejor solución para compartir información es necesaria, una que sea utilizada por diferentes comunidades y modelos para compartir información, permitiendo diferentes métodos para compartir, y que soporte un rango amplio de datos. En particular, los objetivos de la solución ideal son:

- Permitir el poder compartir información de forma más rápida y precisa
- Reducir el análisis humano y liberar a los recursos humanos para realizar trabajo de análisis más valioso.
- Mover las amenazas más conocidas para que sean analizadas por computadoras.
- Permitir que se comparta de forma automática un gran rango de datos, siendo estos datos complejos y no los simples, atómicos indicadores. Esto debería permitir una defensa activa.
- Proteger la información intercambiada.
- Permitir que se agregue información a las bases locales pero contexto y discreción, pero con un menor número de analistas que vean las información.
- Permitir la colaboración de analistas de distintas organizaciones en los incidentes que sean un reto.

### 4.1.6. Que es TAXII

TAXII es un conjunto de especificaciones técnicas y documentación para el intercambio de información de alta fidelidad, dicho intercambio es independiente de la plataforma y realizado de forma segura. Esta diseñado de forma que permita la interoperabilidad de diferentes soluciones en lugar de ligarse a una tecnología o producto en particular. Además se busca incentivar a los proveedores de tecnología a incorporar soporte para las especificaciones de TAXII en sus productos. Ha sido desarrollado con consenso y participación de la comunidad, con la finalidad de permitir un intercambio de eficiente y comprensivo de la información detallada, de forma automática y articulada. Para lograr esto, TAXII utiliza una representación estándar de la información y define un framework para soportar el intercambio. TAXII ofrece una forma de describir e intercambiar los indicadores, dejando a los proveedores la libertad de determinar como sus productos producen, consumen o toman ventaja de los flujos de información especificados por TAXII.

Imagen 2

### 4.1.7. Objetivos de TAXII

Los objetivos de TAXII son:

- Permitir el intercambio seguro y rápido de información referente a amenazas entre comunidades de defensores de seguridad.
- Lograr un standard para permitir compartir indicadores entre otros elementos entre organizaciones.
- Extender el intercambio de indicadores para permitir intercambios seguros, robustos y de gran volumen que tengan una expresividad mayor a la actual.
- Soportar un amplio número de casos de uso y practicas comunes a las comunidades.
- Tomar los estandares existentes que sean adecuados.
- Llegar a una adopción por parte de organizaciones internacionales de standars.

TAXII no ha creado una comunidad para compartir, sino que permite que las comunidades compartan. TAXII mejora las deficiencias existentes proveyendo especificaciones abiertas y comunes para transportar los mensajes con información con capacidades como encriptación, autenticación, direccionamiento, alertas y pedidos entre sistemas.

### 4.1.8. Representación estándar de la información

TAXII utiliza el lenguaje STIX para representar la información. STIX es un lenguaje desarrollado por la comunidad para la especificación, captura, caracterización y comunicación de información de amenazas cibernéticas de forma estandarizada. STIX provee una arquitecutra unificada que soporta varios tipos de información entre los cuales se incluyen Cyber Observables, Indicadores, Incidentes, tacticas, técnicas y procedimientos de los adversarios, etc.

Para maximizar la compatibilidad y facilidad de adopción, STIX utiliza varios standards como CybOX, Common vulnerabilities and exposures (CVE) y common platform enumeration (CPE).

### 4.1.9. Un framework de Intercambio

La segunda parte necesaria en automatizar el intercambio de información es especificar como esta es compartida. Para alcanzar esto, TAXII define especificaciones técnicas

y documentación de soporte. En particular, las especificaciones de TAXII definen un conjunto de capacidades necesarias para el transporte exitoso de mensajes, o como los mensajes TAXII llegan del punto A al B. Los mensajes TAXII llevan datos de amenazas informáticas transformadas a formato STIX. El conjunto completo de los mensajes incluye mensajes con datos y de control. TAXII utiliza protocolos y especificaciones existentes siempre que es posible y los integra con los mecanismos actuales para reducir los costos de implementación y permitir una adopción rápida por parte de las organizaciones ya establecidas que ya comparten información. TAXII esta siendo desarrollado de forma modular para soportar una variedad de mecanismos y formatos de datos para ser intercambiados.

### 4.1.10. Casos de Uso

TAXII ha sido desarrollado para soportar casos de uso comunes para el intercambio de información.

Alertas o Advertencias publicas Estas son advertencias al publico en general o a varios asistentes de varios CSIRT, estas son enviadas a todos los suscriptores. Estas alertas son de una naturaleza tan amplia que no necesitas ser encriptadas o no se necesitan autorizaciones. Sin embargo es importante una firma digital para asegurar la autenticidad. Las entidades u organizaciones deben ser especificadas para identificar la fuente de la alerta.

Alertas y Reportes privados Las alertas privadas son similares a las publicas, exceptuando que la información compartida es sensible y restringida a los socios que comparten datos. Los mecanismos para enviar datos deberían ser similares a los de las alertas publicas. Como las alertas y reportes se suponen sensibles y no para el uso general, es importante que TAXII soporte formas adecuadas de encriptacion, autenticación, autorización y identificación de datos. Dependiendo en la naturaleza de las comunicaciones, manejo explícito de marcas o restricciones en datos compartidos debería ser necesario. Las alertas son generalmente cortas, mensajes estándar con indicadores muy específicos o acciones especificadas. Los reportes son mensajes mas largos, y pueden incluir reportes de incidentes, análisis de malware, análisis de amenazas u otras observaciones.

Soportes para Queries Es común que los analistas de amenazas busquen información de otros entre o por fuera de sus comunidades.

- RFI (Request for Information): es un mensaje simple que se espera sea manejado de forma manual y que permite que se pida información.

- Repository Search: Para este tipo de query, es esperado que una organización ofrezca repositorios en los que buscar, los cuales podrían ser compatibles con TAXII o STIX.

Transferencia Varias organizaciones que transfieren información necesitan en algunas instancias agregar miembros. El nuevo miembro necesitas obtener los datos del repositorio de la organización. Por ello es esperada la transferencia de un gran volumen de datos.

## 4.2. Componentes de TAXII

- Especificación de TAXII: Define la especificación de los componentes y provee guía y requerimientos sobre como dichas especificaciones interoperan en TAXII.
- Especificación de servicios de TAXII: Define una serie de servicios que deben ser implementados para ser compatible con TAXII. Describe información intercambiada a un nivel alto y no se limita a ningún mecanismo de intercambio en especial.
- Implementación de Servicios: Se realiza una implementación de los servicios TAXII para un mecanismo de intercambio. Cada implementación de servicios provee guía técnica y requerimientos para implementar la especificación de los mecanismos de intercambio.
- Modelo de datos de mensajes: Se define una estructura para los mensajes TAXII, incluyendo header, payload, control y mensajes de datos. Los mensajes de datos utilizan STIX para el payload de los mensajes TAXII.
- Implementaciones de los mensajes de datos: Es una implementación del modelo de datos de mensajes, incluyendo el payload STIX, a un formato en particular. Cada implementación de mensajes define la guía técnica y requerimientos para utilizar un formato de mensajes particular para expresar el modelo de datos de mensajes.

### 4.2.1. TAXII Toolkit

Es provisto para soportar la adopción de TAXII y asistir en el desarrollo de capacidades compatibles. El toolkit provee una colección de implementaciones de referencia, un conjunto de herramientas y una colección de librerías e interfaces.

Especificaciones de TAXII

TAXII esta definido por múltiples especificaciones relacionadas. Esta sección describe las especificaciones definidas en TAXII.

- Especificación de Servicios (Service Specification): Provee los requerimientos por los cuales se definen los servicios e intercambios de TAXII. No provee detalles respecto al formato de los datos o como los mensajes TAXII son transportados por la red. Dichos detalles y requerimientos pueden ser encontrados en Protocol Binding Specification y Message Binding Specification.
- Especificación de protocolos de enlace (Protocol Binding Specification): Define los requerimientos para transportar mensajes TAXII por la red. Puede haber varias especificaciones creadas para TAXII. Cada especificación define requerimientos para transportar mensajes TAXII usando protocolos de red y se proveen requerimientos respecto a como los servicios TAXII son soportados por los protocolos de red.
- Especificación de Mensajes (Message Binding Specification): Se definen requerimientos para representar mensajes TAXII en un formato particular. Puede haber múltiples especificaciones para dichos mensajes. Se provee información detallada sobre como la información definida en los especificación de servicios es expresada en los mensajes.

ACA VA LA FIGURA 1 DEL DOCUMENTO DE SERVICE SPECIFICATION

Separación de la especificación de servicios, los protocolos de enlace y los mensajes existe para dar flexibilidad mientras TAXII evoluciona. Debido a que las organizaciones generalmente tienen restricciones respecto a los protocolos que soportan, TAXII busca no ligarse a un único protocolo que excluya a una parte de la comunidad. Cuando se ve que la comunidad expresa interés en un nuevo protocolo o tipo de mensaje, TAXII puede dar soporte para ellos sin cambiar los componentes centrales. Dos grupos que usen el mismo protocolo de red y formato de mensajes serán capaces de intercambios de información estructurada de forma automática. Las políticas de intercambio de los participantes puede limitar estos intercambios si es necesario, pero el uso de servicios compatibles con TAXII asegura que se puede intercambiar cualquier información con los mecanismos definidos por TAXII. Los grupos que usen diferentes protocolos o formatos de mensajes no serán capaces de comunicarse directamente, pero como están utilizando mensajes y servicios en el núcleo de las comunicaciones de sus comunidades significa que es posible establecer caminos para que ocurra la interacción.

### 4.2.2. Especificación de Servicios

Esta especificación provee normativas respecto a los servicios, mensajes e intercambio de mensajes en TAXII. No provee detalles respecto a como los mensajes son transportados, dejando eso a la especificación de los protocolos de enlace. Si bien se provee información

relacionada a la información presente en los mensajes TAXII, no da información respecto a como los mensajes TAXII son expresados. *Versión de los servicios TAXII* En la especificación de los servicios se hace referencia a "version IDs", especificamente TAXII services version Id, TAXII protocol binding version ID y TAXII message binding version ID. Los protocolos de red que transportan mensajes TAXII así como los mensajes en si es necesario en algunos casos que indiquen el número de versión de TAXII así como de la especificación de mensajes o de protocolos de transporte. Los string de version id representan la versión de las especificaciones TAXII utilizadas en los intercambios TAXII. Cada especificación de TAXII está identificada por su propia version id. Diferentes versiones de cada especificación proveerán diferentes version ids. La especificación actual tiene un version id: $TAXII_1$,0

### 4.2.3. Terminios y definiciones

*Conceptos utilizados en TAXII*

- Cyber Threat information: Es cualquier información representable en STIX. Esto incluye, pero no esta limitado a, Observables, Indicadores, incidentes, TTPs (Tactics, Techniques y Procedures), exploit targets, campaigns, threat actors y courses of action.
- TAXII Data Feed: Es una colección de cyber threat information estructurada expresable en uno o mas documentos STIX que pueden ser intercambiados utilizando TAXII. Cada TAXII Data Feed *debe* tener un nombre que lo identifica de forma única entre el resto de los feeds de un productor dado. Cada elemento de un TAXII data feed debe ser etiquetado con un timestamp y puede tener otras etiquetas a discreción del productor.
- Mensae TAXII: Un bloque de información que es pasado de una entidad a la otra. Un mensaje TAXII representa un pedido o una respuesta.
- Intercambio de mensajes TAXII: Una secuencia definida de mensajes TAXII intercambiados entre dos entidades.
- Servicio TAXII: Son funcionalidades albergadas por algunas entidades y que es accedido o invocado usando uno o mas TAXII Message Exchange.
- TAXII Capability: Una actividad de alto nivel soportado por TAXII por medio del uso de uno o mas servicios TAXII.

*Unidades funcionales de TAXII* Las unidades funcionales de TAXII representan conjuntos discretos de actividades requeridas para soportar TAXII. Una unidad funcional representa algún componente con un rol bien definido en TAXII.

- TAXII Transfer Agent (TTA) : Es una unidad funcional conectada a la red que envía o recibe mensajes TAXII. Una TTA interactua con otras TTAs por medio de la red y maneja los detalles de los requerimientos del protocolo de uno o más TAXII Protocol Binding Specifications. Una TTA provee mensajes TAXII a un TAXII Message Handler permitiendo que este último sea independiente del protocolo de red utilizado. De la misma forma, el TTA puede ser independiente del contenido de los mensajes TAXII, dejando el manejo de la información al TAXII Message Handler.
- TAXII Message Handler (TMH): Es una unidad funcional que produce y consume mensajes TAXII. El TMH es responsable de parsear y construir mensajes con el formato especificado en uno o mas TAXII Message Binding Specifications. Un TMH interactua con un TTA, el cual maneja los detalles necesarios para transmitir mensajes por la red. El Back-end TAXII interactua con el TMH para convertir su contenido en mensajes TAXII, y llevar a cabo actividades basadas en los mensajes TAXII que son recibidos por el TMH.
- TAXII Back-end: Cubre todas las unidades funcionales distintas al TTA y al TMH. Las especificaciones de TAXII no proveen requerimientos sobre como son implementadas las capacidades en un back-end mas allá de como debe interactuar con el TMH. Las organizaciones o implementadores pueden decidir que capacidades implementar según los servicios TAXII que deseen soportar o según como quieren dar ese soporte.
- Arquitectura TAXII: Cubre los aspectos de las unidades funcionales de la infraestructura de productor o consumidor que prove o utiliza servicios TAXII. Una arquitectura TAXII incluye una TTA, un TMH y un back-end TAXII.

  IMAGEN DE LA ARQUITECTURA FIG 2 DE DOCS

*Roles en TAXII* Los roles en TAXII son utilizados de acuerdo al uso que se hace de los servicios especificados en TAXII.

- Productor es el rol de una entidad que es la fuente de información estructurada de amenazas.
- Consumidor es el rol de la entidad que recibe información estructurada sobre amenazas.

*Componentes de red* Los siguientes términos son utilizados para definir componentes de una implementación TAXII utilizando un modelo cliente-servidor.

- Una implementación TAXII es un implementación especifica de una arquitectura TAXII.
- Servidor TAXII Es una implementación que provee uno o mas servicios TAXII. Para soportar esta funcionalidad, se asume que un servidor TAXII esta continuamente esperando trafico de red.
- Cliente TAXII Es una implementación TAXII que inicia intercambio con un servidor TAXII. Un cliente no necesita una conexión persistente con internet para operar pero puede abrir conexiones cuando desea interactuar con un servidor y desconectarse de internet cuando la conexión a terminado.
- TAXII endpoint denota una implementación TAXII que puede ser un servidor o un cliente

### 4.2.4. Capacidades

La existencia de TAXII provee capacidades especificas para aquellos que desean compartir información de amenazas cibernéticas. Las capacidades TAXII son el nivel mas alto en el cual se pueden expresar las acciones de TAXII. Hay tres capacidades que soporta la actual versión de TAXII: push messaging, pull messaging y discovery. *Push Messaging* La información puede ser enviada de un productor a un consumidor. Esto puede reflejar una relación pre-existente entre el productor y el consumidor en la que el consumidor a pedido que se le envíen datos desde el productor. También puede usarse en caso de que el consumidor desee aceptar contribuciones de cualquier productor, y estos le envien datos en cualquier momento.

*Pull Messaging* Un consumidor puede requerir información de un productor. Esto no solo le permite al consumidor el control sobre el momento en el que recibe los datos sino que también le permite hacerlo sin tener que aceptar conexiones entrantes. Así como en push messaging, el productor y consumidos pueden tener acuerdos pre-existentes para que el consumidor tenga acceso a los datos del productor. De forma alternativa, un productor puede hacer su información pública y cualquer consumidor puede requerir sus datos. La versión actual de pull messaging, limita a los consumidores a hacer pedidos por medio de las organizaciones productoras de los datos en lugar de por los datos en si. Todos los datos provistos por un productor deben estar organizados en grupos llamados "TAXII Data Feeds". Piezas individuales de información en un TAXII Data Feed son etiquetadas

utilizando timestamps. El productor tiene total discresión sobre como el contenido se mapea en TAXII Data Feeds y en el significado de los timestamps. La capacidad de pull messaging esta atada a entender el contenido del productor.

*Discovery* Para facilitar las comunicaciones automatizadas, TAXII soporta capacidades para descubrir los servicios específicos que ofrece un servidor o grupo de servidores, así como los protocolos o mensajes que este servidor ofrece. Esto no quita la necesidad del involucramiento humano para establecer acuerdos de cooperación lo cual esta por fuera del objetivo de TAXII. Sin embargo permite el intercambio de información respecto a las capacidades que un productor pudiera soportar y cuales son los mecanismos que utiliza para hacerlo.

### 4.2.5. Servicios TAXII

Los servicios TAXII representan un conjunto de mecanismos necesarios para soportar capacidades TAXII. Una implementación TAXII pudiera implementar alguno, todos o incluso ninguno de los servicios definidos. TAXII define los siguientes servicios:

- Servicio de descubrimiento: Es utilizado para recibir y responder a mensajes que requieren información sobre los servicios ofrecidos.
- Feed Managment Service: Es utilizado para recibir o responder a mensajes utilizados para el manejo de subscripciones a TAXII Data Feed.
- Inbox Service: Es utilizado para recibir información de amenazas cibernéticas por medio de intercambios iniciados por el productor en intervalos dictados por este.
- Poll Service: Es utilizado para recibir y responder a mensajes de pedido a el TAXII Data Feed iniciados por el consumidor.

En las siguientes subsecciones se describen los distintos servicios. *Discovery Service* Es un mecanismo para comunicar información referente al uso de servicios TAXII y a su disponibilidad. Para un pedido al servicio, se retorna una lista de los servicios TAXII y como estos pueden ser invocados. Un solo servicio de descubrimiento puede reportar servicios TAXII en diferentes equipos finales o incluso en múltiples organizaciones, los propietarios del servicio pueden definir su alcance a su gusto. Un servicio de descubrimiento puede utilizar varios factores para determinar cuales servicios revelar ante una petición, incluyendo pero no limitado a la entidad del cliente TAXII. El servicio de descubrimiento debe soportar "Discovery Message Exchange".

*Feed Managment Service* Es el mecanismo con el cual un consumidor pide información referente a TAXII Data Feeds, pidiendo subscripciones a estos, o modificando las existentes. Este servicio facilita el intercambio de mensajes para manejar las subscripciones. Este servicio no entrega contenido de los TAXII Data Feed, en su lugar se envia contenido del TAXII Data Feed al servicio de Inbox de un consumidor en intercambios iniciados por un productor o en respuesta directa a un pedido del consumidor al servicio de poll. Dicho servicio debe implementar soporte para subscription managment exchange. Dicho servicio podría implementar soporte de feed information exchange.

*Inbox service* Este servicio es el mecanismo con el cual un consumidor acepta los mensajes en un intercambio iniciado por el productor. Un consumidor puede implementar este servicio para recibir datos del TAXII Data Feed. El servicio de inbox debe implementar soporte para Data Push Exchange.

*Poll service* Es provisto por un productor para permitir pedidos al TAXII Data Feed iniciados por el consumidor. Un consumidor contacta a este servicio explícitamente pidiendo el contenido del TAXII Data Feed. Los productores podrían ofrecer Data Feeds combinando envios al Inbox service del consumidor o por medio de pedidos al servicio de poll de productor. Un implementación de este servicio debe dar soporte a Data Poll Exchange.

# Bibliografía


[1] Mitre Corporation. *Active Defense Strategy for Cyber*. Mitre Corporation, 2012.

[2] Mitre Corporation. *Cyber Information-Sharing Models: An Overview*. Mitre Corporation, 2012.

[3] Mitre Corporation. *A New Cyber Defense Playbook*. Mitre Corporation, 2012.

[4] Mitre Corporation. *STIX Whitepaper*. Mitre Corporation, 2012.

[5] M.J. Cloppert E.M. Hutchins and R.M Amin PH.D. *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. Lockhead Martin, 2012.

[6] D. Curry H. Debar and B. Feinstein. *RFC 4765 - IDMEF*. IETF, 2007.

[7] M. Richard J. Connolly, M. Davidson and C. Skorupka. *TAXII Whitepaper*. Mitre Corporation, 2012.

[8] D. Rolsky D. Chamberlain J. Vincent, R. Spier and R. Foley. *RT Essentials*. A. Randal and T. Apandy, 2005.

[9] K. Moriarty and B. Trammell. *RFC 6546 - RID Messages*. IETF, 2010.

[10] J. Meijer R. Danyliw and Y. Demchenko. *RFC 5070 - IODEF*. IETF, 2007.

[11] B. Trammell. *RFC 6546 - Transport of RID messages over HTTP/TLS*. IETF, 2012.