UNIPAGO | UNISHIELD BY UNIPAGO

INTRODUCCIÓN A STIX Y TAXII

1. Introducción

El presente documento describe los protocolos STIX (Structured Threat Information Expression) y TAXII (Trusted Automated Exchange of Intelligence Information), así como su relevancia dentro del proyecto UNISHIELD, el Centro de Intercambio y Análisis de Información (ISAC) operado por UNIPAGO.

STIX y TAXII se han consolidado a nivel internacional como el binomio estándar para representar e intercambiar inteligencia de ciberamenazas (Cyber Threat Intelligence – CTI). Su adopción dentro de UNISHIELD permite homogeneizar la forma en que las organizaciones miembros documentan, analizan y comparten amenazas, indicadores de compromiso, actores maliciosos, campañas y vulnerabilidades, fortaleciendo así la defensa colectiva del ecosistema digital.

Este documento describe qué son STIX y TAXII, cómo funcionan, los objetos que conforman STIX, su estructura técnica y el contexto general de ambos protocolos, con el fin de servir como referencia técnica para los miembros y operadores del ISAC – UNISHIELD.

2. ¿Qué es STIX?

STIX (Structured Threat Information Expression) es un lenguaje y formato de serialización utilizado para intercambiar inteligencia de ciberamenazas (CTI). Fue desarrollado bajo el comité técnico OASIS Cyber Threat Intelligence (CTI TC) y es de código abierto y de uso libre, lo que permite a la comunidad contribuir, formular preguntas y proponer mejoras de manera abierta.

En términos prácticos, STIX permite representar de forma estructurada todos los aspectos asociados a una amenaza cibernética: sospechas, compromisos, atribución, técnicas, actores, infraestructura y respuesta. Esto se logra mediante un conjunto de objetos definidos y relaciones descriptivas entre ellos.

> **Características clave de STIX**
>
> Lenguaje abierto, libre y mantenido por OASIS (CTI TC).
> Diseñado específicamente para inteligencia de ciberamenazas.
> Representación dual: visual para analistas y JSON para máquinas.
> Compatible con herramientas y plataformas existentes (SIEM, TIP, EDR, SOAR).
> Permite describir amenazas con un nivel de detalle técnico y contextual.

3. ¿Qué es TAXII?

TAXII (Trusted Automated Exchange of Intelligence Information) es un protocolo de aplicación, basado en HTTPS y APIs REST, diseñado específicamente para el intercambio confiable de inteligencia de ciberamenazas. Mientras STIX define el qué se comparte (el contenido), TAXII define el cómo se comparte (el transporte).

TAXII organiza los intercambios mediante el concepto de servidores, API Roots, colecciones (Collections) y canales (Channels). Las colecciones funcionan como repositorios donde productores publican objetos STIX y consumidores los descargan, mientras que los canales soportan modelos de publicación-suscripción para flujos en tiempo real.

> **Características clave de TAXII**
> Protocolo abierto y mantenido por OASIS (CTI TC).
> Basado en HTTPS y APIs REST, fácil de integrar.
> Soporta los modelos de Collection (pull) y Channel (publish/subscribe).
> Compatible con TLS, autenticación y control de acceso por colección.
> Diseñado para transportar de forma nativa objetos STIX 2.x.

4. ¿Por qué son importantes para UNISHIELD?

Para un ISAC como UNISHIELD, contar con un lenguaje común para representar amenazas y un mecanismo seguro y automatizado para intercambiarlas es fundamental. Sin estos estándares, cada organización describiría los incidentes con su propia terminología y cada intercambio requeriría integraciones puntuales, dificultando la correlación, el análisis automatizado y la respuesta coordinada.

Los beneficios de adoptar STIX y TAXII en el contexto del ISAC – UNISHIELD incluyen:

- Facilita la contribución y consumo de CTI entre los miembros del ISAC.
- Permite representar de forma clara y estructurada sospechas, compromisos y atribución.
- La información puede visualizarse para un analista o procesarse como JSON de forma legible por máquinas.
- TAXII automatiza el intercambio sobre HTTPS de manera segura y autenticada.
- Su carácter abierto facilita la integración con herramientas y productos existentes.

- Se adapta a las necesidades específicas de cada analista o red.
- Refuerza la defensa colectiva al normalizar el intercambio entre organizaciones.

5. Contexto y Gobernanza de los Protocolos

STIX y TAXII son desarrollados y mantenidos por el OASIS Cyber Threat Intelligence Technical Committee (CTI TC), un comité técnico abierto que reúne a organizaciones gubernamentales, privadas y académicas a nivel internacional. Esta gobernanza garantiza que ambos estándares evolucionen de forma transparente y consensuada.

Ambos protocolos están diseñados para trabajar en conjunto: STIX define la semántica y los objetos de la inteligencia, mientras TAXII define el transporte. Esta separación permite que las organizaciones puedan elegir el modelo de intercambio que mejor se adapte a su realidad (extracción/pull, envío/push, publicación, suscripción) sin afectar el contenido.

Versiones vigentes: STIX 2.1 y TAXII 2.1 son las versiones actualmente recomendadas por OASIS y las que UNISHIELD adoptará como referencia técnica para el intercambio de CTI.

6. Novedades de STIX 2.1

STIX 2.1 introdujo cambios significativos respecto a STIX 2.0, ampliando la expresividad del lenguaje y mejorando su precisión semántica. Las principales novedades son:

- Nuevos objetos: Grouping, Infrastructure, Language-Content (internacionalización), Location, Malware-Analysis, Note y Opinion.
- Objetos significativamente revisados: Malware y todos los SCOs (STIX Cyber-observable Objects).
- Nuevo concepto de Confianza (Confidence) que permite expresar el grado de certeza sobre una información.
- Los STIX Cyber-observable Objects ahora pueden relacionarse directamente mediante STIX Relationship Objects.
- Renombrado de propiedades en conflicto en los objetos Directory, File, Process y Windows Registry Key.
- Nueva relación "basada-en" ("based-on") entre Indicator y Observed Data.
- Se agregó descripción a Sighting y nombre a Location.

- Algunas relaciones SCO se hicieron externas en Domain-Name, IPv4-Addr e IPv6-Addr.

7. Objetos STIX 2.1

STIX clasifica cada pieza de información mediante objetos con atributos específicos. Encadenando varios objetos a través de relaciones se logra una representación clara y completa de la inteligencia de amenazas, ya sea simple o compleja. STIX 2.1 define dos grandes categorías de objetos: los STIX Domain Objects (SDOs) y los STIX Relationship Objects (SROs).

7.1 STIX Domain Objects (SDOs)

STIX 2.1 define 18 SDOs, cada uno orientado a un aspecto particular de la inteligencia de amenazas:

Nombre		Descripción
Inglés	Español	
Attack Pattern	Patrón de ataque	Tipo de TTP que describe las formas en que los adversarios intentan comprometer objetivos.
Campaign	Campaña	Agrupación de comportamientos adversarios que describe un conjunto de actividades maliciosas u oleadas de ataque dirigidas a un grupo específico de objetivos durante un período de tiempo.
Course of Action	Curso de Acción	Recomendación del productor de inteligencia hacia el consumidor sobre acciones que pueden tomarse en respuesta a esa inteligencia.

Grouping	Agrupación	Indica explícitamente que los Objetos STIX referenciados comparten un contexto común (a diferencia de un STIX Bundle que no transmite contexto).
Identity	Identidad	Individuos, organizaciones o grupos reales (p. ej., ACME, Inc.), así como clases de individuos, organizaciones, sistemas o grupos (p. ej., el sector financiero).
Indicator	Indicador	Contiene un patrón que puede utilizarse para detectar actividad cibernética sospechosa o maliciosa.
Infrastructure	Infraestructura	Tipo de TTP que describe sistemas, servicios de software y recursos físicos o virtuales asociados a un propósito (servidores C2, equipos de defensa, bases de datos atacadas, etc.).
Intrusion Set	Conjunto de Intrusión	Conjunto agrupado de comportamientos y recursos adversarios con propiedades comunes que se cree son orquestados por una sola organización.
Location	Ubicación	Representa una ubicación geográfica.

Malware	Software Malicioso	Tipo de TTP que representa código malicioso.
Malware Analysis	Análisis de Software Malicioso	Metadatos y resultados de un análisis estático o dinámico realizado sobre una instancia o familia de malware.
Note	Nota	Texto informativo que aporta contexto adicional o análisis complementario sobre otros Objetos STIX.
Observed Data	Data Observada	Información sobre entidades de ciberseguridad (archivos, sistemas, redes) representada mediante STIX Cyber-observable Objects (SCOs).
Opinion	Opinión	Evaluación sobre la corrección de la información contenida en un Objeto STIX, producida por una entidad diferente.
Report	Reporte	Colecciones de inteligencia de amenazas centradas en uno o más temas (descripción de un actor, malware, técnica de ataque, etc.) con su contexto y detalles relacionados.
Threat Actor	Actor de Amenaza	Individuos, grupos u organizaciones reales que

		se cree operan con intenciones maliciosas.
Tool	Herramienta	Software legítimo que puede ser utilizado por actores de amenazas para realizar ataques.
Vulnerability	Vulnerabilidad	Defecto en un software que puede ser aprovechado directamente por un atacante para acceder a un sistema o red.

7.2 STIX Relationship Objects (SROs)

STIX 2 define dos SROs que permiten conectar y enriquecer los SDOs y SCOs:

Nombre	Descripción
Relationship/Relación	Se utiliza para enlazar dos SDOs o SCOs con el fin de describir cómo se relacionan entre sí.
Sighting/avistamiento	Refleja la creencia de que algo dentro del CTI (un indicador, malware, herramienta, actor de amenaza, etc.) ha sido observado.

7.3 STIX Cyber-observable Objects SCOs (Objetos Cibernéticamente Observables)

Adicionalmente, STIX define un conjunto de SCOs que representan observables técnicos como archivos, direcciones IP, dominios, procesos, claves de registro de Windows, certificados y más. Los SCOs son la materia prima sobre la que se construyen los Indicadores y los Observed Data.

8. Estructura Técnica de STIX

Los objetos STIX 2 se representan en JSON, un formato ampliamente soportado y fácilmente procesable por máquinas. Cada objeto STIX comparte propiedades comunes como type, id (UUID), spec_version, created y modified, además de propiedades específicas a su tipo.

El siguiente es un ejemplo de un objeto Campaign en STIX 2.1:

```
{
   "type": "campaign",
   "id": "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
   "spec_version": "2.1",
   "created": "2016-04-06T20:03:00.000Z",
   "modified": "2016-04-06T20:03:23.000Z",
   "name": "Green Group Attacks Against Finance",
   "description": "Campaign by Green Group against targets in the financial services sector."
}
```

Como se aprecia, la estructura es clara, autocontenida y procesable. Múltiples objetos pueden encadenarse mediante objetos de tipo Relationship (relación) para construir un grafo completo de inteligencia que represente, por ejemplo, un actor de amenaza que utiliza una herramienta determinada para atacar a una organización en una región geográfica específica.

9. ¿Cómo Funciona el Intercambio TAXII / STIX?

El funcionamiento conjunto de STIX y TAXII puede resumirse en tres etapas: producción, transporte y consumo de inteligencia.

9.1 Producción de inteligencia (STIX)

Una organización productora (por ejemplo, un equipo SOC, un proveedor de inteligencia o un analista del ISAC) detecta una amenaza, la analiza y la representa mediante objetos STIX. Esto incluye crear los SDOs correspondientes (Indicator, Threat Actor, Malware, etc.) y conectarlos mediante Relationship Objects (Objetos de Relación).

9.2 Transporte (TAXII)

Los objetos STIX, agrupados en STIX Bundles (Paquetes STIX), se publican en una colección TAXII expuesta por el servidor del ISAC. Los miembros autenticados consumen esa colección mediante peticiones HTTPS o se suscriben a un canal para recibir nuevos objetos en tiempo real. UNISHIELD utiliza TAXII 2.1 como mecanismo recomendado para el intercambio entre los miembros del ISAC.

9.3 Consumo

La organización consumidora ingiere los objetos STIX en sus herramientas (TIP, SIEM, EDR, SOAR), donde son correlacionados con telemetría interna, generan alertas,

alimentan reglas de detección, enriquecen investigaciones y, eventualmente, generan Sightings (avistamientos) que se reincorporan al ciclo de inteligencia mediante el mismo canal TAXII.

10. Arquitectura TAXII en UNISHIELD

Una arquitectura típica TAXII en el ámbito de UNISHIELD se compone de:

- Un Servidor TAXII operado por UNISHIELD que actúa como punto central de intercambio.
- Una o más API Roots (Raíces de API) que organizan colecciones por sector, criticidad o tipo de inteligencia.
- Colecciones públicas y privadas con permisos de lectura/escritura por miembro.
- Canales de publicación/suscripción para difusión de alertas críticas.
- Clientes TAXII en cada organización miembro (TIP, SIEM o conectores propios) que consumen y publican objetos STIX.
- Mecanismos de autenticación (HTTP Basic, tokens, mTLS) y trazabilidad de los intercambios.

11. Integración con el Traffic Light Protocol (TLP)

Cada objeto STIX puede etiquetarse con marcas de manejo (Marking Definitions, Definiciones de Marcado) que reflejan la clasificación TLP definida en el Código de Conducta y Ética de UNISHIELD:

- **TLP:RED** — Información altamente sensible, compartida solo con destinatarios específicos.
- **TLP:AMBER** — Uso interno limitado dentro de la organización receptora.
- **TLP:GREEN** — Compartible dentro de la comunidad del sector.
- **TLP:CLEAR** — Información que puede hacerse pública.

De esta forma, STIX no solo transporta el contenido técnico de la amenaza, sino también las restricciones de manejo que deben respetar todos los miembros del ISAC al consumirla a través de TAXII.

12. Casos de Uso dentro de UNISHIELD

La adopción de STIX y TAXII en UNISHIELD habilita escenarios de defensa colectiva como:

- Intercambio normalizado y automatizado de Indicadores de Compromiso (IoCs) entre miembros del sector.
- Documentación estructurada de campañas y actores que afectan al sector financiero/empresarial dominicano y regional.
- Distribución coordinada de Course of Action (Cursos de Acción) ante incidentes activos vía canales TAXII.
- Generación de Sightings (avistamientos) que permiten medir la prevalencia real de una amenaza en la comunidad.
- Integración nativa con plataformas de inteligencia (TIP) y herramientas de detección y respuesta de los miembros.
- Construcción de un repositorio histórico común de inteligencia de amenazas del ecosistema.

13. Buenas Prácticas para Miembros del ISAC

- Utilizar siempre las versiones vigentes de los estándares (STIX 2.1 y TAXII 2.1) y mantenerse al tanto de futuras revisiones.
- Aplicar el TLP correcto en cada objeto compartido y respetar el principio de no atribución cuando corresponda.
- Validar los objetos STIX producidos contra el esquema oficial antes de publicarlos en TAXII.
- Enriquecer los objetos con contexto suficiente (descripción, confianza, referencias externas) para maximizar su utilidad.
- Reportar Sightings (avistamientos) cuando se observe una amenaza previamente compartida, fortaleciendo así la inteligencia colectiva.
- Configurar los clientes TAXII con autenticación y TLS, y proteger las credenciales de acceso a las colecciones.
- Mantener la confidencialidad y manejo seguro de la información conforme al Código de Conducta y Ética de UNISHIELD.

14. Recursos y Referencias

Para profundizar en STIX y TAXII, los miembros de UNISHIELD pueden consultar los siguientes recursos oficiales:

- OASIS Cyber Threat Intelligence Technical Committee — sitio oficial del comité responsable de los estándares.

- Especificación oficial de STIX 2.1 (OASIS Standard) — documento normativo del lenguaje.
- Especificación oficial de TAXII 2.1 (OASIS Standard) — documento normativo del transporte.
- Documentación de la comunidad CTI de OASIS — guías introductorias, recorridos guiados (walkthroughs) y ejemplos.
- Repositorios de ejemplos públicos de objetos y bundles STIX 2.1.

15. Conclusión

STIX y TAXII conforman la columna vertebral lingüística y de transporte de la inteligencia de ciberamenazas moderna. Su adopción dentro de UNISHIELD no es solo una decisión técnica, sino una decisión estratégica que habilita la defensa colectiva, la colaboración estructurada y la madurez del ecosistema.

Al estandarizar la forma en que los miembros del ISAC documentan y comparten amenazas, STIX y TAXII permiten que UNISHIELD cumpla su misión: fortalecer la resiliencia digital del sector mediante el intercambio seguro, oportuno y responsable de inteligencia de ciberamenazas.

— FIN DEL DOCUMENTO —