GUIA PARA EL REPORTE DE EVENTOS EN MISP

CONTENIDO

INTRODUCCIÓN 2
CREACIÓN DE EVENTOS 2
1. Crear un evento: 2
2. Usar taxonomías o etiquetas estructuradas: 3
3. Add Attribute: 4
4. Freetext import tool: 5
5. Add Attachment(s): 6
6. Publish events: 7
USO DE EVENTOS 7
1. Visualización de eventos: 7
2. Descarga de eventos: 8
ANEXO 1 CATEGORÍAS DISPONIBLES 10

GUIA PARA EL REPORTE DE EVENTOS EN MISP

INTRODUCCIÓN

El software MISP (Open Source Threat Intelligence and Sharing Platform) facilita el intercambio y el intercambio de inteligencia de amenazas, indicadores de compromiso (IoC) sobre malware y ataques dirigidos, fraude financiero o cualquier inteligencia dentro de su comunidad de miembros de confianza. El intercambio de MISP es un modelo distribuido que contiene información técnica y no técnica que se puede compartir dentro de comunidades cerradas, semiprivadas o abiertas. El intercambio de dicha información debería resultar en una detección más rápida de ataques dirigidos y mejorar la tasa de detección, al mismo tiempo que reduce la cantidad de falsos positivos.

CREACIÓN DE EVENTOS

Para realizar la creación de los eventos en la instancia MISP del CSIRT0 del sector eléctrico, se debe proceder de la siguiente manera:

1. **Crear un evento:**
   Para crear un evento en MISP, siga las instrucciones que se detallan a continuación: En la creación del evento, en la opción AddEvent, se pide rellenar la siguiente información:
   - Date: Indica la fecha en la que ha sucedido el incidente.
   - Distribution: Este parámetro define quién podrá visualizar el evento una vez que se publique. En nuestro caso se publicará con la opción “Your organization only”.
   - Threatlevel: Contempla 4 niveles:
     a. Alta: APTs sofisticados o Zero-days
     b. Medio: Amenazas avanzadas persistentes (APT).
     c. Bajo: Códigos dañinos (Malware) común.
     d. Undefined: Familia de malware desconocida o no definida.
   - Analysis: Indica el estado de análisis del evento: inicial, en progreso o completado.
   - Event Info: Una breve y concisa descripción del evento.
   - Extends Event: Permite relacionar otros eventos que ya existan en la plataforma. Se puede dejar en blanco.

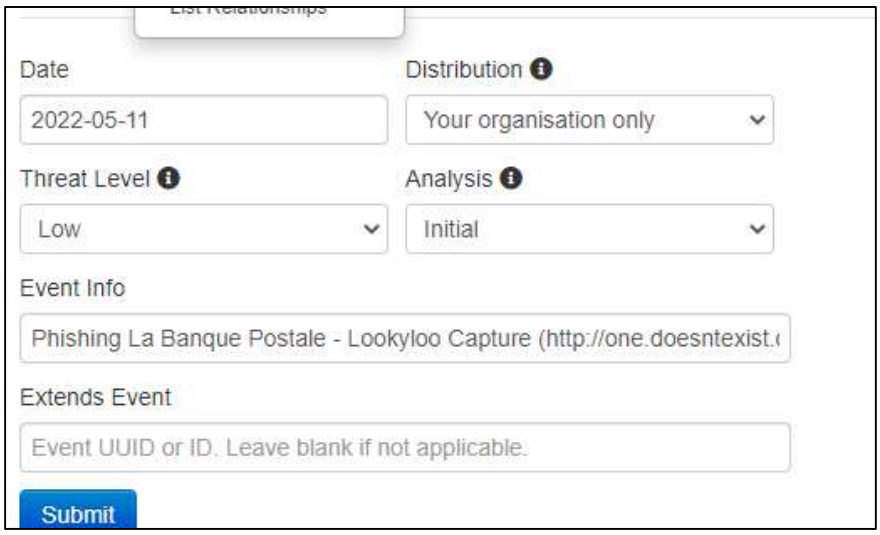

Imagen 1. Crear nuevo evento en MISP

Una vez creado el evento se accede a la vista de este, igual que si se visualizara cualquier otro evento del sistema. A través del panel de la izquierda se podrán realizar acciones sobre el evento:

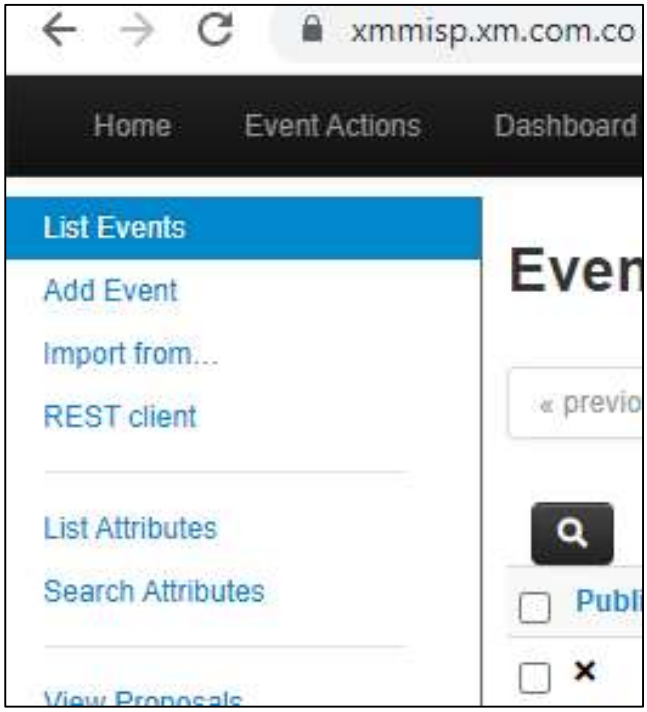

Imagen 2. Acciones sobre el evento

2. **Usar taxonomías o etiquetas estructuradas:**
   Se recomienda utilizar taxonomías o etiquetas estructuradas en vez de etiquetas simples de texto. Las taxonomías sólo deben ser usadas para describir datos y no como una marca de nivel de clasificación de información.

Para el CSIRT0 se usa la taxonomía del ColCERT, que está alineada con la taxonomía del CSIRT Américas y la del TLP (Traffic Light Protocol) para clasificar la información:

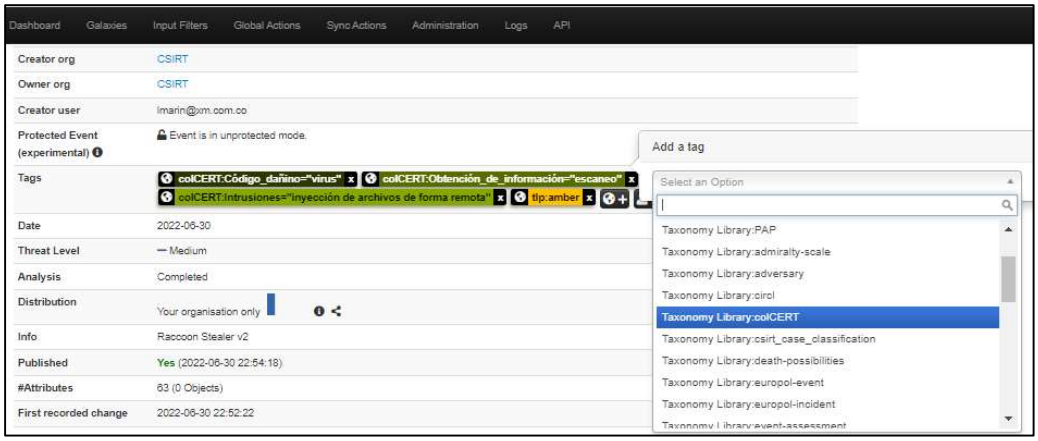

Imagen 3. Agregar taxonomías al evento

3. **Add Attribute:**

El siguiente paso tras la creación de un evento es la inclusión de atributos. Se puede realizar de forma manual o a través de formatos conocidos como freetext import, populateusing a template, OpenIOC import y threatConnect Import CSV. Mediante el botón Add Atribute se pueden añadir atributos al evento.

Imagen 4. Agregar atributos al evento

- Category: Este desplegable define la categoría del atributo indicando qué aspecto del evento se está describiendo. Puede ver en detalle el significado de cada **categoría en el Anexo I.**
- Type: Mientras que las categorías determinan qué aspecto de un evento se está describiendo, el type explica concretamente qué se está describiendo. Como ejemplo, una dirección IP origen de un ataque, una dirección de email o un fichero enviado a través de un adjunto pueden pertenecer a la categoría payloaddelivery si son métodos utilizados para la distribución de un código dañino.
- Distribution: Visibilidad que se le asigna al atributo. Siempre prevalecerá la distribución asignada al evento si ésta es más restrictiva. La visibilidadInheritEvent, permite heredar al atributo la visibilidad asignada al evento.
- Value: El valor asignado al atributo.
- Contextual Comment: Permite añadir un comentario al atributo.
- ForIntrusionDetectionSystem: Esta opción permite al atributo ser usado en una regla de IDS cuando se exporta como reglas NIDS (Snort, Suricata y Bro).
- BatchImport: Si hay varios atributos del mismo tipo, se pueden incluir todos de una vez separados por filas para que el sistema genere un atributo por cada valor insertado.
- First seen (Date-Time) y Last seen (Date-Time): Detalle de la primera y ultima vez que se detecta comportamiento del atributo.

4. **Freetext import tool:**
   Permite añadir una lista de atributos en texto plano. Para hacerlo, basta con dar clic en el icono "**Populate using the freetext import tool**":

Imagen 5. Acceder a Freetext import tool

Para ello sólo requiere copiar y pegar los IOCs que tenga en un archivo de texto y dar clic en "**Submit**":

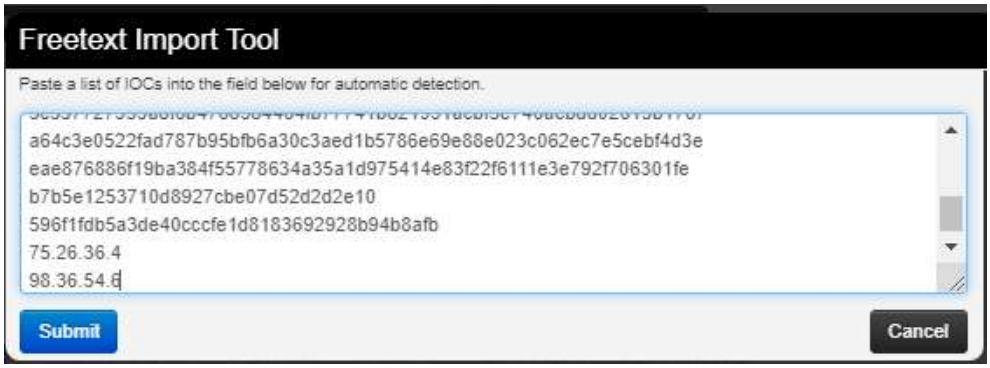

Imagen 6. Agregar IOCs de forma masiva

Ello realizará una precarga de los IOCs clasificándolos por categoría, tipo y distribución, permitiendo realizar una actualización de todos los comentarios:

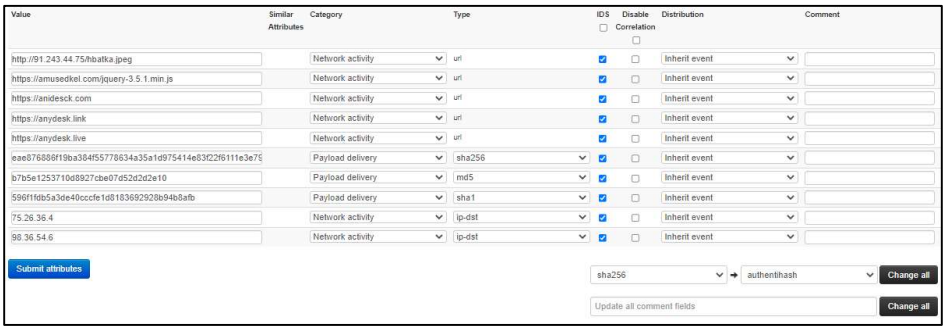

Imagen 7. Carga de IOCs de manera masiva

5. **Add Attachment(s):**

Se pueden añadir adjuntos a un evento como, por ejemplo, evidencias del incidente, documentos con análisis externos relacionados, artefactos generados por un código dañino o, incluso, el propio código dañino. Los campos que se tienen que rellenar son:

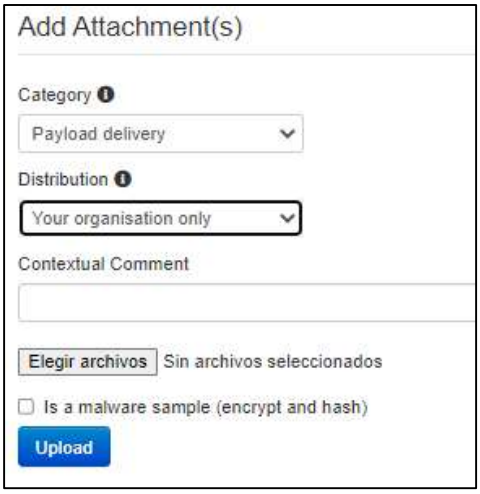

Imagen 8. Agregar adjunto

- Category: Este desplegable define la categoría del atributo indicando qué aspecto del evento se está describiendo. Puede ver en detalle el significado de cada categoría en el Anexo I.
- Distribution: Visibilidad que se le da al atributo. Siempre prevalecerá la distribución asignada al evento si ésta es más restrictiva.
- Contextual Comment: Permite añadir un comentario al atributo.
- Examine: Abre un cuadro de diálogo para subir el fichero.
- CheckBox: Esta casilla indica si el fichero debe marcarse como código dañino o no. Si se trata de código dañino comprime el fichero y le asigna una contraseña para evitar que accidentalmente un usuario pueda ejecutar el fichero e infectarse. Además extraerá los hashes MD519 SHA120 y SHA256.

6. **Publish events:**
   El último paso es la publicación de eventos. Una vez que todos los atributos y adjuntos están subidos, se puede publicar el evento pulsando el botón Publish. Esta acción alertará a los usuarios y propagará el evento a instancias conectadas.

Imagen 9. Publicar evento

USO DE EVENTOS

Una de las principales funcionalidades de MISP además de poder compartir información de amenazas y vulnerabildiades, es la posibilidad de descargar la información y poder usarla en los equipos de seguridad que tenga en la organización, para lo cual me permite visualizar los eventos y descargar los IOCs que tenga relacionados.

1. **Visualización de eventos:**
   En la pantalla del listado de eventos (ListEvents) se puede acceder a cada evento pulsando en su identificador único, Id, que mostrará la información del evento:

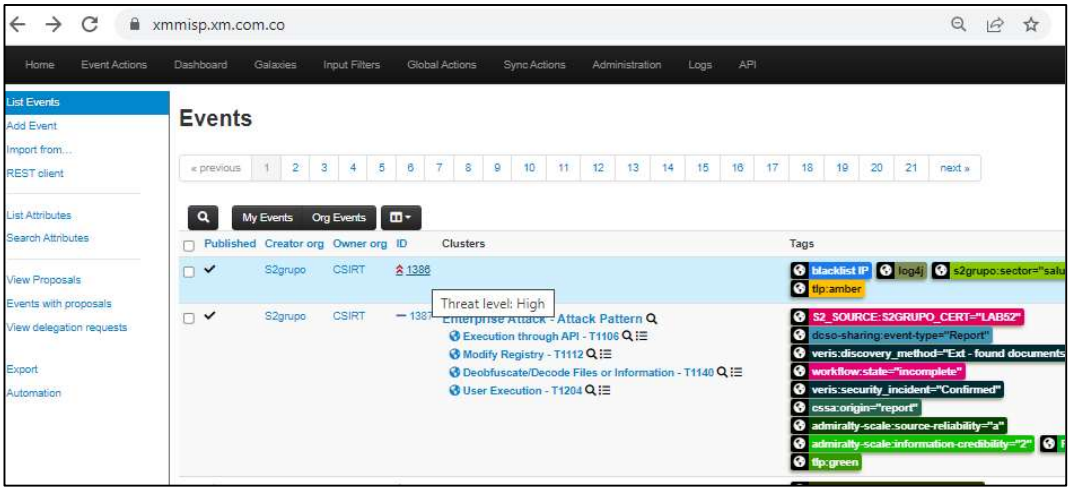

Imagen 10. Lista de eventos

2. **Descarga de eventos:**
   Al dar clic en el ID del evento, se muestra todo el detalle del evento, permitiendo descargar los IOCs dando clic en el enlace "**Download as..**" del panel izquierdo:

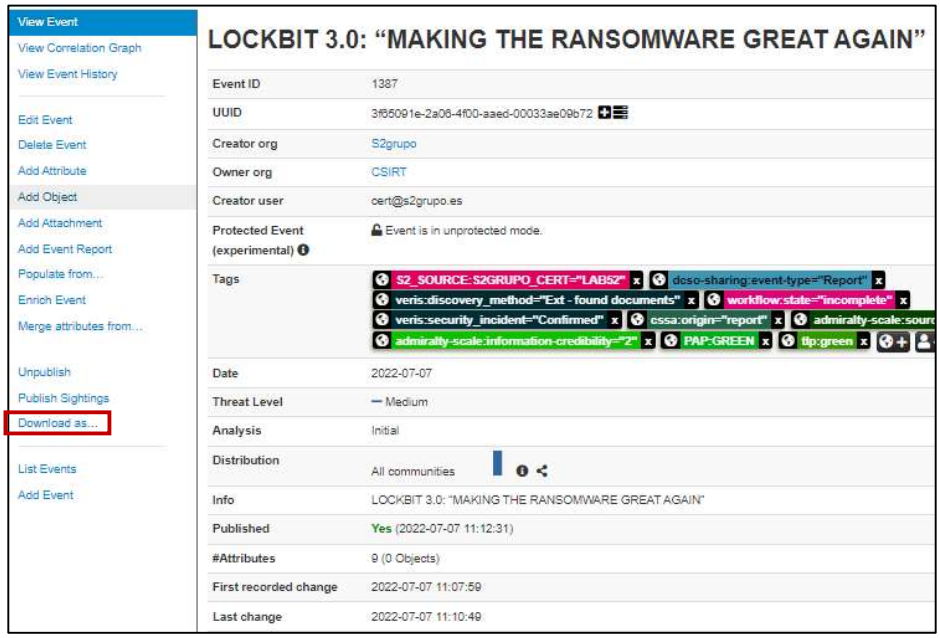

Imagen 11. Descarga de eventos

Download as: Permite la descarga del evento en diversos formatos como CSV, STIX, XML o JSON, PDF, entre otros:

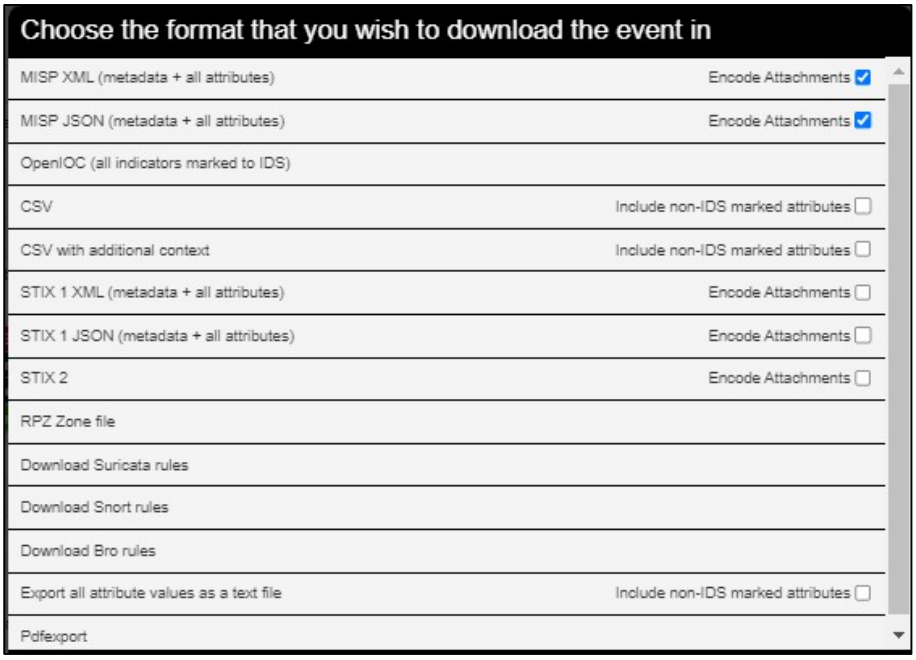

Imagen 12. Formatos de descarga de eventos

ANEXO 1 CATEGORÍAS DISPONIBLES

La siguiente tabla muestra las categorías a las pueden pertenecer los atributos:

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, las direcciones IP origen, etcétera. La muestra del código dañino debería adjuntarse aquí.
Artifacts dropped	Cualquier artefacto (archivos, claves de registro, registros de actividad, herramientas, etcétera) generado por la actividad del código dañino u otras modificaciones al sistema
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, etcétera
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 PoisonIvy o Darkomet, etcétera.
Attribution	Identificación del grupo, organización o país detrás del ataque.
External analysis	Cualquier otro resultado de un análisis adicional del código malicioso, como por ejemplo las salidas de herramientas (salida de analizador de documentos PDF, de entornos de análisis dinámico de código dañino, informes de ingeniería inversa del código dañino, etcétera.)
Financial Fraud	Información relativa a fraude financiero, como cuentas de BitCoin, identificadores bancarios IBAN, BIC o BIN.
Other	Atributos que no son parte de cualquier otra categoría