CIRCL / Team MISP Project

MISP Project
https://www.misp-project.org/

CIISI-IE Dublin 2024

MISP
Threat Sharing

MISP, comenzando desde un caso práctico

- Durante un taller de análisis de malware en 2012, descubrimos que habíamos estado trabajando analizando el mismo malware.
- Quisimos compartir información de forma fácil y automatizada para así **evitar la duplicación de trabajo**.
- Christophe Vandeplas (trabajando en el CERT del MINDEF Belga en aquel entonces) nos mostró su trabajo en una plataforma que luego se convertiría en MISP.
- Una primera versión de MISP fue utilizada por el MALWG y **los comentarios de los usuarios** nos ayudaron a realizar mejoras en la plataforma.
- Actualmente MISP es **un desarrollo impulsado por la comunidad**.

Acerca de CIRCL

El Centro de Respuesta ante Emergencias Informáticas de Luxemburgo (CIRCL) es una iniciativa impulsada por el gobierno, diseñada para proveer una respuesta sistemática a incidentes y amenazas de seguridad informática.

CIRCL es el CERT del sector privado, municipios y entidades no gubernamentales en Luxemburgo y es operado por LHC g.i.e.

MISP y CIRCL

- CIRCL es conducido por el Ministerio de Economía y actúa como el CERT Nacional para el sector privado.
- CIRCL lidera el desarrollo de MISP, la plataforma de código abierto de inteligencia de amenazas, que es utilizada por muchas comunidades militares o de inteligencia, empresas privadas, sector financiero, CERTs nacionales y fuerzas de seguridad (LEAs) en todo el mundo.
- **CIRCL opera múltiples comunidades de MISP, que a diario comparten información de inteligencia de amenazas (threat-intelligence)**.

Co-financed by the European Union
Connecting Europe Facility

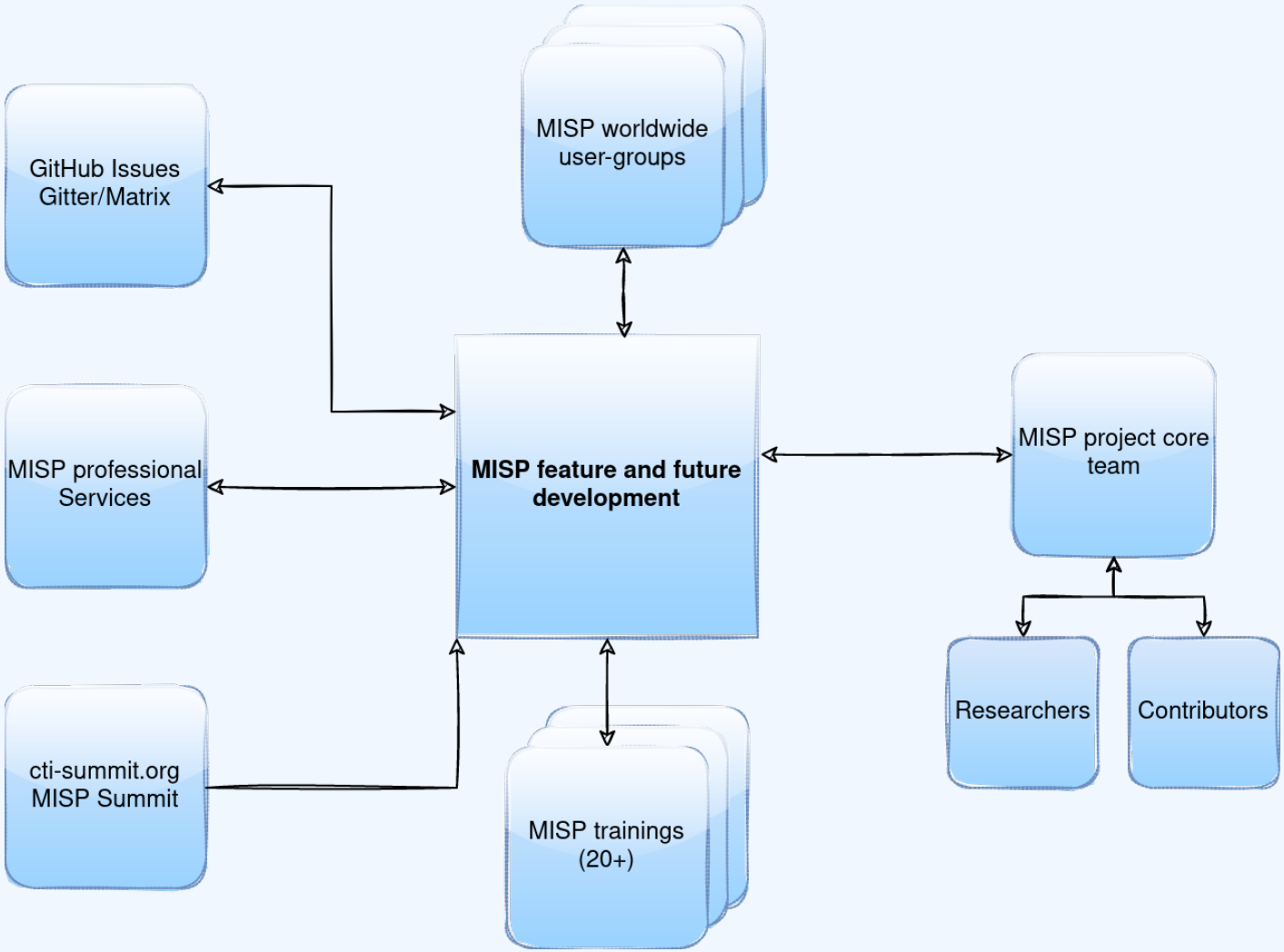
¿Qué es MISP?

- MISP es una plataforma libre y de código abierto para el **intercambio de información de amenazas**.
- Es una herramienta que **recolecta** información proveniente de diferentes participantes, sus analistas, sus herramientas, fuentes de inteligencia, etc.
- Normaliza, **correlaciona** y **enriquece** la información.
- Permite **colaborar** a los diferentes equipos y comunidades.
- **Alimenta** las herramientas de seguridad y de los analistas con sus resultados.

Desarrollo basado en comentarios de los usuarios

- Existen muchos diferentes tipos de usuarios de plataformas de intercambio de información como MISP:
  - **Analistas de Malware** dispuestos a compartir indicadores de compromiso con sus respectivos colegas.
  - **Analistas de Seguridad** buscando, validando y utilizando indicadores en seguridad operacional.
  - **Analistas de Inteligencia** recopilando información acerca de ciertos grupos de adversarios.
  - **Fuerzas de Seguridad** utilizando indicadores para dar soporte a casos de análisis forense digital (DFIR).
  - **Equipos de Análisis de Riesgos** dispuestos a saber más sobre nuevas amenazas, probabilidades e incidencias.
  - **Analistas de Fraude** dispuestos a compartir indicadores financieros para detectar fraudes.

Modelo de gobernabilidad de MISP



Múltiples objetivos según diferentes grupos de usuarios

- Compartiendo indicadores para la **detección**.
  - '¿Existen sistemas infectados en mi infraestructura o en las redes que opero?'
- Compartiendo indicadores para **bloquear**.
  - 'Utilizo estos indicadores para bloquear el acceso o redireccionar el tráfico.'
- Compartiendo indicadores para **realizar actividades de inteligencia**.
  - 'Recopilando información acerca de campañas y ataques. ¿Están relacionados? ¿Quién me tiene como objetivo? ¿Quiénes son los adversarios?'
- $\rightarrow$ Estos objetivos pueden ser contradictorios (p. ej. Los falsos-positivos tienen diferentes impactos)

Comunidades utilizando MISP

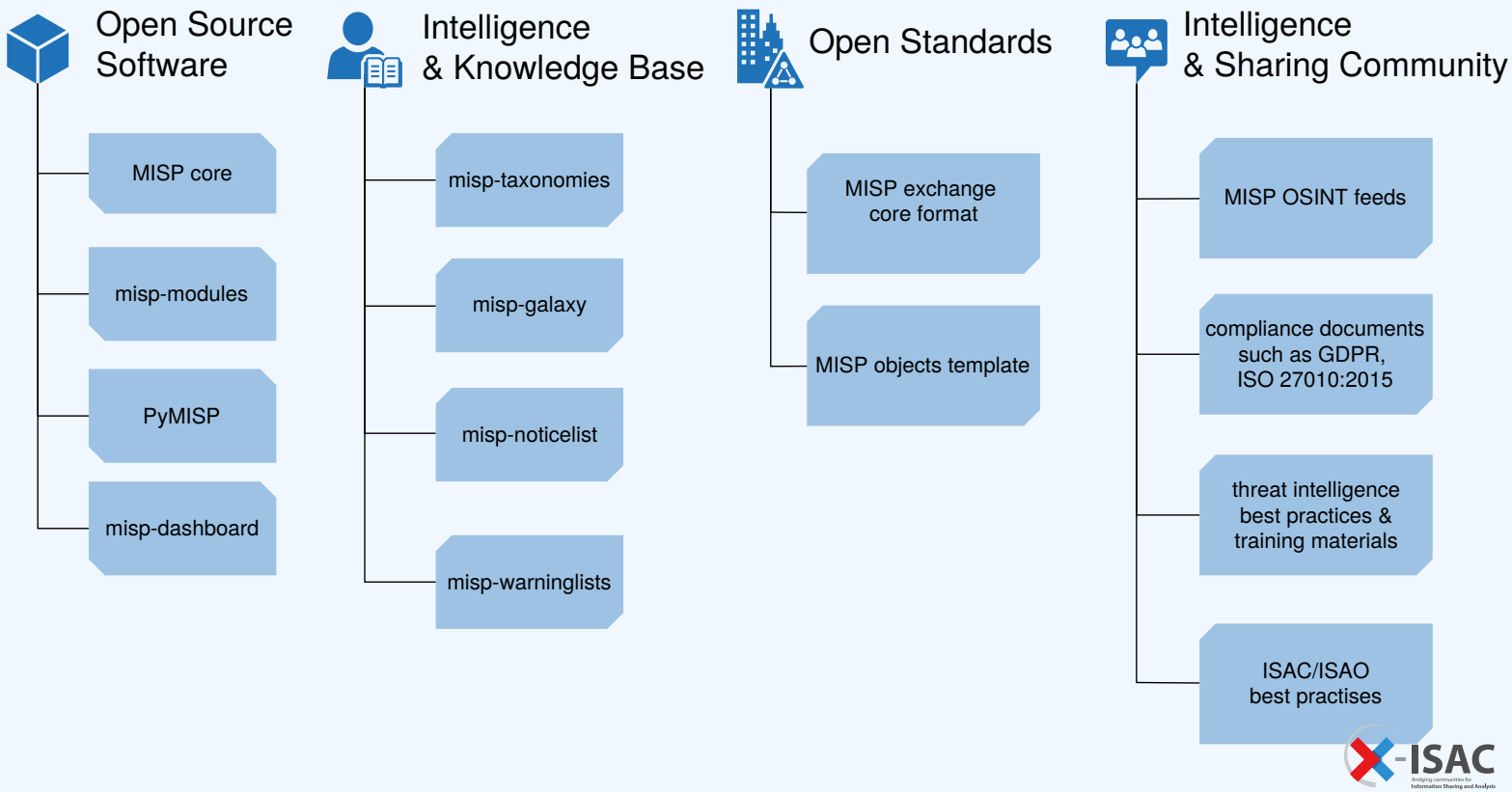
- Las comunidades son grupos de usuarios que comparten un conjunto objetivos o valores comunes.
- CIRCL opera múltiples instancias de MISP con una gran cantidad de usuarios (más de 1200 organizaciones con más de 4000 usuarios).
- **Grupos de confianza** operando comunidades de MISP en modo aislado (air-gapped) o parcialmente conectados.
- **Sector financiero** (bancos, Centros de Análisis e Intercambio de Información (ISACs), organizaciones de procesamiento de pagos) utilizan MISP como mecanismo de intercambio.
- **Organizaciones internacionales y militares** OTAN, CSIRTs militares, CERTs, ...
- **Proveedores de Seguridad** operando sus propias comunidades o interconectados con otras comunidades.
- **Comunidades temáticas** creadas para abordar problemáticas específicas (COVID-19 MISP)

Las dificultades de compartir información

- Las dificultades de compartir información no suelen ser problemas de índole tecnológico, en general se deben a las **interacciones sociales** (p. ej. **confianza**).
- Restricciones legales[1]
  - "Nuestro marco legal no nos permite compartir información."
  - "El riesgo de filtraciones de información es muy alto y riesgoso para nuestra organización y nuestros socios."
- Restricciones prácticas
  - "No tenemos información para compartir."
  - "No tenemos tiempo para procesar o contribuir con indicadores."
  - "Nuestro modelo de clasificación no se ajusta al modelo de MISP."
  - "Las herramientas para intercambio de información están asociadas a un formato específico, nosotros utilizamos otro."

[1] https://www.misp-project.org/compliance/

Vista general del Proyecto MISP



Compartiendo en MISP

- Compartiendo vía listas de distribución - **Grupos de intercambio** (sharing groups)
- **Delegación** para intercambio de información pseudo-anonimizada
- **Propuestas** y **Eventos extendidos** para compartir información en forma colaborativa
- Sincronización, Fuentes (feeds), intercambio aislado (air-gapped)
- **Filtros de intercambio** definidos por el usuario para todos los métodos mencionados anteriormente
- **Almacenamiento en caché** para búsquedas rápidas en grandes volúmenes de datos
- Soporte de múltiples instancias de MISP para enclaves internas

Gestión de la calidad de la Información

- Información correlacionada
- Ciclo de retroalimentación de detecciones vía **Avistamientos** (Sightings)
- **Gestión de falsos positivos** vía el sistema de alertas (warninglists)
- Sistema de **enriquecimiento** vía MISP-modules
- Sistema de **flujos de trabajo** para revisar y controlar la información que se publica
- **Integraciones** con un gran número de herramientas y formatos
- **API** flexible y soporte de **librerías** tales como PyMISP para facilitar la integración
- **Líneas de tiempo** (timelines) para dotar a la información de un marco temporal
- Cadena completa de la **gestión del ciclo de vida de indicadores**

Conclusión

- **Las prácticas de intercambio de información vienen con su uso** y con el ejemplo (p. ej. aprender mediante la imitación de la información compartida).
- MISP es sólo una herramienta. Lo que importa son sus prácticas de intercambio. La herramienta debería darle soporte de la manera más transparente posible.
- Permitir a los usuarios customizar MISP para satisfacer las necesidad de los casos de uso de su comunidad.
- El proyecto MISP combina código abierto, estándares abiertos, mejores prácticas y comunidades para convertir el intercambio de información en una realidad.