MISP

INTELLIGENCE SHARING

Compartir información con MISP

Introducción a una colaboración útil y de confianza

MISP Project / CIRCL

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

Referencia: 3 de noviembre de 2026

Qué podrá explicar al terminar

- Qué se comparte con MISP y por qué importa el contexto.
- Cómo elegir los destinatarios y una respuesta útil.
- Cómo los comentarios mejoran la información compartida.

Empezar con una pregunta común

- El equipo A investiga un mensaje de acceso sospechoso.
- Registra `login-support.example` y `192.0.2.25`.
- El equipo B ha visto el mismo dominio en otro informe.
- ¿Qué pueden aprender juntos y qué sigue siendo incierto?

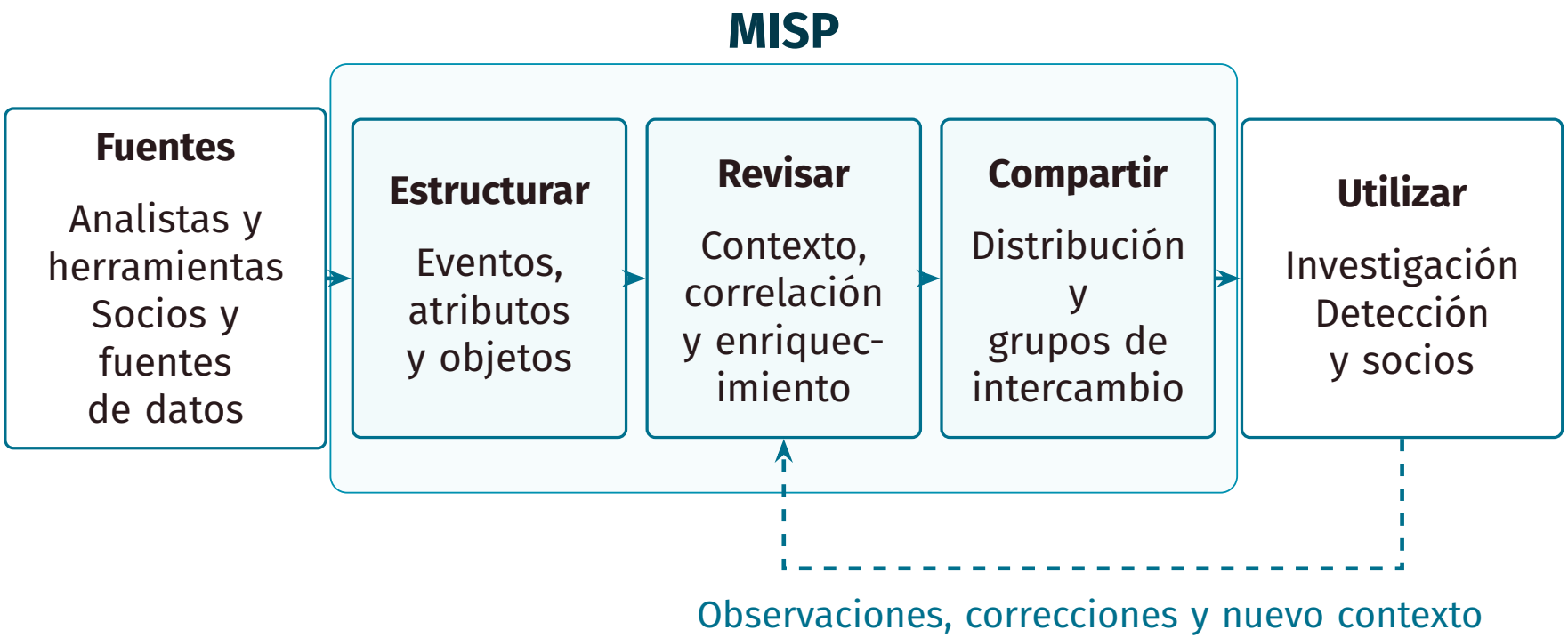
MISP permite reutilizar las observaciones

- Plataforma de código abierto para compartir información estructurada.
- Un lugar para recopilar, relacionar y revisar información de amenazas.
- Una forma de colaboración entre personas, herramientas y equipos.
- Contexto para investigar, detectar y responder.

Conservar la observación junto con su contexto

- Evento: contexto del informe o de la investigación.
- Atributo: una observación tipificada, como un dominio.
- Objeto: atributos relacionados agrupados por una plantilla.
- Etiquetas y Galaxias: clasificación y contexto estructurado.

De las observaciones al contexto compartido



Una correlación es una pista que investigar

- Un valor común puede relacionar informes que conviene comparar.
- Revise la fuente, las fechas y las observaciones relacionadas.
- Considere infraestructura compartida, reutilización y falsos positivos.
- Una coincidencia no demuestra causalidad ni atribución.

Elegir la acción antes que la salida

- Investigar: usar el contexto para formular mejores preguntas.
- Detectar o buscar: localizar observaciones relevantes en sus datos.
- Bloquear: aplicar una política revisada con un impacto aceptable.

Elegir quién puede recibir la información

- Configure la distribución y los grupos de intercambio.
- Revise evento, atributos y destinatarios previstos.
- Utilice etiquetas como TLP junto con controles de acceso.
- Revise publicación y configuración antes del intercambio.

La calidad mejora mediante los comentarios

- Registre procedencia, confianza y contexto temporal útil.
- Revise listas de advertencia y enriquecimientos.
- Aporte observaciones, correcciones y falsos positivos.
- Reevalúe la información antigua y su uso previsto.

Una comunidad necesita acuerdos de trabajo

- Acordar propósito, participantes y aportaciones esperadas.
- Definir prácticas de tratamiento, revisión y corrección.
- Empezar con un grupo pequeño y contenido útil.
- Conectar otras comunidades cuando la política lo permita.

Convertir los obstáculos en un primer paso

Obstáculo	Primer paso útil
Poco tiempo	Compartir una observación pequeña y estructurada con su fuente.
Incertidumbre	Explicar qué se sabe, qué no y qué puede corregirse.
Herramientas distintas	Acordar términos y utilizar formatos de intercambio compatibles.
Obligaciones	Revisar propósito, destinatarios y política aplicable con los responsables.

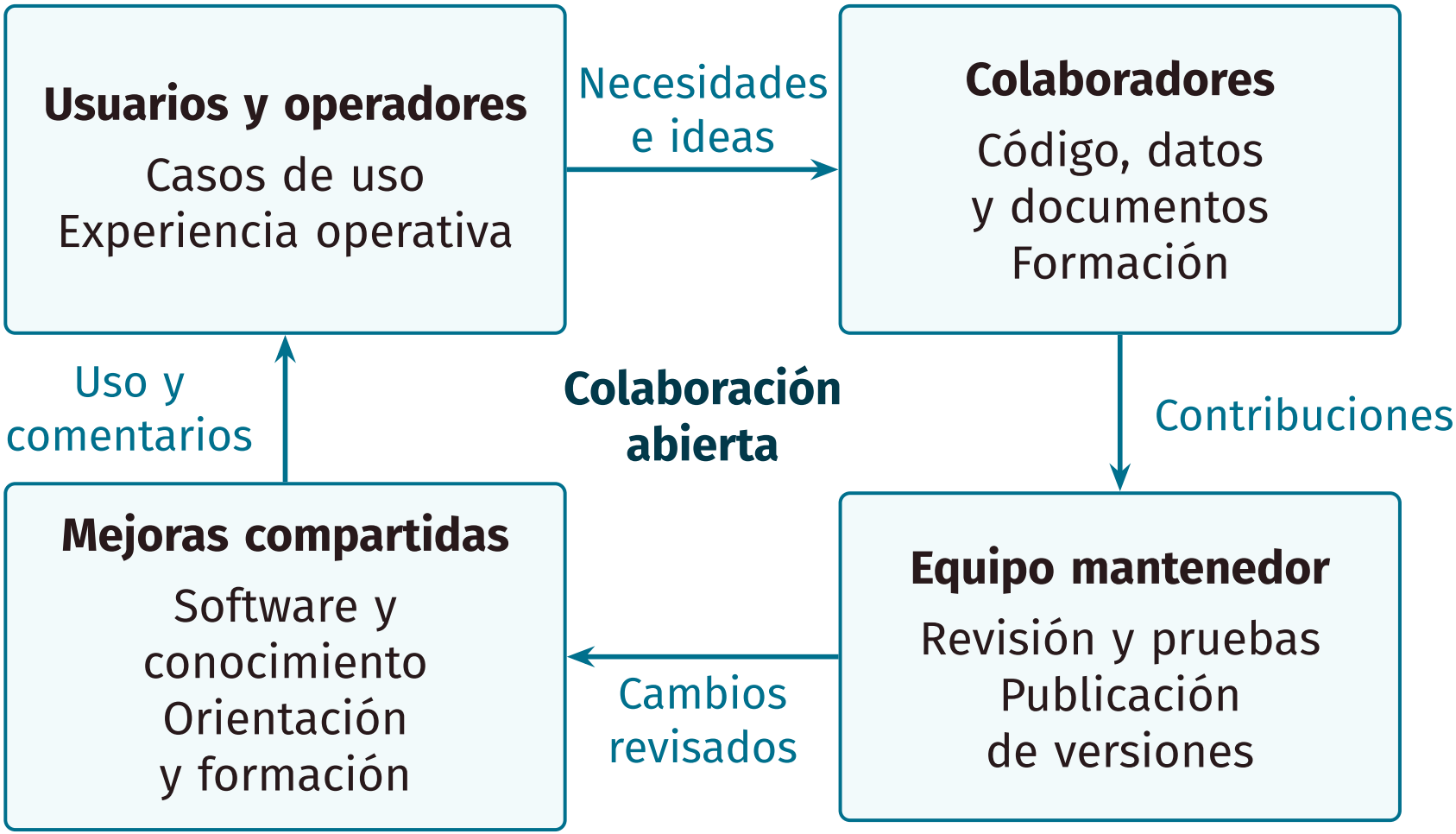
El proyecto nació de una necesidad práctica

- Analistas de malware querían evitar trabajo duplicado.
- La plataforma creció gracias a la experiencia de sus usuarios.
- CIRCL y una comunidad más amplia desarrollan y mejoran MISP.
- Se puede contribuir con código, conocimiento y formación.

El proyecto MISP va más allá de una aplicación

Software	Conocimiento	Estándares	Comunidades
Plataforma MISP API REST y PyMISP misp-modules	Taxonomías Galaxias Listas de advertencia	Formatos de datos Vocabularios Plantillas de objetos	Socios de confianza Prácticas compartidas Formación y comentarios

La comunidad da forma a MISP



Primer ejercicio: explicar un registro útil

1. Preparar un evento privado y sin publicar para el caso ficticio.
2. Añadir dominio e IP con fuente, fecha e incertidumbre.
3. Explicar una posible correlación y una acción adecuada.
4. Revisar destinatarios y tratamiento antes de publicar.

Continuar con el tema que necesite

- Análisis diario: uso de MISP y etiquetado.
- Más contexto: objetos, Galaxias y calidad de información.
- Integración: talleres de API REST y PyMISP.
- Operación de comunidades: administración y buenas prácticas.

Compartir contexto útil y seguir mejorándolo

- Estructurar la observación y conservar su significado.
- Elegir conscientemente la audiencia y la acción.
- Usar los comentarios para mejorar calidad y comprensión.