Si estamos buscando implementar alguna solución OpenSource para Cyber Threat Intelligence, debemos saber que hay varios proyectos disponibles:

OpenCTI

Es una plataforma completa de inteligencia de amenazas orientada a construir una base de conocimiento centralizada. Permite almacenar y relacionar actores, campañas, malware, vulnerabilidades, IOC, TTP, informes y otras entidades mediante STIX 2.1. Su punto fuerte es representar toda esa información como un grafo de relaciones y conectarse con fuentes como MISP, MITRE ATT&CK y feeds externos.

Proyecto de GitHub: https://github.com/opencti-platform/opencti

MISP

Está especialmente orientada a recopilar, correlacionar y compartir inteligencia de amenazas entre organizaciones. Trabaja con eventos, indicadores, atributos, objetos, taxonomías y galaxias, y se utiliza mucho entre SOC, CERT, CSIRT y comunidades de intercambio de inteligencia. Es particularmente fuerte para compartir IOC como direcciones IP, dominios, URLs, hashes y otros indicadores.

Proyecto de GitHub: https://github.com/MISP/MISP

Yeti

Es una plataforma que combina inteligencia de amenazas con capacidades orientadas a DFIR. Permite almacenar observables, actores, campañas, malware y TTP y relacionarlos entre sí para investigar rápidamente si un dominio, IP, hash u otro artefacto ya ha aparecido anteriormente y con qué amenazas está relacionado. Está especialmente pensada para facilitar investigaciones y análisis técnicos.

Proyecto de GitHub: https://github.com/yeti-platform/yeti

IntelOwl

Es una plataforma de automatización y enriquecimiento de inteligencia. Su función principal consiste en recibir un observable, como una IP, dominio, URL, hash o fichero, y analizarlo automáticamente utilizando múltiples servicios y herramientas. Puede consultar fuentes externas como VirusTotal o AbuseIPDB y ejecutar analizadores locales, reduciendo considerablemente el trabajo manual de un analista.

Proyecto de GitHub: https://github.com/intelowlproject/IntelOwl

Cerebrate

Es una plataforma centrada en gestionar comunidades, organizaciones y relaciones de confianza dentro de ecosistemas de intercambio de inteligencia. Está especialmente relacionada con MISP y permite administrar organizaciones, usuarios, contactos, claves criptográficas y conexiones entre distintas instancias. Su función no es tanto analizar amenazas como gestionar quién puede intercambiar inteligencia con quién.

Proyecto de GitHub: https://github.com/cerebrate-project/cerebrate

ThreatBus

Es una plataforma de distribución de inteligencia de amenazas en tiempo real. Funciona como una capa de mensajería que permite que diferentes herramientas publiquen y consuman indicadores y observaciones. Por ejemplo, puede utilizarse para hacer llegar indicadores procedentes de una plataforma CTI a herramientas de detección como Zeek, o para devolver sightings y observaciones desde los sensores hacia los sistemas de inteligencia.

Proyecto de GitHub: https://github.com/tenzir/threatbus

EXTRA

ATT&CK Workbench

No es una plataforma CTI tradicional, sino una base de conocimiento y un framework para describir el comportamiento de los atacantes. Organiza sus técnicas mediante tácticas, técnicas y sub-técnicas que representan las distintas fases y acciones de un ataque. Se utiliza como lenguaje común para relacionar inteligencia de amenazas, detecciones, threat hunting, controles de seguridad y actividad de grupos de amenazas.

Proyectos de Github (tiene varios, pero para una instalación estándar, estos 4):

- https://github.com/mitre-attack/attack-workbench-deployment
- https://github.com/mitre-attack/attack-workbench-frontend
- https://github.com/mitre-attack/attack-workbench-rest-api
- https://github.com/mitre-attack/attack-data-model