Threat Intelligence

1. MISP
• Plataforma de referencia para compartir indicadores de compromiso.
• Útil para consultar campañas activas y correlacionar eventos.
• Muy usada por CERTs y SOCs por su enfoque colaborativo.

2. OpenCTI
• Ofrece una visión completa de actores, TTPs, campañas y relaciones.
• Permite trabajar TI estratégica, táctica y operacional.
• Integraciones sólidas como MITRE ATT&CK y MISP para mayor contexto.

3. VirusTotal (versión gratuita)
• Ideal para reputación de archivos, URLs y dominios.
• Amplia base comunitaria con histórico de muestras.
• Su velocidad la convierte en una herramienta clave para análisis rápidos.

4. AlienVault OTX
• Comunidad global compartiendo pulses e indicadores listos para usar.
• Permite detectar campañas activas sin procesos complejos.
• Muy útil para mantenerse actualizado con fuentes diversas.

5. AbuseIPDB
• Especializada en reputación de direcciones IP.
• Perfecta para validar actividad maliciosa y generar bloqueos.
• Útil para reglas de firewall, SIEM y automatizaciones.

6. ThreatFox (abuse.ch)
• Centrada en IOCs de malware activo, botnets y amenazas emergentes.
• Indicadores renovados constantemente.
• Ideal para análisis de conectividad sospechosa.

7. Pulsedive
• Plataforma rápida para evaluar riesgo de dominios e IPs.
• Recopila información de múltiples fuentes.
• Ofrece una clasificación sencilla para análisis iniciales.

1. MISP (Malware Information Sharing Platform)

Aspecto	Explicación de Uso
Uso Principal	**Intercambio y correlación de Indicadores de Compromiso (IOCs).** Los analistas lo usan para estructurar, enriquecer y compartir datos sobre amenazas (direcciones IP, hashes, dominios) dentro de una comunidad de confianza (CERTs, SOCs).
Escenarios Comunes	1. **Creación de Eventos:** Un SOC detecta un ataque, crea un "Evento" en MISP, y adjunta todos los IOCs, tácticas y atribuciones. 2. **Correlación:** Los sistemas automatizados cotejan los IOCs recibidos de otros miembros con los registros locales para detectar un compromiso ya conocido. 3. **Taxonomías:** Utiliza taxonomías estandarizadas para clasificar la amenaza (ej: tipo de malware, sector afectado).
Ventaja Clave	Su enfoque en la estructuración de datos lo hace ideal para la **automatización** (alimentar SIEMs, *firewalls* y EDRs) y la **colaboración** entre entidades.
Enlace Oficial	https://www.misp-project.org/

2. OpenCTI (Open Cyber Threat Intelligence)

Aspecto	Explicación de Uso
Uso Principal	**Centralizar y mapear el conocimiento de TI.** Es una plataforma de gestión de TI que va más allá de los IOCs, enfocándose en las relaciones entre todos los elementos de una amenaza.
Escenarios Comunes	1. **Mapeo Estratégico:** Mapear un actor de amenaza (ej: APT28) con las Tácticas, Técnicas y Procedimientos (TTPs) que utiliza (integración con MITRE ATT&CK). 2. **Análisis de Campañas:** Visualizar

Aspecto	Explicación de Uso
	las relaciones entre múltiples eventos de MISP, los IOCs asociados, y el *malware* utilizado para entender la campaña completa. 3. **Visualización Gráfica:** Permite crear gráficos de conocimiento para entender el panorama de amenazas (TI estratégica y táctica).
Ventaja Clave	Capacidad para gestionar la **TI en sus tres niveles** (estratégica, táctica y operacional) mediante la visualización de relaciones complejas.
Enlace Oficial	https://www.opencti.io/

3. VirusTotal (versión gratuita)

Aspecto	Explicación de Uso
Uso Principal	**Análisis de reputación y multifacético de archivos, URLs, dominios y direcciones IP.** Ofrece un análisis por múltiples motores de antivirus y servicios de *sandboxing*.
Escenarios Comunes	1. **Análisis de Archivos:** Subir un archivo sospechoso (ej: un adjunto de correo) para ver el veredicto de 70+ motores antivirus y extraer los metadatos y *hashes* asociados. 2. **Reputación Rápida:** Ingresar una URL o IP sospechosa para verificar si ha sido reportada por alguna fuente o si está clasificada como maliciosa. 3. **Buscar y Correlacionar:** Usar *hashes* (MD5, SHA256) o *ja3 hashes* para encontrar muestras relacionadas y su histórico de detección.
Ventaja Clave	Su **velocidad** y la **gran cantidad de fuentes** (antivirus, comunidad, histórico) lo hacen esencial para las primeras etapas de cualquier análisis.
Enlace Oficial	https://www.virustotal.com/

4. AlienVault OTX (Open Threat Exchange)

Aspecto	Explicación de Uso
Uso Principal	**Intercambio global de indicadores de compromiso (IOCs) basado en la comunidad (Pulses).** Permite a los usuarios recibir y compartir información de amenazas en tiempo real.
Escenarios Comunes	1. **Suscripción a Pulses:** Suscribirse a los *Pulses* (paquetes de información de amenazas) creados por la comunidad o por AlienVault, recibiendo IOCs actualizados (IPs, dominios) de campañas específicas. 2. **Integración SIEM:** Los sistemas de seguridad pueden ingerir automáticamente estos *Pulses* para bloquear indicadores en el *firewall* o generar alertas de correlación en el SIEM. 3. **Consulta Rápida:** Buscar un dominio o IP para ver a qué *Pulse* pertenece y qué actores de amenaza lo están utilizando.
Ventaja Clave	La **comunidad masiva** y el formato *Pulse* simple hacen que los indicadores sean accesibles y fáciles de consumir para la defensa.
Enlace Oficial	https://otx.alienvault.com/

5. AbuseIPDB

Aspecto	Explicación de Uso
Uso Principal	**Verificar la reputación y reportar direcciones IP maliciosas.** Se centra exclusivamente en la calidad de la información sobre IPs y en el *score* de confianza de abuso.
Escenarios Comunes	1. **Investigación de Incidentes:** Ingresar la IP de un atacante para ver si tiene un historial de actividades maliciosas (ataques de fuerza bruta, *spam*, *DDoS*, *malware*). 2. **Bloqueo Preventivo:** Usar su *blacklist* (disponible vía API) para alimentar *firewalls* y sistemas de prevención de intrusiones

Aspecto	Explicación de Uso
	(IPS) con IPs de alta confianza de abuso. 3. **Reporte:** Contribuir a la comunidad reportando IPs que han atacado tu red, con detalles sobre el tipo de ataque.
Ventaja Clave	El **Abuse Confidence Score** (puntuación de confianza de abuso) ofrece una medida clara y confiable del riesgo asociado a una IP.
Enlace Oficial	https://www.abuseipdb.com/

6. ThreatFox (abuse.ch)

Aspecto	Explicación de Uso
Uso Principal	**Plataforma de inteligencia centrada en *malware* y C2s (Command & Control).** Recopila y distribuye IOCs de *botnets* y familias de *malware* activas.
Escenarios Comunes	1. **Filtrado de Tráfico Saliente:** Integrar sus *feeds* de IOCs (especialmente los dominios y las IPs de C2) en un *proxy* o *firewall* para detectar y bloquear la comunicación de un *malware* ya instalado en la red. 2. **Identificación de Malware:** Buscar una IP o un dominio sospechoso para determinar a qué familia de *malware* (ej: Emotet, Qakbot, Cobalt Strike) se asocia. 3. **Análisis de Tendencias:** Consultar los IOCs más recientes para mantenerse al día con las amenazas emergentes y sus tácticas de distribución.
Ventaja Clave	El enfoque en **C2s activos** de *malware* y la actualización constante hacen que sus indicadores sean muy valiosos para la detección en tiempo real.
Enlace Oficial	https://threatfox.abuse.ch/

7. Pulsedive

Aspecto	Explicación de Uso
Uso Principal	**Enriquecimiento y contextualización de indicadores de compromiso (IOCs).** Ofrece una clasificación de riesgo simple y recopila información de diversas fuentes en una sola interfaz.
Escenarios Comunes	1. **Triaje Inicial:** Obtener rápidamente un *score* de riesgo para una URL o IP, lo que ayuda a priorizar los indicadores durante una jornada de trabajo. 2. **Enriquecimiento de Datos:** Introducir un IOC y ver una ficha completa que incluye etiquetas, atributos, información de geolocalización, metadatos y links a fuentes externas. 3. **Agregación de Fuentes:** Se utiliza como una capa de agregación para evitar tener que consultar manualmente 10 herramientas diferentes.
Ventaja Clave	**Rapidez y sencillez** en la evaluación de riesgo, proporcionando un contexto amplio para el análisis inicial de cualquier indicador.
Enlace Oficial	https://pulsedive.com/

Flujo de Trabajo del Analista de SOC en un Incidente

Imaginemos que el SIEM (Sistema de Gestión de Eventos e Información de Seguridad) genera una alerta: **"Conexión de servidor interno a IP externa sospechosa."** El analista comienza su investigación:

Fase 1: Triaje y Validación Rápida (VirusTotal, AbuseIPDB, Pulsedive)

El objetivo es determinar si la IP es realmente maliciosa y priorizar la respuesta.

Herramienta	Acción del Analista	Resultado/Propósito
VirusTotal	Introduce la IP externa sospechosa.	Obtiene la reputación inmediata, veredictos de *antivirus* y geolocalización. Si tiene muchos positivos, se confirma la maliciosidad.
AbuseIPDB	Introduce la misma IP.	Verifica el **Abuse Confidence Score**. Si el *score* es alto, se confirma que la IP tiene un historial de ataques de fuerza bruta, *spam* o *malware*.
Pulsedive	Introduce la IP o el dominio relacionado.	Obtiene una **clasificación de riesgo rápida** y ve qué tipo de etiquetas (*tags*) le han puesto otros investigadores.
Resultado de la Fase: La IP tiene un alto *score* de abuso y está etiquetada como un C2 de **Malware X.** Se confirma el incidente y se pasa a la investigación profunda.		

Fase 2: Recolección y Contextualización de IOCs (ThreatFox, AlienVault OTX)

El analista ahora busca todo el contexto posible sobre el **Malware X** detectado para entender la amenaza completa.

Herramienta	Acción del Analista	Resultado/Propósito
ThreatFox	Busca el nombre de la familia de *malware* (ej: Emotet) o la IP que ya encontró.	Obtiene una lista actualizada de todos los **IOCs activos** (otras IPs C2, hashes de muestras de *malware*) asociados a esa familia.
AlienVault OTX	Busca el nombre del *malware* o la IP.	Encuentra *Pulses* creados por la comunidad que describen la campaña. Esto proporciona **contexto narrativo**: el *modus operandi* del ataque, el sector afectado y los vectores de infección comunes.
Resultado de la Fase: El analista tiene una lista completa de IOCs del **Malware X** y entiende la **Táctica** de la amenaza (por ejemplo, que usa un archivo adjunto de Word con macros).		

Fase 3: Estructuración y Enriquecimiento (MISP, OpenCTI)

El analista necesita formalizar la información para compartirla con el resto del equipo y automatizar las defensas.

Herramienta	Acción del Analista	Resultado/Propósito
MISP	Crea un nuevo	Introduce la IP inicial, los *hashes* y los C2s obtenidos de ThreatFox y AlienVault OTX. MISP enriquece

Herramienta	Acción del Analista	Resultado/Propósito
	"Evento" de incidente.	automáticamente estos datos con metadatos y correlaciona con eventos históricos internos.
OpenCTI	Ingesta el Evento de MISP.	Mapea el incidente en su base de datos de conocimiento. El analista puede ver visualmente: **[IP y Hash]** $\rightarrow$ **[Malware X]** $\rightarrow$ **[Actor de Amenaza Y]** $\rightarrow$ **[Técnicas de MITRE ATT&CK Z].**
Ventaja Clave: Esta fase transforma los datos brutos en **Inteligencia Estructurada**, lo que permite a la dirección y a otros equipos tomar decisiones informadas.		

Fase 4: Respuesta y Contención Automatizada

Finalmente, la inteligencia recolectada se utiliza para la defensa activa.

1. **Bloqueo Rápido:** Los IOCs validados y priorizados en **MISP** (IPs, dominios) son exportados automáticamente y enviados al **Firewall** y al sistema **EDR** (Endpoint Detection and Response) para bloquear la conexión de red y buscar los *hashes* en el resto de la infraestructura.
2. **Caza de Amenazas (Threat Hunting):** El analista utiliza las TTPs y las técnicas de MITRE ATT&CK identificadas en **OpenCTI** para buscar proactivamente *otras* máquinas que puedan estar infectadas de forma silenciosa.

3. **Reporte y Lecciones Aprendidas:** El evento en MISP y la relación en OpenCTI se cierran y se archivan, proporcionando documentación histórica para futuras detecciones.

Resumen del Ecosistema

El analista se mueve en un ciclo continuo:

Categoría	**Herramientas Utilizadas**	**Rol en el Ciclo de Vida del Incidente**
Reputación Rápida	VirusTotal, AbuseIPDB, Pulsedive	Detección inicial, validación y priorización.
IOCs en Vivo	ThreatFox, AlienVault OTX	Recolección de indicadores adicionales, contexto de campaña.
Gestión y Contexto	MISP, OpenCTI	Estructuración, correlación interna, mapeo a MITRE ATT&CK, automatización y documentación.

Ejemplo:

Este ejemplo te mostrará cómo un analista de SOC (Security Operations Center) utiliza el ecosistema de herramientas de TI para mapear una actividad maliciosa específica a una técnica dentro del *framework* **MITRE ATT&CK.**

Técnica de MITRE ATT&CK Elegida:

- **T1071.001 - Application Layer Protocol: Web Protocols (HTTP/HTTPS)**
- **Táctica:** Command and Control (C2)
- **Descripción:** El atacante utiliza protocolos web comunes (HTTP/HTTPS) para disfrazar el tráfico malicioso y evadir la detección de *firewalls* y *proxies*.

Escenario: Detección de Tráfico C2

1. Detección Inicial

El **SIEM** o el sistema **EDR** genera una alerta:

- **Alerta:** "Conexión inusual de un servidor de bases de datos interno a un dominio externo de bajo volumen: cdn-updates-xyz[.]com"
- **IOC inicial:** cdn-updates-xyz[.]com y su IP asociada: 45.10.20.30

2. Fase de Triaje y Validación Rápida (AbuseIPDB, VirusTotal, Pulsedive)

El analista necesita confirmar si se trata de un falso positivo o de un C2 real.

Herramienta	Acción del Analista	Resultado Obtenido	Relevancia para MITRE
VirusTotal	Consulta el dominio cdn-updates-xyz[.]com.	Se observa un bajo número de detecciones (ej: 5/70), pero algunas fuentes especializadas lo marcan como **"Suspicious"** y se identifican *hashes* de archivos asociados.	Confirma la baja notoriedad (aún no está en todas las listas negras), pero existe actividad maliciosa.
AbuseIPDB	Consulta la IP 45.10.20.30.	El **Abuse Confidence Score** es alto (ej: 85%). Reportes recientes indican actividad de **Brute-Force** y **Malware Distribution**.	Se valida la reputación negativa de la IP, lo que eleva la prioridad del incidente.
Pulsedive	Consulta el dominio/IP.	Pulsedive lo clasifica como **"High Risk"** y lo etiqueta con **"InfoStealer"**.	Ayuda a la priorización y atribución preliminar.

Conclusión del Triaje: La actividad es maliciosa y probablemente relacionada con un *InfoStealer*.

3. Fase de Recolección de Inteligencia (ThreatFox, AlienVault OTX)

El analista ahora busca el **contexto** y la **familia de *malware***.

Herramienta	**Acción del Analista**	**Resultado Obtenido**	**Relevancia para MITRE**
ThreatFox	Busca la IP 45.10.20.30 o la etiqueta "InfoStealer".	**Resultado Clave:** ThreatFox identifica la IP como un C2 activo de la familia de *malware* **"Vidar Stealer"**. Proporciona el **SHA256** del cargador y, crucialmente, el *path* exacto del tráfico de C2, por ejemplo: /v1/upload-data.php.	**Mapeo de la Técnica:** Se identifica que el C2 utiliza peticiones HTTP POST al *path* /v1/upload-data.php para extraer datos. **Esto es el procedimiento específico de la técnica T1071.001.**
AlienVault OTX	Busca el *Pulse* relacionado con "Vidar Stealer".	Encuentra un informe de la comunidad que detalla que Vidar Stealer usa peticiones HTTP de capa 7 para subir la información robada, disfrazándolas de tráfico normal de API o de actualización.	Aporta la narrativa: el **Objetivo** de la técnica T1071.001 es robar información sin ser detectado.

4. Fase de Estructuración y Mapeo Final (MISP, OpenCTI)

El analista convierte los datos brutos en inteligencia aplicable y los organiza según MITRE ATT&CK.

MISP: El Almacén Operacional

1. **Creación del Evento:** El analista crea un nuevo Evento en MISP llamado: "Incidente Vidar Stealer - 2025/XX/XX".
2. **Ingreso de IOCs:** Ingresa el dominio, la IP y el SHA256 de ThreatFox.
3. **Etiquetado del Procedimiento:** Añade un atributo tipo texto con el *path* de la comunicación C2 (/v1/upload-data.php).
4. **Taxonomía:** Etiqueta el evento con la taxonomía **MITRE ATT&CK** directamente en la plataforma:
    - mitre-attack:command-and-control:T1071.001
    - mitre-attack:exfiltration:T1041 (Exfiltración a través de C2)

OpenCTI: La Vista Estratégica

1. **Ingestión:** OpenCTI consume automáticamente el Evento de MISP.
2. **Mapeo Visual:** El analista utiliza OpenCTI para formalizar la relación. En el gráfico de conocimiento, se crean los siguientes nodos y vínculos:

$$\text{[Vidar Stealer (Malware)]} \rightarrow \text{uses} \rightarrow \text{[T1071.001: Web Protocols (Technique)]}$$

$$\text{[T1071.001]} \rightarrow \text{transports IOC} \rightarrow \text{[cdn-updates-xyz[.]com (Indicator)]}$$

$$\text{[cdn-updates-xyz[.]com]} \rightarrow \text{related to} \rightarrow \text{[45.10.20.30 (Indicator)]}$$

Beneficio Clave:

- **OpenCTI** ofrece la **perspectiva estratégica**, mostrando cómo el *malware* se relaciona con la técnica.
- **MISP** ofrece la **perspectiva operacional**, proporcionando IOCs estructurados listos para ser consumidos por sistemas de defensa.

5. Fase de Contención y Hardening

El mapeo a la técnica **T1071.001** guía la respuesta:

- **Contención:** Se bloquea la IP en el *firewall* (usando las listas de **AbuseIPDB** como referencia).
- **Hardening:** Sabiendo que se usa **T1071.001** (tráfico web), el equipo de red no solo bloquea la IP, sino que crea una regla de inspección profunda de paquetes (DPI) en el *proxy* para alertar o bloquear *cualquier* conexión a IPs desconocidas que contengan el *path* **/v1/upload-data.php** o el *User-Agent* específico, previniendo así futuras variantes de Vidar Stealer que usen el mismo procedimiento.