

La Cyber Threat Information Sharing: differenze di approccio tra MISP e TIP

La Cyber Threat Intelligence è uno dei temi legati al mondo della Cybersecurity, che ogni giorno diventa sempre più pervasivo nelle Aziende; per questo motivo gli aspetti legati alla Cyber Threat Information Sharing ed il bisogno di condividere informazioni sono diventati quasi “assiomatici” nel mondo della sicurezza informatica. Sempre più spesso, le organizzazioni si stanno dotando di sistemi in grado di prevenire e identificare le minacce esterne (c.d. Cyber Threat) nonché proteggersi dalle stesse.

Argomenti quali i formati di dati da utilizzare (STIX, JSON, etc) e Piattaforme (MISP[1] o TIP[2]) utilizzati per effettuare una corretta Cyber Threat Information Sharing sono all’ordine del giorno della comunità internazionale di cybersecurity, ed in particolare per chi svolge un’attività di Cyber Threat Hunting[3]. Ma cosa vuol dire realmente fare **Cyber Threat Information Sharing**? Si tratta di creare un ecosistema dove esiste una condivisione real-time di un’informazione actionable[4] di Cyber Threat, in grado di incrementare le difese di un’organizzazione (privata o pubblica) in ottica di prevenzione, identificazione e mitigazione della Cyber Threat prima che possa esserci un impatto reale sull’organizzazione stessa.

Sebbene questo tema si stia sviluppando in molti paesi della Comunità Europea e non, riscontriamo ancora una situazione a due velocità, tra il mondo pubblico e privato. Il mondo pubblico ha già avviato una serie di progetti e gruppi di lavoro, in cui in prima linea sicuramente c’è l’AGID con il ruolo del CERT-PA ed altri settori del mondo della difesa con il CERT-DIFE, mentre nel mondo privato, il settore in cui si

rileva un maggiore avanzamento risulta essere quello bancario, con il CERT-FIN.

Permangono sicuramente diversi interrogativi che tutte le organizzazioni dovranno porsi: come la seguente vignetta ben rappresenta, tutti hanno l'esigenza di condividere informazioni in un formato interpretabile per i più, ma non tutti sono pronti a condividere le proprie informazioni.



I principali temi da affrontare, in ottica di Cyber Threat Information Sharing, sono riassunti nelle seguenti domande[5]:

- Che cosa condividere?
- Con chi condividere?
- Perché condividere?
- Come condividere?
- Quale uso farne delle informazioni condivise?

Le risposte possono essere diverse, in base a diversi fattori e al tipo di organizzazione, pubblica o privata.

Generalmente, per un ente pubblico è importante condividere informazioni di una potenziale cyber minaccia ad un'infrastruttura critica, mentre per un ente privato è importante ricevere questa informazione come fonte di intelligence esterna.

Va però fatta una distinzione, in quanto ci sono informazioni di interesse pubblico per tutti i settori e informazioni di interesse solo per alcuni come il banking, energy, etc, quindi non tutto va condiviso con tutti.

Gli elementi fondamentali, alla base del processo di Cyber Threat Intelligence Sharing sono rappresentati dai seguenti aspetti:

1. livello di maturità dell'organizzazione

2. "TRUST" rispetto alla fonte da cui proviene l'informazione
3. capacità tecnologica interna di ogni singola organizzazione nel recepire e utilizzare queste informazioni nella modalità più corretta per renderle "actionable".

Ciò che manca ancora è definire pertanto lo scopo, le regole, i formati di scambio e le modalità di utilizzo delle informazioni di Cyber Threat Intelligence.

Mentre sui primi due elementi il settore pubblico sta già lavorando, per il terzo (formati di scambio e modalità di utilizzo delle informazioni), la comunità internazionale ha già delineato un suo standard rappresentato dallo STIX/TAXII e dalle piattaforme di Cyber Threat Intelligence (MISP o TIP).

Un esempio di utilizzo e "consumo" di un'informazione di cyber intelligence, attraverso una TIP combinata con un MISP, è rappresentato nella figura seguente, dove al centro si trova la TIP e la MISP risulta essere una fonte d'informazione esterna.



Sul mercato, **al momento esistono due diversi tipi di piattaforme utilizzate per la Cyber Threat Information Sharing**: una è la MISP (Malware Information Sharing Platform), l'altra è la TIP (Threat Intelligence Platform). Entrambe le piattaforme sono usate per la gestione delle Cyber Threat, ma applicate in modi diversi.

Analizzando meglio nel dettaglio risulta che:

- **MISP**: è una piattaforma usata principalmente per lo *scambio delle informazioni, arricchimento e correlazione dei dati esterni*. Questa piattaforma usa STIX/TAXII solo per lo scambio delle informazioni immagazzinate in formato JSON proprietario ed è usata normalmente come

storage di dati e correlazione di IoCs (Indicatori di compromissione). Attualmente si riscontra un forte utilizzo da parte delle Pubbliche Amministrazioni per lo scambio di IoCs e link con le altre agenzie Europee.

- **TIP:** è una piattaforma utilizzata principalmente per *condividere informazioni, arricchimento, correlazione e analisi / investigazione di dati interni ed esterni di un'organizzazione*. Questa piattaforma può essere nativa STIX/TAXII standard e tutti gli elementi interni e sue componenti usano lo standard di Threat Intelligence; viene utilizzata come storage di dati e come dispositivo di analisi / indagine. Attualmente si riscontra un forte utilizzo da parte di società private, per la conversione e scambio di IoC, i quali a loro volta sono utilizzati per rendere le cyber informazioni “actionable”, sfruttando il collegamento verso i SIEM, SOC e così via. La TIP inoltre è usata in alcuni contesti anche come strumento di collegamento tra la Pubblica Amministrazione e agenzie Europee.

Un ulteriore elemento di differenza, tra una TIP rispetto al MISP, è legato al processo di Cyber Threat Intelligence, rappresentato dalla seguente figura che evidenzia le differenti aree di copertura tra TIP e MISP.



Inoltre, per quanto riguarda le funzionalità tecniche, ad oggi, si rilevano le seguenti differenze.

Feeds ingestion	Threat Intelligence Platform STIX/TAXII-based	MISP Threat Information Sharing Platform
Ingestion of Public Feed	✓	✓

Ingestion of Commercial/Private Feed	✓	x ^([6])
Ingestion of Feed in structured formats	✓	✓ ^([7])
Ingestion of Feed in unstructured formats (e.g. pdf)	✓	x ^([8])

Users	Threat Intelligence Platform STIX/TAXII-based	MISP Threat Information Sharing Platform
Threat Intelligence Teams	✓	✓
SOC / CERT Teams	✓	✓
Fraud & Risk analyst	✓	✓
Management and Executive Teams	✓	x

Scalability	Threat Intelligence Platform STIX/TAXII-based	MISP Threat Information Sharing Platform
Production/Consuming scalability	✓	x
Architecture scalability	✓	✓

Oltre alla macro differenze tecniche, ci sono diversi vantaggi nell'utilizzare un TIP rispetto al MISP e sono:

- **Elevate capacità di analisi:** le società spesso utilizzano e-mail, fogli di calcolo e PDF come primaria

fonte informativa su cui effettuare un'attività di aggregazione, analisi e reporting rispetto alle attività di CTI. Ciò è possibile solo sfruttando alcune funzionalità proprie della TIP, come la qualificazione della fonte, il mapping delle diverse fonti, la navigazione, il filtraggio basato sugli attributi, le informazioni di ricerca avanzate, l'esplorazione e la visualizzazione tramite Link Analysis.

- **Tempo di vita per la condivisione delle informazioni:** le informazioni time-to-live (obsolescenza) degli indicatori IOCs della minaccia dipendono molto dall'indagine e dal processo d'intelligence che si vuole adottare. È fondamentale, tuttavia, che le informazioni di intelligence siano utilizzate dai consumatori di intelligence per stabilire le priorità d'intervento. Attualmente, le informazioni sul time-to-live che non vengono fornite dalla maggior parte dei feed, possono invece essere settate sulla TIP che ha la funzionalità di indirizzare l'intervento verso il SOC o CERT.
- **Formato dati e integrazioni con altre fonti esterne e interne:** la TIP fornisce interfacce e strumenti in grado di connettersi a servizi di terze parti sia per la parte di collection sia per la parte di dissemination, convertendo i dati direttamente nel formato standard STIX, indipendentemente dal tipo di formato prodotto dal vendor.
- **Internazionalizzazione:** la TIP è una tecnologia nata per la gestione delle Cyber Threat e condivisione delle informazioni di Cyber Threat in un formato standard STIX, mentre la tecnologia MISP è una tecnologia solamente Europea ed è utilizzata principalmente solo in Europa dalle agenzie governative e per finalità di Information Sharing.

Per concludere, ad avviso di chi scrive, entrambe le tecnologie possono essere utilizzate come strumenti di Cyber Threat Information Sharing, ma la TIP risulta essere una

piattaforma più completa per la gestione integrata di un processo di Cyber Threat Intelligence, in particolare per il settore privato, in cui la stessa MISP può rappresentare una fonte autorevole di informazione “FEED” da utilizzare.

Al momento, il consiglio più importante resta quello di non interrompere il processo di arricchimento e condivisione di informazioni sia da parte degli enti pubblici che privati, incrementando gli investimenti sul tema e prevedendo una maggiore integrazione tra le due tecnologie al fine di migliorare il processo d’indagine di una Cyber Threat, e di identificazione degli attori “Bad Actor”, delle campagne di attacco e così via, per ogni specifico settore di mercato.

NOTE

- [1] MISP ovvero Malware Information Sharing Platform – <http://www.misp-project.org/>
- [2] Threat Intelligence Platform.
- [3] WP2017 0.3.1.2u3 – Limits of TISPs – https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms/at_download/fullReport
- [4] Cfr. Dalla Malware Analysis alla Cyber Threat Information Sharing – Francesco Schifilliti – HackinBo 2017 Bologna. *Actionable intelligence*, ovvero un’informazione analizzata, contestualizzata, tempestiva, accurata, rilevante e predittiva
- [5] Dalla Malware Analysis alla Cyber Threat Information Sharing – Francesco Schifilliti – HackinBo 2017 Bologna.
- [6] L’ingestion di Feed Commerciali è possibile solo se le informazioni provengono da organizzazioni della stessa community
- [7] Di default gli eventi sono «ingested» solo nel formato JSON MISP. L’ingestion di eventi in formato STIX è in pipeline
- [8] Al momento ogni informazione non strutturata può

essere allegata a un evento. L'ingestione di informazioni non strutturate è in corso. La principale limitazione è legata all'utilizzo del codice Open Source

A cura di: **Ing. Mattia Siciliano**

L'articolo La Cyber Threat Information Sharing: differenze di approccio tra MISP e TIP proviene da ICT Security Magazine.

<https://www.ictsecuritymagazine.com/articoli/la-cyber-threat-information-sharing-differenze-di-approccio-tra-misp-e-tip/>