Differenze di approccio tra tecnologie Open Source e tecnologie commerciali nella Cyber Threat Intelligence

Author : Mattia Siciliano

Date : 15 Maggio 2019

Sempre di più i CISO (Chief Infomation Security Officer) e i direttori dell'area Risk&Compliance valutano le funzionalità e le caratteristiche offerte dai servizi di CTI (Cyber Threat Intelligence) inserendoli nei programmi di sicurezza delle loro aziende.

Entro il 2022, il 20% delle grandi imprese utilizzerà i servizi CTI per definire le proprie strategie di Cybersecurity, il che rappresenta un aumento almeno del 10%[1] rispetto allo scorso anno.

Ad oggi i maggiori fruitori dei servizi di CTI commerciali sono i servizi governativi e finanziari ma si intravede un aumento di altri settori, causato da una maggiore maturità dei programmi di sicurezza, piuttosto che da una specifica tendenza del settore industriale o area geografica.

Anche altri settori - come il trasporto aereo, le assicurazioni sanitarie, oil & gas, energia, servizi di pubblica utilità e vendita al dettaglio - iniziano ad affacciarsi all'utilizzo dei servizi di CTI. Questo fenomeno è maggiormente evidente per le grandi imprese che hanno maggior esposizione del proprio brand e presentano strutture organizzative e programmi di sicurezza più maturi.

La CTI è una caratteristica importante e fondamentale di un programma di Cybersecurity, ed è spesso un elemento di differenziazione verso altri mercati, in particolare per le aziende che lavorano nel mercato digitale.

Esistono diversi fornitori nel mercato globale che promuovono molteplici servizi informativi (FEED), usati principalmente per arricchire i dati interni o raccogliere dati da altre fonti a cui è stata applicata un'analisi specialistica (PORTALI di CTI).

Altri fornitori, invece, sono più focalizzati sulla condivisione delle informazioni di Cyber Intelligence e sulle piattaforme di analisi (TIP - Threat Intelligence Platform), che aggregano i dati di altre fonti aggiungendo metadati e/o arricchendo l'accesso verso terze parti, in cui il valore è rappresentato dalla fusione dei dati interni ed esterni (data fusion) per fornire un

risultato actionable (Strategic Report, Operational Report o Technical Report).

Ad alto livello, i servizi di CTI possono essere utilizzati in due modalità:

- fornire informazioni solo alle macchine o ai sistemi di elaborazione automatica, vale a dire MRTI -Machine-Readable Threat Intelligence;
- fornire informazioni prodotti da un team di specialisti, al TOP Management.

Informazioni leggibili da una macchina/sistema di sicurezza

Sono informazioni principalmente di monitoraggio e/o notifica in tempo reale (IoC – indicator of compromise), ricavati per lo più da fonti esterne e utilizzati per arricchire i sistemi di sicurezza interna. Spesso includono anche informazioni sull'attività operativa che si sta verificando (fonti esterne) o si è già verificata (fonti interne) ma con approcci e obiettivi puramente tecnici.

Informazioni prodotto da un team di specialisti

Sono informazioni acquisite da diverse fonti (Commerciali o Open Source), contenenti elementi come TTP, Threat Actor o report prodotti da analisti umani. Queste informazioni includono generalmente un'analisi su misura per il cliente, con dettagli delle azioni di rimedio da effettuare.

Tutte queste informazioni sono generate utilizzando standard di mercato come STIX, JSON, etc. ed elaborate da piattaforme commerciali come TIP[2] (commerciali) od Open Source come MISP[3] (open source) utilizzate per effettuare una corretta Cyber Threat Information Sharing e, in particolare, per svolgere un'attività di Cyber Threat Hunting[4] [5].

Il mercato si divide tra tecnologie/piattaforme di Cyber Threat Intelligence commerciali e open source. Entrambe le tecnologie/piattaforme sono usate per la gestione delle Cyber Threat, ma applicate in modi diversi.

Esistono diversi elementi da considerare per effettuare un confronto tra le diverse tecnologie da adottare nel mondo della CTI. In particolare possiamo distinguere 5 principali elementi caratterizzanti, che sono:

- gestione dei feed e fusione di diverse fonti;
- capacità di arricchimento, analisi e discovery dei dati;
- taggatura dei dati e delle fonti e information sharing;
- gestione degli utenti e collaborazione tra i team;
- scalabilità e supporto.

La figura seguente illustra le principali differenze in merito alle maggiori tecnologie/piattaforme commerciali e open source disponibili sul mercato rispetto alle diverse categorie di elementi (category) e caratteristiche tecniche per ogni singola categoria (features) su cui poi è stato applicato un confronto.

Category	Features	TIP	MISP	The Hive	Cortex
feed	Ingestion of Public Feed	Yes	Yes	Yes, MISP out of the box	No,can use hippocampe to aggregate feed
feed	Ingestion of Commercial feed	Yes	Partially,Ingestion of commercial feed is available only if feeds comes from the same community	Partially,Digital Shadow,Synapse,ZeroFox using TheHive4py	No
feed	Ingestion of private feed	Yes	Yes	yes	No
feed	Ingestion of Feed in unstructured formats (e.g. pdf)	Yes	Actually every non structured data can be attached to an event.The ingestion of non structured data is in progress.Main limitation is due to use of open source	No	Not out of the box,can be developed with an analyzer or via API, pdf not work
feed	Report Creation	Yes (STIX and HTML)	No	No	No
Analist Gui & capabilities	Link Analysis and Investigation	Yes,stix based, link analysis and correlation	Yes,correlation	Investigation via analyzers	No
Analist Gui & capabilities	Enrichment	Yes	Yes	Yes leveraging Cortex	Yes
Analist Gui & capabilities	Case Management	Yes related to Intelligence Analysis	No	Yes,very structured related to IR	No
Analist Gui & capabilities	Discovery	yes	yes	yes	yes
Analist Gui & capabilities	Pivot	yes	yes	Yes	No
Analist Gui & capabilities	Dashboard	yes	yes	yes	yes
Int management & Automation	Data Ingest/Data Fusion	Yes in many formats via stix,csv,txt,json,pdf,api etc out of the box	Yes,Json and CSV,also stix 1.2 via taxii can't be configured via GUI	Yes,MISP Json,txt	Partially with hippocampe Json
Int management & Automation	Automation	Yes in many formats via stix and taxii, csv, json	No	Yes,some workflow can be automatized,mostly related to case management and task with synapse	No
Int management & Automation	Source Reliability	Yes	Yes https://github.com/MISP/misp-taxonomies/tree/master/admiralty-scale	No	No
Int management & Automation	Taxonomies	Yes	Yes	No	No
Int management & Automation	Traffic Light Protocol	Yes	Yes	No	No
Int management & Automation	Maliciousness (Setting level of maliciousness of IOC)	Yes	No	No	No
Int management & Automation	Half life (setting TTL of the IoC)	Yes	No	No	No
Int management & Automation	Information Sharing	Yes in many formats via stix and taxii, csv, json	Partially with other misp ,also stix 1.2 via taxii,can't be configured via GIU	Via MISP or via responser	No
Scalability & Support	Production/Consuming scalability	Yes	Yes	Yes	Yes
Scalability & Support	Architecture scalability	Yes	Yes	Yes	Yes
Scalability & Support	Maintenance & Support	Yes	No	No	No
Users & Collaboration	Threat Ingellicence Teams	Yes	Yes	Yes	Yes
Users & Collaboration	SOC/Cert	Yes	Yes	Yes	Yes
Users & Collaboration	Risk Analysit group	Yes	Yes	No	No
Users & Collaboration	Management and Executive Team	Yes	No	No	No
Users & Collaboration	Collaboration Between Teams	Yes	No	Yes	Yes

Figura 1 - Differenze tra piattaforme commerciali e open source

Si può notare facilmente che le soluzioni commerciali offrono caratteristiche tecniche maggiori rispetto a soluzioni open source, spesso legate alla possibilità di generazione di report *ad hoc (**Category**: Feed e **Features**: Report)* e alla possibilità di effettuare un'opportuna taggatura delle fonti FEED attraverso gli elementi cardine della CTI come Half Life, maliciousness [6] *(**Category**: Int. Management and Automation e **Features**: Half Life, maliciousness)*.

Gli altri elementi distintivi delle soluzioni commerciali rispetto alle soluzioni open source sono:

- il non pieno utilizzo dello standard STIX/TAXII da parte di tecnologie open source;
- necessità di aggregare più soluzioni open source per avere gli stessi benefici di una soluzione commerciale integrata.

Ultimo elemento da non sottovalutare è rappresentato da supporto e maintenance, elemento cardine di soluzioni commerciali ma completamente assente per soluzioni open source *(**Category**: Scalability and Support e **Features**: Maintenance and support)*.

Pertanto uno dei vantaggi di utilizzare servizi e tecnologie di CTI, siano esse commerciali od open source, è rappresentato dalla possibilità di migliorare il processo decisionale aziendale, in modo da rendere giustificabile la necessità di risorse aggiuntive e/o delineare al meglio la strategia da adottare.

I CISO sono spesso tenuti a rispondere a domande come:

- Perché viene implementato un particolare cambiamento di policy?
- Le minacce diffuse dai media esistono anche al mio interno ? Qual è la loro rilevanza per l’azienda?
- Quali potrebbero essere le minacce nel prossimo futuro?
- Quali sono i KPI che posso definire per effettuare un corretto monitoraggio del mio livello di sicurezza?

Per concludere, ad avviso di chi scrive, entrambe le tecnologie/piattaforme possono essere utilizzate come strumenti di analisi delle Cyber Threat, ma la TIP risulta essere una piattaforma più completa per la gestione integrata di un processo di Cyber Threat Intelligence, a differenza di tecnologie puramente Open Source.

La figura seguente mostra una possibile integrazione delle due tecnologie.

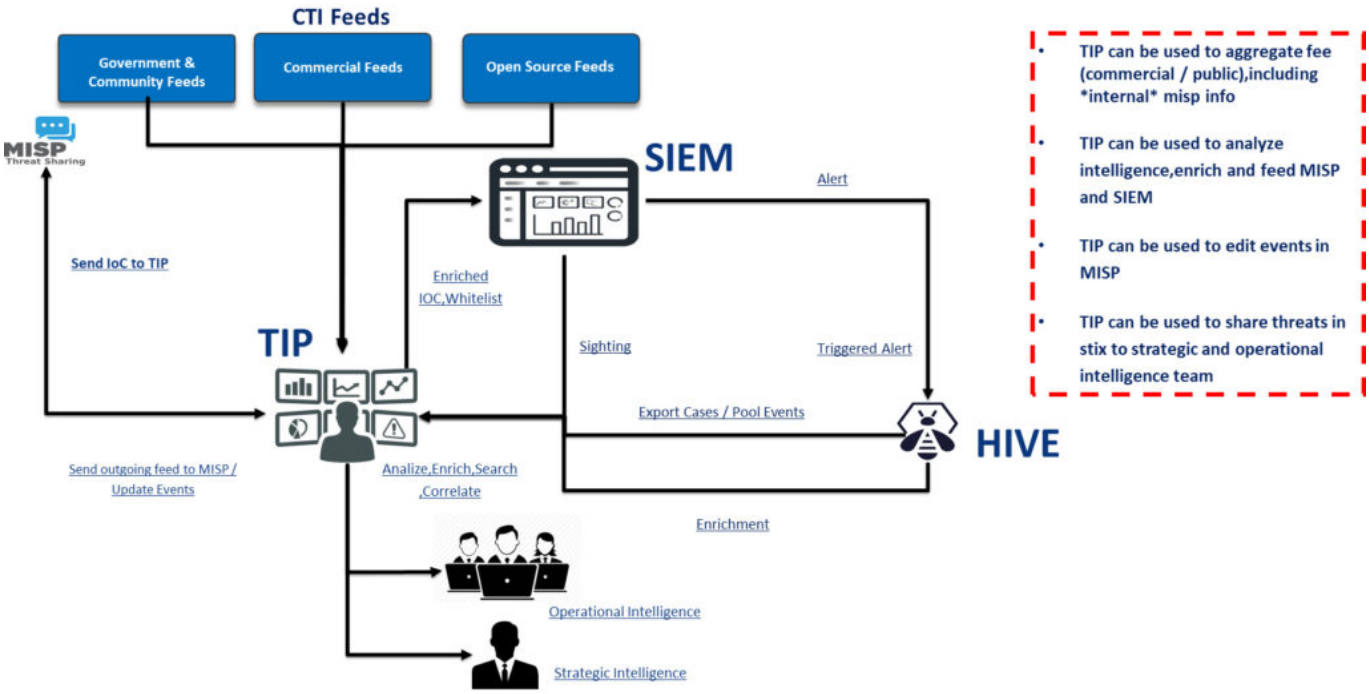

Figura 2 - Possibile modello d'integrazione tra tecnologie commerciali e open source

Al momento, il consiglio più importante resta quello di non limitarsi agli aspetti puramente tecnologici ma vedere i servizi di CTI come un processo integrante di una strategia di Cybersecurity aziendale, incrementando gli investimenti sul tema e prevedendo una maggiore integrazione tra le due tecnologie/piattaforma (commerciali e open source), al fine di migliorare il processo d'indagine di una Cyber Threat e di identificazione dei "Bad Actor", delle campagne di attacco e così via, per ogni specifico settore di mercato.

Note:

[1] Gartner, Market Guide for Security Threat Intelligence Products and Services – 19 Febbraio 2019.

[2] Threat Intelligence Platform.

[3] MISP ovvero Malware Information Sharing Platform, http://www.misp-project.org/.

[4] WP2017 O.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.

[5] La Cyber Threat Information Sharing: differenze di approccio tra MISP e TIP, https://www.ictsecuritymagazine.com/articoli/la-cyber-threat-information-sharing-differenze-di-

approccio-tra-misp-e-tip/.

[6] L’attività di taggatura della fonte risulta essere uno step fondamentale per effettuare una corretta analisi dei dati in fase di hunting.

Articolo a cura di **Mattia Siciliano**