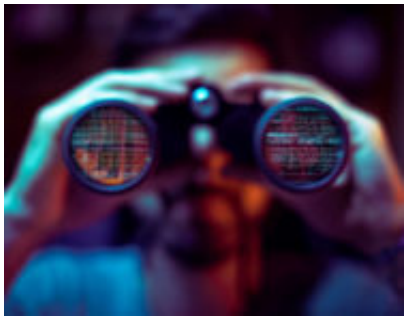
Combattere le minacce usando il Cyber Threat Hunting

Author : Giampaolo Darelli

Date : 3 dicembre 2018



Le minacce informatiche odierne sono diventate sempre più complesse da individuare a causa della loro continua mutevolezza, asimmetricità e diversificazione degli autori. Secondo i più recenti report[1] le attività di attacco “cyber” si consumano in poche ore e le exfiltration di dati avvengono in pochi giorni, mentre l’identificazione dell’incidente nei 2/3 dei casi rimane inosservata per un periodo che va dagli 80 ai 200 giorni[2]. Il processo di Cyber Threat Intelligence, ovvero la possibilità di avvalersi di una knowledge base costruita su fonti esterne ed interne al fine di aumentare la conoscenza dell’avversario, risulta particolarmente efficace nell’affrontare consapevolmente le minacce e diminuire i tempi di identificazione dell’incidente. In tandem con il processo di Cyber Threat Intelligence troviamo il concetto di Cyber Threat Hunting, ovvero quell’approccio che, sfruttando le fonti di intelligence, mira alla ricerca, all'individuazione e alla comprensione dell’attaccante sfruttando un metodo di generazione/validazione di ipotesi (SANS 2018[3]).

Come descritto nella Threat Survery 2018 della SANS[4] una grossa percentuale delle organizzazioni attaccate reagisce agli attacchi in maniera scomposta e lo fa solo dopo esserne diventata bersaglio, utilizzando poi le informazioni provenienti dall’attacco per la generazione di automatismi di controllo basati su IoC (Indicatori di Compromissione); questa risposta è una risposta di tipo reattivo, mentre diventa desiderabile, vista la complessità degli attacchi odierni, valutare ulteriori modalità di risposta di tipo preventivo e proattivo.

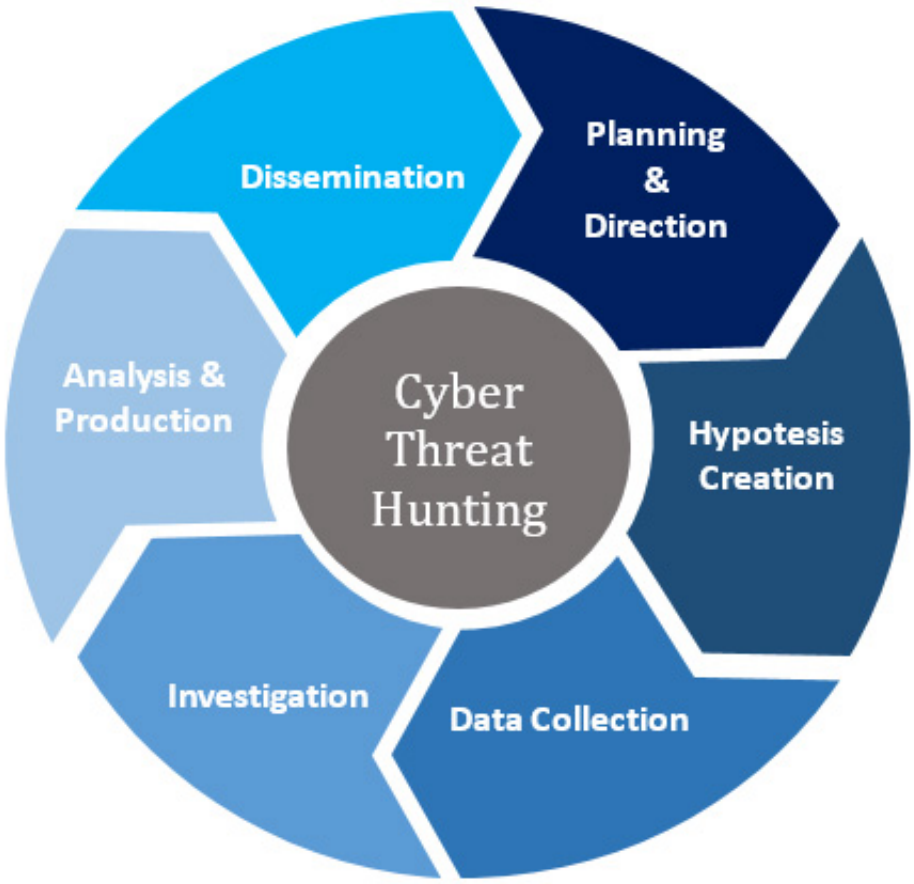
E’ necessario dunque pensare ad una difesa in cui venga considerata, oltre alla quantità, **la qualità degli IoC**, possibilmente contestualizzati ed arricchiti ed alla collaborazione tra gli analisti di Cyber Threat Intelligence e le figure preposte al Digital Forensic e Incident Response, al fine di costruire un team che sappia estrapolare dagli indicatori iniziali le tecniche, le tattiche, le procedure ed eventualmente l’identità dell’attaccante.

Fine ultimo è, oltre all’individuazione della minaccia, generare nuova intelligence, sia di tipo strategico che di tipo operativo.

Si vuole dunque proporre un framework di Cyber Threat Hunting che sappia conciliare processi, strumenti e persone e dove **il fattore umano** posso avere l’importanza che merita, in quanto

l’intrusione cyber è **sempre perpetrata da un soggetto umano** ed è quindi fondamentale **interpretarne la sua psicologia per comprendere le intenzioni e rispondere in maniera efficace alla minaccia**[5].

Il framework proposto, basato principalmente sul lavoro di sqrll[6][7] e della SANS[8], oltre che sui concetti dell’intelligence classica, è composto da 6 fasi sequenziali, dove le fasi di Hypotesis Creation, Data Collection, Investigation ed Analysis condividono strumenti e talvolta metodologie.



- Planning & Direction
- Hypotesis Creation
- Data Collection
- Investigation
- Analysis e production
- Dissemination

Planning & Direction

Questa è la fase dove viene definita una strategia e vengono scelti i PIR (Priority Intelligence

Requirements)[9] e gli obiettivi da raggiungere. Per il successo di questa fase è auspicabile una stretta collaborazione tra l'executive board e gli analisti, oltre all'utilizzo di fonti di intelligence aggiornate utili a definire il contesto in cui si opera.

Hypotesis Creation

La fase di creazione delle ipotesi è il momento più razionale dell'intero ciclo, dove il team di Cyber Threat Intelligence, con la guida dell'executive e la collaborazione dei team di Digital Forensic e Incident Response, valuta minacce, topografia/vulnerabilità dei sistemi ed obiettivi da raggiungere. Il team di Cyber Threat Intelligence, grazie all'esperienza pregressa, all'utilizzo di metodologie strutturate di analisi (ACH, Key Assumptions Check, Brainstorming, volte a diminuire i «bias» cognitivi, ovvero pregiudizi e debolezze che possono inficiare il lavoro dell'analista), metodologie proprio della cybersecurity (cyber killchain) e di strumenti tecnici, formula delle ipotesi (i.e. Siamo oggetto di un attacco? Abbiamo un Exfiltration?).

Data Collection

In questa fase si scelgono i dati sui cui verrà effettuata l'investigation, ovvero la validazione delle ipotesi e la successiva analisi. I dati scelti appartengono sia alla categorie dei logs appartenenti ai vari apparati, sia ad evidenze provenienti dal campo del Digital Forensic ed Incident Response, oltre che a fonti interne ed esterne di intelligence.

Investigation

E' in questa fase che avviene l'hunt vero e proprio, ovvero la verifica/validazione delle ipotesi generate in precedenza attraverso l'utilizzo di ragionamenti logici[10] (induttivo, deduttivo, abduttivo), strumenti di machine learning[11] e strumenti tecnici, per lo più appartenenti ai processi ed alle metodologie proprie della Digital Forensic e Incident Response. Si spazia dall'utilizzo dei SIEM e/o piattaforme specifiche[12] a piattaforme di Threat Intelligence[13], dalla link/network analisys[14] all'utilizzo di tassonomie operative integrate con strumenti[15][16]. Se **consideriamo i dati raccolti come testi**, e **paragoniamo la Cyber Threat Intelligence all'intelligence classica**, possiamo pensare a questo momento ed ai precedenti momenti di creazione delle ipotesi e raccolta di dati, come momenti "ermeneutici"[17], ovvero momenti in cui gli analisti usufruiscono, in termini di esperienza, sia del frutto del lavoro sull'interpretazione del dato, sia dell'esperienza degli altri membri del gruppo di lavoro.

L'operatore di intelligence è soprattutto un ermeneuta perché quando entra in contatto con la notizia scritta, prima ancora di essere un analista, è un interprete e, in quanto, entra in rapporto con un testo che parla di cose, al **quale si avvicina non come una tabula rasa**, bensì con la sua pre-comprensione (Vorverständnis), cioè con i suoi pregiudizi (Vorurteile), le sue pre-supposizioni e le sue attese[...] ed è qui che l'esperienza deve potersi arricchire grazie al rinnovarsi della feconda reazione tra essa stessa**, la creatività e l'intuito**" [18]

Il frutto del lavoro svolto in questa fase è **intelligence operativa e tecnica che, nella fase successiva di analisi/produzione, verrà trasformata in intelligence tattica e strategica**.

Analisi & Production

Come sopra citato in questa fase l'intelligence operativa viene rifinita e contestualizzata attraverso una serie di macro fasi, l'utilizzo di tassonomie[19], di fonti di intelligence pubbliche e private e di metodologie proprie della cybersecurity come la cyber killchain e la diamond analysis.

Fine ultimo è avere una conoscenza quanto più possibile approfondita dell'avversario in termini di tecniche, tattiche, procedure ed identità. Una conoscenza che, insieme all'utilizzo del concetto della Pyramid Of Pain, ovvero che l'attaccante cambia più lentamente le sue tattiche rispetto agli indicatori base come ip e dominio, permette all'organizzazione di assumere una postura proattiva e reagire rallentando l'avversario.

Il sapere «come» opera l'avversario, ed eventualmente la sua identità (soggetto singolo, collettivo, criminale, soggetto istituzionale) e le sue motivazioni (politiche, finanziarie, etc.) aiutano l'azienda a sviluppare nuovi pattern di difesa da affiancare ai tradizionali e a produrre nuova intelligence strategica e tattica da condividere e riutilizzare.

Dissemination

La fase finale del ciclo è il momento di **dissemination**, ovvero il momento in cui i risultati prodotti dalle fasi precedenti vengono condivisi con l'executive, gli stakeholder, gli altri team e la comunità. Il successo di questa fase dipende dalla forza dei processi di condivisione dell'organizzazione verso la comunità e gli altri apparati, e soprattutto dagli strumenti utilizzati: l'utilizzo di protocolli condivisi e free come taxii e stix[20], che permettono di condividere facilmente IOC, e l'utilizzo di una TIP[21](Threat Intelligence Platform) che permette di creare report per il management e condividere modelli complessi riguardanti tecniche, tattiche, procedure ed analisi di threat, incrementano decisamente la forza di condivisione e sono il primo tassello per la creazione di una comunità di condivisione delle informazioni, veloce ed aggiornata.

In conclusione tutte le organizzazioni sentono l'esigenza di individuare le minacce in anticipo e comprendere chi o cosa li sta attaccando, pertanto l'utilizzo di un framework di Cyber Threat Hunting, grazie alla combinazione di più processi e all'utilizzo di più strumenti, aiuta ad individuare minacce interne, generare nuova intelligence e ad aumentare la propria capacità di ***difesa passando da una modalità di risposta reattiva ad una risposta articolata e proattiva***.

Note

- [1] https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf
- [2] https://www.deepcyber.it/it/11-approfondimenti/17-cyber-threat-intelligence-come-abilitatore-nelle-attivita-di-cyber-protection

- [3] I processi da cui il Cyber Threat Hunting attinge conoscenze sono principalmente la Cyber Threat Intelligence, l'Incidendent Response ed il Digital Forensic.
- [4] https://www.sans.org/reading-room/whitepapers/threats/2018-threat-hunting-survey-results-38600
- [5] https://www.amazon.it/fattore-umano-nella-cybersecurity-Engineering/dp/1983349364
- [6] https://sqrrl.com/media/Framework-for-Threat-Hunting-Whitepaper.pdf
- [7] https://sqrrl.com/the-threat-hunting-reference-model-part-2-the-hunting-loop/
- [8] https://www.sans.org/reading-room/whitepapers/threats/paper/37172
- [9] https://fas.org/irp/doddir/army/fm34-2/Appd.htm
- [10] https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2018/03/pensiero-critico-in-analisi-intelligence-Conio.pdf
- [11] https://www.sans.org/reading-room/whitepapers/analyst/closing-skills-gap-analytics-machine-learning-38115
- [12] https://github.com/Cyb3rWard0g/HELK
- [13] https://www.eclecticiq.com/platform
- [14] https://www.corvil.com/blog/2015/data-visualization-and-linked-data-analysis-of-electronic-trading-activity
- [15] Sysmon - https://car.mitre.org/wiki/Sysmon_(2.0)
- [16] OSQuery e mitre att&ck : https://paper.tuisec.win/detail/c1ba45dc7fee720
- [17] L'ermeneutica in filosofia è di base l'interpretazione di testi scritti, che non si esaurisce però nella semplice interpretazione, ma sfocia nel circolo ermeneutico, ovvero in quel continuo scambio tra cose conosciute e quelle da conoscere, "le parti", che vanno a loro volta a modificare il complesso del sapere, "il tutto".
- [18] Dario Antiseri, Adriano Soi, L'intelligence e metodo scientifico pag.115-117
- [19] https://github.com/MISP/misp-taxonomies
- [20] https://stixproject.github.io/
- [21] https://www.ictsecuritymagazine.com/articoli/la-cyber-threat-information-sharing-differenze-di-approccio-tra-misp-e-tip/

Articolo a cura di **Giampaolo Darelli**