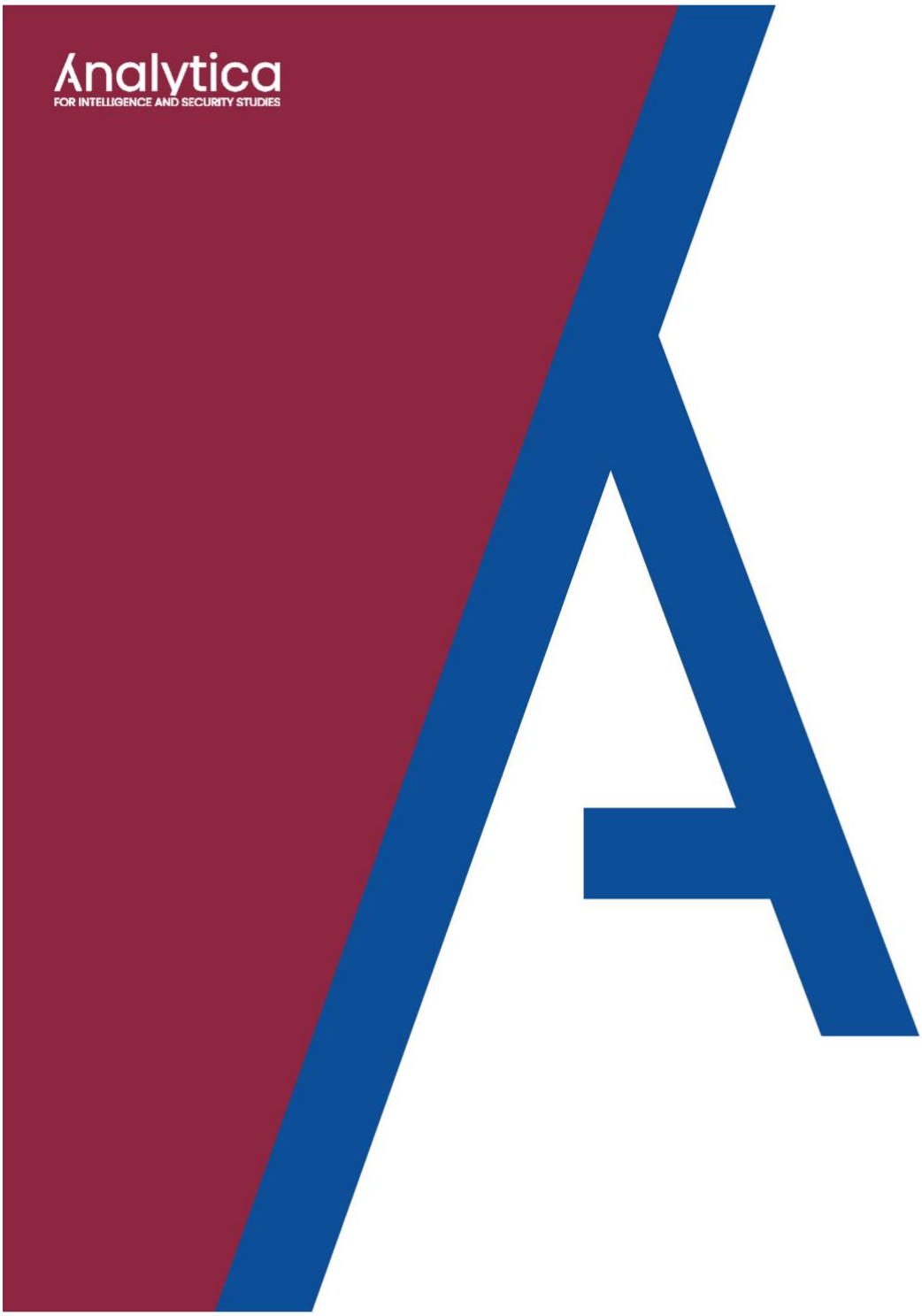

The elephant in the room?
L’intelligence alla sfida dell’era cybernetica.

Francesca Caravita

Analytica for intelligence and security studies

Paper Cyber-Security

ISSN: 2784-8779

The elephant in the room?
L'intelligence alla sfida dell'era cibernetica.

Francesca Caravita.

Correzioni e revisioni a cura del Dottor SPELTA Maurizio

Direttore del Dipartimento Cyber - Security

Torino, giugno 2021

È sempre stata questione di strategia. Fin fai tempi di Sun Tzu, la protezione dall'esterno, dal nemico, si basa sulla capacità di prevedere come l'avversario ha intenzione di organizzare le sue mosse, come questo intende la conflittualità e qual è lo sforzo in termini di tempo e risorse che prevede di impiegare; in sintesi, si tratta dell'essere in grado di "sapere prima" l'atteggiamento del nemico, ovvero conoscerne la strategia ed agire di conseguenza. Questo era vero quando le guerre si combattevano sul campo e gli attori coinvolti erano i soldati addestrati ed armati, ed è ancora più vero oggi in una situazione radicalmente mutata, dove alle tre tradizionali dimensioni del conflitto se n'è aggiunta una quarta, iper-complessa, ovvero la dimensione cibernetica, nella quale il campo di battaglia è la rete, gli obiettivi sono i sistemi e le infrastrutture informatiche ed informative ed il nemico è un'entità virtuale sconosciuta. In questa nuova dimensione in che modo è possibile dunque attuare delle previsioni circa la strategia del nemico, che fra l'altro non è neanche sempre identificabile? Ancora una volta, Sun Tzu fornisce una risposta attuale come non mai: "Pertanto il sovrano illuminato e il saggio generale che useranno gli uomini più intelligenti per lo spionaggio raggiungeranno grandi risultati. Le spie sono l'elemento più importante della guerra." [1]L'idea dello spionaggio come arma è intrinseca nella storia dell'uomo e si è evoluta storicamente nel vasto settore dell'intelligence, ovvero la raccolta sistematica di dati e informazioni riguardanti il target individuato al fine di indirizzare le decisioni. La storia dell'intelligence ha origini antichissime, partendo dagli egiziani, passando per i romani, consolidandosi nell'impero britannico e diventando elemento centrale nel mondo bipolare, ma tuttora l'intelligence ricopre funzioni fondamentali per la sicurezza nazionale sia pubblica che privata, ma se le minacce oggi si sono spostate dal campo fisico, reale, a quello virtuale, oggi l'intelligence assume necessariamente un nuovo ruolo, ovvero quello associato al mondo della cyber security. Si assiste infatti alla fusione di due ambiti, l'intelligence e la cyber security, che danno vita ad una nuova attività di analisi e di raccolta delle informazioni che viene definita cyber threat intelligence.

Il presente paper ha lo scopo di spiegare in che modo l'intelligence può essere applicata al campo della cyber security e dimostrare che la cyber threat intelligence deve essere considerata un elemento chiave e fondamentale della sicurezza informatica, per cui tutte le realtà da quelle governative a quelle aziendali, dovrebbero considerare l'implementazione di soluzioni CTI nei loro piani di cyber security. Per rispondere a queste due domande e capire l'importanza dell'"*elephant in the room*", il lavoro si articola in tre parti. Nella prima si definisce il concetto di cyber threat intelligence descrivendo nel dettaglio come il ciclo di analisi dell'intelligence si applica all'ambito

[1] Tzu S., *L'arte della guerra*, Feltrinelli, 2013, p.94

cyber; nella seconda sezione si illustrano invece gli ambiti di applicazione della CTI ed i suoi obiettivi; infine, nell'ultima parte, si discute un case study, ovvero l'esperienza di CTI di un'azienda leader di settore per capire praticamente quali sono i risultati di un'analisi di intelligence in campo cibernetico.

1. Cyber Threat Intelligence necessaria evoluzione dell'intelligence tradizionale

L'intelligence come "*attività di raccolta ed elaborazione delle notizie*"[2] al fine di supportare le scelte di un decisore è una metodologia efficace, puntuale e necessaria che viene applicata al giorno d'oggi in vari settori, in quanto si tratta di uno strumento molto duttile e in grado di adattarsi a situazioni diverse; per questa ragione alle tradizionali attività di intelligence associate alla cosa pubblica e alla sicurezza nazionale, si sono sviluppate nuove applicazioni del metodo di intelligence, come la *business intelligence*, l*'epidemic intelligence*[3] o la *cyber intelligence*. Ed è proprio quest'ultima tipologia che deve essere ritenuta come un'evoluzione naturale del mondo dell'intelligence, per due semplici motivi.

Innanzitutto, la sfera cibernetica ed informatica rappresenta il futuro, l'interconnessione fra l'uomo e la macchina è in crescita esponenziale e continuerà a svilupparsi in modo da velocizzare e semplificare i processi umani in tutti i suoi settori; questo campo rappresenta dunque la strada maestra dello sviluppo umano per cui non può essere sottovalutata e non considerata. Giusto per capire la grandezza del fenomeno cibernetico, il *Cisco Annual Inernet Report* (2018-2023)[4] afferma che entro il 2023 il numero di dispositivi connessi a *network IP* sarà più di tre volte la popolazione mondiale e il trasferimento di dati M2M, ovvero da una macchina ad un'altra senza l'intervento umano crescerà dal 33% rilevato nel 2018 al 50% previsto per il 2023, questo vuol dire che le connessioni M2M raggiungeranno la quota di 14.7 miliardi. Per non parlare dell'incremento dei dispositivi IoT (Internet of Things, ovvero tutti i dispositivi domestici connessi in rete, dai cellulari ai frigoriferi, sistemi di riscaldamento etc.), che nel 2021 hanno raggiunto la soglia dei 93 milioni di connessioni.[5]

---

[2] Antiseri D. e Soi A., *Intelligence e metodo scientifico*, Rubettino Editore, 2013, p.96.
[3] Si tratta di tutte quelle le attività volte all'identificazione precoce di rischi in sanità pubblica, la loro validazione, valutazione e indagine, finalizzate alla raccomandazione di misure di controllo.
[4] Cisco Annual Internet Report (2018-2021), 9 marzo 2020, https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html
[5] http://tendenzeonline.info/articoli/2021/04/14/connessioni-iot-italia/

Secondariamente, proprio il mondo cyber, che rappresenta di fatto una nuova dimensione, ha delle implicazioni nel campo della sicurezza tanto da modificarne il concetto di sicurezza stessa. L'idea di sicurezza fisica, vista come la necessità di proteggere fisicamente gli asset aziendali o pubblici, come luoghi produttivi, piuttosto che spazi militari o della difesa aventi una rilevanza strategica, passa quasi in secondo piano se consideriamo il rischio e la quantità di minacce alle quali sono esposti i sistemi informatici ed informativi. La rete ha sostituito di fatto il luogo fisico e il problema sta proprio in questa "sostituzione". Infatti, se prima in qualche modo la security, vista come l'apparato che ha il compito di mettere in sicurezza i luoghi fisici, aveva ben chiaro il suo perimetro di competenza e poteva in qualche modo essere in grado di quantificare e qualificare la minaccia esterna, adesso, non solo non è sempre immediato capire quanto estesa è la rete e tutti i sistemi ad essa connessa, ma, inoltre, è quasi impossibile capire quante e quali sono le minacce a cui è esposta. Questo è dovuto alla caratteristiche più intrinseche della cyber security, in primis la velocità e la rapidità in termini di operatività e sviluppo di tutti i processi, di tutti i meccanismi e di conseguenza anche dell'evoluzione delle minacce: una minaccia informatica individuata ieri potrebbe essere radicalmente modificata domani e questo rende i sistemi da proteggere molto più vulnerabili ed esposti a minacce sempre più diversificate e sempre più tecnologicamente avanzate. Infatti, la seconda caratteristica della cyber è proprio il suo aspetto tecnologico. In una realtà così dinamica, l'innovazione e l'evoluzione tecnologica vanno di pari passo al dinamismo dei processi, per cui l'efficacia di una minaccia è anch'essa sottoposta ad una spinta esponenziale continua, per cui le minacce cyber sono drasticamente sempre più invasive e difficili da estirpare.

In un panorama così descritto, dove la cyber non rappresenta solo il nuovo "tavolo di gioco", ma anche e soprattutto il nuovo "campo di battaglia", l'intelligence non può che inserirsi in questo aggrovigliamento di situazioni intensamente dinamiche e giocare un ruolo fondamentale, così come ha sempre fatto. In questo caso l'intelligence, che applicata alla sfera cibernetica, prende il nome di cyber threat intelligence, quindi l'intelligence della minaccia informatica, assume uno scopo chiaro e definito: la raccolta delle informazioni circa la minaccia informatica alla quale un'azienda pubblica o privata che sia, potrebbe essere esposta. In questo ambito l'intelligence ha l'obiettivo dunque di fornire una descrizione ampia del panorama delle minacce in modo da permettere al decisore di prendere delle decisioni in termini di prevenzione ed eventualmente di reazione. Infatti, il prodotto di intelligence fornisce un'analisi della tipologia di minacce, delle sue caratteristiche, i principali potenziali attaccanti, le proprie motivazioni e le modalità di attacco (le cosiddette TTP).

Ovviamente la sola cyber intelligence non potrà mai minimizzare il rischio di attacchi o combattere la minaccia, ma come nel caso dell'intelligence tradizionale, fornisce una solida base di *acknowledgment* che serve per comprendere la situazione all'interno della quale bisogna muoversi, ma deve essere integrata ed associata ad altre tecnologie di contrasto alla minaccia, come i SIEM, SOAR o altri meccanismi di difesa, che devono essere armonizzati all'interno di una strategia di cyber security.

1.2 La metodologia della CTI

La cyber threat intelligence, come spiegato nella sezione precedente, rappresenta un approccio generale all'analisi delle minacce informatiche, ma assume una rilevanza specifica in base alla necessità della struttura che decide di adottare questa metodologia e soprattutto al suo grado di tecnologie disponibili. Più precisamente si identificano due tipologie di CTI: *operational intelligence* e *strategical intelligence*.

Nel primo caso si tratta della raccolta di dati inerenti gli attacchi cyber, gli eventi, gli scenari che sono attualmente in corso. Di base, fornisce dati elaborati riguardo a delle situazioni che il potenziale ufficio cyber sta rilevando e dunque la CTI fornisce dettagli su come comportarsi, su come agire per arginare la minaccia. Solitamente questa tipologia di informazioni viene direttamente elaborata dalle macchine, ovvero da piattaforme automatiche, attive sui sistemi informatici che sono in grado di rilevare qual è la tipologia di attacco che l'azienda sta subendo, quali sono i vettori di attacco, quindi la modalità e quali sono le vulnerabilità che la minaccia intende sfruttare per entrare nei sistemi (le famose "porte di ingresso"). Proprio per la sua natura *raw*, questa tipologia di intelligence viene spesso definita "tecnica" perché si basa principalmente su *threat data feed*, ovvero su un insieme di informazioni tecniche specifiche su uno definito indicatore di rischio. Lo scopo dell'*operational intelligence* è quello di supportare un ufficio IT coinvolto nell'ambito della difesa dei sistemi, in modo da indirizzare nel modo più completo la risposta e la reazione ad un attacco *ongoing*. Per maggiore completezza è doveroso sottolineare che diverse fonti accostano a questa tipologia di intelligence, la cosiddetta tactical intelligence, che, anche in questo caso, tratta dati tecnici relativi ai potenziali TTP dell'attaccante.

I deliverables prodotti da questa tipologia sono gli indicatori di compromissione (IOC) che vengono utilizzati per arricchire le piattaforme di difesa e/o i SOC.[6]

Il secondo caso, invece, è quello che maggiormente si avvicina alla concezione di intelligence vera e propria, ed è quello della intelligence strategica. In questo caso si tratta della definizione di un'analisi di intelligence che ha l'obiettivo di delineare il panorama delle minacce che potenzialmente potrebbero attaccare l'azienda in oggetto. Ha quindi uno scopo predittivo, tipico dell'intelligence in stricto sensu. L'intelligence strategica ha sicuramente una connotazione meno tecnica rispetto alla precedente, in quanto è *business oriented*, nel senso che ragiona su quegli scenari di security informatica che potrebbero in qualche modo intaccare il business dell'azienda, sia in termini produttivi o di fornitura di servizio, ma anche reputazionali. Le analisi prodotte sono dunque prodotti di intelligence al 100% e si basano su dati che provengono da fonti disparate, non solo da elementi tecnici, i *threat data feed*, ma anche da documenti diffusi da istituzioni governative e non, da articoli proveniente da media o social media, e da white papers o altri documenti realizzati da aziende di sicurezza private, ma anche da forum e gruppi specifici di singoli privati. Queste fonti possono fornire informazioni preziose circa le nuove minacce e tecnologie emergenti, ma anche attori coinvolti e potenziali target. Si tratta di un lavoro sia di OSINT, quindi di una ricerca basata su fonti aperte, ma anche di CLOSINT, fonti chiuse e a pagamento. Se tutta questa attività di *data collecting* può essere sicuramente svolta da software di aggregatori di dati e dunque può essere in parte fornita in modo automatizzato, la differenza rispetto alla prima tipologia, sta proprio nell'intervento umano che è necessario, in quanto l'analista deve *connect the dots* in modo da trovare degli spunti chiave nelle fonti che possono essere applicati alla propria realtà di analisi.

Dopo aver chiarito la differenza fra le tipologie di CTI è necessario spiegare in che modo la metodologia classica di intelligence, quella che viene solitamente elaborata secondo le sei fasi del ciclo di intelligence, viene adattata ed impiegata alla sfera cyber.

Primo step, la fase preliminare, sta nell'individuare gli *intelligence requirements*, ovvero quali sono gli obiettivi che si intende raggiungere attraverso l'intero processo. Gli obiettivi possono essere chiariti solamente dopo aver definito il cosiddetto *Threat Modeling*, ovvero il modello della minaccia che implica l'individuazione degli elementi che potenzialmente potrebbero essere targetizzati da un attaccante. Può trattarsi di dati finanziari, di dati inerenti la proprietà intellettuale o dei sistemi stessi. È quindi necessario condurre un'analisi dei rischi per capire quali sono i sistemi informatici ed informativi più vulnerabili e più esposti a un attacco e l'impatto che un eventuale

[6] CREST, *What is cyber threat intelligence and how is it used?*, CREST, 2019 https://crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf p.10

attacco genererebbe sul business.

L'analisi dei rischi informatici permette inoltre di prioritizzare in modo analitico i sistemi che hanno più urgenza di essere messi in sicurezza tenendo conto della gravità dell'impatto e della probabilità che l'attacco si realizzi. A questo punto, è necessario capire la tipologia di intelligence da applicare in modo da poter mettere in sicurezza i sistemi identificati, quindi individuare se l'azienda necessita di un intervento in termini strategici, quindi quale settore aziendale è più vulnerabile, o se in termini operativi/tecnici, quindi quali sono le minacce in corso nell'azienda o come identificare la minaccia per eliminarla. In conclusione, questa pre-fase è quella che solitamente viene definita come la definizione del "fabbisogno informativo concretamente articolato in obiettivi informativi".[7]

La prima fase vera e propria del ciclo di intelligence è la fase di collezione dei dati sulla base degli obiettivi di intelligence definiti. In questo caso è doveroso fare una premessa sulla tipologia di dati che si intende ricercare, in quanto non si tratta dei comuni dati ai quali solitamente si fa riferimento. Si individuano due "classi di dati", la prima sono quei dati "tecnici" di cui si accennava nella sezione precedente, ovvero i *threat data feed*, la seconda invece riguarda tutti quei dati che possiamo definire "di contesto", ovvero che servono per contestualizzare i dati tecnici e *raw* che abbiamo a disposizione grazie alle macchine. I *threat data feed*[8] sono stringhe di dati *real time* che forniscono informazioni su potenziali attacchi e minacce cyber. Vengono elaborati sottoforma di liste di indicatori di compromissione (IoC) circa un'area di interesse, come per esempio stringhe di codici malevoli, IP o URL malevoli o codici di hashes. Questi dati grezzi possono essere reperiti da molteplici fonti. La fonte che andrebbe prioritariamente considerata è l'analisi condotta internamente dall'azienda attraverso i sistemi di sicurezza che monitorano le attività all'interno delle infrastrutture informatiche, come per esempio i registri dei firewall e dei router. Allo stesso modo, si possono rilevare dalle attività dei SIEM condotte sui fornitori riguardanti le infrastrutture ed i log. Inoltre, questi dati si possono trovare in rete, sia su internet, che nel dark/deep web, ma in questo caso è fondamentale tener conto dell'affidabilità della fonte e della "data" di scadenza di quei dati. Più affidabili sono invece i data feed rilasciati da aziende specializzate in sicurezza che forniscono i feed, chiaramente a pagamento. I *threat data feed* devono essere contestualizzati per poter essere utilizzati e la contestualizzazione è permessa grazie alla seconda tipologia, ovvero i "dati di contesto" che permettono di creare una panoramica generale dell'evento di cyber. Questi dati rispondono alle domande "cosa/chi/dove/quando/come" e si tratta di informazioni come il nome delle minacce, la geolocalizzazione, il *timestamp* o l'evoluzione della minaccia.

---

[7] Antiseri D. e Soi A., *Intelligence e metodo scientifico*, Rubettino Editore, 2013, p.98

[8] Kaspersky Cyber security Services, 2017, p.5.https://media.kaspersky.com/en/business-security/enterprise/catalogue-2017-css-en.pdf?_ga=2.241217611.899241511.1619352861-1978372819.1619352861

I dati di contesto si possono trovare attraverso l'uso di tecniche OSINT, quindi andando a ricercare nella rete fra le fonti pubbliche aperte, come articoli su giornali online, *social network*, blog e forum specializzati; fra queste, si inseriscono anche piattaforme di *information sharing*, all'interno delle quali vengono diffuse informazioni circa gli attaccanti e le minacce cyber più in voga. Infine, è possibile attivare delle campagne di ricerca nel dark web e nei relativi forum, in quanto gli attaccanti sono soliti cercare informazioni riguardanti i target e le modalità di attacco e dunque risulta essere un buon modo per "entrare nella mente del nemico". Allo stesso tempo, anche in questo caso, questi dati possono essere reperibili grazie a processi attivati internamente nell'azienda, come, per esempio, in caso di *malware detection*.[9] La ricerca e l'analisi di malware che hanno colpito le infrastrutture interne possono essere utilizzate dagli analisti per capire in che modo l'attaccante ha implementato l'attacco cyber, sfruttando quali vulnerabilità e attraverso quali vettori. Il processo di ricerca e raccolta dati, a prescindere dalla tipologia, può essere automatizzata attraverso l'uso di piattaforme ad hoc che si occupano di generare delle *query* di ricerca interrogando le fonti predefinite, in modo da ottenere elevate quantità di dati che poi dovranno essere selezionate dall'analista. In questo caso il processo verrà velocizzato, ma saranno necessarie risorse in termini di capitale umano per procedere con l'analisi dei risultati emersi.

La seconda fase è la cosiddetta fase di elaborazione, che si tratta dell'"*insieme delle attività necessarie per trasformare la notizia*- i dati- *vale a dire l'elemento conoscitivo di base, in informazione*"[10]. Anche nel caso della CTI i dati raccolti devono essere trasformati in un linguaggio tale per il quale è possibile trasmettere il messaggio che essi contengono: dal dato grezzo all'elaborazione di un'informazione comprensibile pronta per essere sottoposta, nella fase successiva, all'analisi. Questa fase può essere processata secondo diversi metodi e framework che, prima di tutto, permettono di gestire ed organizzare i dati grezzi rilevati, contestualizzarli e collegarli fra loro e inoltre forniscono un linguaggio comune per veicolare le informazioni elaborate all'interno dell'azienda. Senza la fase di elaborazione sarebbe impossibile procedere con l'analisi, in quanto ci si troverebbe davanti a pagine e pagine di numeri e codici che di per sé hanno un significato limitato. Fra i framework utilizzati in questo ambito si riporta il "Lockheed Martin Cyber Kill Chain"[11].

---

[9] CREST, *What is cyber threat intelligence and how is it used?*, CREST, 2019 https://crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf

[10] Antiseri D. e Soi A., *Intelligence e metodo scientifico*, Rubettino Editore, 2013, p.98

[11] Lockhed M., *Gaining the Advantage*, https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

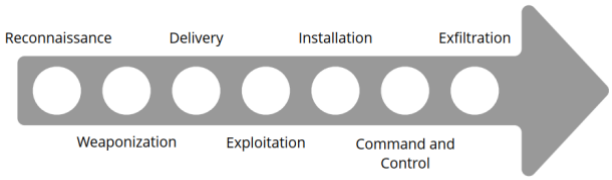

Figura 1: Kill Chain Model

Questo modello deconstrutturalizza un attacco in sette fasi (Figura 1)[12] e permette di elaborare delle contromisure in base alla fase in cui l'attacco viene identificato. Ogni fase presenta le azioni che l'attaccante pone in essere nella realizzazione di un attacco. Se applicato alla fase di elaborazione questo modello può servire per associare i dati rilevati ad una specifica fase della *kill chain* e dunque riuscire ad individuare se e in che modo questi possano essere ricondotti ad un attacco. Per esempio, se viene rilevato un contenuto malevolo all'interno di una e-mail, allora si potrà pensare che è in corso un attacco nel suo stadio *"Delivery"* della catena e dunque si potrà procedere con approfondimenti in questo senso.[13] In questo modo è possibile clusterizzare e ricondurre i dati all'interno di macrocategorie di scenari malevoli che potranno poi condurre alla fasi di analisi. Un altro metodo che può essere utilizzato è il cosiddetto "*Diamond Model*". Questo modello rappresenta le componenti di un attacco, ovvero l'avversario, la vittima, l'infrastruttura, e le *capabilities* dell'attaccante (Figura 2)[14] Ogni "punta" del diamante viene definita come un "*pivot point",* ovvero un punto di aggregazione che permette all'analista di mettere in correlazione diversi aspetti di un attacco. Anche in questo caso, se il modello viene impiegato nella fase di elaborazione, è possibile clusterizzare i dati e ricavare connessioni e collegamenti fra questi in modo da individuare un eventuale attacco e le sue caratteristiche. Per esempio, grazie al modello si può associare una capabilities ad un avversario e capire quali parti dell'infrastruttura è solito colpire; se il dato iniziale è un IP malevolo e rientra fra le "*capabilities*" del diamante, allora si potrà risalire a informazioni più specifiche riguardanti l'attaccante e ai target che è solito attaccare.[15]

[12] Pokorny Z., *The Threat Intelligence Handbook*, Cyber Edge, pp. 96-97
[13] Lockhed M., *Gaining the Advantage*, p.6 https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf
[14] Pokorny Z., *The Threat Intelligence Handbook*, Cyber Edge, p. 98
[15] Ibidem

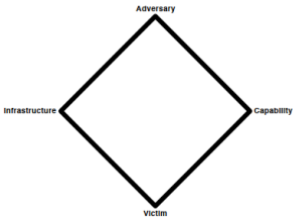

Figura 2- The Diamond Model

La fase successiva è il cuore dell'intero processo ed è l'analisi. Si tratta del momento in cui i dati processati in informazioni devono acquisire un senso pratico; ovvero una volta individuate le problematiche come si intende agire. I dati hanno preso forma, sono stati contestualizzati e hanno rilevato una potenziale minaccia o un attacco in corso, ora si tratta di capire come reagire e quali azioni intraprendere. L'analista ha il compito di elaborare un prodotto di intelligence, sotto forma di paper o report o presentazione, all'interno della quale presenta i risultati elaborati e propone delle possibili azioni successive, tenendo sempre presente che la sua analisi deve essere la base portante della decisione che verrà presa in seguito. Il modello teorico CROSSCAT[16] [17]enuncia gli otto principi fondamentali che ogni prodotto di intelligence dovrebbe rispettare al fine di realizzare un elaborato che sia efficace e che raggiunga il suo obiettivo di rappresentare la panoramica elaborata durante l'intero processo. Il modello definisce otto elementi chiave dei quali si analizzano solo quelli più rilevanti. Il primo è l'accessibilità, fondamentale infatti è in questa fase tener conto dell'audience, ovvero di chi riceverà l'analisi ed adeguare il linguaggio in tal senso. Il *Top management* avrà sicuramente un approccio più *business oriented* rispetto al *Chief Information Officer* il quale preferirà avere una panoramica più *data oriented.* Secondariamente, il fattore tempo, un'analisi di intelligence deve sempre consegnata rispettando la deadline, in quanto spesso le decisioni vengono prese in un lasso di tempo molto breve; fra l'altro, nel caso della cyber, le situazioni si evolvono così rapidamente per cui l'attesa è sicuramente un potenziale danno alle scelte. Terzo elemento, la centralizzazione, ovvero la capacità del team di intelligence di definire un punto di contatto, ovvero una figura che possa dirigere l'intero ciclo e che abbia una visione ampia di tutta l'analisi. Quarto elemento è la *Responsiveness*, in questo caso si intende il fatto che l'analista deve attenersi rigorosamente agli obiettivi fissati nella prima fase dal committente. Questo criterio va di pari passo con il concetto di oggettività, nel senso che l'analista deve essere in grado di giudicare i fatti senza farsi condizionare da preconcetti e bias.

---

[16] CREST, *What is cyber threat intelligence and how is it used?*, CREST, 2019 https://crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf p.9

[17] Payment UK, *Cyber Threat Intelligence Research paper*, http://www.foo.be/docs/informations-sharing/Payments%20UK%20Cyber%20Threat%20Intelligence%20Research%20Paper.pdf p.26

Infine, un elaborato efficace sarà tale solo se il ciclo di intelligence, così come la metodologia, viene scrupolosamente seguita e rispettata, i dati devono essere gestiti secondo dei criteri metodologici coerenti e comprovati.

Infine, l'ultima fase è quella della trasmissione del prodotto elaborato in primis al decisore, ovvero a colui che deve scegliere come agire e quali reazioni o azioni di prevenzione attivare in base alla minaccia rilevata; ma le analisi possono essere veicolate anche ad altre unità dell'azienda che potrebbero trarre benefici dalla condivisione del prodotto, anche in ottica preventiva. In seguito alla trasmissione, sarebbe buona norma realizzare dei feedback sul lavoro svolto in modo da capire se le analisi condotte hanno rispettato i *requirements* iniziali e se lo studio è stato condotto in modo efficace. Dai feedback possono nascere future analisi specifiche che daranno il via ad un nuovo ciclo di intelligence.

2. Cyber threat intelligence abilitatore di cyber defence

Nel primo capitolo è stato ampliamente definito il concetto di CTI, cercando di spiegare in che modo l'intelligence può essere impiegata nell'ambito della cyber security. A questo punto risulta necessario approfondire la tematica della CTI esplorando le sue applicazioni pratiche possibili nell'ambito delle attività di *cyber defense*, così come i suoi obiettivi, in modo da dimostrare come l'elemento di CTI risulta essere oramai imprescindibile in qualunque tipo di strategia di sicurezza e difesa cibernetica.

La cyber threat intelligence può essere impiegata in numerose situazioni differenti e proprio per la sua capacità di modellarsi alle esigenze di diversi ambiti viene spesso impiegata in modo trasversale all'interno della stessa organizzazione. Inoltre, in considerazione del fatto che la CTI viene utilizzata spesso come funzione di supporto a sistemi già esistenti e sviluppati, è necessario verificare lo "stato dell'arte" tecnologico, a livello di sistemi, software ed infrastrutture, in modo da capire in che modo le potenzialità della CTI potrebbero essere sfruttate al meglio sulla base di ciò che è già presente.

2.1 Aree di applicazione della CTI

Prima di entrare nel dettaglio dell'applicazione nuda e cruda della CTI all'interno delle diverse funzioni organizzative, è necessario analizzare gli obiettivi della threat intelligence; in questo modo risulterà più chiaro capire il perché di un'applicazione piuttosto che un'altra. Fra l'altro, è interessante notare che, come nel caso del ciclo di intelligence descritto nel capitolo uno, all'interno del quale è emersa una coerenza metodologica fra il processo di intelligence tradizionale e quello della CTI, anche in questo frangente, si rileva che gli obiettivi della CTI sono sulla stessa linea d'onda dei *main goals* della dottrina classica di intelligence. Questo per sottolineare come la CTI si può delineare come un'evoluzione, o meglio, una costola della tradizionale intelligence. Tali obiettivi possono essere riassunti in tre macro-categorie.

Prima di tutto, la CTI si prefigge come scopo quello di proporre delle previsioni su un determinato evento malevolo che potrebbe occorrere ai danni dell'organizzazione. Tipicamente questo è il focus della cyber threat intelligence strategica che, come nel caso della tradizionale intelligence strategica, punta a "*monitorare e descrivere scenari di rischio legati a fenomeni o minacce oppure a delineare le potenziali linee di azioni di attori di particolare attenzione*"[18].

[18] Antiseri D. e Soi A., *Intelligence e metodo scientifico*, Rubettino Editore, 2013, p.103.

La prevenzione risulta un momento chiave all'interno dell'ambiente dell'organizzazione, in quanto, in termini di costo, l'investimento per attività preventive è sicuramente minore rispetto ai potenziali danni sia materiali, che reputazionali, in caso di un attacco informatico. Si ricorda che il solo attacco informatico *Wannacry*, il ransomware[19] che ha attaccato numerosi sistemi aziendali in tutto il mondo, ha provocato nel 2018 danni per 8 miliardi di dollari globali[20].

Secondariamente, la CTI può essere impiegata all'interno delle attività di *detection*, si tratta della fase in cui l'organizzazione è in grado di identificare la presenza di una possibile minaccia all'interno della rete o del sistema. Può essere dunque utilizzata come chiave per individuare il potenziale attacco o per intercettare le fasi iniziali di un attacco, come abbiamo visto nella sezione precedente nel framework di Lockheed.

Infine, la CTI viene utilizzata per elaborare azioni di risposta e reazione una volta che l'attacco è stato perpetuato. Fornendo informazioni circa i TTPs e le caratteristiche e/o intenzioni dell'attaccante è in grado di fornire un quadro esatto della minaccia e dunque delle possibili soluzioni di contrattacco o difesa. A questa tipologia si potrebbe affiancare quella che viene detta nel mondo dell'intelligence come "analisi di primo impatto" ovvero quegli studi che vengono condotti "*a ridosso di un particolare evento"*[21] analizzandone le caratteristiche.

Tenendo conto di questi obiettivi si può descrivere ora quali sono i due macro ambiti di applicazione della CTI[22], scelti come i più rappresentativi all'interno di una gamma di applicazioni. In relazione alla sua funzione predittiva ed identificativa, la CTI può essere impiegata all'interno delle security operations, ovvero le attività che vengono intraprese all'interno di un SOC; mentre relativamente alla sua capacità di offrire soluzioni di reazione/risposta, la CTI viene utilizzata nelle attività di Incident Response, ovvero tutte le procedure attuate nel momento in cui si è soggetti ad un attacco informatico.

2.1.1 Prevenire: CTI e Cyber Security Operations

Prima di tutto, si deve chiarire il concetto di *cyber security operations* e si tratta di tutte quelle attività operative, condotte all'interno di un SOC, che intendono monitorare determinate infrastrutture ed identificare/individuare eventuali minacce informatiche.

---

[19] Attacchi informatici in grado di bloccare l'utilizzo di un dispositivo e dei dati relativi richiedendo un riscatto da pagare per sbloccare il device.

[20] https://www.startmag.it/innovazione/attacco-hacker-danni-economici-catastrofe-naturale/

[21] Antiseri D. e Soi A., *Intelligence e metodo scientifico*, Rubettino Editore, 2013, p.103

[22] ENISA, *Exploring the opportunities and limitations of current Threat Intelligence Platforms*, 2017, pp.12-13

Inoltre, gli operatori del SOC si occupano anche di contenere la minaccia ed, eventualmente ed in collaborazione con l'Incident Response Team, di elaborare una risposta contro l'attacco. Più precisamente il SOC utilizza delle piattaforme automatizzate (come SIEM o EDR oppure integrate in una TIP) le quali sono impostate in modo da indagare in modo continuo la rete, i sistemi, i database, le applicazioni, gli endpoint, i server cercando degli elementi che potrebbero essere considerati sospetti, i già citati *Indicator of Compromise*. Queste piattaforme generano una quantità enorme di dati (*big data*) e rilevano gli IoC tramite l'invio di Alert, ovvero delle segnalazioni, alla dashboard della piattaforma che viene continuamente consultata dall'analista. E qui emerge una prima difficoltà, la cosiddetta "*Alert fatigue*", ovvero il fatto che l'analista non è in grado di consultare ogni singolo alert ricevuto ed analizzarlo nel dettaglio, per cui vi è il rischio che qualche potenziale minaccia venga scartata o non adeguatamente indirizzata. Il report annuale di CISCO[23] riporta che fra coloro che affermano di essere soggetti a questo fenomeno, il 93% riceve quasi 5000 avvisi al giorno; sempre secondo il report "*la quantità di aziende che ricevono 100.000 o più avvisi giornalieri è aumentata dall'11% del 2017 al 17% del 2020*."[24] E' in una situazione come questa, dove emerge di fatto un gap fra informazioni generate e forza lavoro, che la CTI entra in campo, ma in che modo? In sostanza l'intelligence, o meglio la piattaforma di CTI (TIP), assume il ruolo di "*triage*", ovvero permette all'analista di capire se un determinato avviso è rilevante o meno e se si tratta di un falso positivo. Infatti, la TIP fornisce tutti quei dati di contesto all'interno del quale collocare gli avvisi ricevuti, così da valutarne la rilevanza. La CTI può fornire non solo il contesto della minaccia, ma anche altri elementi determinanti provenienti da fonti esterne, come i *threat data feed*. Elaborando un quadro completo di una specifica situazione, in cui gli indicatori di compromissione assumono un senso perché associati ad un contesto ed intersecati fra loro, l'analista sarà in grado di associare al dato che riceve dal SIEM o dalla piattaforma di CTI stessa, un valore ben definito, decidendo o meno se procedere con l'indagine. Una piattaforma di CTI offre una visualizzazione della minaccia a 360 gradi, in cui il dato grezzo viene arricchito con tutte le informazioni ricavate da fonti esterne che permettono di definire una "fotografia" immediata della minaccia e delle eventuali ripercussioni sull'organizzazione. Nell'immagine si riporta un esempio di dashboard di Swascan, un provider di CTI/TIP, che aiuta a capire in che modo i dati grezzi vengono trasformati in informazione e come questa viene messa in correlazione con altri ambiti.

[23]CISCO, Cisco Cybersecurity Report Series 2020: Proteggere il presente ed il futuro, 2020 https://www.cisco.com/c/dam/global/it_it/pdf/IT-CISO-Benchmark-Report-2020.pdf
[24] Ibidem, p. 19

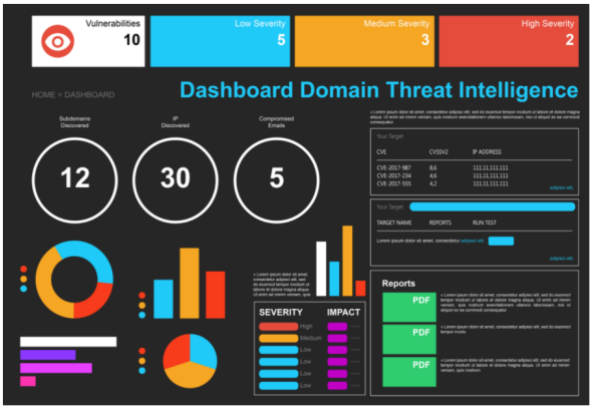

Figura 3: Esempio dashboard CTI

2.1.2 Reagire: CTI e Incident Response

Doveroso è un focus sul panorama degli attacchi cyber che sono stati perpetuati nell'ultimo anno, in modo da aver ben chiaro quanto la minaccia cyber è tuttora da considerarsi uno degli scenari più pericolosi sia a livello privato che pubblico e dunque le procedure di incident response devono essere assolutamente efficaci ed adeguate. Per il privato infatti i rischi sono connessi non solo ad una diminuzione della produzione o della fornitura dei servizi e di conseguenza ad una perdita in termini monetari, ma di particolare rilevanza è anche il danno reputazionale; infatti essere soggetti a un attacco cyber provoca un impatto negativo sugli utenti in termini di perdita di dati e disservizi, causando una notevole diminuzione della fiducia dei consumatori verso il brand e la conseguente perdita di profitto. A livello nazionale, invece, il rischio si rileva in termini di sicurezza nazionale. Infatti, il danno causato da un attacco cyber ad aziende private (come per esempio settore energetico, gas, acqua), e pubbliche può avere implicazioni su larga scala andando a causare dei rischi all'intero sistema paese. Non è un caso che sia la Direttiva NIS (e la NIS 2) che il Perimetro Cibernetico Nazionale si sono mossi in questo senso, ovvero hanno lo scopo di aumentare la sicurezza degli operatori essenziali, ovvero quelle figure che si occupano della fornitura di servizi essenziali, il cui disservizio o blocco causerebbe danni ingenti a livello europeo o nazionale. Secondo la Relazione annuale al Parlamento 2020[25] redatta dal Comparto di Intelligence delle 25.000 segnalazioni ricevute dallo CSIRT, il 13,5%, quindi all'incirca 3500, sono state classificate come incidenti informatici e di conseguenza gestite come tali. Inoltre, fra questi, 117 casi sono stati ritenuti "critici" e dunque potenzialmente rischiosi per la sicurezza nazionale.

[25] Sistema di Informazione per la Sicurezza Nazionale, *Relazione sulla politica dell'informazione per la sicurezza*, 2020 https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2021/02/RELAZIONE-ANNUALE-2020.pdf, pp.20-21

Il rapporto Clusit[26] del 2020 riporta che rispetto all'anno precedente si è avvertito un aumento del 12% degli attacchi informatici riportati a livello globale e nello specifico si rileva una media di 156 attacchi gravi al mese. Interessante è notare che di questi attacchi, più della metà (81%) sono da ricondurre all'interno della categoria del *cybercrime,* ovvero l'attività criminale perpetuata attraverso l'utilizzo di componenti tecnologiche informatiche per scopi di lucro. Fra le tecniche più diffuse fra i cybercriminali si conferma la tendenza degli anni precedenti dell'utilizzo dei malware, quasi il 42% del totale degli attacchi. Il malware è un codice maligno che infetta un dispositivo informatico in grado di disturbare le operazioni svolte dallo stesso; fra i malware i ransomware rappresentano la categoria più diffusa ovvero il 67% del totale; i ransomware sono dei malware particolari che bloccano o limitano l'accesso al dispositivo da parte dell'utente e richiedono una somma di denaro, un riscatto, per poter ripristinare la normale funzionalità del dispositivo.

Questa breve carrellata di dati fa capire quanto i sistemi informatici siano continuamente sotto attacco e per cui una procedura e dei meccanismi di *incident response* risultano vitali per qualsiasi tipo di organizzazione. Inoltre, se all'ingente quantità di incidenti che si verificano aggiungiamo anche l'evoluzione esponenziale della tecnologia e dunque dell'efficacia degli attacchi perpetuati e la difficoltà nella loro eradicazione, la situazione risulta essere ancora più critica.

Secondo il NIST, l'incident response è "*è un processo strutturato che le organizzazioni utilizzano per identificare e gestire gli incidenti di sicurezza informatica. La risposta comprende diverse fasi, tra cui la preparazione agli incidenti, il rilevamento e l'analisi di un incidente di sicurezza, il contenimento, l'eradicazione e il recupero completo, nonché l'analisi e l'apprendimento post-incidente"*[27]. Per capire in che modo la CTI può essere impiegata all'interno di questo processo e massimizzare le sue potenzialità bisogna capire prima di tutto il processo stesso. La prima fase è la rilevazione dell'incidente, che come si è spiegato nel precedente paragrafo, può essere operata da sistemi automatici come SIEM o EDR che generano degli alert in modo da avvertire il team della possibilità di un evento malevolo in corso; a quel punto è necessario capire cosa sta succedendo, attraverso l'analisi si chiarisce l'evento in sé e come si può reagire, quindi la definizione di un piano di azione; poi si passa alle due fasi più operative ovvero si mettono in atto le azioni di rimedio identificate per contenere l'attacco e minimizzare il danno per poi riparare i danni causati dall'attacco ed eliminare definitivamente la minaccia.

[26] CLUSIT, *Rapporto Clusit sulla sicurezza ICT in Italia*, 2021 pp.15-22
[27] NIST, *Computer Security Incident Handling Guide*, US Department of Commerce, 2012 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

L'ultima fase è quella dedicata alla "formazione", ovvero assimilare l'attacco avvenuto in modo da creare una *lesson learned* per il futuro. In un processo di questo tipo la reattività dell'*incident response team* risulta fondamentale in modo da limitare il più possibile i danni ed evitare la propagazione del codice malevolo. Secondo il testo *Threat Intelligence Handbook*[28], la soluzione per rendere più efficiente questo processo è basata su due attività: la previsione delle categorie di attacco e la prioritizzazione; in entrambi le casistiche la CTI può essere un elemento chiave. Per previsione si intende tutto quello di cui abbiamo già parlato prima, ovvero individuare dei segnali che possono far presupporre l'esistenza di una minaccia potenziale. Ma qui si fa un passo in avanti, non basta prevenire, ma bisogna *clusterizzare* le minacce in modo da definire un pacchetto di potenziali minacce per l'azienda, *tailorizzate* sulle sue vulnerabilità e caratteristiche, e collegarle alle possibili soluzioni. In questo modo ogni qualvolta che si notano determinati IoC e si riconducono ad una minaccia, si agirà subito con la r*emediation* collegata, in modo da evitare analisi aggiuntive e risparmiando molto tempo e diminuendo la pressione sull'intero team. Secondo aspetto, è necessario che sia ben chiara una lista delle priorità, una classifica di cosa è più pericoloso di altro, sulla base di un attenta analisi dei rischi, così da sapere cosa trattare con priorità in casi di estremi *overload* di lavoro. Anche questo diminuisce drasticamente le tempistiche e l'*effort* del team. La CTI può fornire delle risposte efficaci nei confronti di questi due aspetti. In particolare:

- Da un lato, la CTI può fornire tutte le informazioni di contesto necessarie per essere integrate ai dati grezzi rilevati dagli strumenti tecnologici (come SIEM, TIP etc.), in questo modo sarà possibile creare una catena di prevenzione assolutamente strutturata ed efficiente. Inoltre, gli strumenti di CTI sono in grado di eliminare i falsi positivi, grazie all'enorme quantità di dati esterni ed interni, in modo da alleggerire il carico di lavoro del capitale umano. In questo modo il team dovrà trattare solo le minacce verificate e già contestualizzate all'interno di una fotografia ben chiara e potrà procedere alle attività più operative;
- Dall'altro la CTI, grazie alla sua capacità di creare collegamenti e arricchire il processo di identificazione delle minacce, è in grado di assegnare alle minacce dei punteggi di rischio *(score)* così da permettere una classificazione delle minacce e di conseguenza fornirà al team la capacità di prioritizzare gli eventi rilevati.

[28] Pokorny Z., *The Threat Intelligence Handbook*, Cyber Edge, pp. 34-36

Secondo l'azienda di sicurezza Recorded Future, uno dei leader di settore nella fornitura di soluzione di CTI, l'impiego dell'intelligence nelle attività di Incident Response ha velocizzato di dieci volte le tempistiche per processare un attacco informatico[29] rispetto ai tempi impiegati nella fase pre-intelligence. Se la CTI può essere sicuramente un valore aggiunto per l'Incident Response, questa deve comunque essere impiegata tenendo conto di alcuni elementi.

Prima di tutto, il processo di intelligence deve considerare un'amplissima gamma di fonti, esterne, interne, in modo da "farcire" il più possibile i dati e renderli affidabili, in questo modo l'analista potrà basarsi solo su quelli per condurre l'analisi. Quindi individuare le fonti e verificarne l'affidabilità è un elemento determinante anche nel caso dell'intelligence applicata all'ambito cyber.

Secondariamente, le informazioni devono essere *organization oriented*, ovvero le minacce identificate devono avere un senso per l'azienda. Tener conto delle caratteristiche e delle vulnerabilità del contesto in cui si opera è vitale per eliminare i falsi positivi ed escludere le notizie che potrebbero essere irrilevanti e poco determinanti. La tecnologia esistente, in particolare quella dell'*Artificial Intelligence*, si sta sviluppando sempre di più in questo senso, ovvero le piattaforme sono in grado di imparare sulla base delle informazioni del contesto di base e su ciò che viene non scartato. In questo modo, si otterrà una piattaforma di CTI personalizzata e personalizzabile.

Infine, la CTI deve sempre essere trattata come un elemento integrante la tecnologia esistente. Si tratta di uno strumento aggiuntivo che deve essere in grado di parlare con ciò che si ha già all'interno dei propri sistemi di sicurezza. La cyber defense è un insieme di tanti meccanismi che solo integrati alla perfezione possono operare al massimo della loro funzionalità.

2.2 I limiti della Cyber Threat Intelligence

Come spiegato nei paragrafi precedenti, la CTI presenta tantissimi vantaggi per un'azienda che intende incrementare il livello di sicurezza delle proprie infrastrutture, tuttavia, vi sono alcuni elementi che possono essere identificati come limiti, o meglio come *challenges*, che devono sempre essere tenute in considerazione quando si parla di CTI. In realtà gli elementi che seguono sono gli stessi (o almeno in parte) che si possono individuare in qualsiasi attività di intelligence.

Primo elemento che può essere determinante nel ciclo di intelligence sono le fonti e la loro validazione. Per una spiegazione dettagliata della dottrina delle fonti si rimanda al testo *"OSINT Application Layer"*[30].

[29] https://www.recordedfuture.com/threat-intelligence/

[30] Nacci G., *Open Source Intelligence Application Layer*, Edizioni Epoké, 2016, pp.75-102

Per riassumere è necessario che tutte le fonti scelte o inserite in una piattaforma vengano accuratamente verificate e validate al fine di utilizzare solo dati veritieri e non potenziali generatori di *fake news.*

Secondo elemento: il rischio di *overloading*[31]. Secondo una ricerca pubblicata dall'ENISA[32], il 70% degli intervistati dichiara che le informazioni ricevute in termini di CTI sono troppo voluminose e richiederebbero troppo tempo per poter essere tutte analizzate. Questo è dovuto al fatto che le informazioni vengono spesso raccolte "manualmente", e non tramite software di aggregazione di dati e inoltre le informazioni non sono centralizzate all'interno di una piattaforma (infatti, le piattaforme di CTI sono ancora dei casi relativamente rari) per cui è difficile "tenere dietro a tutto"; in più si aggiunge il fatto che gli analisti che dovrebbero analizzare i feed non sono abbastanza esperti in materia, per cui le potenzialità della CTI si tramutano in limiti in termini di tempo e risorse. In questo caso una piattaforma di CTI dedicata potrebbe, come spiegato in precedenza, risolvere il problema dell'*overloading* grazie ai meccanismi di *triage e alerting.*

Il terzo elemento è legato invece all'impostazione delle piattaforme di CTI, ovvero il fatto che molte siano ancora più focalizzate sulla raccolta e l'analisi di IoC, mentre i dati di contesto risultano solo una parte marginale dell'intera attività. Come descritto nel paragrafo precedente, la contestualizzazione del dato grezzo è fondamentale per capire la minaccia e per evitare di trascurare informazioni importanti. Viene rilevato dunque un "peso maggiore" alla fase di raccolta dati rispetto alla fase di analisi e processo; emerge una lacuna in termini di *"advanced analytics capabilities"* e ne consegue il rischio di avere piattaforme che si limitano a individuare liste infinite di dati senza che questi assumano un valore rilevante.

Infine, l'ENISA individua un ulteriore elemento che potrebbe essere inquadrato come un limite, ovvero la difficoltà nella creazione di un legame di fiducia fra l'organizzazione e l'azienda vendor. È fondamentale che si crei un rapporto di fiducia fra i due attori affinché la CTI sia efficiente. Innanzitutto, il cliente deve fidarsi del fatto che la piattaforma in uso stia considerando fonti affidabili, che non stia infrangendo nessuna regolamentazione o normativa e che la qualità delle analisi sia di alto livello. Inoltre, l'azienda deve sentirsi tutelata in quanto condivide con il vendor dati sensibili e altamente rischiosi se condivisi. Allo stesso modo, il vendor deve confidare nel fatto che il cliente non diffonda i dati raccolti ed analizzati e che li condivida solo secondo una catena di *information sharing* decisa di comune accordo. Se non vi è un legame di questo tipo, il rischio è che le potenzialità di una piattaforma, quali la rapidità e l'efficacia, non vengano sfruttate a pieno.

---

[31] Sahrom A. , Siti Rahayu S., Aswami A., Robiah Y., Cyber Threat intelligence: challenges and issues, in "Indonesian Journal of Electrical Engineering and Computer Science" Vol. 10, No. 1, April 2018

[32] ENISA, *Exploring the opportunities and limitations of current Threat Intelligence Platforms,* 2017, pp.14-17

3. A case study: Crowdstrike experience

Sulla base delle fonti aperte disponibili non è semplice capire se e quali aziende abbiano implementato dei meccanismi di CTI come parte integrante delle proprie strategie di cyber security, proprio perché queste tematiche risultano estremamente sensibili per cui la condivisione di certi dati legati alle minacce risulterebbe pericoloso a livello di esposizione alla minaccia stessa. Ciò che invece è più semplice capire è il fatto che difficilmente le organizzazioni decidono di sviluppare un servizio di CTI interno alla funzione cyber, ma piuttosto scelgono di esternalizzare la CTI a leader del settore. Per esempio, sia Leonardo, che Autostrade per l'Italia, che ENEL hanno investito in questo ambito decidendo di acquistare contenuti di intelligence relative alle minacce in modo *outsourced*, i cui dati vengono poi analizzati ed integrati dagli analisti interni. Esternalizzare un servizio di questo tipo risulta essere più conveniente per l'azienda sotto diversi punti di vista. Prima di tutto si tratta di budget e risorse di capitale umano, infatti un'intera funzione specializzata interamente sulla raccolta ed analisi di elementi utili alla CTI rappresenterebbe non solo un costo non sostenibile, ma, inoltre, necessiterebbe un alto numero di personale a discapito di altre attività altrettanto necessarie. Secondariamente, le aziende di security fornitrici di questo tipo di servizio sono altamente specializzate in questo contesto e impiegano expertise e risorse ad hoc, fornendo dati e analisi puntuali ai clienti finali. Infine, le fonti alle quali queste aziende possono attingere sono molto più ampie, si pensi al dark/deep web, rispetto ad aziende finali che avrebbero difficoltà ad ottenere informazioni da fonti non convenzionali. Quindi, se risulta difficile analizzare il CTI di un'azienda finale, più agevole è invece l'analisi di un'azienda supplier di prodotti. In particolare, nel seguente capitolo si andrà ad analizzare il leader di mercato a livello globale, ovvero CrowdStrike con la sua piattaforma di CTI Falcon X. In un primo momento si andrà a descrivere brevemente la piattaforma in modo da capirne il funzionamento, successivamente si farà un focus su uno dei risultati più rilevanti del 2021 emersi dalla ricerca di intelligence dell'azienda inerente le minacce informatiche provenienti dalla Cina.

3.1 CrowdStrike Falcon X

CrowdStrike è un'azienda americana, avente sede in California, attiva dal 2011 nel settore delle fornitura di servizi tecnologici a tutela dei sistemi e delle infrastrutture informatiche ed informative. Nata come un'azienda dedicata interamente alla sicurezza in cloud si sviluppa investendo sul settore della cyber threat intelligence acquisendo lo status di leader del settore; nella classifica Forrester Wave del 2021, che analizza le migliori piattaforme di CTI attive nel mercato, CrowdStrike si posiziona sul podio dei migliori *vendor* in termini di miglior strategia e offerta di mercato.[33]

CrowdStrike[34] offre un servizio di cyber threat intelligence completo, denominato *Falcon X*. Sulla base di quanto detto in precedenza una piattaforma di CTI deve essere composta da due elementi: uno strumento di raccolta dati grezzi automatizzato e un'attività di raccolta e analisi di dati di contesto condotta da analisti. Il primo elemento viene fornito dalla piattaforma Falcon, ovvero un sistema cloud-native progettato per la messa in sicurezza degli endpoint in modo da identificare e bloccare le intrusioni. I punti di forza della piattaforma sono identificabili in due elementi: prima di tutto si tratta di una piattaforma interamente in cloud, ovvero grazie ai dati raccolti in *crowdsourcing* e alle analisi presenti in cloud, identifica e blocca le intrusioni in modo semplice, automatico e veloce; inoltre la piattaforma è alimentata da big data e dall'intelligenza artificiale incrementando l'efficacia e la precisione dei risultati. Si tratta dunque di un meccanismo che conduce un'attività di investigazione degli incidenti e delle potenziali minacce ai danni delle infrastrutture aziendali, producendo dati grezzi, come IoC o analisi di malware. Per quantificare il lavoro della piattaforma, si pensi che questa è in grado di rilevare più di 5 trilioni di eventi malevoli a settimana. Il secondo elemento, ovvero quello umano, in grado di contestualizzare, valorizzare, correlare i dati fra loro sulla base di altre tipologie di fonti, fornisce al cliente delle dashboard di visualizzazione dei dati (Vedi figura 4), dei report e delle analisi di intelligence chiare e complete dove vengono esposti i rischi e le minacce rilevate contestualizzate all'interno dell'ambiente dell'organizzazione. Inoltre, l'azienda garantisce dei servizi ad hoc per il cliente, in modo da fornire un quadro informativo specializzato sul settore e sulle necessità del cliente stesso, come per esempio, attività di monitoraggio dei social media, dei *botnets*, dei *paste sites* in modo da valutare l'esposizione dell'azienda, del suo personale e del brand. Infine, è possibile anche integrare a queste funzioni "base" la possibilità di ricevere soluzioni di difesa e risposta sulla base delle minacce rilevate.

---

[33] Kime B. e Pikulik E., *The Forrester Wave™: External Threat Intelligence Services, Q1 2021 The 12 Providers That Matter Most And How They Stack Up*, Forrester Research, 2021

[34] https://www.CrowdStrike.com/endpoint-security-products/falcon-x-threat-intelligence/

Infatti, si rileva che annualmente, grazie alle soluzioni fornite, siano stati bloccati più di 75000 *data breach.*[35]

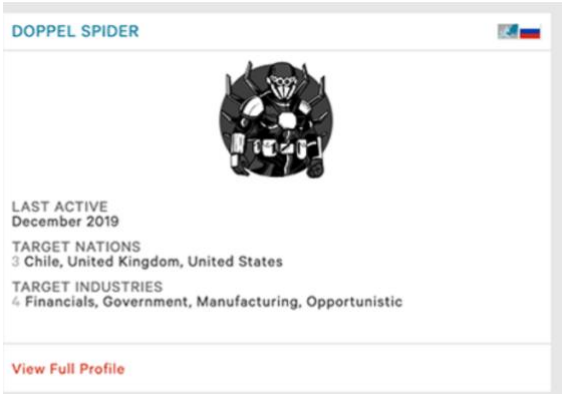

Figura 4: Esempio di dashboard

3.2 Un risultato tangibile: la minaccia informatica della Cina

Dopo aver descritto la piattaforma offerta dal colosso CrowdStrike è interessante riportare un esempio di report elaborato dagli analisti grazie alla CTI in modo da capire concretamente in che modo viene definito e condiviso un prodotto di intelligence in ambito cyber. L'esempio che si analizza, parte del Report annuale condiviso da Crowstrike inerente le minacce più rilevanti identificate attraverso la piattaforma e i servizi ad essa collegati nel 2021[36], si focalizza sulla tipologia di intrusione definita "mirata" e "motivata da interessi strategici nazionali e tentativi di spionaggio", nello specifico, quella riguardante le minacce provenienti dalla Cina. Si è optato per il caso cinese in quanto la Repubblica Popolare Cinese risulta essere determinante nel contesto cyber soprattutto in questo periodo di pandemia.

[35] https://www.CrowdStrike.com/wp-content/uploads/2020/03/threat-graph.pdf
[36] CrowdStrike, *Global Threat Report 2021*, 2021, https://go.CrowdStrike.com/rs/281-OBQ-266/images/Report2021GTRIT.pdf

Grazie ai dati e all'analisi condotte è possibile definire un quadro della minaccia cyber collegata allo stato cinese sotto tre punti di vista:

1. Obiettivo e motivazione degli attaccanti. Sulla base dei dati ricavati ed incrociati fra loro, è emerso che la maggior parte dei gruppi cybercriminali individuati sono *nation-state*, ovvero presumibilmente finanziati e supportati dallo stato cinese. Secondo CrowdStrike, la Cina si classifica fra gli attaccanti *nation-state* più attivi, si sono registrati infatti almeno 11 attaccanti noti cinesi e 7 potenzialmente riconducibili alla Cina considerando la tipologia di attività. Non a caso, infatti, gli obiettivi degli attacchi rientrano nell'ambito dello spionaggio industriale, furto di proprietà intellettuale e sorveglianza.
2. Settori maggiormente attaccati. Sono stati identificati i settori produttivi e di servizi maggiormente colpiti da attacchi di questo tipo; rientrano fra questi il settore tecnologico, sanitario, delle telecomunicazioni e quello pubblico/governativo.
3. TTP. Relativamente alla tipologia di minaccia, sono stati individuati attacchi caratterizzati dall'utilizzo di nuove tecnologie e strumenti, confermando l'intenzione della Cina di investire nel settore cyber. In particolare, si è registrato come avversario maggiormente attivo quello definito come *Wicked Panda;* si tratta di un attore attivo ad ampio spettro capace di sfruttare diverse vulnerabilità (CVE- 2019-19781; CVE-10189)[37] colpendo diverse aree e settori. A livello di strategia di intrusione, *Wicked Panda* è in grado di compromettere il sistema utilizzando una varietà di strumenti *open source*[38] per infettare e navigare nella rete del sistema; fra l'altro, analizzando la tipologia di intrusione, si potrebbe dedurre che questi sistemi siano riconducibili ad appaltatori pubblici, giusto per confermare l'ipotesi di *nation state basis*. Dopo essere entrato nel sistema, l'attaccante opera impiantando il *payload* Cobalt Strike o Meterpreter per richiedere un riscatto alla vittima. Cobalt Strike e Meterpreter rientrano nella categoria dei malware e sono stati creati in modo da controllare da remoto un sistema e viene eseguito direttamente nella memoria del dispositivo. Questi malware permettono altri malware di infettare il sistema, come per esempio dei ransomware che operano crittografando i dati della vittima e proponendole un riscatto in cambio dei dati decriptati.[39]

[37] Codici identificativi di vulnerabilità
[38] https://www.CrowdStrike.com/blog/meet-CrowdStrikes-adversary-of-the-month-for-july-wicked-spider/
[39] https://www.pcrisk.it/guide-per-la-rimozione/9603-meterpreter-trojan

Il report di intelligence appena analizzato, riporta dunque una parte descrittiva della minaccia e delle sue caratteristiche e aggiunge anche una parte predittiva sull'evoluzione della criticità individuata. Infatti, gli analisti prevedono che nel corso del prossimo anno questa tipologia di minaccia continuerà a svilupparsi seguendo questo *template* di attacco sfruttando le vulnerabilità descritte e utilizzando gli stessi vettori di attacco. L'esempio riportato chiarisce come, a partire da dati grezzi, ed elaborati in connessione con dati di contesto relativi alla situazione cinese, ad obiettivi politico strategici ed altre informazioni collegate agli attaccanti, è stato possibile fornire una panoramica chiara della minaccia cyber e della sua rischiosità.

Conclusioni

Attraverso l'analisi condotta nel presente paper della Cyber Threat Intelligence e delle sue caratteristiche si è dimostrato come il mondo dell'intelligence e quello della cyber security sono due ambiti estremamente connessi in particolare in un periodo come quello attuale dove la tecnologia e il digitale rappresentano la quotidianità ed il nostro futuro.

Nel primo capitolo, attraverso l'analisi della teoria e della metodologia associata alla CTI, si è spiegato come l'intelligence possa essere applicata al campo della sicurezza informatica ed in particolare, si è illustrato come il ciclo tipico dell'intelligence tradizionale si possa adattare all'ambito della cyber. Approfondendo le diverse fasi del ciclo sono state evidenziate le analogie fra i due ambiti e si è dimostrato come la cyber threat intelligence non è altro che una costola dell'intelligence, la quale risulta essere un metodo di analisi assolutamente attuale e necessario per lo studio di fenomeni quali le minacce cibernetiche.

Nel secondo capitolo, invece, ci si è addentrati nel livello più operativo della CTI illustrando quali sono le principali applicazioni della CTI in ambito sicurezza informatica, in particolare, ci si è soffermati sulle *security operations* e sull'*incident response*. Valutando nel dettaglio entrambi gli ambiti è emerso come la CTI possa essere uno strumento facilitatore di questi processi in termini di efficacia e reattività. La CTI, infatti, permette di incrementare il processo di raccolta dati e di analisi in modo da fornire risposte in tempi più brevi ed estremamente più precisi in termini di contenuto. Di conseguenza, appare chiaro il fatto che la CTI dovrebbe rappresentare un elemento chiave delle strategie di cyber security delle aziende sia a livello pubblico che privato. Ancora una volta, l'intelligence assume un ruolo decisivo nell'offrire un supporto al decisore.

Infine, nel terzo capitolo, si è illustrato un case study, sebbene le informazioni a disposizione fossero poche e di alto livello data la sensibilità dei temi affrontati, descrivendo la proposta di una piattaforma di CTI offerta da un leader di settore.

Dopo aver brevemente spiegato le caratteristiche della TIP, si è preso in esame uno dei risultati emersi nel corso di un anno, ovvero la minaccia cibernetica proveniente dalla Cina, sulla base dei dati raccolti ed analizzati dall'azienda. In questo modo si è cercato di mostrare quale fosse il risultato tangibile di un documento di intelligence prodotto dalla CTI, sottolineando come questa non è fatta di soli codici e numeri, ma di contenuti elaborati di alto livello.

Come è stato ampliamente discusso nel corso del presente lavoro nonostante i vantaggi associati alla CTI, i casi di applicazione nelle realtà italiane sono ancora pochi. Risulta necessario un approfondimento di questa tematica da parte delle aziende, incluse le PMI, in modo da integrare la CTI nelle strategie cyber così da sfruttare le sue potenzialità contro la crescente minaccia cyber.

SIGLE ED ABBREVIAZIONI

CISO: Chief Information Security Officer

CLOSINT: Close Source Intelligence

CSIRT: Computer Security Incident Response Team

CTI: Cyber Threat Intelligence

EDR: End point Detection and Response

ENISA: European Network and Information Security Agency

IOC: Indicators of Compromission

OSINT: Open Source Intelligence

M2M: Machine to machine

NIS: Network and Information Security

NIST: National Institute of Standards and Technology

PMI: Piccole e medie imprese

SOC: Security Orchestration, Automation and Response

TIP: Threat Intelligence Platform

TTP: Tactics, techniques and procedures