UNIVERSITÀ
DEGLI STUDI
DI BRESCIA

Relazione per il Corso di “SICUREZZA INFORMATICA”

PROIEZIONE DI STRUMENTI IN AMBITO CYBERSECURITY RISPETTO A METODOLOGIE STANDARD E PROTOCOLLI DI COMUNICAZIONE CTI

Docente del corso:
Prof. Federico Cerutti

Studenti:
Mattia Gozzoli - 710042
Matteo Rubagotti - 715162

A.A. 2021/2022

INDICE

Introduzione

Questo elaborato ha lo scopo di documentare l'analisi di strumenti software in ambito cybersecurity per ottenere informazioni sulla copertura rispetto alle metodologie standard più utilizzate e ai linguaggi, protocolli e piattaforme di comunicazione più diffuse in ambito Cybersecurity.

Nella prima parte, dopo un'introduzione riguardo all'importanza dell'*Information Security,* la trattazione prosegue descrivendo e analizzando le metodologie standard più diffuse presenti in letteratura. La prima metodologia descritta è la normativa *ISO 27000,* seguita dal *Framework NIST* per poi passare alla *Cyber Kill Chain*, un modello che illustra una sequenza di fasi di un possibile attacco informatico.

Nella seconda parte vengono illustrati la metodologia utilizzata per condurre l'analisi degli strumenti CTIA e i risultati ottenuti. L'analisi dettagliata è stata svolta sfruttando un file Excel, allegato alla relazione, in modo da ottenere una visualizzazione più immediata e intuitiva delle informazioni elaborate.

Infine vengono presentati gli standard di comunicazione più diffusi in ambito *cybersecurity* e viene effettuata una mappatura per determinare quali tool tra quelli presi in considerazione siano conformi a questi standard.
In quest'ottica verranno presentati gli standard STIX/TAXII, MAEC e MISP.

In coda alla relazione sono presenti quattro appendici: **Appendice A**, **Appendice B**, **Appendice C** e **Appendice D** che descrivono in modo più approfondito alcuni concetti delle metodologie e degli standard di comunicazione precedentemente citati.

1 Information Security

1.1 La sicurezza delle informazioni

La protezione delle risorse informative attraverso la definizione, il raggiungimento, il mantenimento e il miglioramento della sicurezza delle informazioni è essenziale per consentire a un'organizzazione di raggiungere i propri obiettivi e mantenere e migliorare la propria conformità legale oltre che garantire un'immagine positiva dell'azienda.
Il termine "*Information Security*" si basa generalmente sul fatto che le informazioni siano considerate un bene il cui valore richiede un'adeguata protezione, ad esempio contro la perdita di disponibilità, riservatezza e integrità. Poiché i rischi per la sicurezza delle informazioni e l'efficacia dei controlli cambiano a seconda delle mutevoli circostanze, le organizzazioni devono costantemente:

- monitorare e valutare l'efficacia dei controlli e delle procedure implementate;
- identificare i rischi emergenti da trattare;
- selezionare, attuare e migliorare i controlli appropriati secondo le necessità.

Per correlare e coordinare tali attività di sicurezza delle informazioni ogni organizzazione deve stabilire la propria politica e obiettivi per la sicurezza delle informazioni da raggiungere in modo efficace.

1.2 Le difficoltà in ambito di sicurezza delle informazioni

Le tecnologie evolvono rapidamente e le tecniche di attacco e i crimini informatici crescono quotidianamente, ampliando sempre di più il proprio ambito di applicazione (per es. sistemi finanziari, e-commerce, infrastrutture critiche). Oltre a questo, le complessità in merito alla gestione delle informazioni e dei dati che devono essere gestiti all'interno di un'organizzazione crescono in maniera vertiginosa ogni giorno e anche i requisiti legali evolvono nel tempo per andare incontro alle garanzie di libertà degli individui (come nel caso del Regolamento generale sulla protezione dei dati, *GDPR*). Anche le necessità di conservazione per statistiche e conformità diventano sempre più ampie, basti pensare alla conservazione a norma dei documenti digitali. In questo scenario, spesso le organizzazioni aziendali approcciano il problema della sicurezza solo da un punto di vista tecnico, non considerando quanto segue:

- l'approccio tecnico risulta parziale e incompleto: è un approccio non formale e rappresenta una reazione successiva ad un evento già accaduto (all'azienda o a terzi);
- le parti interessate spesso non sono formalmente e direttamente coinvolte;
- i proprietari delle informazioni e dei dati non sono ben definiti;
- non si ha coscienza di quali siano le informazioni gestite e quanto queste siano critiche per l'azienda;
- la sola conformità a requisiti o leggi non è sufficiente.

2 Le metodologie in ambito di Sicurezza Informatica

Partendo dalle difficoltà descritte nei paragrafi precedenti, alcune metodologie come il *Framework NIST* e la normativa *ISO 27000* si sono distinte come guide per le organizzazioni che vogliono implementare le corrette misure tecnologiche e organizzative nell'ambito della sicurezza delle informazioni.
Entrambi gli standard sono tecnologicamente neutri, in quanto non impongono specifiche precise, ed hanno lo scopo di conseguire benefici aziendali pur rispettando i requisiti legali e normativi oltre alle esigenze di tutte le parti interessate. La somiglianza maggiore sta nel fatto che entrambi sono basati sulla gestione del **rischio**: ciò significa che entrambi richiedono che le salvaguardie siano implementate solo se vengono rilevati determinati rischi di sicurezza informatica.
È importante considerare anche la prospettiva di un attaccante in modo da permettere ai team di cybersecurity di prevenire e mitigare con più facilità attacchi informatici, e per questo è bene esaminare ed analizzare la *Cyber Kill Chain*.

Nei successivi paragrafi vengono proposti i concetti fondamentali per comprendere ciascuna metodologia.

2.1 La serie ISO/IEC 27000

La serie *ISO/IEC 27000* "*Information Security Management Systems* (*ISMS*) *Family of Standards*" (nota in Italia come famiglia di norme SGSI, "*Sistemi di Gestione per la Sicurezza delle Informazioni*") è uno standard di sicurezza informatica redatto dalla *International Organization for Standardization* che raggruppa un insieme di norme internazionali che si prefiggono di proteggere le informazioni che vengono mantenute ed elaborate da un'organizzazione. Attraverso questa famiglia di norme, le organizzazioni possono sviluppare ed implementare un proprio sistema per la gestione della sicurezza informatica per le informazioni finanziarie, la proprietà intellettuale ed i dati dei dipendenti, di clienti o di terzi. Lo scopo ultimo è quello di proteggere le informazioni da possibili attacchi informatici, errori umani, calamità naturali o da qualsiasi altra vulnerabilità che si può presentare durante l'utilizzo di un sistema informatico.
Questi standard possono essere utilizzati anche per preparare valutazioni indipendenti (audit[1]) del loro *ISMS* applicato alla protezione delle informazioni.

La serie *ISO/IEC 27000* fornisce un modello, definito da esperti di settore, da seguire nella creazione e nel mantenimento di un sistema di gestione e, data la natura dinamica del rischio e delle tecnologie in ambito di sicurezza delle informazioni, si basa su un approccio ciclico (PDCA[2]) rivolto al miglioramento continuo.

[1] **audit**: processo sistematico, indipendente e documentato, volto ad acquisire elementi probativi e valutarli oggettivamente per determinare la misura in cui i criteri di audit sono soddisfatti. Un audit può essere un audit interno (*first party*) o esterno (*second/third party*) e può essere un audit combinato (che combina due o più discipline).
[2] **PDCA**: il ciclo di Deming (o ciclo di PDCA, acronimo dall'inglese *Plan-Do-Check-Act*, in italiano "Pianificare - Fare - Verificare - Agire") è un metodo di gestione iterativo in quattro fasi utilizzato per il controllo e il miglioramento continuo dei processi e dei prodotti.

2.2 Il Framework NIST

Il ***NIST Cybersecurity Framework*** è un insieme di linee guida per mitigare i rischi per la sicurezza informatica delle organizzazioni, pubblicato dal *National Institute of Standards and Technology* (NIST) degli Stati Uniti sulla base di standard, linee guida e pratiche esistenti. Il *framework* fornisce una struttura organizzativa comune per molteplici approcci alla sicurezza informatica riunendo standard, linee guida e pratiche che oggi funzionano efficacemente, oltre a linee guida per quanto riguarda la protezione della privacy e delle libertà civili in un contesto di sicurezza informatica. In quest'ottica il *Framework NIST* è un documento vivo e continuerà ad essere aggiornato e migliorato nel tempo ove necessario.

Basandosi su tali standard, linee guida e pratiche, il *framework* fornisce una tassonomia e un meccanismo comune a tutte le organizzazioni per:

1) Descrivere la loro attuale situazione di sicurezza informatica;
2) Descrivere il profilo di sicurezza informatica che vogliono raggiungere;
3) Identificare e dare priorità alle opportunità di miglioramento nel contesto di un processo continuo e ripetibile;
4) Valutare i progressi effettuati allo scopo di raggiungere il profilo determinato;
5) Impostare una linea comunicativa ben definita che aiuti nella gestione del rischio informatico.

Il *Framework NIST* è diviso in tre componenti fondamentali: *Core*, *Profile*, *Implementation Tier*. Ciascun componente del *framework* rafforza la connessione tra business/mission driver e le attività di cybersecurity. Il ***Core*** contiene una serie di attività, risultati e riferimenti su aspetti e approcci alla sicurezza informatica. Gli ***Implementation Tier*** vengono utilizzati da un'organizzazione per chiarire a se stessa e ai suoi partner come viene affrontato il rischio per la sicurezza informatica e il grado di sofisticatezza del suo approccio di gestione. Un ***Profile*** è un elenco che un'organizzazione ha scelto tra le categorie e le sottocategorie, in base alle proprie esigenze e alle valutazioni del rischio.

2.2.1 Il Core

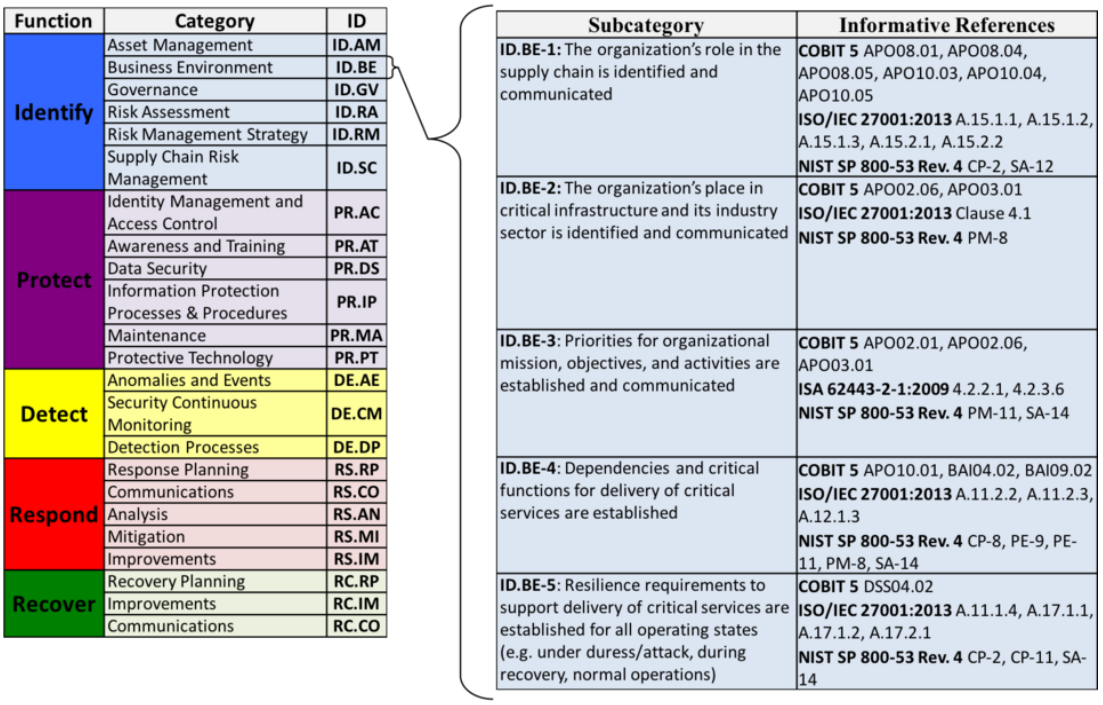
Il ***Core*** è un insieme di attività di sicurezza informatica, risultati desiderati e riferimenti applicabili comuni a tutti i settori delle infrastrutture critiche. L'obiettivo di questo componente è quello di favorire la comunicazione e la collaborazione tra team multidisciplinari evitando un linguaggio tecnico in favore di uno più semplice e intuitivo. Il *Core* è costituito da tre parti: *Funzioni*, *Categorie* e *Sottocategorie*.

Le ***Funzioni*** sono cinque e vengono descritte attraverso un alto livello di astrazione: *Identify, Protect, Detect, Respond, e Recover*. Se considerate insieme, queste funzioni forniscono una visione strategica di alto livello del ciclo di vita della gestione del rischio di sicurezza informatica da parte di un'organizzazione. Il *Core* identifica quindi le ***Categorie*** e le ***Sottocategorie*** chiave sottostanti, che sono risultati discreti, per ciascuna funzione e le abbina a riferimenti informativi di esempio come standard, linee guida e pratiche esistenti per ciascuna sottocategoria. L'utilità di queste cinque funzioni è che esse possono essere utilizzate non solamente in un discorso prettamente informatico, ma sono

applicabili anche in contesti di gestione del rischio più generali. Per ognuna di queste, proseguendo, vi sono assegnate diverse categorie per un totale di **23**.

Le ***Categorie*** vengono utilizzate per riportare i possibili obiettivi che da un punto di vista della sicurezza informatica un'organizzazione dovrebbe perseguire. A tal fine, queste sono state progettate senza essere eccessivamente dettagliate in modo tale da fornire un raggio d'azione il più ampio possibile: vengono infatti affrontati tematiche quali, a titolo esemplificativo e non esaustivo, la sicurezza fisica, la sicurezza logica o la sicurezza dei dati personali. A loro volta, infine, le categorie presentano delle sottocategorie.

Le ***Sottocategorie*** rappresentano il livello di astrazione più profondo del *Core*. Ci sono **108** sottocategorie e ciascuna di queste è una dichiarazione orientata ai risultati che fornisce considerazioni per creare o migliorare un programma di cybersecurity.
Esempi di sottocategorie includono: "*I sistemi di informazione esterni sono catalogati*", "*I dati inattivi sono protetti*" e "*Le notifiche dai sistemi di rilevamento vengono esaminate*".
Ogni sottocategoria, infine, è corredata da un insieme di riferimenti a documenti tecnici aggiuntivi, detti ***Informative Reference***, che possono essere utilizzati, a discrezione dell'organizzazione, come elementi di riferimento da seguire per raggiungere gli obiettivi prefissati nelle sottocategorie. Un esempio di referenza sono le norme *ISO 27000* correlate alla sottocategoria considerata.



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Figura 1: La struttura del Core - Fonte:
https://www.nist.gov/cyberframework/online-learning/components-framework

2.2.2 Le cinque funzioni

Lo scopo delle cinque funzioni è quello di fornire una guida agli operatori del settore e fissare quelle che sono, a livello astratto, le attività principali da eseguire al fine di

intraprendere un efficace programma di miglioramento della sicurezza di un'infrastruttura informatica.

La prima funzione indicata nel *framework* è l'*identificazione* (***identify***). Come in molti contesti legati alla gestione del rischio, anche nell'ambito della sicurezza informatica mettere a fuoco quello che è il contesto organizzativo comprendendo elementi quali l'ambito applicativo dell'organizzazione, l'ambiente esterno o gli asset da tutelare rappresenta un passo fondamentale per la buona riuscita di un programma per la messa in sicurezza di un'infrastruttura informatica.
Esempi di categorie includono: gestione degli *asset*, ambiente di business, governance, valutazione del rischio e strategia di gestione del rischio.

La seconda funzione indicata nella metodologia è la *protezione* (***protect***). In questa attività si vanno a identificare quelle soluzioni che hanno il ruolo di impedire il verificarsi di un incidente di sicurezza informatico o, quantomeno, di mitigare gli effetti negativi. Esempi di categorie di risultati all'interno di questa funzione includono: gestione dell'identità e controllo degli accessi, consapevolezza e formazione, la sicurezza dei dati, processi e procedure di protezione delle informazioni, manutenzione e tecnologia protettiva.

La terza funzione è quella di *rilevamento* (***detect***), nella quale vengono indicate delle metodologie volte a rilevare tempestivamente e identificare degli eventi potenzialmente configurabili come incidenti informatici. Un risultato desiderato in questo ambito sarebbe quello per cui all'interno dell'organizzazione si fosse sempre in grado di rilevare eventuali eventi anomali e stabilire il loro potenziale impatto sull'infrastruttura. Esempi di categorie di risultati all'interno di questa funzione includono: anomalie ed eventi, monitoraggio continuo della sicurezza e processi di rilevamento.

La quarta funzione è quella di *risposta* (***respond***) e riguarda quell'insieme di attività che dovrebbero essere intraprese al verificarsi di un incidente di sicurezza. L'obiettivo di queste attività è, dunque, ridurre il più possibile l'impatto degli effettivi negativi che un incidente ha provocato all'interno dell'infrastruttura organizzativa.
Un esempio sono le attività di mitigazione dell'incidente per prevenire che l'impatto e gli eventuali danni dell'incidente si espandano e colpiscano una porzione più ampia dell'infrastruttura. Altri esempi di categorie includono: pianificazione della risposta; comunicazioni e analisi.

La quinta ed ultima funzione è quella di *ripristino* (***recover***): una volta che l'incidente è stato rilevato e gestito bisognerà ripristinare lo stato dell'infrastruttura a una situazione di normalità. Al fine di raggiungere questo stato è necessario implementare delle soluzioni che influiscono sulla resilienza dell'infrastruttura e che permettono di effettuare delle attività di ripristino. Esempi di categorie di risultati all'interno di questa funzione includono: pianificazione del recupero, miglioramenti e comunicazioni.

2.3 ISO 27000 e Framework NIST a confronto

La peculiarità che più spicca dello standard *ISO 27000* è che le aziende possono ottenere la relativa certificazione: questo significa che una società può dimostrare ai propri clienti, partner, azionisti, agenzie governative che può effettivamente mantenere le proprie informazioni al sicuro. Inoltre, a differenza del *NIST Cybersecurity Framework*, l'*ISO 27000*:

- definisce chiaramente quali documenti siano obbligatori e quale sia il minimo livello di misure da implementare;
- definisce un approccio di sistema e un insieme di requisiti che hanno delle relazioni specifiche tra loro;
- stabilisce che cosa deve essere soddisfatto e non in che modo questo debba essere soddisfatto.

Infine, mentre il *Framework NIST* si concentra su come pianificare e attuare la sicurezza informatica, lo standard *ISO 27000* adotta un approccio molto più ampio: la sua metodologia basata sul ciclo *Plan-Do-Check-Act* (*PDCA*) mira a costruire un sistema di gestione che non solo progetta e implementa la cybersecurity, ma mantiene e migliora anche l'intero sistema di gestione delle informazioni. Questo aspetto è rilevante perché la pratica ha dimostrato che non è sufficiente pianificare ed implementare un sistema, in quanto, senza misurazione, revisione, audit, azioni correttive e miglioramenti costanti tale sistema tenderebbe a deteriorarsi gradualmente nel tempo fino a perdere il proprio scopo.

2.4 Un terzo possibile approccio: la Cyber Kill Chain

La *Cyber Kill Chain*, sviluppata dalla Lockheed Martin Corporation[3], è un modello a fasi che consente di identificare i vari passaggi necessari all'esecuzione di un attacco informatico rendendolo più comprensibile e in questo modo avere meno difficoltà nell'individuare le misure tecniche per contrastarlo.
Una nuova classe di minacce, soprannominata *Advanced Persistent Threat* (APT), rappresenta avversari ben dotati e addestrati che conducono campagne di intrusione pluriennali che prendono di mira informazioni economiche, proprietarie o di sicurezza nazionale altamente sensibili. Questi avversari raggiungono i loro obiettivi utilizzando strumenti e tecniche avanzate, progettate per sconfiggere la maggior parte dei meccanismi di difesa delle reti di computer convenzionali.

Utilizzare un modello di *Kill Chain* per descrivere le fasi delle intrusioni, mappare degli indicatori, identificare i modelli che collegano le intrusioni individuali a campagne più ampie e comprendere la natura iterativa della raccolta di informazioni costituiscono la base di quella che viene definita *Intelligence-driven Computer Network Defence*.
Questo approccio riduce la probabilità di successo dell'avversario, fornisce metriche per quanto riguarda prestazioni ed efficacia e aiuta nella definizione delle priorità degli investimenti in risorse per la sicurezza delle informazioni.

[3] **Lockheed Martin Corporation**: è un'impresa statunitense attiva nei settori dell'ingegneria spaziale e della difesa formata nel 1995. [Fonte: *Wikipedia*]

Con il termine "*Kill Chain*" si indica quindi la struttura dell'intrusione ed il modello corrispondente che fornisce l'analisi per informare l'intelligence di sicurezza in merito alle azioni da intraprendere. L'analisi della *Kill Chain* illustra come l'avversario debba progredire con successo attraverso ogni fase della catena prima di poter raggiungere l'obiettivo desiderato, ma anche solo una mitigazione di una fase è in grado di interrompere la catena e perciò anche l'attacco dell'avversario.

2.4.1 La struttura della Cyber Kill Chain

La *Kill Chain* è definita nelle fasi seguenti:
1. **Reconnaissance** - Ricerca, identificazione e selezione di obiettivi, spesso rappresentati come scansioni di siti Web, atti di conferenze, mailing list, relazioni sociali o informazioni su tecnologie specifiche.

2. **Weaponization** - Accoppiare un trojan di accesso remoto con un exploit in un payload consegnabile, in genere per mezzo di uno strumento automatizzato chiamato *weaponizer*. Sempre più spesso i file di dati delle applicazioni client come PDF o documenti di Microsoft Office vengono utilizzati come arma per l'attacco dato che risultano meno sospetti alla maggioranza delle persone che utilizzano un dispositivo elettronico.

3. **Delivery** - Trasmissione dell'arma all'ambiente preso di mira.
I tre vettori di consegna più utilizzati dagli attori *APT*, come osservato dal *Lockheed Martin Computer Incident Response Team* per gli anni 2004-2010, sono allegati e-mail, siti Web e dispositivi USB rimovibili.

4. **Exploitation** - L'exploit attiva il codice malevolo degli intrusi.
Spesso vengono prese di mira applicazioni o vulnerabilità del sistema operativo, ma potrebbero semplicemente venir sfruttati gli utenti o funzionalità del sistema operativo che eseguono automaticamente il codice.

5. **Installation** - L'installazione di un trojan o di una backdoor di accesso remoto sul sistema vittima consente all'avversario di mantenere la persistenza all'interno dell'ambiente.

6. **Comando e Controllo** (C2) - In genere, gli host compromessi devono inviare un beacon in uscita ad un server per stabilire un canale C2. Il malware APT richiede in particolare un'interazione manuale piuttosto che un'esecuzione automatica. Una volta stabilito il canale C2 gli intrusi hanno accesso all'interno dell'ambiente della vittima.

7. **Actions on Objectives** - Solo ora, dopo aver superato le prime sei fasi, gli intrusi possono intraprendere azioni per raggiungere i loro obiettivi originali.
Tipicamente l'obiettivo è l'esfiltrazione dei dati che comporta la raccolta, la crittografazione e l'estrazione di informazioni dall'ambiente della vittima; anche le violazioni dell'integrità o della disponibilità dei dati e/o servizi sono potenziali obiettivi.

3 Analisi degli strumenti CTIA

Questa sezione si occupa di definire la metodologia che è stata adottata durante l'analisi degli strumenti maggiormente utilizzati dai team di *Cyber Threat Intelligence Analysis (CTIA)* con particolare attenzione alla copertura che ogni tool è in grado di garantire rispetto alle funzioni caratterizzanti del *Cybersecurity NIST Framework* e alle fasi della *Cyber Kill Chain*.

Di seguito viene riportato l'elenco degli strumenti sottoposti alla nostra analisi:

1. *ESET Endpoint Security*
2. *ESET Endpoint Encryption*
3. *Cynet 360 AutoXDR Platform*
4. *SolarWinds*
5. *ManageEngine ServiceDesk*
6. *VirusTotal*
7. *Joe Sandbox Cloud Basic/Hybrid Analysis*
8. *MXToolBox*
9. *Scamalytics*
10. *IPalyzer*
11. *IPinfo*
12. *Burp Suite (PortSwigger)*
13. *Qualys*
14. *Rapid7*

3.1 Fase preliminare

Dopo aver analizzato a fondo la documentazione relativa allo standard *ISO 27000*, al *Framework NIST*, alla *Cyber Kill Chain* e al *Diamond Model*[4], e dopo aver effettuato una prima rapida analisi dei tool CTIA presi in considerazione, abbiamo deciso di concentrare la nostra indagine di mapping dei tool in primo luogo sul *Framework NIST* e successivamente in relazione alla *Cyber Kill Chain*. Questa scelta è stata principalmente dettata dalla mancanza esaustiva di documentazione relativa ai tool considerati e all'importanza delle due metodologie in ambito cybersecurity.

Relativamente allo standard *ISO 27000* non sono state trovate informazioni ufficiali per nessuno dei tool analizzati. Non potendo inferire nulla di certo rispetto alle numerose norme di uno standard ben definito e data l'esistenza di tabelle di conversione[5] dal *Framework NIST* a *ISO 27000*, si è preferito concentrare l'analisi sul *Framework NIST*, molto più chiaro nella sua suddivisione in 5 funzioni, spesso richiamate all'interno delle documentazioni.

Per quanto riguarda la relazione tra i tool CTIA e la *Cyber Kill Chain*, dato che si tratta di una tipologia di modello di attacco si è deciso di procedere con una sorta di mapping

[4] **Diamond Model**: è un modello che permette di creare dei collegamenti *temporali-causali* tra diversi eventi ma è comunque basata sulle fasi della *Cyber Kill Chain* e non risulta una metodologia adatta per lo scopo dell'analisi, per questo motivo non è stata presa in considerazione.
[5] https://www.nist.gov/system/files/alternative-view-framework-core-021214.pdf

"inverso"; essendo caratterizzato da una successione di fasi che fanno riferimento agli step di un attacco, la domanda che ci siamo posti per ciascuno degli strumenti è stata: "*Questo tool può essere utile per impedire o mitigare un attacco in una determinata fase della Cyber Kill Chain?*". È stata quindi ricercata una possibile copertura di uno o più dei livelli di controllo per ciascuna fase della *Kill Chain*.

3.2 Organizzazione del lavoro

Per ogni strumento è stata eseguita una prima analisi speculativa per inquadrare le principali funzionalità ed i casi d'uso correlati in modo da creare una prima bozza di una tabella informativa con eventuali commenti per facilitare la comprensione e per permettere di categorizzare i diversi strumenti.

Successivamente è iniziata un'analisi più approfondita utilizzando la documentazione ufficiale (ove disponibile), le informazioni all'interno dei siti ufficiali, video descrittivi e trial di ciascun tool. Abbiamo quindi individuato e riportato all'interno di una tabella le parole chiave che ci hanno permesso di capire se lo strumento fosse in grado di ricoprire una o più funzioni/fasi delle metodologie prese come riferimento. Questa fase è stata eseguita da entrambi gli studenti in modo da ridurre la possibilità di tralasciare informazioni importanti per condurre l'analisi.

Dopodiché sono state create due tabelle in Excel in cui nelle righe sono stati riportati i singoli strumenti mentre nelle colonne sono state riportate rispettivamente le funzioni del *Cybersecurity NIST Framework* e le fasi della *Cyber Kill Chain (CKC)*. Le tabelle sono state opportunamente completate in funzione delle informazioni acquisite durante la fase precedente e ci ha permesso di avere una visione riassuntiva e generale della copertura dei tool coinvolti nell'analisi.

Infine, per ogni strumento è stato creato un foglio Excel in cui vengono descritte le funzionalità principali, riportati i link alla documentazione ed inseriti eventuali commenti per sottolineare aspetti particolari o note rilevanti. Per ciascun tool sono state inserite due tabelle, una per ogni framework di riferimento: nella tabella relativa al *Framework NIST* sono state riportate tutte le *categorie* per ciascuna funzione ed evidenziate quelle che sono ricoperte dallo strumento[6]. Nella tabella della *Cyber Kill Chain* sono stati aggiunti cinque livelli di controllo per ogni fase ed è stata eseguita un'attività analoga applicata alla tabella del *NIST*. Per l'analisi rispetto alla *Cyber Kill Chain*, sono stati considerati i seguenti livelli di implementazione del controllo:

- **Detect**: determinare quando e come un utente malintenzionato stia eseguendo un'azione malevola contro un'organizzazione o una rete;
- **Deny**: impedire il verificarsi dell'attacco impedendo la divulgazione di informazioni o l'accesso non autorizzato;
- **Disrupt**: modificare o interrompere il flusso di informazioni o l'esfiltrazione di dati verso l'attaccante;
- **Degrade**: limitare l'efficacia o l'efficienza di un attacco;

[6] Per semplicità sono state considerate solo le *categorie* di ciascuna funzione e perciò non è stata svolta un'analisi approfondita considerando le diverse *sottocategorie* in modo da avere una valutazione di alto livello e più semplice da gestire.

- **Deceive**: interferire con un attacco utilizzando indicazioni errate o informazioni errate.

3.3 Risultati

Al seguente link Analisi Strumenti CTIA è possibile navigare tra i diversi fogli di lavoro di ***Google Sheets*** e visualizzare i risultati ottenuti dall'analisi. All'interno dei primi due fogli [NIST FRAMEWORK] e [CYBER KILL CHAIN] sono contenute due tabelle riassuntive, con i rispettivi grafici, rispetto al *Framework NIST* e alla *Cyber Kill Chain*. Cliccando sul nome di uno specifico tool in una riga della tabella, vi è un reindirizzamento al foglio contenente maggiori informazioni: una breve descrizione, eventuali link alla documentazione, commenti e le rispettive tabelle di copertura rispetto alle metodologie considerate. Per una visualizzazione più intuitiva e immediata sono presenti anche due grafici che mostrano le percentuali di copertura degli strumenti rispetto alle categorie per il *NIST* e ai livelli di controllo per ciascuna fase della *Cyber Kill Chain*.

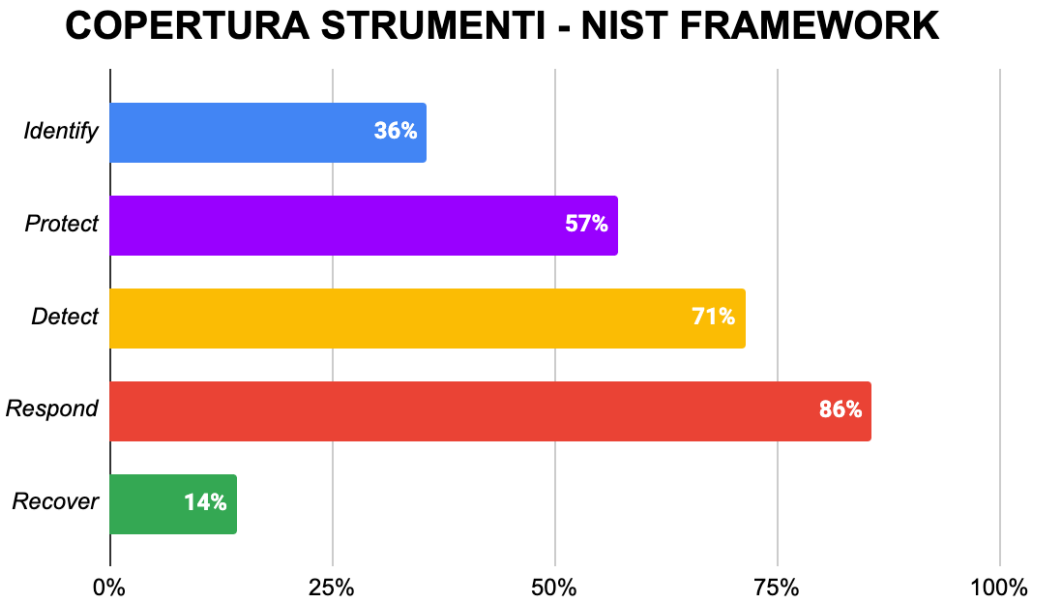


Figura 2: Copertura strumenti rispetto alle funzioni del Framework NIST

Come mostrato in Figura 2, gli strumenti analizzati offrono un'ottima copertura rispetto alle funzioni di *Detect* (71% degli strumenti) *e Respond* (86% degli strumenti); in particolare in fase di risposta ricoprono spesso la categoria di *Analysis* che risulta un'attività fondamentale che deve essere eseguita dai team di cybersecurity. La funzione di rilevamento è stata colmata in tutte le sue categorie in modo frequente grazie alla presenza di funzionalità dei tool in grado di monitorare costantemente i sistemi informativi, individuare anomalie e nuove minacce. La funzione di *Protect* (57% degli strumenti) è stata individuata in circa la metà dei tool analizzati, molti dei quali sono caratterizzati da servizi più specifici di protezione degli *endpoint*, gestione delle autenticazioni e sicurezza dei dati. Solo una minima percentuale (36% degli strumenti) presenta alcune delle categorie specifiche della funzione di *Identify*, tra cui la gestione degli *asset* aziendali e una valutazione del rischio.

La funzione più critica che è stata identificata è quella di *Recover* (14% degli strumenti), individuata solamente all'interno di due strumenti e le principali funzionalità offerte sono di gestione dei backup e di ripristino dei sistemi.

Rispetto al modello proposto all'interno della *Cyber Kill Chain* differenti fasi sono state ricoperte discretamente, come si può vedere in Figura 3. La fase di *Reconnaissance* e *Delivery* sono quelle con una frequenza maggiore in quanto molti degli strumenti forniscono informazioni sugli indirizzi IP, siti Web, domini, e-mail. Anche la fase di *Exploitation* presenta una buona copertura dato che diversi tools forniscono attività di *penetration test* automatizzate per individuare vulnerabilità che possono essere utilizzate da un attaccante.
Le fasi terminali della *Kill Chain* sono ricoperte soprattutto da strumenti che garantiscono un monitoraggio costante dei sistemi in modo da essere in grado di riconoscere anomalie e quindi processi malevoli in corso sui dispositivi.
Una fase critica è sicuramente la *Weaponization* in quanto si trova nella fase iniziale della *CKC* ma nell'analisi condotta solo due strumenti permettono di individuare ed esaminare malware all'interno di file.

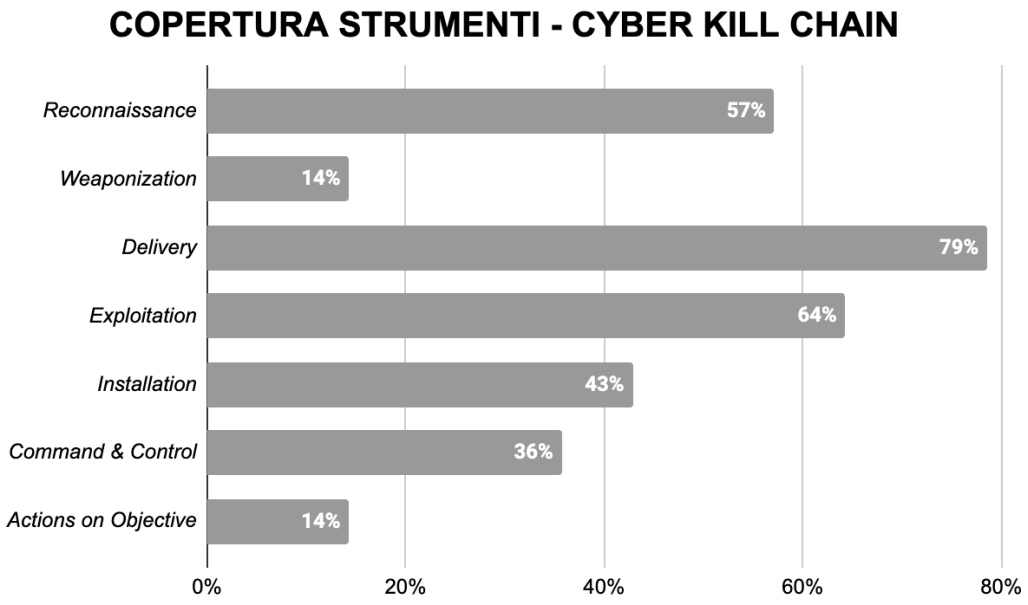


Figura 3: Copertura strumenti rispetto alle fasi della Cyber Kill Chain

4 Standard e piattaforme di comunicazione CTI

4.1 Panoramica generale

Un'organizzazione non può da sola costruirsi una consapevolezza "globale" delle minacce che possono mettere a rischio la sicurezza delle proprie informazioni. L'unica soluzione al problema è condividere le informazioni riguardanti la sicurezza informatica con partner e comunità di fiducia. Tale scambio di informazioni è vantaggioso per tutti i partecipanti perché possono analizzare meglio la situazione reale, le relative attività dannose in corso e contrastare efficacemente eventuali minacce. Per fare in modo che questo scambio di informazioni sia efficiente e strutturato sono nati diversi formati concettuali e piattaforme di interscambio.

Tra i diversi formati esistenti i più diffusi sono **STIX** (*Structured Threat Information eXpression*) e **MAEC** (*Malware Attribute Enumeration and Classification*). Tra le piattaforme più diffuse per lo scambio di dati troviamo invece **MISP** (*Malware Information Sharing Platform*) e **TAXII** (*Trusted Automated eXchange of Intelligence Information*).

4.2 MAEC: Malware Attribute Enumeration and Classification

MAEC è un linguaggio strutturato per la codifica delle informazioni sul malware in base ad attributi come comportamenti, artefatti e relazioni tra campioni di malware. Il MAEC è sponsorizzato dall'*Office of Cybersecurity and Communications* del Dipartimento per la sicurezza interna degli Stati Uniti (DHS) ed è gestito da *MITRE Corporation*, che fornisce anche una guida tecnica ai membri della *MAEC Community*.

L'obiettivo di MAEC è trasformare i processi di ricerca e la risposta ai malware migliorando la comunicazione, riducendo la potenziale duplicazione degli sforzi di analisi e consentendo uno sviluppo più rapido di contromisure grazie alla capacità di sfruttare le risposte alle istanze di malware osservate in precedenza.
Il modello dati MAEC può essere rappresentato come un grafico connesso di nodi e archi, in cui gli oggetti di livello superiore MAEC definiscono i nodi e le relazioni MAEC definiscono gli archi. Una relazione è un collegamento tra oggetti MAEC che descrive come gli oggetti sono correlati tra loro. Come mostrato nella *Figura 4*, MAEC definisce diversi oggetti di primo livello: comportamenti, azioni malware, famiglie di malware, istanze di malware e raccolte. Le relazioni tra gli oggetti (inclusi gli oggetti STIX) sono rappresentate da archi orientati nel diagramma: le relazioni "*embedded*" (quelle che sono specificate direttamente su un oggetto di livello superiore come proprietà dell'oggetto) sono etichettate con dei caratteri **`neri`** mentre le relazioni dirette vengono etichettate utilizzando uno **`sfondo azzurro`**.

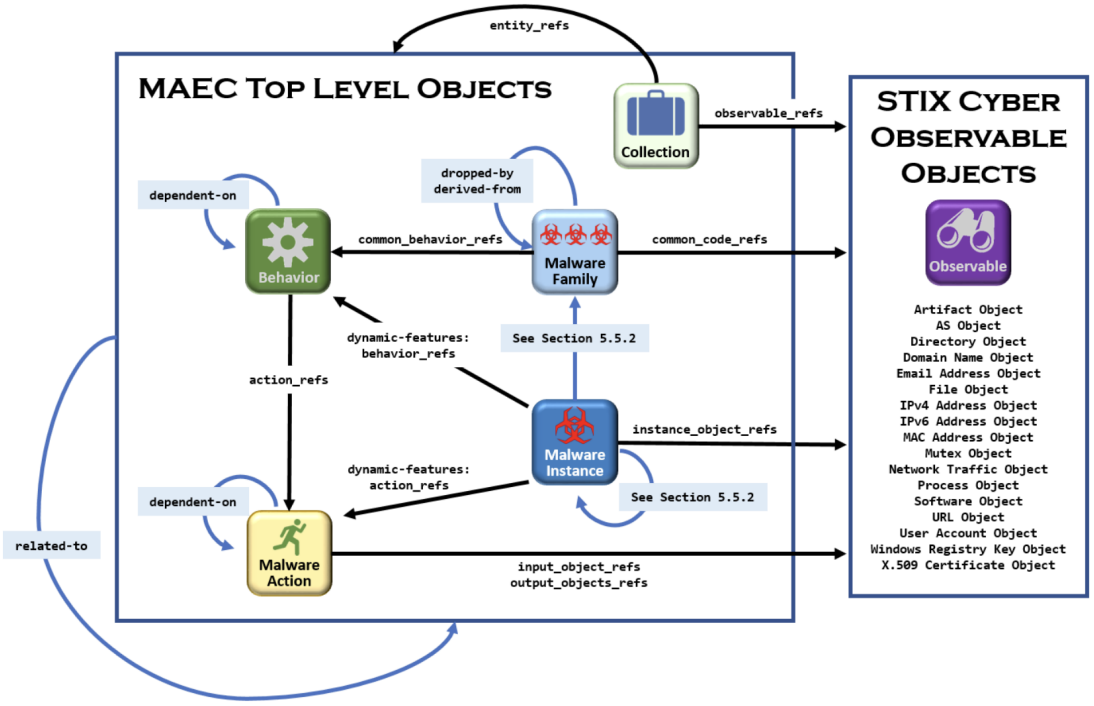


Figura 4: Diagramma MAEC Top Level Objects

4.3 STIX: Structured Threat Information eXpression

STIX è un linguaggio standardizzato sviluppato da *MITRE* e dall'*OASIS Cyber Threat Intelligence Technical Committee* per descrivere i dati relativi alle minacce informatiche. Adottato come standard internazionale da varie organizzazioni e community di condivisione dell'intelligence ed è progettato per la condivisione tramite TAXII, ma può essere condiviso anche con altri mezzi. STIX è strutturato in modo da consentire agli utenti di descrivere motivazioni, abilità, capacità e risposte alle minacce. Tra gli obiettivi principali di *STIX* si possono citare: *Collaborative Threat Analysis*, *Automated Threat Exchange* e *Automated Detection and Response*.
Le informazioni in formato *STIX* possono essere facilmente visualizzate da un *CTI Analyst* oppure memorizzate all'interno di un file JSON in modo da essere maggiormente *machine-readable*. Con la versione **STIX 2.1** sono stati definiti 18 ***STIX Domain Object*** (*SDO*) i quali possono essere connessi tra di loro attraverso *relazioni* che permettono di rappresentare al meglio le informazioni di *CTI*.

Si rimanda all'**Appendice D** per un esempio di uno scenario d'uso di STIX.

4.4 MAEC e STIX a confronto

MAEC e STIX sono stati progettati pensando a casi d'uso molto diversi e quindi svolgono ruoli diversi quando si tratta di acquisire informazioni riguardanti i malware. MAEC ha lo scopo di fornire un modo completo e strutturato per acquisire informazioni dettagliate sui campioni di malware ed è quindi rivolto principalmente agli analisti di malware. STIX ha invece lo scopo di acquisire un ampio spettro di informazioni relative alle minacce informatiche, comprese le informazioni di base sul malware, e per questo è rivolto per un utilizzo in diversi contesti. Sia STIX che MAEC sono basati a loro volta su un linguaggio chiamato CybOX (*Cyber Observable eXpression*), nato per descrivere eventi di proprietà *stateful* osservabili in ambito cybersecurity, e questo garantisce l'interoperabilità tra i due linguaggi. Infatti, il contenuto MAEC può anche essere incorporato all'interno di STIX e questo consente ai due linguaggi di completarsi a vicenda. Se utilizzati insieme consentono l'acquisizione di informazioni dettagliate sui malware insieme alle relative informazioni sulle minacce informatiche. Ciò permette di stabilire ed esprimere relazioni utili e dettagliate tra il malware e il più ampio contesto di minacce informatiche.

4.4.1 Opzioni per l'acquisizione di informazioni sul malware

Sia STIX che MAEC possono essere utilizzati singolarmente per acquisire informazioni sul malware. Tuttavia, in alcune situazioni, potrebbe essere preferibile incorporare il contenuto MAEC all'interno di un documento STIX. I tipi di informazioni relative al malware acquisite da ciascuna di queste opzioni – MAEC, STIX e MAEC+STIX – sono mostrati nella *Tabella 1* di seguito.

MAEC	**STIX**	**MAEC + STIX**
Acquisisce informazioni strutturate e dettagliate sul malware: ● Capacità ● Comportamenti ● Azioni ● Classificazione ● Oggetti estratti ● Relazioni ● Metadati associati	Acquisisce informazioni di base e non strutturate sul malware: ● Tipo ● Nome ● Descrizione	Acquisisce un'ampia gamma di informazioni sul malware: ● Informazioni di base e descrittive tramite STIX che permettono l'identificazione ● Informazioni dettagliate e strutturate tramite MAEC che forniscono una comprensione più ampia. Ad esempio, una breve descrizione di una famiglia di malware e descrizioni dettagliate dei suoi membri
Fornisce un ***contesto analitico***: ● "Cosa" fa il malware? ● "Come" opera il malware?	Fornisce il ***contesto circostante***: ● "Chi" ha utilizzato il malware? ● "Dove" è stato utilizzato il	Fornisce un ***contesto completo***: ● Collega le informazioni dettagliate sul malware a un contesto di minacce più ampio

	malware?	Ad esempio, "quali" caratteristiche specifiche di un'istanza di malware sono associate a un particolare attore di minacce?

Tabella 1: Combinazioni MAEC/STIX per acquisizione di informazioni di malware

4.5 TAXII: Trusted Automated eXchange of Indicator Information

Trusted Automated Exchange of Intelligence Information (TAXII) è un protocollo applicativo per lo scambio di CTI tramite HTTPS. TAXII definisce un'*API RESTful* e un insieme di requisiti per client e server TAXII. Come illustrato di seguito (Figura 5), TAXII presenta due servizi primari per supportare una varietà di modelli di condivisione comuni:

- **Collections** - Una *Collection* è un'interfaccia ad un repository logico di oggetti CTI fornito da un server TAXII che consente a un produttore di ospitare una serie di dati CTI che possono essere richiesti dai consumatori: client e server TAXII si scambiano informazioni in un modello di *Request-Response*.
- **Channels** - Gestito da un server TAXII, un canale consente ai produttori di inviare dati a molti consumatori e ai consumatori di ricevere dati da molti produttori: i client TAXII scambiano informazioni con altri client TAXII in un modello di *Publish-Subscribe*.

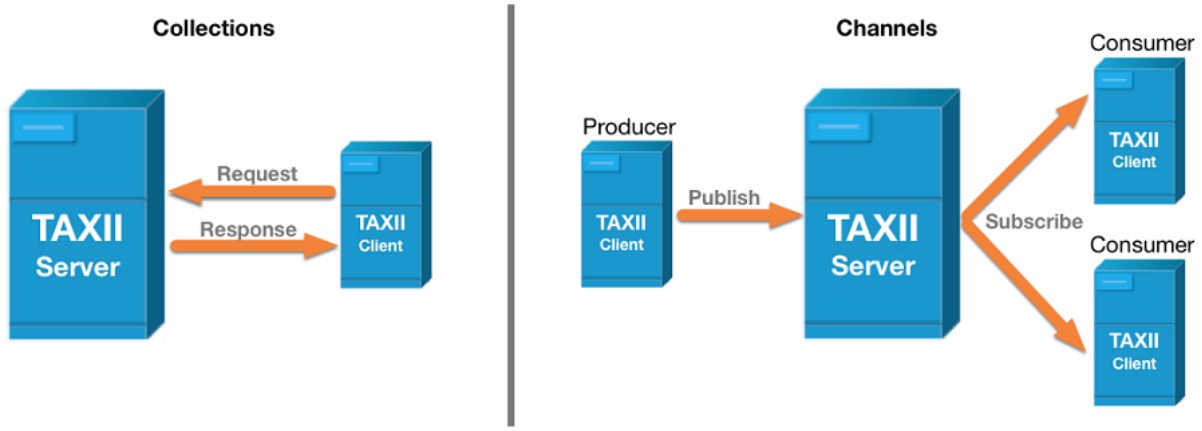


Figura 5: Modalità di utilizzo del protocollo TAXII

Collections e **Channels** possono essere organizzati in diversi modi. Ad esempio, possono essere raggruppati per supportare esigenze particolari.

Un'istanza del server TAXII può supportare una o più *API Root*. Le *API Root* sono raggruppamenti logici di canali e raccolte TAXII che possono essere considerate come istanze delle API TAXII disponibili su URL diversi, dove ciascuna *API Root* è l'URL "*root*" di quella particolare istanza dell'API TAXII.
TAXII si basa sui protocolli esistenti quando possibile. In particolare, i server TAXII vengono scoperti all'interno di una rete tramite i record del servizio DNS e/o da un *Discovery*

Endpoint, un URL e un metodo HTTP con una richiesta e una risposta definite che consente ai client autorizzati di ottenere informazioni su un server TAXII e ottenere un elenco di *API Root*. Inoltre, TAXII utilizza HTTPS come trasporto per tutte le comunicazioni e utilizza HTTP per la negoziazione e l'autenticazione del contenuto.

TAXII è stato progettato specificamente per supportare lo scambio di CTI rappresentato in STIX tuttavia può essere utilizzato anche per condividere dati in altri formati. È importante notare che STIX e TAXII sono standard indipendenti: le strutture e le serializzazioni di STIX non si basano su alcun meccanismo di trasporto specifico e TAXII può essere utilizzato per trasportare dati *non-STIX*. I principi di progettazione di TAXII includono la riduzione al minimo delle modifiche operative necessarie per l'adozione, facile integrazione con gli accordi di condivisione esistenti e supporto per tutti i modelli di condivisione delle minacce ampiamente utilizzati: *hub-and-spoke*, *peer-to-peer* e *source-subscriber*.

4.5 MISP: Malware Information Sharing Platform

MISP è lo standard delineato negli ultimi anni dalla comunità internazionale di cybersecurity per lo scambio delle informazioni, l'arricchimento e correlazione dei dati esterni. Si tratta di un prodotto *open source*, anche scelto per la neutralità del fornitore (*Computer Incident Response Center Luxembourg*). L'architettura prevede un'istanza centrale della piattaforma con funzioni di *hub*, con la quale le varie organizzazioni appartenenti alla community possono sincronizzarsi utilizzando la propria istanza locale, oppure con il proprio software interno attraverso le API fornite da MISP, o infine accedendo via browser direttamente all'istanza centrale.
I membri possono decidere se partecipare solo in modo passivo, cioè eseguendo delle richieste *pull*, o in modo attivo, ovvero anche attraverso richieste *push*. Le organizzazioni che possiedono specifici feed commerciali e open source, possono condividere parte dei loro *Indicator of Compromise* (IoC) ritenuti utili alla community, nel rispetto delle norme di riservatezza e degli accordi con le specifiche aziende fornitrici.
Il processo di raccolta, arricchimento e correlazione dei dati viene integrato tipicamente attraverso uno scambio dati, tra MISP e una *Threat Intelligence Platform* (TIP) conforme allo standard STIX/TAXII, il che consente ulteriori arricchimenti e indagini, nonché la possibilità di generare allarmi e report. Le *cyber-informazioni* diventano così "*actionable*", cioè sfruttano il collegamento verso i SIEM e SOC in grado di bloccare automaticamente l'attacco.

Una volta definita l'architettura, bisogna decidere cosa condividere e come. Il "cosa" dipende naturalmente dal contesto in cui si opera: una community di natura finanziaria sarà interessata alle campagne a tema bancario, mentre per esempio i gestori PEC saranno più concentrati sulle minacce che circolano sulla posta elettronica certificata. Riguardo al "come", bisogna innanzitutto garantire un approccio comune alla condivisione, quindi definire un framework che comprende formato dati, terminologia, convenzioni e tassonomie basate su protocolli noti e open source. Alcuni esempi sono il *MITRE ATT&CK* per descrivere le tattiche, le tecniche e le procedure. Per la condivisione di attori, malware e profili possono essere utilizzati i *MISP Cluster*, mentre per quanto riguarda le tassonomie è possibile scegliere da una lunga lista open source messa a disposizione da

MISP. Per il formato dati, MISP fornisce il suo modello[7] proprietario basato su JSON, ma sono disponibili altri modelli per le integrazioni, tra cui lo STIX 2.1/TAXII.

4.6 Conformità degli strumenti analizzati rispetto agli standard di comunicazione

Al seguente link Protocolli Standard di Comunicazione CTI è possibile visualizzare una tabella contenente diverse informazioni sulla conformità concettuale di un numero limitato di strumenti analizzati di cui è stato possibile ottenere informazioni attraverso le documentazioni ufficiali e/o versioni trial dei tools. Per questi tools è presente anche una pagina contenente un esempio di output.

Tra i diversi tools che permettono di supportare le attività di *Cyber Threat Intelligence Analysis*, i protocolli standard che risultano essere trasversali in più strumenti sono *STIX* e *MISP* mentre solo all'interno di ***Joe Sandbox Cloud Basic*** è possibile esportare le informazioni in formato *MAEC*. Questo è un risultato ragionevole in quanto lo standard *MAEC* permette un report più dettagliato in seguito all'analisi di un malware.

Un aspetto particolare riguardante invece ***VirusTotal Graph*** è la possibilità di ottenere una visualizzazione grafica di oggetti (p.e. file, URL, domini, e-mail) e possibili relazioni tra di essi attraverso un'interfaccia caratterizzata da icone semantiche e una certa dinamicità in grado di avere un maggiore impatto visivo, soprattutto per garantire una panoramica generale più intuitiva.

[7] 3.1 Data model

5 Conclusioni

Complessivamente è stato riscontrato che gli strumenti più modulari, ovvero costituiti da diversi tool che offrono funzionalità più specifiche, sono in grado di ricoprire in generale più categorie del *Framework NIST* anche se alcune risultano meno tecniche e perciò richiedono inevitabilmente delle attività svolte da un essere umano, come per esempio la comunicazione con enti esterni oppure la gestione delle pubbliche relazioni.
Gli strumenti caratterizzati da funzionalità limitate a specifici casi d'uso hanno invece dimostrato di avere una copertura circoscritta ad una o due funzioni.

Rispetto alla *Cyber Kill Chain* i software analizzati riescono ad individuare, in buona percentuale, attacchi che si trovano nelle fasi iniziali permettendo al team di intelligence di simulare le fasi successive e permettere un rilevamento anticipato e più sofisticato per campagne di attacco nel futuro.

Per quanto riguarda gli standard di comunicazione, *STIX* rimane indubbiamente quello più supportato e citato nelle documentazioni anche se esistono diverse librerie e moduli dei tool in grado di convertire i file di output tra i diversi formati standard.

Una possibile integrazione futura interessante potrebbe essere quella di effettuare un'analisi analoga rispetto a strumenti CTIA *open-source* in modo da comparare le percentuali di copertura e valutare se alcuni tool che richiedono licenze costose possono essere sostituiti permettendo di indirizzare gli investimenti in settori che necessitano di maggiori risorse finanziarie.

Appendice A

A.1 Che cos'è un ISMS?

Un *Information Security Management Systems* (***ISMS***) è costituito dalle policy, procedure, linee guida, risorse e attività associate gestite collettivamente da un'organizzazione con l'obiettivo di proteggere il proprio patrimonio informativo. Un *ISMS* è un approccio sistematico per stabilire, implementare, far funzionare, monitorare, rivedere, mantenere e migliorare la sicurezza delle informazioni di un'organizzazione per raggiungere gli obiettivi di business.

Un *ISMS* si basa su una valutazione del rischio e sui livelli di accettazione del rischio dell'organizzazione progettati per trattare e gestire efficacemente i rischi. L'analisi dei requisiti per la protezione delle risorse informative e l'applicazione di controlli appropriati per garantire la protezione di queste risorse informative contribuisce alla corretta implementazione di un *ISMS*. Questi controlli devono essere specificati, implementati, monitorati, ri-esaminati e migliorati ove necessario, per garantire che la sicurezza delle informazioni specifiche e gli obiettivi aziendali dell'organizzazione siano raggiunti. I controlli di sicurezza delle informazioni rilevanti dovrebbero essere perfettamente integrati con i processi aziendali di un'organizzazione.

I seguenti principi fondamentali contribuiscono alla corretta attuazione di un *ISMS*:

- consapevolezza della necessità di sicurezza delle informazioni;
- attribuzione di responsabilità per la sicurezza delle informazioni;
- l'impegno del management e gli interessi degli stakeholder;
- valorizzazione degli aspetti sociali in ambito di sicurezza;
- effettuare valutazioni del rischio che determinino controlli adeguati per raggiungere livelli di rischio accettabili;
- la sicurezza come elemento essenziale di reti e sistemi informativi;
- prevenzione e rilevazione attiva degli incidenti di sicurezza;
- garantire un approccio globale alla gestione della sicurezza;
- la continua rivalutazione della sicurezza delle informazioni e l'eventuale modifica.

A.2 L'importanza di un ISMS

In un mondo interconnesso, le informazioni e i relativi processi, sistemi e reti costituiscono asset aziendali critici. Le organizzazioni e i loro sistemi e reti affrontano minacce alla sicurezza provenienti da un'ampia gamma di fonti, tra cui frodi informatiche, spionaggio, sabotaggio, vandalismo, incendi e inondazioni. I danni ai sistemi informativi e alle reti causati da codice dannoso, pirateria informatica e attacchi Denial of Service sono diventati più comuni, più ambiziosi e sempre più sofisticati.

L'interconnessione di reti pubbliche e private e la condivisione del patrimonio informativo aumentano la difficoltà di controllo, accesso e trattamento delle informazioni. Inoltre, la

distribuzione di dispositivi mobili di archiviazione contenenti asset informativi può indebolire l'efficacia dei controlli tradizionali.
Proprio per questo un *ISMS* è un fattore che supporta l'e-business ed è essenziale per le attività di gestione del rischio. Quando le organizzazioni adottano la famiglia di standard ISMS, la capacità di applicare principi di sicurezza delle informazioni coerenti e reciprocamente riconoscibili può essere anche dimostrata ai partner commerciali e ad altre parti interessate.

L'adozione con successo di un *ISMS* è importante per proteggere le risorse informative e consente ad un'organizzazione di:

- ottenere una maggiore garanzia che il proprio patrimonio informativo sia adeguatamente protetto contro le minacce su base continua;
- mantenere un quadro strutturato e completo per identificare e valutare i rischi per la sicurezza delle informazioni, selezionare e applicare i controlli applicabili e misurare e migliorare la loro efficacia;
- migliorare continuamente il proprio ambiente di controllo;
- conseguire efficacemente la conformità legale e regolamentare.

A.3 Istituzione, monitoraggio, mantenimento e miglioramento di un ISMS

Un'organizzazione deve intraprendere le seguenti fasi per stabilire, monitorare, mantenere e migliorare il proprio *ISMS*:

1) identificare le risorse informative e i relativi requisiti di sicurezza delle informazioni;
2) valutare e trattare i rischi per la sicurezza delle informazioni;
3) selezionare e attuare i controlli pertinenti per gestire i rischi inaccettabili;
4) monitorare, manutenere e migliorare l'efficacia dei controlli associati al patrimonio informativo dell'organizzazione.

Per garantire che l'*ISMS* protegga efficacemente il patrimonio informativo dell'organizzazione in modo costante è necessario che i passaggi da 1) a 4) vengano continuamente ripetuti, in un'ottica *PDCA*, per identificare i cambiamenti nei rischi o nelle strategie o negli obiettivi aziendali dell'organizzazione.

A.4 Selezione e attuazione dei controlli

Una volta identificati i requisiti di sicurezza delle informazioni, determinati e valutati i rischi per le risorse informative identificate e prese le decisioni per il trattamento dei rischi per la sicurezza delle informazioni deve avvenire l'attuazione dei controlli per la riduzione del rischio.

I controlli dovrebbero garantire che i rischi siano ridotti a un livello accettabile tenendo conto di:

1) requisiti e vincoli della legislazione e dei regolamenti nazionali e internazionali;
2) obiettivi organizzativi;
3) esigenze e vincoli operativi;

4) il loro costo di attuazione e di funzionamento in relazione alla riduzione dei rischi e rimanendo proporzionale ai requisiti e ai vincoli dell'organizzazione;
5) i loro obiettivi per monitorare, valutare e migliorare l'efficienza e l'efficacia dei controlli di sicurezza delle informazioni a supporto degli obiettivi dell'organizzazione. (La selezione e l'attuazione dei controlli dovrebbero essere documentate all'interno di una dichiarazione di applicabilità per assistere con i requisiti di conformità);
6) la necessità di bilanciare l'investimento nell'attuazione e nell'operatività dei controlli con la perdita che potrebbe derivare da incidenti di sicurezza delle informazioni.

I controlli specificati nella *ISO/IEC 27002* sono riconosciuti come le *best practices* applicabili alla maggior parte delle organizzazioni e prontamente ritagliati per adattarsi a organizzazioni di varie dimensioni e complessità.

A.5 Il miglioramento continuo

L'obiettivo del miglioramento continuo di un *ISMS* è aumentare la probabilità di raggiungere obiettivi riguardanti la conservazione della riservatezza, disponibilità e integrità delle informazioni. L'obiettivo è quello di cercare opportunità di miglioramento e non presumere che le attività di gestione esistenti siano sufficientemente buone.

Le azioni di miglioramento includono quanto segue:
- analizzare e valutare la situazione esistente per individuare aree di miglioramento;
- stabilire gli obiettivi di miglioramento;
- ricerca di possibili soluzioni per il raggiungimento degli obiettivi;
- valutare tali soluzioni ed effettuare una selezione;
- attuare la soluzione prescelta;
- misurare, verificare, analizzare e valutare i risultati dell'attuazione per determinare il raggiungimento degli obiettivi;
- formalizzare le modifiche.

I risultati vengono esaminati nuovamente, se necessario, per determinare ulteriori opportunità di miglioramento. In questo modo il miglioramento è un'attività continua, cioè le azioni si ripetono frequentemente.
Il feedback dei clienti e di altre parti interessate, gli audit e la revisione del sistema di gestione della sicurezza delle informazioni possono essere utilizzati anche per identificare opportunità di miglioramento.

A.6 ISMS Critical Success Factors

Un gran numero di fattori sono fondamentali per implementare con successo un *ISMS* e consentire a un'organizzazione di raggiungere i propri obiettivi di business.

Esempi di fattori critici includono:

- policy di sicurezza delle informazioni e attività in linea con gli obiettivi;
- un approccio e un framework per la progettazione, l'attuazione, il monitoraggio, il mantenimento e il miglioramento della sicurezza delle informazioni coerenti con la cultura organizzativa;
- supporto e impegno da parte di tutti i livelli dirigenziali, in particolare il top management;
- la comprensione dei requisiti di protezione del patrimonio informativo raggiunti attraverso l'applicazione della gestione del rischio per la sicurezza delle informazioni (*cfr. ISO/IEC 27005*);
- un programma efficace di sensibilizzazione, formazione e istruzione in materia di sicurezza delle informazioni, che informi tutti i dipendenti e le altre parti interessate dei loro obblighi in materia di sicurezza delle informazioni stabiliti nelle politiche, standard, ecc. sulla sicurezza delle informazioni e li motiva ad agire di conseguenza;
- un efficace processo di gestione degli incidenti di sicurezza delle informazioni;
- un approccio efficace alla gestione della continuità operativa;
- un sistema di misurazione utilizzato per valutare le prestazioni nella gestione della sicurezza delle informazioni e feedback suggerimenti per il miglioramento.

A.7 Struttura dei documenti della famiglia ISMS

La famiglia di standard *ISMS* è costituita da standard interconnessi, già pubblicati o in fase di sviluppo, e contiene una serie di componenti strutturali significativi. Questi componenti sono focalizzati su:

- ➔ norme che descrivono i requisiti *ISMS* (*ISO/IEC 27001*);
- ➔ requisiti dell'organismo di certificazione (*ISO/IEC 27006*) per coloro che certificano la conformità alla *ISO/IEC 27001*;
- ➔ quadro dei requisiti aggiuntivi per le implementazioni settoriali dell'*ISMS* (*ISO/IEC 27009*).

Altri documenti forniscono una guida per vari aspetti dell'implementazione dell'*ISMS*, affrontando un processo generico e una guida specifica per il settore di interesse.

Appendice B

B.1 Gli Implementation Tier del Framework NIST

I livelli di implementazione forniscono un contesto su come un'organizzazione considera il rischio di sicurezza informatica e i processi in atto per gestirlo. I livelli, che vanno da Parziale (*Tier 1*) ad Adaptive (*Tier 4*), descrivono un grado crescente di rigore e sofisticatezza nelle pratiche di gestione del rischio di sicurezza e aiutano a determinare la misura in cui la gestione del rischio di sicurezza è compatibile ed integrata con le esigenze e con le pratiche aziendali.
Il processo di selezione del *tier* considera le attuali pratiche di gestione del rischio di un'organizzazione, l'ambiente delle minacce, i requisiti legali e normativi, le pratiche di condivisione delle informazioni, gli obiettivi aziendali/della missione, i requisiti di sicurezza informatica della catena di approvvigionamento e i vincoli organizzativi.
Le organizzazioni dovrebbero determinare il livello desiderato, assicurando che il livello selezionato soddisfi gli obiettivi dell'organizzazione, sia fattibile da implementare e riduca il rischio di sicurezza informatica per le risorse e le risorse critiche a livelli accettabili per l'organizzazione.
I livelli hanno lo scopo di supportare il processo decisionale dell'organizzazione su come gestire il rischio di sicurezza informatica, nonché quali dimensioni dell'organizzazione hanno la priorità più alta e potrebbero richiedere risorse aggiuntive. Il passaggio a livelli più elevati è incoraggiato quando un'analisi costi-benefici indica una riduzione fattibile ed economicamente vantaggiosa del rischio di sicurezza informatica. La corretta implementazione del *framework* si basa sul raggiungimento dei risultati descritti nei profili target dell'organizzazione e non sulla determinazione del livello. Tuttavia, la selezione e la designazione del livello influiscono sui profili del *framework*.

B.2 Il concetto di profilo all'interno del Framework NIST

Il ***Profilo*** è l'allineamento di *Funzioni, Categorie* e *Sottocategorie* con i requisiti aziendali, la tolleranza al rischio e le risorse dell'organizzazione. Un profilo consente alle organizzazioni di stabilire una tabella di marcia per la riduzione del rischio di sicurezza informatica che sia ben allineata con gli obiettivi organizzativi, tenga conto dei requisiti legali/normativi, delle best practices e che rifletta le priorità di gestione del rischio.
I profili possono essere utilizzati per descrivere lo stato attuale o lo stato di destinazione desiderato di specifiche attività di sicurezza informatica.
I profili supportano i requisiti aziendali e aiutano a comunicare il rischio all'interno e tra le organizzazioni. Il *Framework NIST* non prescrive modelli di profilo, consentendo di fatto flessibilità nell'implementazione.
Il confronto dei profili (ad esempio *Profilo attuale* e *Profilo target*) può rivelare lacune da colmare per raggiungere gli obiettivi di gestione del rischio.
Questo approccio basato sul rischio consente a un'organizzazione di misurare le risorse necessarie (ad es. personale, finanziamenti) per raggiungere gli obiettivi di sicurezza informatica in modo conveniente e prioritario.

B.3 Istituzione o miglioramento di un programma di sicurezza informatica secondo il Framework NIST

I passaggi seguenti illustrano come un'organizzazione potrebbe utilizzare il *framework* per creare un nuovo programma di sicurezza informatica o migliorarne uno esistente.
Questi passaggi dovrebbero essere ripetuti, se necessario, per avere un processo di miglioramento continuo:

- *Passaggio 1: assegnare priorità e ambito.*
  L'organizzazione identifica i suoi obiettivi di business e le priorità organizzative di alto livello. Con queste informazioni vengono prese decisioni strategiche in merito alle implementazioni della sicurezza informatica e viene determinato l'ambito dei sistemi e delle risorse che supportano la linea o il processo di business selezionato.
- *Passaggio 2: orientare.*
  Una volta che l'ambito del programma di sicurezza informatica è stato determinato per la linea o il processo di business, l'organizzazione identifica i sistemi e le risorse correlate, i requisiti normativi e l'approccio generale al rischio. L'organizzazione consulta quindi le fonti per identificare le minacce e le vulnerabilità applicabili a tali sistemi e risorse.
- *Passaggio 3*: *creare un profilo corrente.*
  L'organizzazione sviluppa un profilo attuale indicando quali risultati di categorie e sottocategorie dal framework Core vengono attualmente raggiunti.
  Se un risultato è parzialmente raggiunto questo aiuterà a supportare i passaggi successivi fornendo informazioni di base.
- *Passaggio 4: condurre una valutazione del rischio.*
  Questa valutazione potrebbe essere guidata dal processo complessivo di gestione del rischio dell'organizzazione o da precedenti attività di valutazione del rischio.
  È importante che le organizzazioni identifichino i rischi emergenti e utilizzino le informazioni sulle minacce informatiche provenienti da fonti interne ed esterne per ottenere una migliore comprensione della probabilità e dell'impatto degli eventi di sicurezza informatica.
- *Passaggio 5: creare un profilo target.*
  L'organizzazione crea un profilo target incentrato sulla valutazione delle categorie e sottocategorie del framework che descrivono i risultati desiderati per la sicurezza informatica dell'organizzazione, sviluppando eventuali proprie categorie e sottocategorie aggiuntive per tenere conto dei rischi organizzativi unici. L'organizzazione può anche considerare influenze e requisiti di stakeholder esterni come entità del settore, clienti e partner commerciali durante la creazione di un profilo target. Il profilo dell'obiettivo dovrebbe riflettere adeguatamente i criteri all'interno del livello di attuazione dell'obiettivo.
- *Passaggio 6: determinare, analizzare e assegnare priorità alle lacune.*
  L'organizzazione confronta il profilo corrente e il profilo target per determinare le lacune. Successivamente, crea un piano d'azione e determina quindi le risorse, compresi i finanziamenti e la forza lavoro, necessarie per colmare tali lacune.

- *Passaggio 7: attuare il piano d'azione.*
  L'organizzazione determina quali azioni intraprendere per colmare le eventuali lacune individuate nel passaggio precedente e quindi adegua le sue attuali pratiche di sicurezza informatica al fine di raggiungere il profilo target. Per ulteriori indicazioni, il framework identifica esempi di *Riferimenti Informativi* relativi alle *Categorie* e *Sottocategorie*, ma le organizzazioni dovrebbero determinare quali standard, linee guida e pratiche, comprese quelle specifiche del settore, funzionino meglio per le loro esigenze.

Appendice C

C.1 Intelligence-driven Computer Network Defense

L'*Intelligence-driven Computer Network Defense* (*ICND*) è una strategia di gestione del rischio che affronta la componente di minaccia del rischio incorporando l'analisi degli avversari, le loro capacità, i loro obiettivi, e i loro limiti. Questo è necessariamente un processo continuo, che sfrutta gli indicatori per scoprire nuove attività con ancora più informazioni da sfruttare. Questo processo inoltre richiede una nuova comprensione delle intrusioni stesse, che non vanno più concepite come eventi singolari, ma piuttosto come progressioni graduali e continue.

L'effetto dell'*ICND* è quello di costruire una posizione di sicurezza più resiliente.
Gli attori APT, per loro natura, tentano un'intrusione dopo l'altra, adattando le loro operazioni in base al successo o al fallimento di ogni tentativo. Se i difensori implementano le contromisure più velocemente di quanto si evolvano gli avversari, aumenteranno i costi e lo sforzo che un attaccante dovrà sostenere per raggiungere i propri obiettivi.

Questo modello mostra perciò, contrariamente alla saggezza convenzionale, che tali aggressori non hanno alcun vantaggio intrinseco sui difensori.

C.2 Gli Indicatori e il loro ciclo di vita

Un indicatore, elemento fondamentale in questo modello di *Intelligence-driven CND*, è una qualsiasi informazione che descrive oggettivamente un'intrusione. Gli *indicatori* possono essere suddivisi in tre tipi:

- **Atomici** - sono quegli indicatori che non possono essere scomposti in parti più piccole e mantengono il loro significato nel contesto di un'intrusione. Esempi tipici sono indirizzi IP oppure indirizzi e-mail.
- **Calcolati** - sono quegli indicatori derivati dai dati coinvolti in un incidente di sicurezza. Gli indicatori calcolati comuni includono ad esempio valori hash ed espressioni regolari.
- **Comportamentali** - sono raccolte di indicatori calcolati e atomici, spesso soggetti a qualificazione per quantità e possibilmente logica combinatoria che permettono di descrivere il comportamento dell'attaccante durante le fasi dell'attacco.
  Un esempio potrebbe essere la seguente affermazione: "*L'intruso inizialmente avrebbe utilizzato una backdoor che generasse traffico di rete corrispondente a [espressione regolare] alla velocità di [una certa frequenza] a [un certo indirizzo IP], quindi la sostituiva con una corrispondente all'hash MD5 [valore] una volta stabilito l'accesso.*"

Gli indicatori vengono rivelati, maturano e vengono utilizzati quando viene scoperta un'attività corrispondente, che se indagata porta spesso a indicatori aggiuntivi che saranno soggetti allo stesso insieme di azioni e stati. Questo ciclo di azioni, e gli stati degli indicatori corrispondenti, formano il **ciclo di vita** dell'indicatore illustrato nella *Figura C.1*.

Ciò si applica indiscriminatamente a tutti gli indicatori, indipendentemente dalla loro accuratezza o applicabilità. Monitorare la derivazione di un determinato indicatore dai suoi predecessori può risultare dispendioso in termini di tempo e problematico se non si dispone di un tracciamento sufficiente, quindi è obbligatorio che gli indicatori soggetti a questi processi siano validi e applicabili al problema considerato. Se non si presta attenzione a questo fattore gli analisti potrebbero trovarsi ad applicare queste tecniche ad attori di minacce per cui non sono state progettate o ad attività del tutto benigne.

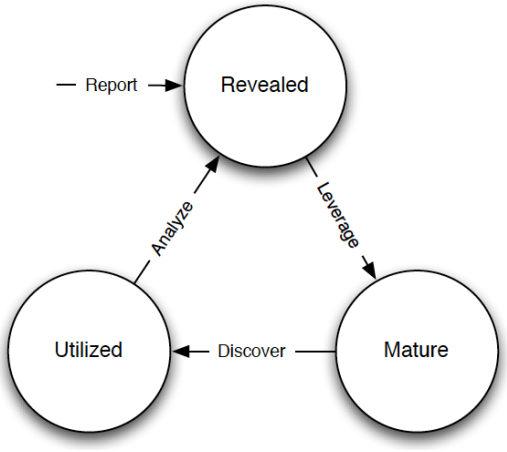


Figura C.1: Ciclo di vita degli Indicatori

C.3 La ricostruzione delle intrusioni

La *Kill Chain* è un nuovo modello di analisi delle intrusioni e aiuta gli analisti a capire quali informazioni sono o potrebbero essere disponibili per azioni difensive. Inoltre, in base al rilevamento in una determinata fase, gli analisti possono presumere che le fasi precedenti dell'intrusione siano già state eseguite correttamente. Di conseguenza risulta essere di estrema importanza un'analisi completa delle fasi precedenti, come mostrato nella Figura C.2, poiché è possibile intraprendere azioni in quelle fasi per mitigare eventuali intrusioni future.
Se ad esempio non si può ricostruire la fase di *delivery* di un'intrusione, inevitabilmente non si potrà agire sulla fase di *delivery* di successive intrusioni dello stesso avversario.

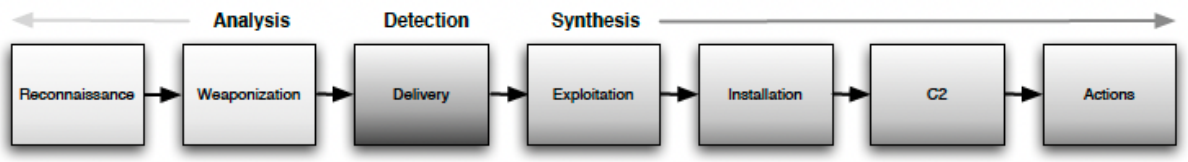


Figura C.2: Fase di *detection* di un attacco

I difensori devono essere in grado di spostare il rilevamento e l'analisi lungo le diverse fasi e, cosa più importante, di implementare percorsi di azione lungo la *Kill Chain*. Affinché un'intrusione sia economica gli avversari devono riutilizzare strumenti e infrastrutture; comprendendo completamente un'intrusione e sfruttando l'intelligence su questi elementi,

i difensori costringono l'avversario a cambiare ogni fase della loro intrusione per raggiungere con successo i loro obiettivi nelle intrusioni successive. In questo modo, i difensori della rete sfruttano la persistenza delle intrusioni degli avversari nei loro confronti per raggiungere un elevato livello di resilienza.

Altrettanto importante quanto l'analisi approfondita delle compromissioni riuscite con successo è la sintesi delle intrusioni fallite; man mano che i difensori raccolgono informazioni sugli avversari, spingeranno il rilevamento dalle ultime fasi a quelle precedenti.
Anche il rilevamento e la prevenzione nelle fasi pre-compromissione richiedono una risposta. I difensori devono raccogliere quante più informazioni possibili sull'intrusione mitigata, in modo da poter sintetizzare cosa sarebbe potuto accadere se le intrusioni future avessero superato le protezioni e i rilevamenti attualmente efficaci. Ad esempio, se un'e-mail dannosa mirata viene bloccata a causa del riutilizzo di un indicatore noto, la sintesi della *Kill Chain* rimanente potrebbe rivelare un nuovo *exploit* o *backdoor* in essa contenuto. Senza questa conoscenza, le future intrusioni, sfruttando mezzi diversi, potrebbero non essere rilevate. Se i difensori implementano le contromisure più velocemente di quanto si evolvano i loro noti avversari, mantengono un vantaggio tattico.

C.4 Analisi delle campagne di attacco

A livello strategico, l'analisi di più *Intrusion Kill Chain* nel tempo identifica punti in comune e indicatori sovrapposti. La Figura C.3 illustra come è possibile identificare la correlazione altamente dimensionale tra due intrusioni attraverso più fasi della kill chain. Attraverso questo processo, i difensori riconosceranno e definiranno le campagne di intrusione, collegando insieme forse anni di attività grazie ad una particolare minaccia persistente. Gli indicatori più coerenti e gli indicatori chiave delle campagne forniscono importanti informazioni ai difensori per dare priorità allo sviluppo e all'uso delle linee d'azione.

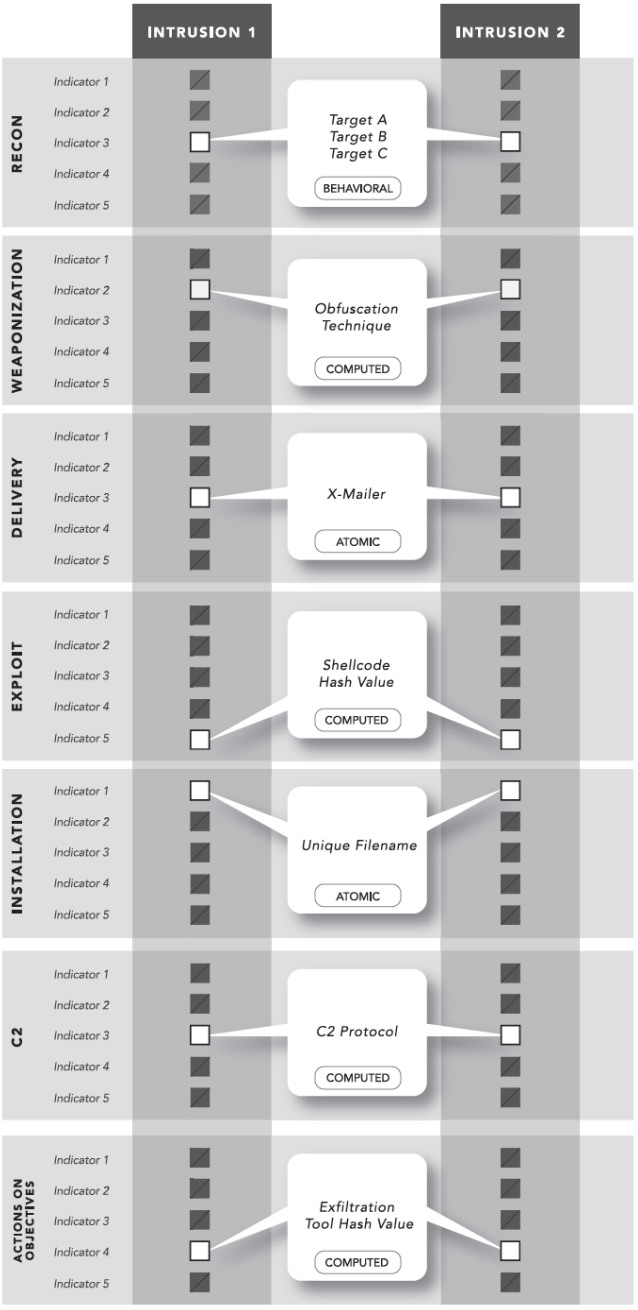


Figura C.3: Indicatori comuni tra diverse intrusioni

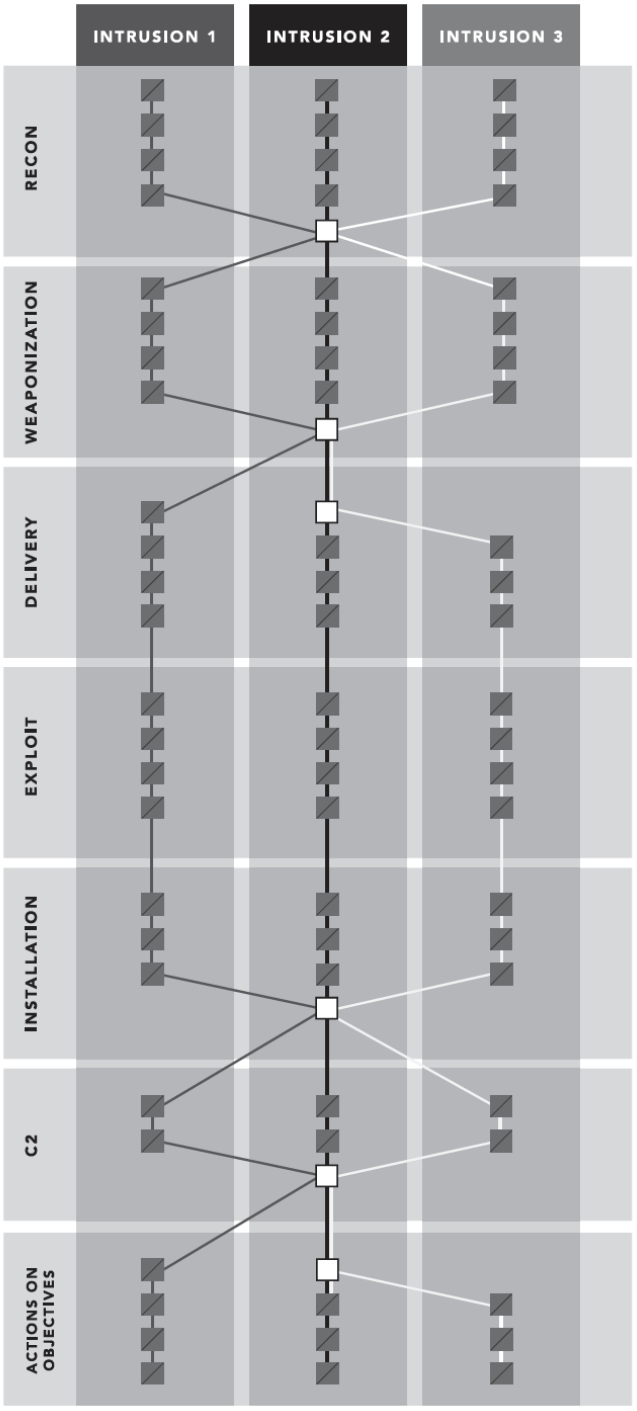


Figura C.4: Correlazione tra Indicatori

La Figura C.4 mostra come le intrusioni possono avere vari gradi di correlazione, ma i punti di flesso in cui gli indicatori si allineano più frequentemente identificano questi indicatori chiave. Ci si può aspettare che questi indicatori meno volatili rimangano coerenti, prevedendo le caratteristiche delle future intrusioni con maggiore sicurezza quanto più frequentemente vengono osservate. In questo modo, la persistenza di un avversario diventa un'informazione che il difensore può sfruttare per rafforzare le proprie difese.

L'obiettivo principale dell'analisi delle campagne è determinare i modelli e i comportamenti degli intrusi, le loro tattiche, tecniche e procedure (*TTP*), per rilevare in che modo (*how*) operano piuttosto che comprendere le azioni che hanno svolto (*what*).

L'obiettivo secondario è quello di attribuire positivamente l'identità degli intrusi mentre è più rilevante valutarne le capacità, la dottrina, gli obiettivi e i limiti; l'attribuzione di un intruso, tuttavia, potrebbe essere un prodotto collaterale di questo livello di analisi. Mentre i difensori studiano una nuova attività di intrusione, la collegheranno a campagne esistenti o forse identificheranno una nuova serie di comportamenti di una minaccia fino a quel momento sconosciuta e la tracceranno come una nuova campagna.
I difensori possono valutare la loro posizione difensiva relativa campagna per campagna e, sulla base del rischio valutato di ciascuno, sviluppare linee d'azione strategiche per coprire eventuali lacune.
Un altro obiettivo fondamentale dell'analisi della campagna è comprendere l'intento degli attaccanti. Nella misura in cui i difensori possono determinare tecnologie o individui di interesse, possono iniziare a comprendere gli obiettivi dell'attaccante. Ciò richiede intrusioni di tendenza nel tempo per valutare i modelli di targeting ed esaminare da vicino tutti i dati sottratti dagli intrusi. Ancora una volta questa analisi si traduce in una tabella di marcia per dare priorità a misure di sicurezza altamente mirate per difendere questi individui, reti o tecnologie maggiormente vulnerabili.

Appendice D

D.1 Scenario di utilizzo di STIX/TAXII

In questa appendice viene illustrato come utilizzare indicatori, malware, segnalazioni e le relazioni *STIX 2.1* in un comune scenario di condivisione degli indicatori.
Lo scenario descrive la creazione di un indicatore di attività dannosa come indicatore STIX da parte di un produttore (*Società A*) e la condivisione di tali informazioni con un'altra organizzazione (*Società B*) che utilizza l'indicatore per rilevare attività dannose e segnalare la presenza di tale attività dannosa al produttore iniziale.

STIX Producer: Società A

In questo scenario, la società A rileva alcune attività dannose sulla propria rete e decide di condividere il modo in cui l'hanno rilevato. Viene quindi creato un ***SDO*[8] *Indicator***. Questo indicatore contiene uno schema, come l'hash del file dell'attività dannosa rilevata, che fornisce la base per la creazione di relazioni tra l'indicatore e altri oggetti STIX. Per questo scenario, supponiamo che il pattern rilevi un hash di file per un noto malware (*CryptoLocker*). Per condividerlo, la società A utilizzerà un ***SDO Malware***, che contiene ulteriori informazioni sull'istanza di malware specifica.

Successivamente, l'azienda A può creare uno ***SRO*[9]** per rappresentare la relazione tra l'indicatore e gli oggetti malware. Per questo tipo di relazione, l'indicatore segnala l'esistenza del malware. Se dovessimo rappresentare visivamente questa relazione in un grafico, gli SDO Indicator e Malware sarebbero considerati nodi e l'oggetto relazione rappresenterebbe un arco orientato che collega i due oggetti, vedi *Figura D.1*.

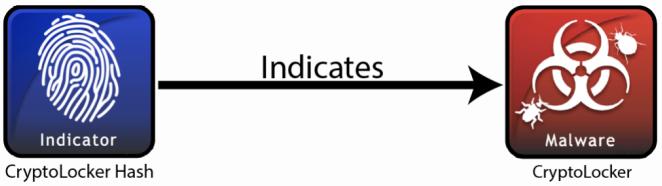


Figura D.1: Diagramma della SRO tra Indicator e Malware

Ora che l'azienda A ha generato contenuti STIX può condividere queste informazioni, racchiuse in un *Bundle STIX*, ovvero un contenitore, con altre organizzazioni. La società A pubblica quindi queste informazioni su un server TAXII dove saranno disponibili per il recupero da altri client TAXII.

[8] **SDO**: *STIX Domain Object*
[9] **SRO**: *STIX Relation Object*

STIX Consumer: Società B

La società B è iscritta al server TAXII su cui la società A ha appena pubblicato il proprio pacchetto. In questo scenario quindi il contenuto STIX viene ricevuto dalla società A.

Dopo aver cercato nella rete l'indicatore inviato dalla società A, la società B rileva lo stesso malware sulla propria rete. La società B può ora generare un oggetto di tipo ***SRO Sighting*** per riferire alla comunità di condivisione di aver individuato l'hash del malware considerato all'interno del *SDO Malware*. Quindi, in questo caso, la relazione ***SRO Sighting-Of*** permette di comunicare che l'*SDO Indicator* generato per la prima volta dalla società A è stato rilevato dalla società B. Infine, la società B può agire come *producer* pubblicando a sua volta la rilevazione sul server TAXII.

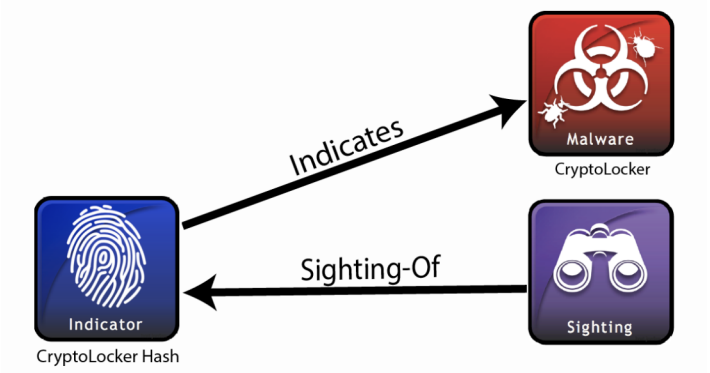


Figura D.2: Diagramma con l'oggetto di rilevamento (SDO Sighting)

D.2 Oggetti utilizzati

Di seguito vengono presentati gli oggetti e le relazioni utilizzate in questo scenario in modo più dettagliato.

Proprietà comuni

Ogni **SDO** e **SRO** in STIX utilizza proprietà comuni a tutti gli oggetti. Alcune di queste sono necessarie per ogni oggetto, come il ***type***, ovvero la tipologia di oggetto identificato (ad esempio *"indicator"*), un ***id*** che identifica in modo univoco l'oggetto e le proprietà ***created*** e ***modified*** che sono timestamp per rappresentare rispettivamente la prima versione e l'ultima versione dell'oggetto.

```
{
    "type": "indicator",
    "id": "indicator--71312c48-925d-44b7-b10e-c11086995358",
    "created": "2017-02-06T09:13:07.243000Z",
    "modified": "2017-02-06T09:13:07.243000Z"
}
```

Figura D.3: Esempio di proprietà comuni di tutti gli SDO/SRO

Nella *Figura D.3* le proprietà ***created*** e ***modified*** sono le stesse, il che significa che questa è la prima versione di quell'oggetto. Quando viene creata una nuova versione di un oggetto, la proprietà ***modified*** viene aggiornata e conterrà un timestamp successivo rispetto alla proprietà creata.

Ci sono altre proprietà comuni facoltative che non verranno discusse in dettaglio per questo scenario. Tuttavia oltre alle proprietà comuni che si trovano in tutti gli oggetti STIX, ogni oggetto ha il proprio insieme di proprietà che rappresentano le informazioni specifiche per un particolare oggetto. Nel nostro scenario per l'azienda A, è stato utilizzato un *Indicator* e un *Malware*.

Indicator Object

L'oggetto ***Indicator*** contiene proprietà che descrivono quell'indicatore, come il suo nome (***name***), un ***pattern*** utilizzato per il rilevamento, un elenco di ***indicator_types*** che specificano il tipo di indicatore e una proprietà ***valid_from*** che descrive in dettaglio l'ora da cui questo indicatore è ancora considerato valido.


```
{
   "type": "indicator",
   "spec_version": "2.1",
   "id": "indicator--71312c48-925d-44b7-b10e-c11086995358",
   "created": "2017-02-06T09:13:07.243000Z",
   "modified": "2017-02-06T09:13:07.243000Z",
   "name": "CryptoLocker Hash",
   "description": "This file is a part of CryptoLocker",
   "pattern": "[file:hashes.'SHA-256' = '46afeb295883a5efd6639d4197eb18bcba3bff49125b810ca4b9509b9ce4dfbf']",
   "pattern_type": "stix",
   "indicator_types": ["malicious-activity"],
   "valid_from": "2017-01-01T09:00:00.000000Z"
}
```


Figura D.4: SDO Indicator

La proprietà ***pattern*** per questo particolare indicatore contiene la rappresentazione STIX per un hash di file *SHA-256* insieme al valore hash della variante di *CryptoLocker*. L'***indicator_types*** descrive questo particolare tipo di indicatore come attività dannosa. I valori per l'etichettatura degli *Indicator* provengono dal Indicator Types Vocabulary presente nelle specifiche STIX.

Malware Object

Un ***Malware SDO*** viene utilizzato per rappresentare le informazioni sul malware *CryptoLocker* rilevato dalla società A. Insieme alle proprietà comuni acquisisce proprietà come: il nome (***name***) del malware, una descrizione (***description***) e anche un elenco di ***malware_types*** che caratterizza il tipo di malware.

```
{
    "type": "malware",
    "id": "malware--81be4588-96a8-4de2-9938-9e16130ce7e6",
    "spec_version": "2.1",
    "created": "2017-02-06T09:26:21.647000Z",
    "modified": "2017-02-06T09:26:21.647000Z",
    "name": "CryptoLocker",
    "description": "CryptoLocker is known to hold files hostage for ransom.",
    "malware_types": ["ransomware"]
}
```


Figura D.5: SDO Malware

La proprietà **malware_types** indica che questo particolare malware è un *ransomware*. Questo valore deriva da un altro vocabolario aperto visto nella sezione Malware Type Vocabulary delle specifiche.

Relationship Object

Una relazione SRO collega l'indicatore dell'azienda A al malware. Questo oggetto contiene le stesse proprietà comuni degli SDO STIX insieme alle proprietà richieste necessarie per definire la relazione tra i due oggetti. Ad esempio, ogni relazione richiede una ***source_ref***, che acquisisce l'*id* dell'SDO di origine, e un ***target_ref***, che contiene l'*id* dell'SDO di destinazione. Insieme a queste due proprietà, abbiamo bisogno di una proprietà ***relationship_type*** per identificare il tipo di relazione. Ulteriori informazioni sull'oggetto Relazione e l'elenco completo delle proprietà sono disponibili nella sezione Relationship delle specifiche.


```
{
    "type": "relationship",
    "id": "relationship--a19fac85-f6f5-47f3-aacd-4bfb54557852",
    "spec_version": "2.1",
    "created": "2017-02-06T09:30:51.987000Z",
    "modified": "2017-02-06T09:30:51.987000Z",
    "relationship_type": "indicates",
    "source_ref": "indicator--71312c48-925d-44b7-b10e-c11086995358",
    "target_ref": "malware--81be4588-96a8-4de2-9938-9e16130ce7e6"
}
```


Figura D.6: Relationship SRO

STIX Bundle

La società A utilizza un ***STIX Bundle*** per contenere questi tre oggetti STIX. I *Bundle* vengono utilizzati per condividere una raccolta di oggetti STIX in un documento JSON e possono avere un numero qualsiasi di oggetti arbitrari e non correlati. In questo scenario gli oggetti sono correlati, ma ciò non è necessario o richiesto per i bundle. Un *Bundle* non è un oggetto STIX, quindi non contiene tutte le proprietà comuni che possiedono gli oggetti. Tuttavia, contiene una proprietà che specifica il fatto che sia un bundle e un ***id*** univoco. Maggiori informazioni su Bundle sono disponibili nelle specifiche nella sezione

Bundle. La società A può quindi pubblicare questo pacchetto su un server TAXII a cui la società B è iscritta affinché lo recuperi e lo utilizzi.

Complessivamente, lo *STIX Bundle* della società A avrà questo aspetto:


```
{
    "type": "bundle",
    "id": "bundle--1736e032-a96a-41e9-8302-126677d4d781",
    "objects": [
        {
            "type": "indicator",
            "id": "indicator--71312c48-925d-44b7-b10e-c11086995358",
            "spec_version": "2.1",
            "created": "2017-02-06T09:13:07.243000Z",
            "modified": "2017-02-06T09:13:07.243000Z",
            "name": "CryptoLocker Hash",
            "description": "This file is a part of CryptoLocker",
            "pattern": "[file:hashes.'SHA-256' = '46afeb295883a5efd6639d4197eb18bcba3bff49125b810ca4b9509b9ce4dfbf']",
            "pattern_type": "stix",
            "indicator_types": ["malicious-activity"],
            "valid_from": "2017-01-01T09:00:00.000000Z"
        },
        {
            "type": "malware",
            "id": "malware--81be4588-96a8-4de2-9938-9e16130ce7e6",
            "spec_version": "2.1",
            "created": "2017-02-06T09:26:21.647000Z",
            "modified": "2017-02-06T09:26:21.647000Z",
            "name": "CryptoLocker",
            "description": "CryptoLocker is known to be malicious ransomware.",
            "malware_types": ["ransomware"]
        },
        {
            "type": "relationship",
            "id": "relationship--a19fac85-f6f5-47f3-aacd-4bfb54557852",
            "spec_version": "2.1",
            "created": "2017-02-06T09:30:51.987000Z",
            "modified": "2017-02-06T09:30:51.987000Z",
            "relationship_type": "indicates",
            "source_ref": "indicator--71312c48-925d-44b7-b10e-c11086995358",
            "target_ref": "malware--81be4588-96a8-4de2-9938-9e16130ce7e6"
        }
    ]
}
```


Figura D.7: STIX Bundle

Sighting Object

Se la società B utilizza l'indicatore fornito dalla società A e ottiene una corrispondenza, significa che probabilmente ha lo stesso malware *CryptoLocker* sulla propria rete. Si tratta di informazioni importanti da condividere con la propria comunità e per farlo possono generare un oggetto di tipo ***Sighting***. Questo è l'altro tipo di SRO in STIX 2.1 e significa che è stato visto qualche oggetto.

L'oggetto *Sighting* contiene le stesse proprietà comuni di altri oggetti STIX ma ha solo una proprietà richiesta, ***sighting_of_ref***; questa proprietà contiene un riferimento all'oggetto che è stato avvistato. Altre proprietà opzionali non sono state utilizzate ma possono essere visualizzate nella tabella delle proprietà nella sezione Sighting delle specifiche.

```
{
    "type": "sighting",
    "id": "sighting--4eebf1e1-5351-49ed-9b7b-28f0da806d82",
    "spec_version": "2.1",
    "created": "2017-02-07T20:08:31.154Z",
    "modified": "2017-02-07T20:08:31.154Z",
    "sighting_of_ref": "indicator--71312c48-925d-44b7-b10e-c11086995358"
}
```


Figura D.8: Sighting Object

La società B può anche pubblicare nuovamente l'oggetto sul server TAXII in modo da permettere ad altri che hanno visto anche questo malware presente nella loro rete.

D.3 Note conclusive all'esempio

Quanto presentato sopra è uno sguardo molto semplice a uno scambio di dati tra due organizzazioni utilizzando i concetti in STIX 2.1 e rappresenta una minima parte di ciò che è possibile fare con STIX. Esistono molti altri oggetti utilizzati per modellare le informazioni sulle minacce come *Threat Actors*, *Campaigns*, *Intrusion Set*, *Observed Data* e *Vulnerability*, solo per citarne alcuni. È anche possibile utilizzare dei ***Data Markings*** per limitare il modo in cui informazioni, oggetti e proprietà possono essere condivise.

Per ulteriori informazioni su tutti questi concetti si rimanda alla specifica STIX 2.1, che contiene tutte le informazioni necessarie.

Bibliografia

[1] Barrett, Matthew P. "*Framework for Improving Critical Infrastructure Cybersecurity version 1.1*." National Institute of Standards and Technology (2018).

[2] Schweizerische, S. N. V. "*Information technology - Security techniques - Information security management systems - Requirements*." ISO/IEC International Standards Organization (2013).

[3] Amin, R. M., Hutchins, E. M., Cloppert, M. J. "*Intelligence-driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*". Lockheed Martin Corporation (2010).

[4] "*Information technology - Security techniques - Information security management systems - Overview and vocabulary*". ISO/IEC International Standards Organization (2018).

[5] Cody Delzer. "*How the Cyber Kill Chain can help you to protect against attacks*". SBS CyberSecurity (2019).
URL:
https://sbscyber.com/resources/how-the-cyber-kill-chain-can-help-you-protect-against-attacks

[6] *STIX/TAXII Documentation*: https://oasis-open.github.io/cti-documentation/

[7] MAEC Core Specification. (2017):
https://maecproject.github.io/releases/5.0/MAEC_Core_Specification.pdf

[8] *MISP Documentation*: https://www.misp-project.org/