Università Politecnica delle Marche

Facoltà di Ingegneria

Dipartimento di Ingegneria dell'Informazione

Corso di Laurea Magistrale in Ingegneria Informatica e dell'Automazione

Tesi di Laurea

Ottimizzazione e automazione dei processi di un SOAR integrato in SOC distribuiti operanti in contesti eterogenei

Optimization and automation of the processes of a SOAR integrated in distributed SOCs operating in heterogeneous contexts

Relatore

Prof. Domenico Ursino

Candidato

Edoardo Balducci

Correlatore

Alessandro Morsicani

Anno Accademico 2018-2019

Indice

Elenco delle figure

Elenco dei listati

Introduzione

Il mondo in cui viviamo sta cambiando, sempre di più e sempre più rapidamente. Le nuove frontiere tecnologiche permettono di connettere tutto e tutti. Questa trasformazione sta guidando l'innovazione ad una velocità senza precedenti e sta portando miglioramenti, inimmaginabili fino a poco tempo fa, nel nostro modo di vivere e lavorare.

Questo nuovo mondo, fatto di opportunità, va però protetto e solo la giusta combinazione di esperienza, skill e tecnologie assicurerà una trasformazione sicura e controllata. Si ha la necessità di esperienza nel campo della Cybersecurity e di essere preparati alle continue evoluzioni delle minacce.

Gli attacchi informatici suscitano allarme nella popolazione, causano danni ingenti all'economia e mettono in pericolo la stessa incolumità dei cittadini quando colpiscono reti di distribuzione di servizi essenziali come la sanità, l'energia, i trasporti, vale a dire le infrastrutture critiche della società moderna.

Inoltre, un attacco informatico andato a buon fine potrebbe rappresentare un momento di non ritorno per la credibilità di un'azienda, per lo sviluppo del suo business e per la capacità di vendere prodotti in un regime di sana concorrenza.

Gli attaccanti si stanno evolvendo; sono persone preparate le quali conoscono strumenti e vulnerabilità dei software che le aziende utilizzano; non agiscono più individualmente, ma in gruppo. Essi possono usufruire di tecnologie avanzate e di hardware con alta capacità computazionale.

L'incremento degli attacchi, che diventeranno sempre più intelligenti e complessi, anche grazie all'utilizzo dell'Intelligenza Artificiale, sarà una costante nel prossimo futuro.

Le organizzazioni denunciano la carenza di personale con esperienza, qualificato nel campo della Cybersecurity e competente nella gestione di incidenti di sicurezza gravi. Inoltre hanno difficoltà a dimostrare di essere conformi a tutte le regolamentazioni che sono in vigore per la protezione dei dati e della privacy dei propri clienti.

Un'altra grave mancanza riguarda il coordinamento dei diversi team durante la gestione di un incidente. La perdita di tempo nel reagire ad un attacco, per coordinare i vari team di risposta, per informare i clienti e per contattare i manager della sicurezza, può fare la differenza nel futuro del business di un'azienda.

Per ridurre il tempo, durante l'analisi di un incidente si ha la necessità di coinvogliare, il più velocemente possibile, in un unico punto, tutte le informazioni relative all'attacco in corso, in modo tale che le decisioni da prendere successivamente, avranno maggiore efficenza.

Sono sempre più necessarie delle linee guida specifiche per ogni tipologia di attacco, create da qualcuno con maggiore esperienza nel campo della Cybersecurity, con lo scopo di guidare durante un incidente il personale meno formato. Nel momento in cui persone istruite in questo ambito vanno in pensione o cambiano azienda, le informazioni da esse distribuite non dovranno andar perse.

Gli attacchi sono inevitabili, e quando si verificano chi si occupa di sicurezza informatica deve trovarsi pronto. Serve una strategia in grado di assicurare che i dati e i beni fondamentali di un'organizzazione rimangano al sicuro. È necessario preparare i team, proprio come si fa per i piani antincendio, ad agire con efficienza e velocità.

Perciò la strategia di Cybersecurity diventa parte integrante di un'organizzazione aziendale e va dalla prevenzione e rilevamento, per ridurre il verificarsi degli attacchi, alla mitigazione, per reagire una volta che l'attacco si è verificato.

Non tutte le organizzazioni sono in grado di gestire autonomamente le strategie da applicare per attuare una risposta, così scelgono di affidarsi ad aziende specializzate in sicurezza informatica, che offrono servizi di Security Operation Center (SOC).

Il SOC, specializzato in questo ambito, è composto da tre fattori principali:

- persone;
- processi;
- tool.

Esso ha l'obiettivo di difendere gli asset informatici dei propri clienti. La velocità di reazione ad un attacco, nell'ambito della sicurezza informatica, è un fattore fondamentale. Per diminuire il tempo di risposta serve uno strumento capace di coordinare le persone appartenenti al SOC, i suoi processi di sicurezza e le tecnologie utilizzate; tale orchestratore è il Security Orchestration, Automation and Response (SOAR).

Questa tesi si colloca proprio in tale contesto e si pone come obiettivi l'analisi delle tecnologie e dei processi interni di un SOC distribuito ed eterogeneo e l'applicazione della piattaforma SOAR per l'automatizzazione e l'ottimizzazione di tali processi.

In una prima fase sarà condotta un'analisi dei processi interni di un SOC e delle attività che vengono svolte per rispondere ad un attacco. Compresi questi, si passerà ad uno studio delle tecnologie utilizzate internamente, come il Security Information and Event Management e le fonti di threat intelligence. Infine verrà effettuata l'installazione di del SOAR Resilient, l'implementazione di funzioni automatiche, utili per effettuare l'enrichment di un incidente, e lo sviluppo di un flusso di lavoro con lo scopo di guidare gli analisti durante un attacco.

La presente tesi è strutturata come di seguito specificato:

- Nel primo capitolo verranno introdotte le nuove tipologie di attacco e verrà descritto come la Cybersecurity si sia evoluta di conseguenza.

- Nel secondo capitolo si parlerà del contesto di riferimento e delle regolamentazioni a cui deve sottostare.
- Nel terzo capitolo si descriveranno i processi interni e la stratificazione del Security Operation Center.
- Nel quarto capitolo verranno illustrati il Security Information and Event Management e le fonti di threat intelligence utilizzate.
- Nel quinto capitolo si discuterà della tecnologia SOAR e delle integrazioni sviluppate in essa.
- Nel sesto capitolo sarà analizzata l'implementazione di un workflow automatico per la risposta di un incidente di tipo Malware.
- Nel settimo capitolo saranno valutati i punti di forza, di debolezza, le opportunità e le minacce relative all'integrazione della piattaforma SOAR da noi effettuata.
- Nell'ottavo capitolo saranno tratte delle conclusioni riguardo al lavoro effettuato e verranno mostrati anche dei possibili sviluppi futuri.

1

Uno sguardo alla Cybersecurity

Nella prima parte di questo capitolo verrà descritto, come negli anni, si sono evolute le minacce cyber, più nel dettaglio come sono cambiati gli attaccanti e gli attacchi. Nella seconda parte verrà descritto come si sono evoluti i processi e le nuove tecnologie di difesa nel corso degli anni.

1.1 Evoluzione del Cybercrime

Cybersecurity è il gruppo di attività e competenze multidisciplinari, complesse e sofisticate, molte delle quali non informatiche, che sono oggettivamente di difficile integrazione con le attuali prassi di gestione dell'ICT e di allocazione di budget relativi, poichè la loro implementazione richiede di superare paradigmi tecnologici e silos organizzativi costruiti negli anni a partire da esigenze di compliance e da metodi e strumenti propri della sicurezza informatica "tradizionale". Mentre, per Cybercrime si intendono attività criminali effettuate mediante l'uso di strumenti informatici [5].

Si potrebbe pensare che le minacce provengano soltanto da fonti esterne alle imprese, ma non è sempre così. Bisogna saper reagire sia ad attacchi mirati sia ad una minaccia interna. Ci troviamo in un'era in cui siamo sempre più connessi alla rete; ci sono dati che vengono inviati ogni secondo, documenti che vengono salvati nei Cloud, c'è l' Internet Of Things, si leggono documenti confidenziali con gli smartphone.

Tutta questa connessione online agevola il lavoro, velocizza i processi, rende disponibile ogni cosa quando si vuole e dove si vuole, ma tutta questa bellezza ha un lato negativo, la superficie di attacco aumenta notevolemente.

La superficie d'attacco di un sistema è il sottoinsieme delle risorse che un attaccante può utilizzare per attaccare un sistema. Un attaccante può utilizzare i punti di ingresso e di uscita di un sistema nonchè i canali non attendibili per inviare dati nel sistema, per ricevere dati dal sistema o per attaccare il sistema. Di conseguenza, l'insieme dei punti di entrata e di uscita, l'insieme dei canali e l'insieme dei dati non attendibili rappresentano il relativo sottoinsieme di risorse che fanno parte della superficie di attacco [3].

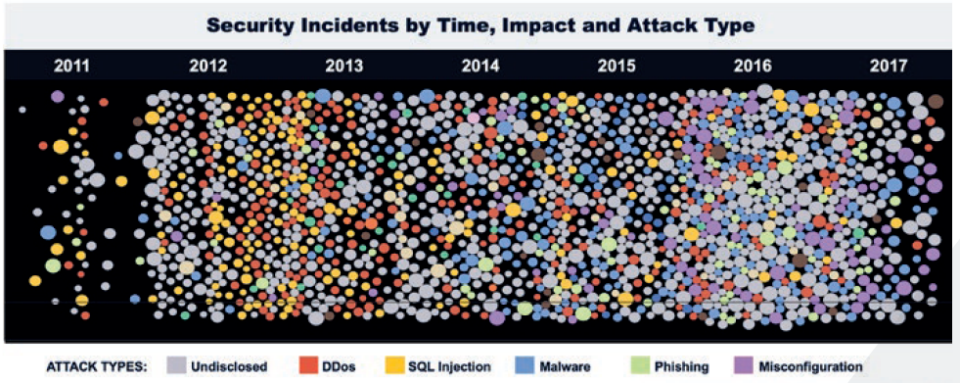

Figura 1.1. Evoluzione degli incidenti di sicurezza

Come si può vedere dal grafico in Figura 1.1, gli incidenti di sicurezza sono aumentati in modo esponenziale dal 2011 al 2017, ma secondo il rapporto del 2019 del CLUSIT, Associazione Italiana per la Sicurezza Informatica, il 2018 è stato l'anno peggiore di sempre in termini di evoluzione delle minacce cyber e dei relativi impatti, non solo dal punto di vista quantitativo ma anche e soprattuto da quello qualitativo, evidenziando un trend di crescita degli attacchi, della loro gravità e dei danni conseguenti mai registrato in precedenza.

Nell'arco temporale 2014-2018 la crescita degli attacchi gravi è stata del +77,8% e nel solo biennio 2017-2018, gli attacchi sono cresciuti del +37,7%, come evidenziato in Figura 1.2.

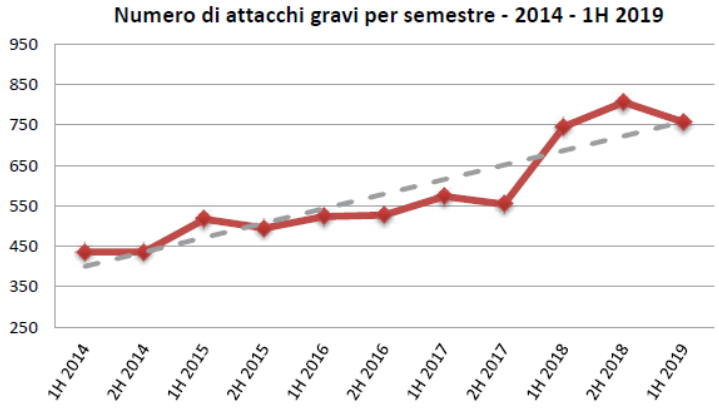

Figura 1.2. Andamento degli attacchi gravi

Siamo in un cambiamento di fase nei livelli globali di cyber-insicurezza, causata dall'evoluzione degli attori, delle modalità e delle finalità degli attacchi.

1.1.1 Tipologia di attaccante

Non si deve pensare ad un hacker come ad una singola persona, senza nessuna capacità sociale, chiuso in una stanza dove programma tutto il giorno. Dobbiamo cambiare visione e renderci conto che oggi giorno gli attaccanti sono persone preparate, organizzate in gruppi a cui vengono fornite delle risorse notevoli per i loro scopi. Definiamo le varie categorie dei possibili attaccanti:

- *Cybercrime:* sono attacchi condotti da persone che effettuano dei crimini tramite l'uso di strumenti informatici, senza nessuna finalità specifica.
- *Hacktivism:* sono azioni, compresi gli attacchi informatici, effettuate per finalità politiche o sociali.
- *Espionage/Sabotage:* sono azioni commissionate da aziende competitor per ottenere informazioni sensibili e avere un vantaggio competitivo.
- *Information Warfare:* sono un insieme di tecniche di raccolta, elaborazione, gestione e diffusione delle informazioni per ottenere un vantaggio in campo militare, politico o economico.

Anche le tipologie degli attaccanti durante gli anni si sono evolute ed hanno cambiato il loro trend, come è evidenziato in Figura 1.3.

ATTACCANTI PER TIPOLOGIA	2014	2015	2016	2017	2018	1H 2018	1H 2019	1H 2019 su 1H 2018	Trend 2019
Cybercrime	526	684	751	857	1232	591	640	8,3%	↑
Hacktivism	236	209	161	79	61	29	19	-34,5%	↓
Espionage / Sabotage	69	96	88	129	203	99	80	-19,2	↘
Information Warfare	42	23	50	62	56	27	18	-33,3%	↓
Espionage / Sabotage + Inform. Warfare	111	119	138	191	259	126	98	-22,2%	↘

Figura 1.3. Trend delle tipologie di attaccanti

Oggi risulta difficile distinguere nettamente tra Cyber-espionage e Information Warfare; quindi, sommando gli attacchi di entrambe le categorie, nel primo semestre del 2019, questi rappresentano il 13% del totale.

1.1.2 Tipologia di attacco

Gli attaccanti hanno molti modi per poter recare danni ai loro obiettivi; le principali tecniche di attacco utilizzate sono le seguenti:

- *Malware:* applicazioni finalizzate ad arrecare danno in qualche modo alla vittima.

- *Vulnerabilità note / Misconfigurazioni:* vulnerabilità risolvibili con aggiornamenti software che, spesso non vengono effettuati o, più semplicemente, configurazioni sbagliate dei servizi.
- *Phishing / Social Engineering:* tecnica che induce la vittima, mediante una falsa comunicazione in posta elettronica, a collegarsi verso un sito simile a quello originale al fine di intercettare le informazioni trasmesse, come le credenziali di accesso.
- *Account hacking / Cracking:* tecnica che, tramite attacchi di brute force e tentativi multipli in poco tempo effettuati da script, si pongono come obiettivo quello di scoprire il nome dell'utente e la password.
- *DDoS:* Attacchi voluti a rendere inaccessibili alcuni tipi di servizi, utilizzando più dispositivi cordinati.
- *0-day:* è una vulnerabilità sconosciuta o non affrontata da coloro che dovrebbero essere interessati a mitigarlo.
- *Phone hacking:* attività di hacking che ha come oggetto i sistemi telefonici.
- *SQL Injection:* Tecnica di attacco basata sull'uso di query indirizzate a database SQL che consentono di ricavare informazioni ed eseguire azioni anche con privilegi di amministrazione.

Il trend delle diverse tecniche di attacco utilizzate nel periodo di tempo che va dal 2014 al primo semestre del 2019 è riportato in Figura 1.4.

TECNICHE DI ATTACCO PER TIPOLOGIA	2014	2015	2016	2017	2018	1H 2018	1H 2019	1H 2019 su 1H 2018	Trend 2019
Malware	127	106	229	446	585	295	310	5,1%	↗
Unknown	199	232	338	277	408	210	160	-23,8%	↘
Known Vulnerabilities / Misconfigurations	195	184	136	127	177	82	71	-13,4%	↘
Phishing / Social Engineering	4	6	76	102	160	62	127	104,8%	↑
Multiple Techniques / APT	60	104	59	63	98	46	34	-26,1%	↘
Account Hacking / Cracking	86	91	46	52	56	18	34	88,9%	↑
DDoS	81	101	115	38	38	20	8	-60,0%	↓
0-day	8	3	13	12	20	12	11	-8,3%	↘
Phone Hacking	3	1	3	3	9	1	1	-	-
SQL Injection	110	184	35	7	1	0	1	-	-

Figura 1.4. Trend delle tecniche di attacco

Avendo definito come si stanno evolvendo in volume gli attacchi informatici, a che

tipologia di gruppo potrebbero far parte gli attaccanti e quali tipologie di attacchi potrebbero utilizzare, si cercherà nel seguito di definire come è cambiata la visione difensiva.

1.2 Evoluzione delle tattiche di difesa

L'obiettivo degli attacchi sono sempre le informazioni, che possono essere relative ai clienti di un'organizzazione oppure ai processi industriali, per poi rivendere al miglior offerente le informazioni ottenute oppure, per ricattare la stessa azienda a cui sono state sottratte.

L'organizzazione di un'efficace tattica di difesa e la capacità di risposta agli attacchi informatici comporta diverse decisioni e azioni importanti. L'organizzazione deve decidere quali strumenti e servizi mettere a disposizione del team di risposta agli incidenti.

Negli anni gli attaccanti hanno mutato i modi di attaccare e le loro motivazioni di attacco. Come si è evoluto il fronte offensivo, si è evoluto anche quello difensivo. Sono migliorati i processi interni di gestione di un incidente, è cambiata la mentalità su come affrontare un attacco e sono state sviluppate nuove tecnologie di difesa.

1.2.1 Processi interni

Essendo mutate e migliorate le tecniche di attacco, in risposta sono cambiati e si sono adattati ad esse i processi interni dei gruppi di sicurezza per gestire un incidente informatico.

Sono stati definiti dei modelli formali per indirizzare il flusso delle operazioni da svolgere per prepararsi ad un eventuale attacco, per gestire un possibile attacco avvenuto e per ritornare in uno stato sicuro quando il malware è stato eliminato dall'infrastruttura.

Come è stato detto nella sezione precedente, ci sono diverse tipologie di attacco; per ognuna di queste esistono processi formali per la loro gestione. Ci sono, anche, delle organizzazioni, ad esempio il National Institute of Standards and Technology (NIST), che forniscono delle linee guida di alto livello per la gestione degli incidenti informatici.

In seguito verranno analizati due casi specifici di gestione di attacchi informatici, uno relativo ad un attacco di tipo malware ed un altro relativo alla gestione di un attacco di tipo phishing.

Non sono migliorati soltanto i processi, ma anche l'organizzazione e la gestione del personale. Infatti, ora, all'interno delle organizzazioni ci sono ruoli e responabilità del personale ben definiti, ogni persona ha un ruolo e delle competenze specifiche. Sono presenti, anche, delle stratificazioni in base alle competenze specifiche del personale.

Un altro miglioramento fondamentale ha riguardato la continua interazione tra i vari team, ad esempio tra il Security Operation Center e il Network Operation Center, per raggiungere l'obiettivo comune, rimanere in sicurezza.

Durante gli anni è migliorata la consapevolezza del rischio di non difendersi, e ciò ha spinto le aziende ad investire di più in sicurezza e formare personale adeguato.

Un'altra mossa fondamentale per combattere il Cybercrime è "cristallizzare" l'eredità appresa nel campo durante gli anni dalle singole persone. Infatti, l'esperienza in questo campo è fondamentale e non si può perdere tanta conoscenza quando un esperto cambia azienda oppure va in pensione. Per questo motivo sono importanti i processi interni di ogni azienda così ad ogni nuovo ingresso, si hanno delle linee guida da seguire per la gestione degli incidenti, già testate e approvate dal Security Operation Center.

1.2.2 Tecnologie di difesa

Negli anni è cambiato il modo di vedere un attacco. Prima, nei propri personal computer si aveva un antivirus non connesso in rete che scansionava i file cercando delle corrispondenze e aggiornando il proprio database dei malware periodicamente.

Le case produttrici degli antivirus hanno cambiato mentalità adottando l'idea di una condivisione online. Gli antivirus si sono spostati nel cloud; quando viene scoperto un nuovo malware non presente nel database, viene memorizzato e poi distribuito ai singoli dispositivi che possiedono quell'antivirus.

Dal momento che le informazioni relative ai malware sono diventate una fonte di ricchezza, le case produttrici vendono le signature dei malware ad altre case produttrici; quindi più dispositivi, anche con antivirus di diverse case produttrici, hanno accesso ad un bacino più grande di informazioni.

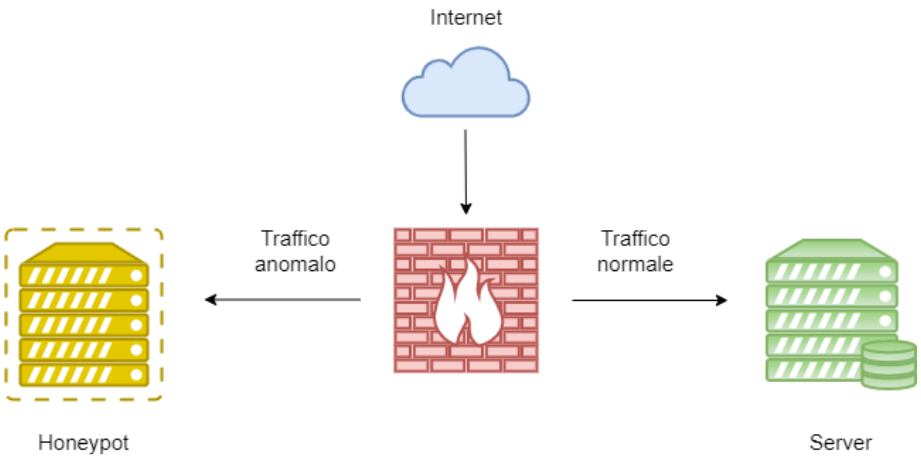

Figura 1.5. Schema di funzionamento di un Honeypot

Le case produttrici degli antivirus installano diversi honeypot sparsi nel mondo, così da raccogliere più informazioni possibili provenienti dai diversi continenti, Figura 1.5

Gli honeypot sono programmi speciali scritti con un unico scopo: subire exploit. Gli honeypot possono emulare l'esistenza della vulnerabilità, per cui gli aggressori, i virus e i worm sono attratti da questo sistema che appare poco sicuro. Essi raccolgono quante più informazioni possibili sugli attacchi che provengono da varie

fonti, il che permette di analizzarli e studiarli in seguito un pò più a fondo. Questo può essere un ottimo strumento da utilizzare per rivelare eventuali zero-day che non sono ancora stati scoperti.

Ci sono, invece, altre organizzazioni open source che rendono reperibili gratuitamente delle Threat Source raccolte da loro, ad esempio Malware Information Sharing Platform (MISP).

Il fronte difensivo si coalizza per ottenere maggiore consapevolezza e conoscenza per avere accesso ad un bacino più ampio di feed relativi a degli attacchi informatici.

La Cybersecurity sta facendo un uso sempre maggiore dell'intelligenza artificiale. Si sta spingendo sull'impiego di forme di automazione intelligente basate su algoritmi di Predictive Analytics e Machine Learning. Si stima che, entro il 2021, almeno il 50% degli allarmi di sicurezza dei SOC saranno gestiti attraverso l'automazione, che porterà a misure di risposta automatica senza l'intervento diretto degli analisti di sicurezza.

2

Contesto di sviluppo

Nella prima parte di questo capitolo verrà descritto il contesto di svolgimento del tirocinio e la visione di Cybertech nel mondo della Cybersecurity. Nella seconda parte verranno descritti i regolamenti legislativi a cui sono sottoposte le aziende nell'era digitale infine, verranno presentati i processi interni di un Security Operation Center.

2.1 Visione e progetto di Cybertech

Come è stato detto nel capitolo precedente, le minacce stanno aumentando sia di quantità che di qualità. Le aziende molto spesso non hanno idea di quanto valgono le loro informazioni; quindi, di conseguenza, non riescono a calcolare il giusto investimento da fare per proteggersi. Molte volte non riescono a sostenere il costo di un team di sicurezza interno, ma vogliono comunque sentirsi sicure.

Si immagini un'azienda che deve custodire i propri segreti relativamente la produzione o i dati dei propri clienti, ma che non operi in ambito informatico; non sarebbe in grado di mettersi in sicurezza in maniera autonoma.

Creare un team di risposta agli incidenti internamente ad un'azienda ha un costo molto alto, riguardante gli strumenti ed il personale esperto da dover assumere. La soluzione migliore sarebbe lasciare il compito della sicurezza dei dati e delle reti ad un'organizzazione esterna, la quale è specializzata in Cybersecurity.

In questa crescente richiesta si è inserita Cybertech (Figura 2.1), azienda specializzata in sicurezza informatica, composta da team specializzati nel campo della Cybersecurity (Figura 2.2).

Figura 2.1. Logo di Cybertech

Al suo interno ci sono gli specialisti di reti che appartengono al gruppo del Network Operations Center (NOC), specialisti in attacchi informatici appartenenti al gruppo dei Penetration Tester (PT) ed, infine, specialisti in sicurezza informatica e risposta ad eventuali attacchi, appartenenti al gruppo del Security Operations Center (SOC).

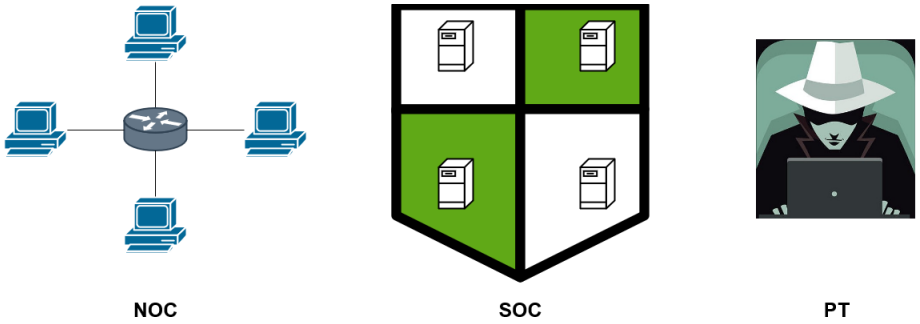

Figura 2.2. Gruppi esistenti all'interno di Cybertech

Cybertech ha creato il servizio Security Operation Center nel 2018, dopo un anno di attività, nel 2019 è entrata a far parte del gruppo Engineering Ingegneria Informatica, come azienda specializzata in servizi di Cybersecurity.

Ad oggi Cybertech ha in carico 450 clienti, ha al suo interno 4 SOC certificati, gestisce 21000 server, risponde in media a 43,2 miliardi di eventi al giorno, intercetta 123 miliardi di vulnerabilità note al giorno e rende sicuri oltre 10 petabyte di dati. Cybertech gestisce clienti appartenenti a diverse nazioni, eroga servizi di Cybersecurity in Europa, USA e Sud America.

Cybertech garantisce una sicurezza informatica costante, così chi si affida a questo servizio può concentrarsi alla crescita del proprio business non prepuccupandosi di controllare le reti, salvaguardare i dati e di dover prevenire e rispondere alle minacce informatiche.

Per motivi di privacy, relativi a Cybertech, nel seguito verranno esposti dei processi più generali rispetto a quelli che vengono seguiti dal personale appartenente al SOC. I processi illustrati rappresentano, comunque, le basi di ogni team di incidenti alla risposta; poi questi ultimi vengono adattati in base alle esigenze specifiche di ogni azienda.

2.2 Conformità ai regolamenti governativi

Gli enti governativi e i leader dei settori industriali hanno concluso che tutte le aziende e le organizzazioni spesso non riescono a proteggere in modo opportuno le informazioni sensibili, causando danni agli individui e alle altre organizzazioni; così i governi e i leader dei settori industriali hanno imposto degli standard di conformità, insieme a penalizzazioni potenzialmente severe, per coloro che non sono conformi, in uno sforzo di ridurre le perdite e di proteggere le vittime innocenti.

Non solo un'organizzazione deve ora soddisfare tali richieste di sicurezza, numerose e nuove, ma deve anche dimostrarlo.

Il pervasivo utilizzo delle tecnologie digitali offre ai cittadini, alle istituzioni e alle imprese, nuove opportunità di connessione, favorendo la diffusione delle informazioni e lo sviluppo di nuovi modelli di business. I cosidetti "cyber criminali", come già detto in precedenza, tentano quotidianamente di sottrarre dati e compromettere il funzionamento dei sistemi transnazionali di comunicazione che, essendo altamente connessi, risultano particolarmente vulnerabili.

L'attenzione nei confronti della Cybersecurity è cresciuta perché correlata alla prosperità e alla sicurezza di cittadini e imprese. Si pensi che, solo nel 2016, all'interno dell'Unione Europea, sono stati registrati più di 4000 attacchi ransomware al giorno e l'80% delle imprese ha subito almeno un incidente di Cybersecurity. Negli ultimi quattro anni l'impatto economico della cyber-criminalità è quintuplicato.

Proprio per questo motivo sono nate delle regolamentazioni apposite per garantire la sicurezza dei singoli individui, a cui ogni azienda appartenente all'Unione Europea deve sottostare, a titolo di esempio, citiamo i seguenti:

- *Cybersecurity Act:* Regolamento UE 2019/881, in vigore dal 27 giugno 2019; ha lo scopo precipuo di creare un quadro unico per l'introduzione di un sistema europeo di certificazione per la sicurezza informatica dei prodotti e dei servizi digitali. Essendo un regolamento, una volta entrato in vigore, diviene immediatamente applicabile in tutti gli Stati membri, fatte salve alcune limitate disposizioni, ad esempio quelle in materia di sanzioni [4].
- *General Data Protection Regulation (GDPR):* Regolamento Generale sulla Protezione dei Dati (GDPR 2018) in vigore dal 25 Maggio 2018; esso stabilisce le nuove regole per trattare i Dati Personali all'interno della Comunità Europea e disciplinare l'esportazione dei Dati Personali al di fuori dei confini UE. Nel nuovo Regolamento GDPR/18 si definisce "Dato Personale" qualunque informazione relativa a un individuo, collegata alla sua vita sia privata, sia professionale che pubblica, come nomi, foto, indirizzi email, dettagli bancari, interventi su siti web di social network, informazioni mediche o indirizzi IP di computer. La direttiva 2018 è applicata a partire dal 25 Maggio 2018, data in cui le imprese e le Pubbliche Amministrazioni hanno il dovere di mettersi in regola. Il nuovo Regolamento per la Protezione dei Dati definisce i requisiti per il rispetto del Codice della Privacy. I diritti degli interessati devono essere gestibili in qualunque fase del ciclo di trattamento dei Dati Personali su Internet e nei sistemi informatici; tali diritti sono il Diritto alla Cancellazione del Dato Personale, il Diritto all'Oblio del Dato Personale sui motori di ricerca su Internet, e il Diretto al Blocco del Trattamento del Dato Personale [1].

Questi sono solo due regolamenti governativi a cui le aziende appartenenti all'Unione Europea devono sottostare.

Per molte aziende italiane rendersi conformi a queste normative e dimostrarlo formalmente non è semplice; il Security Operation Center si prende carico di questa responsabilità e lascia libera l'azienda di non preoccuparsi di multe o penalizzazioni.

2.3 Processi interni ad un Security Operation Center

Come già detto in precedenza, per motivi di privacy aziendali, non verranno descritti dettagliatamente i processi interni del Security Operation Center in cui è stato svolto il tirocinio, ma verrà descritta la base di partenza di tutti i team di risposta.

L'obiettivo degli attacchi è sempre rappresentato dalle informazioni, che possono essere relative ai clienti di un'organizzazione o a dei processi industriali. Una volta ottenute le informazioni, il malintenzionato può rivenderle al miglior offerente, oppure può usarle per ricattare la stessa azienda a cui sono state sottratte.

L'organizzazione di un'efficace capacità di risposta agli attacchi informatici comporta diverse decisioni e azioni importanti. L'organizzazione deve decidere quali strumenti e servizi mettere a disposizione del team di risposta agli incidenti.

Il piano di risposta agli incidenti, la politica e la creazione di procedure è una parte importante, in modo che la risposta sia eseguita in modo efficace, efficiente e coerente e che il team sia in grado di fare ciò che deve essere fatto.

Il piano, le politiche e le procedure devono riflettere le interazioni del team con altri team all'interno dell'organizzazione.

Gli attacchi compromettono, spesso, i dati personali e aziendali, ed è fondamentale rispondere ad essi con la massima tempestività. Il concetto di risposta agli incidenti in materia di sicurezza informatica è diventato ampiamente accettato e implementato.

Uno dei vantaggi di avere una capacità di risposta agli incidenti è che essa sostiene la risposta sistematica agli incidenti in modo che siano adottate le azioni appropriate. La risposta agli incidenti aiuta il personale a ridurre al minimo la perdita o il furto di informazioni e l'interruzione dei servizi a causa di incidenti.

Un altro vantaggio della risposta agli incidenti è la capacità di utilizzare le informazioni acquisite durante la gestione degli stessi per prepararsi meglio ad una futura gestione di incidenti simili e per garantire una maggiore protezione dei sistemi e dei dati. Una capacità di risposta agli incidenti aiuta anche ad affrontare adeguatamente le questioni legali che possono sorgere durante gli stessi.

Le organizzazioni dovrebbero avere un approccio formale, mirato e coordinato per rispondere agli incidenti, compreso un piano di risposta che fornisca la tabella di marcia per l'implementazione della capacità di risposta.

Ogni organizzazione ha bisogno di un piano che soddisfi i suoi requisiti specifici; tale piano deve riguardare la missione, le dimensioni, la struttura e le funzioni dell'organizzazione. Esso dovrebbe prevedere le risorse necessarie e il supporto gestionale. Il processo di risposta agli incidenti, come si può vedere in Figura 2.3, si articola in diverse fasi, di natura sia sequenziale che ciclica.

2.3.1 Preparazione

La fase iniziale prevede l'istituzione e la formazione di un team di risposta e l'acquisizione degli strumenti e delle risorse necessarie.

Durante la preparazione, l'organizzazione cerca anche di limitare il numero di incidenti che si verificheranno selezionando e implementando una serie di controlli basati sui risultati delle valutazioni dei rischi.

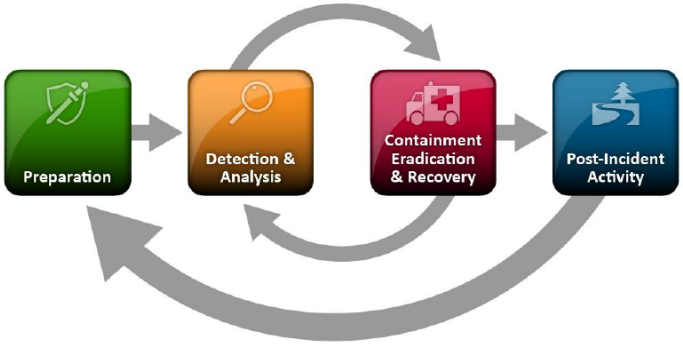

Figura 2.3. Gestione di un incidente informatico

Tuttavia, il rischio residuo persisterà inevitabilmente dopo l'attuazione dei controlli. Per tale ragione è necessario, comunque prepararsi a gestire gli incidenti; per esempio, un'organizzazione deve avere più meccanismi di comunicazione e di coordinamento in caso di fallimento di uno di questi. Mantenere il numero di incidenti ragionevolmente basso è molto importante per proteggere i processi aziendali dell'organizzazione.

Se i controlli di sicurezza sono insufficienti, possono verificarsi volumi più elevati di incidenti, che possono travolgere il team di risposta agli stessi. Questo può portare a risposte lente e incomplete, che si traducono in un maggiore impatto negativo sul business dell'organizzazione.

2.3.2 Rivelazione e analisi

Gli incidenti possono verificarsi in innumerevoli modi, per cui non è possibile sviluppare istruzioni passo dopo passo per la gestione di ogni tipologia di incidente.

Le organizzazioni dovrebbero essere generalmente preparate a gestire qualsiasi incidente; in particolare, dovrebbero essere pronte a gestire gli incidenti che utilizzano vettori di attacco comuni.

Diversi tipi di incidenti meritano strategie di risposta diverse. Per molte organizzazioni, la parte più impegnativa del processo di risposta agli incidenti consiste nel rilevare e valutare accuratamente i possibili incidenti, determinando se un incidente si è verificato e, in caso affermativo, il tipo, l'estensione e l'entità del problema.

L'individuazione e l'analisi degli incidenti sarebbe facile se si garantisse la precisione di ogni indicatore degli attacchi; purtroppo non è così. I sistemi di rilevamento delle intrusioni possono produrre falsi positivi.

Il team di risposta agli incidenti dovrebbe lavorare rapidamente per analizzare e convalidare ogni incidente, seguendo un processo predefinito e documentando ogni passo compiuto.

Quando il team ritiene che si sia verificato un incidente, deve eseguire rapidamente un'analisi iniziale per determinare la sua portata. L'analisi iniziale dovrebbe fornire informazioni sufficienti per consentire al team di dare priorità alle attività successive, come il contenimento dell'incidente e un'analisi più approfondita degli effetti di quest'ultimo.

2.3.3 Contenimento e recupero

Il contenimento è importante prima che un incidente travolga le risorse o aumenti i danni.

La maggior parte degli incidenti richiede il contenimento, per cui è una considerazione importante nelle prime fasi della gestione di ogni incidente. Il contenimento fornisce il tempo per sviluppare una strategia di riparazione su misura.

Una parte essenziale del contenimento è il processo decisionale (ad esempio, spegnere un sistema, scollegarlo da una rete, disabilitare alcune funzioni). Tali decisioni sono molto più facili da prendere se esistono strategie e procedure predeterminate per contenere l'incidente. Le organizzazioni dovrebbero definire rischi accettabili nel gestire gli incidenti e sviluppare strategie di conseguenza.

Dopo che un incidente è stato contenuto, può essere necessario sradicarlo per eliminare i componenti dell'incidente, come l'eliminazione del malware e la disabilitazione degli account utente violati, nonché l'identificazione e l'attenuazione di tutte le vulnerabilità che sono state sfruttate.

Durante l'eradicazione, è importante identificare tutti gli host interessati all'interno dell'organizzazione in modo che possano essere corretti. L'individuazione di violazioni della sicurezza è quindi necessaria per allertare l'organizzazione.

In linea con la gravità dell'incidente, l'organizzazione può mitigare l'impatto dell'incidente contenendolo e, in ultima analisi, recuperandolo.

Durante questa fase, l'attività ritorna spesso al rilevamento e all'analisi, ad esempio per vedere se altri host sono infettati dal malware mentre sradicano un evento malware.

2.3.4 Attività post-incident

Una delle parti più importanti della risposta agli incidenti è l'apprendimento e il miglioramento. Ogni team di risposta agli incidenti dovrebbe evolvere per affrontare le nuove minacce e migliorare la tecnologia.

Dopo che si sono verificati attacchi gravi, di solito vale la pena di tenere riunioni post-mortem che attraversano i confini del team e dell'organizzazione per fornire un meccanismo di condivisione delle informazioni.

La considerazione principale nello svolgimento di tali riunioni è garantire che siano coinvolte le persone giuste. Non solo è importante invitare persone che sono state coinvolte nell'incidente analizzato, ma è anche saggio considerare chi dovrebbe essere invitato al fine di facilitare la cooperazione futura.

Dopo che l'incidente è stato adeguatamente gestito, l'organizzazione pubblica un rapporto che descrive in dettaglio la causa e il costo dell'incidente e le misure che l'organizzazione dovrebbe adottare per prevenire futuri incidenti.

L'aggiornamento delle politiche e delle procedure di risposta agli incidenti è un'altra parte importante del processo di apprendimento. Le lezioni apprese durante le riunioni offrono altri vantaggi.

I resoconti di queste riunioni sono un buon materiale per la formazione dei nuovi membri del team, mostrando loro come i membri del team più esperti hanno risposto agli incidenti passati.

3

Il Security Operation Center

Nella prima parte di questo capitolo verranno descritte le componenti e le fasi funzionali del Security Operation Center di Cybertech. Nella seconda parte verrà descritto come il SOC è suddiviso gerarchicamente in responsabilità, alla fine verrà descritto come orchestrare tutto il SOC, integrando le tre componenti relative alle Persone, ai Processi e alle Tecnologie.

3.1 Componenti e fasi operative di un SOC

Le attività connesse alla presente tesi fanno riferimento al Security Operation Center (SOC) di Cybertech, presente a Roma. L'obiettivo è stato quello di comprendere le analisi che venivano effettuate, imparare le tecnologie utilizzate, individuare eventuali processi ripetitivi degli analisti così da automatizzarli per ottimizzare i tempi di analisi e di risposta di un incidente informatico.

Il SOC è un team organizzato e altamente qualificato, la cui missione è quella di monitorare e migliorare continuamente la posizione di sicurezza di un'organizzazione, prevenendo, analizzando e rispondendo agli incidenti di sicurezza informatica, con l'aiuto sia della tecnologia che di processi e procedure ben definiti.

Ci sono dei principi chiave su cui è basata la sicurezza dei dati. Senza una profonda comprensione di tali concetti e di come essi siano correlati all'ambiente in cui opera un'organizzazione, non si sarà in grado di definire in modo accurato i bisogni informativi di un programma di sicurezza.

CIA è l'acronimo di Confidentiality, Integrity e Availability, (Figura 3.1). Lo scopo di un programma di sicurezza e dei corrispettivi membri che se ne occupano, è quello di proteggere la riservatezza, l'integrità e la disponibilità degli asset informativi di maggiore valore di un'organizzazione.

Il SOC gestisce gli incidenti di sicurezza e coordina la risposta a cyber-attacchi esterni ed interni, al fine di garantire la triade CIA dei dati dei suoi clienti. Vedremo più in dettaglio il significato dei tre termini che compongono la triade.

- *Integrità:* sicurezza che i dati non possano impropriamente essere modificati o distrutti. Proteggere l'integrità delle informazioni richiede che queste ultime non

possano essere, e non sono state, modificate in modo inappropriato. La protezione dell'integrità delle informazioni non permette delle modifiche inappropriate dei dati. La validazione dell'integrità verifica che i dati non siano stati modificati.

- *Riservatezza:* sicurezza che il dato non venga visto da terze parti non autorizzate. Equivale a dire, essere sicuri che i segreti rimangono tali. Il modo più comune di mantenere riservate le informazioni consiste nell'utilizzo di forti controlli sugli accessi, ad esempio utilizzando la crittografia.
- *Disponibilità:* sicurezza che gli utenti autorizzati possano accedere ai dati quando ne hanno bisogno. Se nessuno può accedere ad un'informazione , naturalmente quell'informazione è sicura da qualsiasi attacco, ma è anche assolutamente inutile. Assicurarsi che le informazioni critiche siano accessibili quando è necessario rappresenta l'obiettivo della Disponibilità. Ci sono molti modi per mantenere la disponibilità , ad esempio utilizzando sistemi ridondanti.

Figura 3.1. La triade CIA dei dati

Massimizzare tutte e tre questi principi è un'utopia perchè, nel loro insieme, è come se si operasse su una coperta; se si tira troppo da una parte l'altro lato rimarrà scoperto, quindi bisogna considerare le esigenze delle organizzazioni ed adattare i principi in base a queste.

Il SOC è composto da quattro macro componenti e fasi operative distinte, (Figura 3.2). Questi sono:

1. *Sorgenti degli eventi:* possiamo distinguere due famiglie principali di sorgenti di eventi: i generatori di dati basati sugli eventi (ad esempio i firewall), che generano eventi in base alle applicazioni o alle reti e le sorgenti di dati basate sullo stato delle macchine, che generano un evento in base alla reazione ad

uno stimolo esterno, ad esempio il ping, il controllo dell'integrità dei dati o il controllo dello stato dei demoni.

2. *Raccolta e correlazione degli eventi:* durante questa fase vengono raccolte informazioni da sensori diversi e vengono tradotte in un formato standard, in modo da avere una base omogenea di messaggi. Utilizzando algoritmi di correlazione, si cerca di individuare attacchi informatici e ridurre al minimo il numero di falsi positivi.
3. *Analisi e risposta:* partendo da una forte conoscenza degli analisti si cerca di capire se si è in presenza di un attacco. In particolare, viene definito l'insieme degli strumenti di reazione e di segnalazione per reagire agli eventi illeciti, che si verificano sui sistemi supervisionati. Se si è in presenza di un attacco si risponde il più velocemente possibile.
4. *Reportistica e presentazione dei risultati:* la fase di reportistica è fondamentale per dimostrare il lavoro che si sta facendo, rispettando gli accordi presi con il cliente. Il report è uno strumento di comunicazione tra il SOC ed il Cliente.

Queste fasi verranno trattate più approfonditamente nel seguito.

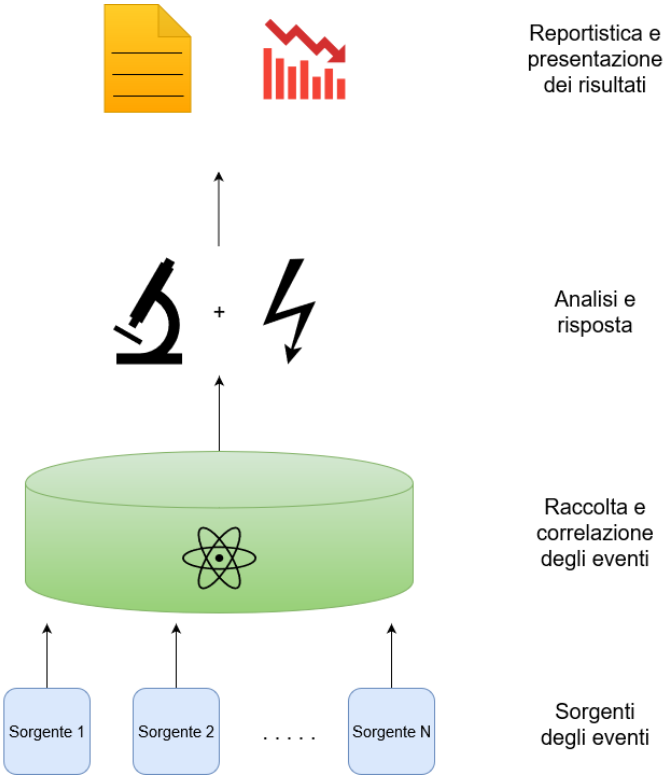

Figura 3.2. Fasi e componenti operazionali del SOC

3.1.1 Sorgenti degli eventi

Ogni azienda ha nella sua rete installati molti firewall. Quest'ultimo è un sistema di sicurezza di rete che monitora e controlla il traffico in entrata e in uscita sulla base di regole di sicurezza predeterminate.

Esso stabilisce una barriera tra una rete interna fidata e una rete esterna non fidata, nonchè una o più barriere nella rete interna (Figura 3.3). Ci sono diverse tipologie di firewall:

- *Intrusion Detection System (IDS):* è un sistema di rilevamento e monitoraggio. Esso non interviene da solo, ma richiede il coinvolgimento di una persona o di un altro sistema per esaminare i risultati e decidere le azioni da intraprendere.
- *Intrusion Prevention System (IPS)*, mentre gli IDS sono sistemi di monitoraggio, gli IPS sono sistemi di controllo. Essi catturano e bloccano pacchetti potenzialmente pericolosi, richiedendo che i database, dei malware conosciuti, siano regolarmente aggiornati.

Il traffico di un'azienda passa tutto attraverso i firewall. Questi ultimi possono essere classificati anche in *perimetrali*, se si frappongo tra la rete esterna e quella interna, e i *interni*, per capire se viene effettuato del traffico sospetto internamente all'azienda.

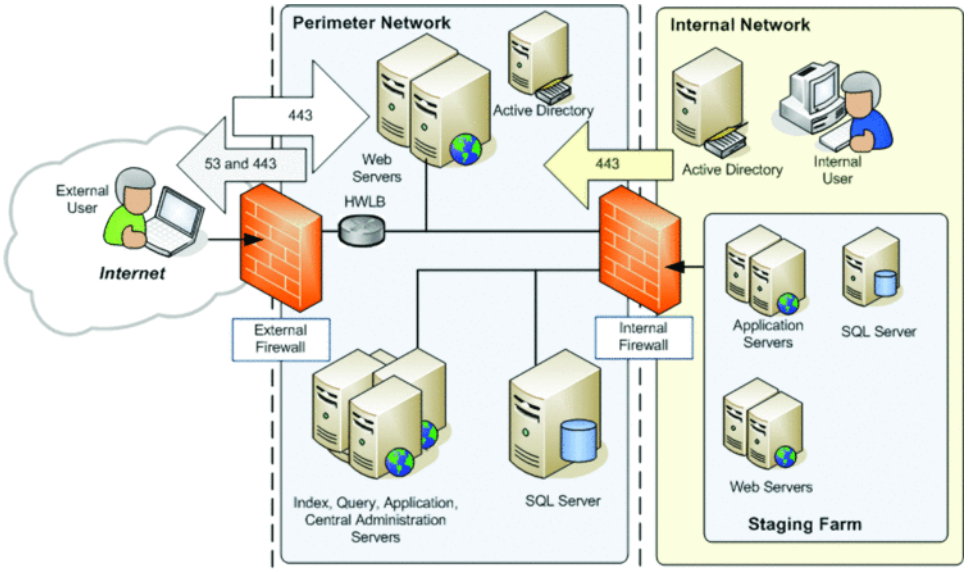

Figura 3.3. Schema di esempio di installazione di più firewall

Il formato standard per il salvataggio dei log di rete e di sistema è sysolog. Questo è uno standard per la registrazione dei messaggi, ogni messaggio contiene molte informazioni. I campi più significativi di un log sono:

- *Data ora:* momento in cui è stato generato il traffico.

- *Sorgente:* tipologia di firewall che ha rilevato il traffico.
- *Device_id:* id univoco del dispositivo per poter, così, risalire al punto a partire da cui è stato generato il traffico.
- *Type:* nome identificativo dell'azione effettuata dal dispositivo, ad esempio firewall permit o firewall drop.
- *Ip_sorgente:* è l'indirizzo IP da cui il traffico è stato generato.
- *Ip_destinazione:* è l'indirizzo IP verso cui il traffico è diretto.

Ogni riga di un log contiene questi ed altri campi riguardanti il traffico generato, in un secondo i firewall inviano circa 1000 righe con questi campi e inviano dati a tutte le ore a tutti i giorni.

I firewall non sono le uniche sorgenti di informazioni, ma ne esistono anche altre. Altri generatori di eventi possono essere i Domain Controller (DC) dei server Windows. Un DC è un server che risponde alle richieste di autenticazione di sicurezza all'interno di un dominio informatico; quindi grazie ad esso, possono essere controllati i vari login effettuati nelle macchine durante il giorno. Vengono salvati tutti i tipi di login, sia quelli che hanno avuto successo sia quelli che non lo hanno avuto; questi i login che non hanno avuto successo potrebbero essere segnali di un tentativo di attacco.

Un'altra sorgente di informazione sono i server e-mail; questi sono i distributori di e-mail dell'azienda e tutte le e-mail in entrata o in uscita passano attraverso di essi.

Ad esempio se siamo in presenza di un possibile attacco di phishing, l'e-mail passa attraverso il server; quindi è possibile leggere tutto il contenuto per capire se è malevola oppure no. Il server e-mail ha la funzione di essere un filtro per il flusso di tutte le email.

Il problema sorge nella gestione di questo flusso continuo di informazioni. Esse vengono gestite dal collettore di eventi.

3.1.2 Raccolta e correlazione degli eventi

Come è stato detto nella sezione precedente, le informazioni da gestire sono molte e vengono generate continuamente ogni giorno. Tutte le informazioni generate dalle sorgenti sono importanti perchè potrebbero aiutare a comprendere se è in corso un attacco informatico, quando ha avuto inizio e da quale sorgente è partito. Quindi non si possono perdere informazioni relative al traffico avvenuto.

Per gestire una quantità di dati significativa, in arrivo sotto forma di log di eventi dai sistemi, viene utilizzato un sistema di Security Information and Event Management (SIEM). Un SIEM agisce come un repository centrale di log generati dai sistemi e consente ad un esperto, attraverso delle regole logiche che egli può determinare, di monitorare specifici eventi di interesse. Le principali operazioni svolte dai collettori sono la ricezione di messaggi grezzi, attraverso diversi protocolli e diverse formattazioni provenienti dalle diverse sorgenti. Una volta formattatto, il messaggio viene memorizzato in un database di eventi.

Un SIEM ha diverse funzionalità che possono essere d'aiuto per un utente. Esso riesce a gestire tutti i log ricevuti dalle varie sorgenti, effettuare il loro parsing ed organizzarli per renderli facilmente reperibili. Esso, inoltre, memorizza tutto quello

che arriva in un database storico sempre accessibile. Il SIEM è stato implementato in primo luogo in risposta ai requisiti di conformità governativi, di cui si è già parlato.

Per migliorare la qualità di un'analisi e per ridurre lo sforzo di dover analizzare tutto il traffico vengono studiate ed implementate delle regole di correlazione.

Lo scopo di tali regole è quello di analizzare sequenze di informazioni complesse e produrre eventi semplici, sintetizzati e precisi. Trovare le squenze di pattern matching è l'operazione più comune usata per generare regole di correlazione. Il suo scopo è quello di identificare una sequenza di messaggi che sarebbe caratteristica di un tentativo di intrusione.

3.1.3 Analisi e risposta

Da una locazione centralizzata, come il collettore di eventi è possibile, vedere informazioni da una grande varietà di dispositivi e collegare eventi provenienti da dispositivi multipli e che potrebbero indicare un attacco alla rete.

Su tutte le informazioni raccolte dai SIEM vengono efettuate delle analisi per capire se un traffico è malevolo oppure no.

Oltre a delle sequenze di eventi viene considerato il tempo in cui questi ultimi compaiono. Quindi si analizza un comportamento malevolo, lo si considera come modello e si esaminano le sequenze di dati trasmesse per vedere se una di questi coincide con quella malevola.

Il SIEM effettua un monitoraggio in tempo reale, correlando i vari eventi ricevuti e mostra tutto il traffico in dashboard interrogabili dagli analisti.

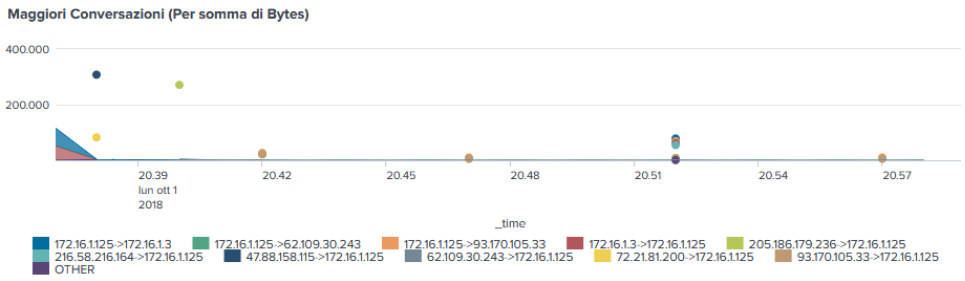

Figura 3.4. Esempio di una dashboard di analisi delle conversazioni tra IP

Un'altra funzione di un SIEM, che viene in aiuto agli analisti, è quella di visualizzazione del traffico tramite dashboard; in questo modo, gli analisti hanno uno strumento grafico di facile interpretazione per effettuare delle analisi più velocemente.

Un esempio di una dashboard viene mostrato in Figura 3.4. In essa vengono evidenziate le somme di tutti bytes trasmessi in ogni singola conversazione tra due indirizzi IP.

Gli attacchi compromettono spesso i dati personali e aziendali, ed è fondamentale rispondere in modo rapido ed efficace quando si verificano violazioni della sicurezza.

Il concetto di risposta agli incidenti di sicurezza informatica è diventato ampiamente accettato e implementato. Uno dei vantaggi di disporre di una capacità

di reazione agli incidenti è che questa ultima supporta la risposta sistematica agli incidenti, seguendo una metodologia coerente di gestione degli stessi, in modo che siano adottate le azioni appropriate. La risposta agli incidenti aiuta il personale a ridurre al minimo la perdita o il furto di informazioni e l'interruzione dei servizi causati dagli incidenti.

Un altro vantaggio della risposta agli incidenti è la capacità di utilizzare le informazioni acquisite durante la gestione degli incidenti per prepararsi meglio a gestire gli incidenti futuri e fornire una maggiore protezione dei sistemi e dei dati. Una capacità di risposta agli incidenti aiuta, anche, a gestire correttamente le questioni legali che possono sorgere durante questi ultimi [7].

L'individuazione e l'analisi degli incidenti sarebbe facile se si garantisse la precisione di ogni regola di correlazione o se la lista dei pattern matching ricoprisse ogni comportamento malevolo; purtroppo non è così. Si presenta, anche, il problema opposto, ovvero che le sequenze non malevole facciano scattare dei pattern match malevoli facendo, quindi, generare dei falsi positivi.

3.1.4 Reportistica e presentazione dei risultati

Una volta effettuata e conclusa l'analisi e una volta terminata la risposta per contrastare l'incidente avvenuto, viene stilato un report riguardante tutte le azioni intraprese dal Security Operation Center. Con il report il SOC motiva tutte le azioni intraprese riguardanti l'attacco, motiva le analisi effettuate e cerca di spiegare al cliente che ha subito l'attacco come quest'ultimo è stato rilevato e, di conseguenza, cosa è stato fatto per contenerlo ed eradicarlo.

Effettuare i report ha due finalità; da una parte essi servono a garantire che chi fornisce il servizio SOC lo ha fatto in maniera giusta. I SOC servono anche, per illustrare come sono stati gestiti, analizzati e chiusi gli incidenti informatici.D'altra parte essi servono ai clienti per dimostrare che stanno rispettando i regolamenti governativi. Quindi il report è un mezzo di comunicazione tra il SOC ed i vari clienti.

All'interno del report vengono anche presentati i Key Performance Indicators (KPI), che sono degli indicatori di performance del SOC. Un esempio dei KPI sono:

- *Tempo medio tra l'apertura e la chiusura di un incidente*
- *Numero di offenses aperte*
- *Regole con falsi positivi*
- *Percentuali di incidenti ricorrenti*

I KPI servono per valutare il servizio di un SOC. Infatti quando un cliente sceglie il servizio di un Security Operations Center, vengono stabiliti dei Service Level Agreement (SLAs) in base ai KPI scelti dal cliente.

Data l'eterogeneità dei clienti che richiedono il servizio SOC, gli SLAs cambiano da cliente a cliente, ad esempio alcuni clienti esigono un tempo medio dall'apertura alla chiusura di un incidente.

3.2 Stratificazione interna del SOC Cybertech

Gli analisti sono i protagonisti del Security Operation Center; essi sono qualificati sui principali argomenti relativi alla Cybersecurity. Gli analisti possiedono nozioni sui protocolli di rete, sulla web exploitation e sugli exploit. Si aggiornano continuamente sui nuovi attacchi informatici avvenuti nel mondo, prevedendo una possibile soluzione se uno di questi attacchi arrivasse ai propri clienti.

Le attività di un SOC si svolgono 24 ore al giorno e 7 giorni su 7. Ad ogni analista durante il proprio turno vengono assegnati più clienti contemporaneamente, quindi diverse esigenze, diverse policy di risposta ad un possibile attacco, un perimentro maggiore da controllare anche fuori dalla propria nazione. I SOC nelle principali organizzazioni sono stratificati, come si può vedere dalla Figura 3.5. In particolare è possibile individuare i seguenti tre livelli:

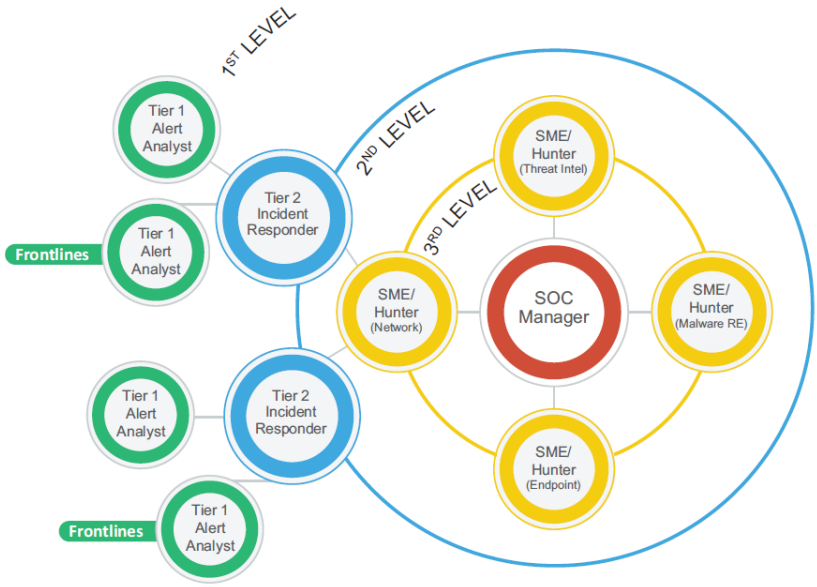

Figura 3.5. Stratificazione in livelli di responsabilità del SOC

- *Primo livello:* durante questa fase arrivano tutte le sequenze di pattern matching, con behaviour malevolo, generate dai SIEM. A seguito di ciò viene effettuata una prima analisi veloce; coloro che fanno parte del primo livello hanno come obiettivo quello di eliminare il più possibile i falsi positivi che sono scattati, cercando di scalare al secondo livello soltanto quelle minacce che hanno bisogno di un'analisi più approfondita. Infatti, questo livello ha come scopo quello di capire la presenza di traffico malevolo oppure no. Quindi, se risulta un falso positvo viene chiuso l'incidente in questo livello, altrimenti si procede a scalare al secondo livello.

- *Secondo livello:* quando una minaccia passa dal primo livello al secondo significa che è stato individuato qualcosa o che gli analisti del primo livello hanno rilevato qualcosa di sospetto, ma non sono sicuri. A questo punto viene efettuata un'analisi più approfondita riguardante il traffico avvenuto al momento del rilevamento, ma anche a giorni o a settimane prima dell'incidente, così da capire quando l'attacco ha avuto inizio. Se il risultato dell'analisi non ha riscontrato alcuna azione malevola, l'incidente viene chiuso; se, invece, è stato rilevato qualcosa di dannoso, si cerca di rispondere immediatamente e di ridurre il danno per ritornare in uno stato sicuro. A tal fine viene effettua un'analisi più profonda correlando, anche, dati provenienti da fonti diverse, per capire se un sistema critico è stato impattato nell'attacco e, in caso affermativo, per cercare di fornire delle indicazioni per porvi rimedio.
- *Terzo livello:* i membri di questo livello hanno una profonda conoscenza riguardanti le reti, gli endpoint di threat intelligence, analisi forense e malware reverse. Essi conoscono come sono strutturate gerarchicamente le organizzazioni e come sono le loro infrastrutture IT. Quando arriva un incidente, essi non aspettano per scalare, ma agiscono immediatamente perchè siamo già ad un livello critico. Il terzo livello viene coinvolto nello sviluppo, nella personalizzazione e nell'implementazione di rilevamento analitico delle mincacce.
- *SOC Manager:* egli gestisce le risorse, incluso il personale e il budget, e sceglie le strategie e le tecnologie per soddisfare i Service Level Agreements di ogni organizzazione che affida la propria sicurezza al SOC.

3.3 Orchestrazione tra persone, processi e tool

In questo capitolo abbiamo descritto la struttura generale di un Security Operation Center. Il SOC di Cybertech ha delle caratteristiche aggiuntive, in quanto è distribuito ed eterogeneo. Avendo sedi sparse in Europa si può definire come SOC distribuito; avendo in carico dei clienti operanti in settori produttivi diversi, esso è anche eterogeneo.

Avendo diverse tipologie di clienti, il SOC ha anche diverse metodologie di gestione. Di seguito si riportano degli esempi di gestione in base ai settori dei clienti:

- *Assicurativo:* per questa tipologia di cliente, la gestione viene effettuata 24 ore su 24 e 7 giorni su 7. I livelli 1, 2 e 3 ed il SOC Manager sono tutti interni nella sede a Roma.
- *Servizi:* tutti i livelli sono interni nella sede a Roma il servizio viene erogato 24 ore su 24 e 7 giorni su 7.
- *Trasporto Navale:* il livello 1 è situato nella sede in Svizzera, mentre i livelli 2 e 3 ed il SOC Manager sono situati nella sede a Roma.
- *Automobilistico:* questo settore ha richiesto soltanto il monitoraggio del livello 1, nella fascia oraria 20.00 - 08.00.

Nell'ambito della sicurezza informatica la velocità è un fattore importantissimo. Per aumentare la velocità di risposta serve un orchestratore tra le persone appartenenti al SOC, i processi di sicurezza e le tecnologie utilizzate. Tale orchestratore è il Security Orchestration, Automation and Response (SOAR).

Come si può vedere dalla Figura 3.6, il SOAR è l'insieme di tre funzioni, ovvero il Security Orchestration and Automation (SOA), il Security Incident Response Plattform (SIR) e il Threat Intelligence Platform (TIP).

Figura 3.6. Insieme di funzioni di un SOAR

Il SOAR ha numerosi benefici che consentono ai security analyst di guadagnare tempo rispetto ai task ripetitivi per focalizzarsi sull'analisi e la mitigazione delle minacce più sofisticate.

Un SOAR si focalizza nel consentire alle tecnologie di sicurezza, presenti in un determinato ambiente, di lavorare insieme, in maniera armonizzata e il più possibile automatizzata. Esso permette di connettere vari sistemi di sicurezza, consolidando vari workflow, anche complessi.

Uno dei primi valori tangibili di un SOAR consiste nell'avere una visibilità consolidata degli eventi e sull'automatizzare le sequenze di risposta. L'automazione, quindi, è in grado di eseguire numerosi processi e workflow senza richiedere l'intervento umano, tranne quando ciò è oggettivamente necessario.

Il beneficio più visibile del SOAR consiste nella sua abilità ad integrarsi virtualmente con ogni processo di sicurezza o strumento in uso in azienda, aumentandone performance e valore aggiunto. Unificare ed orchestrare gli strumenti di sicurezza, piuttosto che averli in silos separati è quindi, un valore inestimabile.

Un'altra funzione fondamentale del SOAR è quella di riuscire a concentrare in un unico punto tutte le informazioni, relativamente ad ogni singolo attacco, raccolte da fonti esterne, le cosiddette threat source. Raccogliendo in un singolo punto tutte le informazioni, gli analisti riescono ad effettuare un'analisi più veloce, invece di andare a cercare le informazioni ogni volta che si presenta un incidente informatico.

Il SOAR facilita, anche, la comunicazione tra gli analisti ed i clienti, con delle dashboard interrogabili e configurabili in base alle esigenze di ciuscuno di essi.

Fondamentalmente il SOAR ha come obiettivo quello di orchestrare i tre fattori principali di un Security Operation Center, (Figura 3.7), ovvero:

- *Le persone:* come è già stato detto ci sono molte persone che lavorano internamente al SOC con diverse responsabilità. Ci sono, anche, persone di diverse nazioni che collaborano.
- *I processi:* ogni cliente può richiedere diversi processi, e diversi workflow con cui risolvere un incidente.
- *Le tecnologie:* è necessario orchestrare tutte le tecnologie di threat source, di risposta e di visualizzazione grafica.

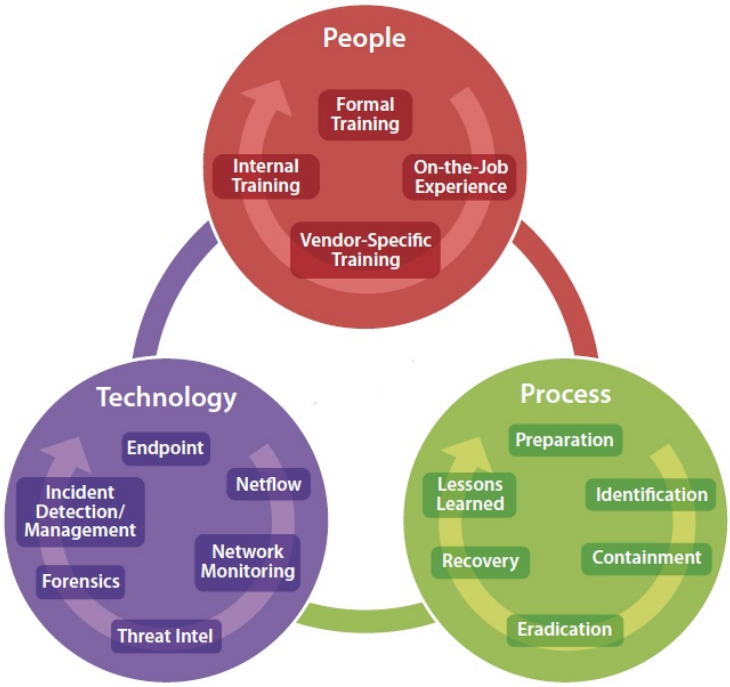

Figura 3.7. Collaborazione tra persone, processi e tecnologie

4

Tecnologie adottate in un contesto applicativo reale

Nella prima parte di questo capitolo verrà descritto il funzionamento del SIEM IBM QRadar e come questo viene utilizzato in un campo applicativo reale. Nella seconda parte verranno descritte le threat intelligence usufruite e come vengono adoperate in un contesto aziendale.

4.1 Tecnologia di monitoraggio, IBM QRadar

Il SIEM utilizzato dal SOC di Cybertech è IBM QRadar. Nello studio pubblicato nel 2018 da Gartner Magic Quadrant (MQ) sui SIEM, IBM QRadar è stato riconosciuto come leader. Nel report, Gartner ha collocato IBM QRadar tra gli esponenti di punta per la migliore "completezza di visione".

Come si può vedere dalla Figura 4.1, QRadar è suddiviso in tre strati software:

1. *Event collector*
2. *Event processor*
3. *Console*

Questi verranno esaminati in dettaglio nelle prossime sottosezioni.

4.1.1 Event collector

Lo strato software dell'event collector ha la funzione di raccogliere i dati provenienti da sorgenti eterogenee, come server Windows, server Unix, firewall e server proxy. Quando i dati grezzi entrano nell'event collector, vengono normalizzati per essere presentati in un formato strutturato ed utilizzabile.

I dati rappresentano gli eventi che si verificano in un momento specifico nel tempo e nell'ambiente dell'utente; essi comprendono, ad esempio i login degli utenti, le e-mail, le connessioni VPN, i firewall denys e le connessioni proxy.

Altri dati importanti sono le attività di rete o le informazioni relative ad una sessione tra due host. QRadar traduce e normalizza i dati grezzi in indirizzi IP, porte, conteggio dei byte e altre informazioni che rappresentano, effettivamente, una sessione.

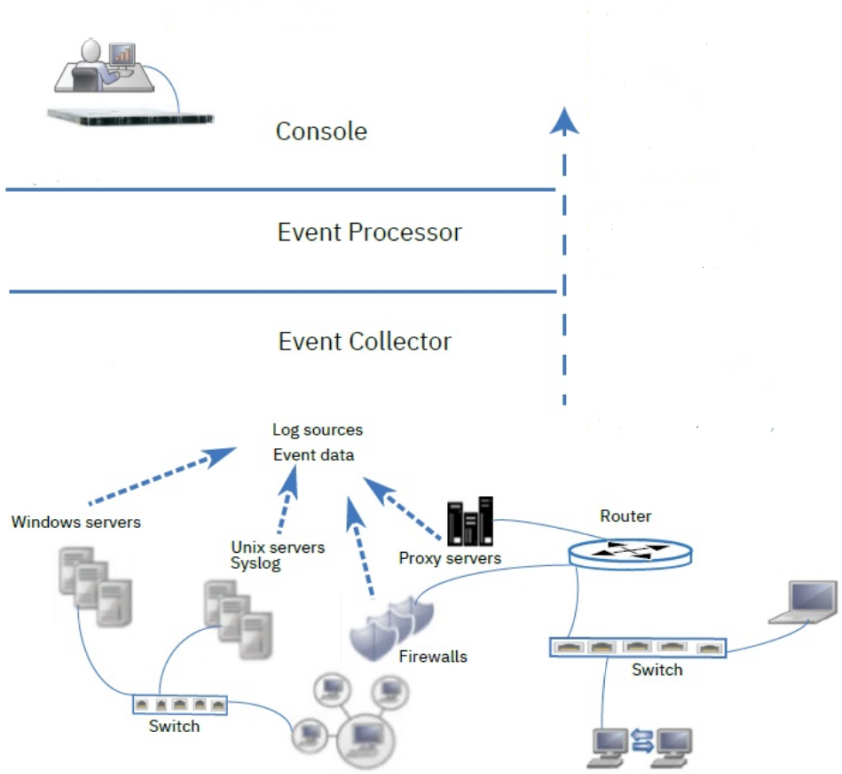

Figura 4.1. Schema delle componenti software di QRadar

Nella Figura 4.2 vengono mostrate le form da dover compilare per inserire una nuova sorgente di log. I campi più significativi, durante l'inserimento, sono la sua tipologia e il protocollo di configurazione (quest'ultimo permette a QRadar di interpretare le informazioni in arrivo), e l'event collector, che stabilisce dove vengono salvate le informazioni.

Nell'esempio presentato, in Figura 4.2, viene inserita una nuova log source, relativa ad un firewall Fortigate, che invia i suoi dati in formato syslog.

Una volta configurate tutte le sorgenti di log in ingresso, è possibile monitorare in ogni momento lo Status, il Protocol, il Log Source Type, il Last Event Time e il Creation Date, come viene illustrato in Figura 4.3.

4.1.2 Event processor

Lo strato software dell'event processor è responsabile dell'elaborazione degli eventi ricevuti dall'event collector. Inoltre, esso ha il compito di confrontare gli eventi con delle regole logiche, definite dagli analisti. Queste ultime hanno lo scopo di far focalizzare l'analisi in un preciso istante e soltanto in particolari eventi.

Un esempio di una regola logica è "Host Discovery Behaviour Detected". Essa serve a comprendere se un attaccante sta effettuando una scansione della rete. La regola è composta dalle sequenti condizioni:

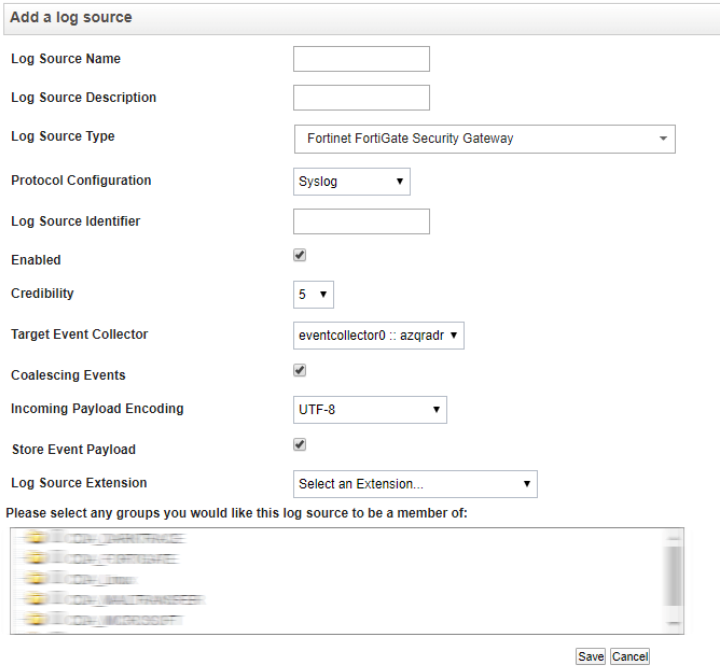

Figura 4.2. Campi disponibili per l'aggiunta di una nuova sorgente di log

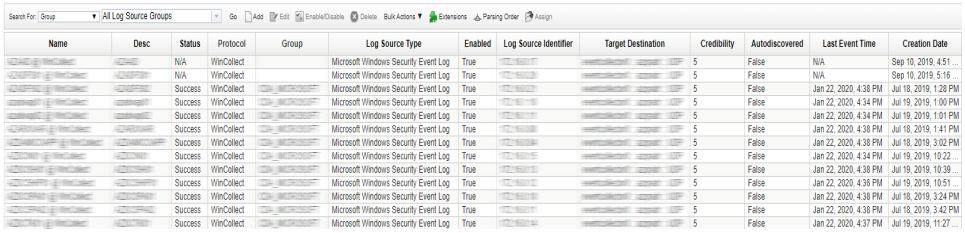

Figura 4.3. Lista di tutte le sorgenti di log presenti in un caso reale

- quando l'Internet Protocol utilizzato è ICMP
- AND NOT il source IP è uno degli hosts monitorati
- AND almeno 20 eventi sono stati generati dallo stesso source IP verso un differente IP di destinazione, in un minuto.

Quando un evento rende vere tutte le condizioni di una regola, l'event processor genera un oggetto, chiamato offense.

Le offenses, al loro interno, hanno tutti gli eventi che fanno scattare una specifica regola logica, di conseguenza gli analisti non devono analizzare tutto il traffico, ma soltanto la porzione di tempo che ha fatto generare quella offense.

Prima di creare una regola logica, è necessario comprendere le conseguenze della sua creazione. Se una regola è troppo generale, essa genererà un numero elevatissimo di offense; di conseguenza si caricherebbero di lavoro gli analisti. Se, invece, è troppo

dettagliata, c'è la possibilità opposta, cioè di non far generare alcuna offense, anche se si è in presenza di traffico malevolo.

Un'altra regola è stata creata a seguito della diffusione del malware Emotet. Emotet è un trojan bancario, avanzato e modulare, che ruba le credenziali dei conti bancari delle vittime ed ha la funzionalità di downloader o dropper di altri trojan bancari. La diffusione di Emotet è in continua ascesa; esso viene considerato tra i malware più gravosi, che tendono a colpire i settori privati e quelli pubblici. Emotet è diffuso principalmente tramite malspam; esso utilizza riferimenti familiari per indurre il destinatario all'apertura dei documenti. Le campagne più recenti imitano le ricevute di PayPal, notifiche di spedizione o fatture scadute [2].

Nella Figura 4.4, viene mostrata la regola che è stata creata a seguito della diffusione del malware Emotet.

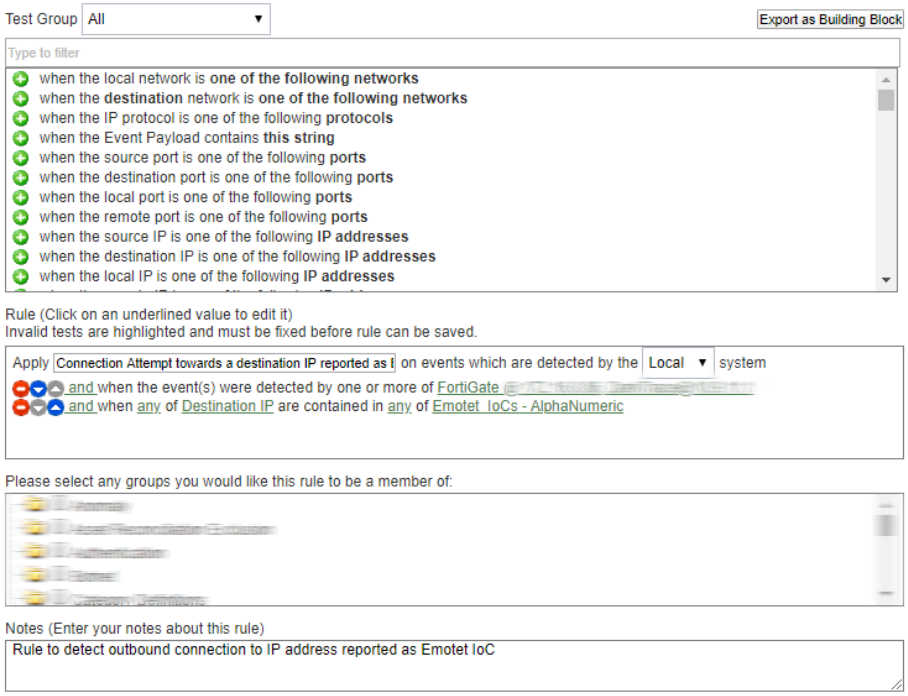

Figura 4.4. Regola creata per la rivelazione del malware Emotet

La regola afferma che, quando l'evento è stato rilevato da uno o più firewall Fortigate, e quando uno qualsiasi degli IP di destinazione è contenuto in uno qualsiasi degli Indicator of Compromise (IoC) di Emotet, viene generata una offense con tutti gli eventi interessati.

Tipici IoC sono le firme dei virus, gli indirizzi IP, gli hash MD5 dei malware, gli URL o i nomi di dominio dei server di comando e controllo delle reti bot. Prima della creazione di questa regola è stata effettuata una fase di ricerca degli IoC relativi al malware Emotet.

In Figura 4.5 vengono presentati gli IoC di Emotet, utilizzati per la creazione della regola sopra descritta.

IPv4
173.255.214.126
51.159.23.217
73.60.8.210
198.71.233.109
104.18.42.81
64.90.43.196
192.252.149.25
185.20.50.158
91.74.175.46
125.212.226.135
162.241.30.109
96.38.234.10
104.31.82.77

MD5
f28f56f627c080ad7cdda0c2850b77e7
2fb48d23aaa5778bc4e9d0b599e99439
212aa92bd1e66db81b231928086d139e
497ac1351ba086c6600d24cbee6a6c92
86c6ece219f08717fa25d2946de05d48
2ce0dc95097ac38238ce36f3ed20f8e0
5572cd455ca9d62366c6f9ec5e6ccca1
377bed4713b59afe9fa463dd25e4920d
9b49fe410a4b0deb92225e428b15376f
82bebd98b094c11c6c22bb0c9d6dcf3f
c44dec16880519ffcd8013b8c22db477
d948e40eaaedf7d7c5ae812c8d57d7fc
a8c903575ade6dd9cae81b28676bc912
ffbb2f5c28ee8869a87297c8b8c8c065
bb717c6046c06b4b5b223e785de661e8
d851bad5a6745f27e90df380f43ec26f
95b5d8598edc45306eafe64eb1d60491
41fc19e405c20ebd55d46aa60b8f4fc8
1673d0c29fe26d612d369dd41648ea7a
cb5671b4a89ef9eb776e1c73d973b5e4
cecbe1b4442be6b9030bc58b4c79b0a5
c108dd879b25603b66f0f89845c06995
a16caee4c32f81f0a23271b0d449a0b3
54c3a205fa76f533f42e11c0b993f5aa

URL
http://173.255.214.126:8080/smtzdyy1v
http://113.61.76.239/peh0r42uhichf
http://73.60.8.210/smtzdyy1v
http://73.60.8.210/0bpgbojzupwoyp
http://51.159.23.217:443/0yhw9myl
http://173.255.214.126:8080/0yhw9myl
http://hasbrew.com/includes/zw21y53110/
http://greencrosscc.com/contact-form/7c457119/
http://gunnertalk.com/wp-admin/2z07/
http://norikkon.com/administrator/qjv32/
http://baoho.zweb.xyz/wp-admin/wkeadc76/
http://91.74.175.46/sftljv5aozradcb
http://gessuofk.net/test/6ns631/
http://rampbay.com/var/r3kb2/

Dominio
rampbay.com
greencrosscc.com
gessuofk.net
gunnertalk.com
hasbrew.com
norikkon.com
baoho.zweb.xyz

Figura 4.5. Indicatori di compromissione del malware Emotet

Un altro fattore da prendere in considerazione, durante la creazione di una regola, è la sua efficenza. Il modo migliore per crearne una è limitare prima il contesto di ricerca e poi inserire condizioni logiche sempre più dettagliate, così da effettuare una ricerca più efficente.

Nella regola presentata in Figura 4.4, viene definito, come prima cosa, il contesto di ricerca; in particolare, vengono presi in considerazione solo gli eventi provenienti dalla sorgente Fortigate; successivamente viene effettuata una ricerca più specifica sugli IoC, forniti da Cert-Pa, relativi al malware Emotet.

Quando uno o più eventi verificano le condizioni della regola, viene generata una offense con il nome identificativo uguale al nome della regola che è scattata.

4.1.3 Console

Nello strato software della console, i dati raccolti ed elaborati da QRadar sono messi a disposizione degli analisti; cosicchè questi ultimi possono effettuare ricerche, analisi, segnalazioni e indagini sugli attacchi.

Tutti i dati vengono raccolti, elaborati e memorizzati su QRadar. La console viene utilizzata principalmente come interfaccia utente per gli analisti, dove possono quest'ultimi avere una visione più ampia delle reti dei clienti.

Come è stato detto nella sezione precedente, quando degli eventi fanno scattare una regola logica, viene generata una offense.

Gli analisti utilizzano la console per gestire tutte le offense, che si sono generate durante il proprio turno. Ogni volta che ne viene generata una, gli analisti devono prenderla in carico e gestirla; come prima cosa devono capire se sia un falso positivo oppure no.

In Figura 4.6 viene presentata la schermata in cui vengono visualizzate tutte le offense, scattate nel turno di un analista. Per ognuna di queste, QRadar mette a disposizione uno strumento grafico per analizzarle. Viene effettuata un'analisi solo sugli eventi che l'hanno generata, come si può vedere dalla Figura 4.7.

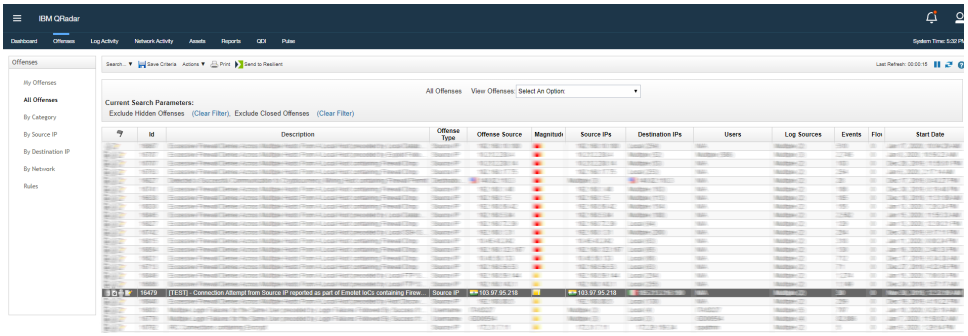

Figura 4.6. Lista delle offense

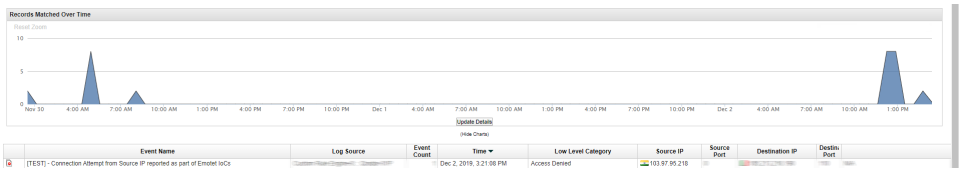

Figura 4.7. Analisi degli eventi di una offense

Un'altra funzionalità dello strato console è la generazione di dashboard configurabili ed interrogabili. Un esempio di questa viene illustrato in Figura 4.8. Nella dashboard viene presentata una visione globale della situazione di un singolo cliente. Si possono vedere i cinque rettangoli in alto, dove viene mostrato lo stato delle offense; in base alla loro colorazione, viene indicatato quali delle offense siano più gravi. Nella mappa sottostante, vengono mostrate tutti gli IP di destinazione, collegati con una linea alle source IP sorgenti del cliente. Nel grafico a linee in fondo, viene mostrato lo stato di salute di tutte le sorgenti di log, di quel cliente.

Grazie a QRadar è possibile raccogliere e normalizzare il flusso delle informazioni generate dai clienti. Tramite le regole logiche si riesce a concentrare l'attenzione soltanto sulle offense e non in tutto il traffico. Utilzzando le dashboard si ha una visione globale del flusso in tempo reale.

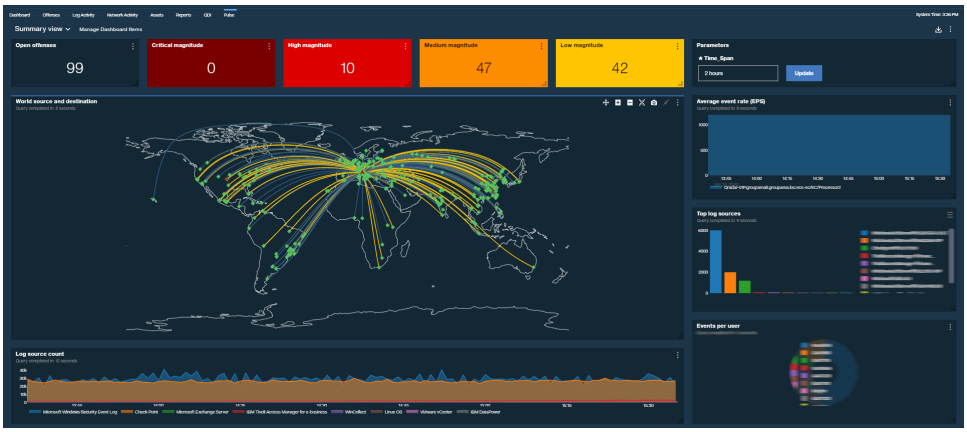

Figura 4.8. Esempio di una dashboard in QRadar

QRadar è una tecnologia vantaggiosa tramite cui si possono effettuare delle analisi sul traffico proveniente da molteplici sorgenti di log. Tale tecnologia ha, anche, degli strumenti per concentrare l'attenzione soltanto nella parte coinvolta in un possibilie attacco. Per effettuare un'analisi completa. QRadar non è sempre sufficente; infatti non ha strumenti per arricchire informazioni relative ad un'offense; così si ha la necessità di una sorgente di threat intelligence con cui arricchire le analisi.

4.2 Fonti di Threat intelligence impiegate

Il panorama della sicurezza informatica odierno è contrassegnato da una serie di problematiche comuni: enormi volumi di dati e attacchi degli avversari sempre più complessi. Una fonte di threat intelligence sarà, normalmente, capace di gestire tre funzioni chiave:

- *aggregazione di intelligence da sorgenti multiple;*
- *normalizzazione e arricchimento dei dati;*
- *condivisione di threat intelligence.*

Le sorgenti di threat intelligence installate e usufruite, durante lo svolgimento del tirocinio, sono state:

- *Virustotal;*
- *Malware Information Sharing Platform and Threat Sharing (MISP);*
- *Whois;*
- *T-Pot.*

Esse saranno illustrate in dettaglio nelle prossime sottosezioni.

4.2.1 Virustotal

Virustotal ispeziona gli elementi con oltre 70 scanner antivirus e servizi di blacklist di URL/domini. Ogni utente può selezionare un file dal proprio computer utilizzando il browser e inviarlo a VirusTotal. Quest'ultimo offre una serie di metodi per l'invio di file, tra cui l'interfaccia web, caricatori desktop, estensioni del browser e un'API a supporto del programmatore.

Al momento dell'invio di un file o di un URL, i risultati di base vengono pubblicati e condivisi, cosicchè altre persone li possono utilizzare per migliorare i propri sistemi. Di conseguenza, inviando file, URL e domini a VirusTotal si contribuisce ad aumentare il livello di sicurezza globale.

Virustotal fornisce anche una community, denominata VirusTotal Community; si tratta di una rete che permette agli utenti di commentare file e URL e di condividere le note tra loro.

Questo è un servizio maturo, di cui non c'è stato bisogno di apportare alcuna configurazione. Si è creato in seguito un collegamento tra questa fonte di threat intelligence e gli incidenti di sicurezza monitorati dal SOC.

4.2.2 Malware Information Sharing Platform and Threat Sharing

Malware Information Sharing Platform and Threat Sharing (MISP) è una soluzione software open source per la raccolta, l'archiviazione e la distribuzione di IoC. Essa, inoltre, permette la condivisione delle minacce relative all'analisi degli incidenti e dei malware. MISP è progettato da e per analisti di incidenti, professionisti della sicurezza e malware reverser.

L'obiettivo di MISP è quello di promuovere la condivisione di informazioni strutturate, all'interno della comunità della sicurezza e all'estero.

Le funzionalità di MISP sono:

- Un database di IoC che consente di memorizzare informazioni tecniche e non tecniche su campioni di malware, incidenti, aggressori e intelligence.
- Un modello di dati flessibile in cui oggetti complessi possono essere espressi e collegati tra loro, per rappresentare l'intelligenza delle minacce, gli incidenti o gli elementi collegati.
- Condivisione dei dati, scambio e sincronizzazione automatica con altre parti e gruppi di fiducia tramite MISP.
- API flessibili per integrare MISP con altre soluzioni. Un'API `restSearch` per cercare facilmente gli indicatori in MISP ed esportare quelli in tutti i formati da esso supportati.

Per avere accesso alla piattaforma MISP è necessario installare una propria instanza collegata alla rete, così da poter fare il pooling in automatico degli eventi.

Una volta installato e configurato MISP, bisogna aggiungere più feed possibili al suo interno provenienti da organizzazioni fidate. In questo modo è possibile avere un bacino più ampio di informazioni, relative all'evoluzione delle tattiche di attacco.

Una volta aggiunti tutti i feed, inizia una fase di pooling degli eventi. MISP aggiunge eventi costantemente, modificando le informazioni in base a come si evolve il malware specifico.

Finita la fase di pooling, si avrà una lista di eventi relativi ad un attacco, che la vittima ha deciso di pubblicare nella piattaforma MISP.

In ogni evento, si può vedere da quale organizzazione è stato pubblicato, che livello di gravità è stato assegnato ad esso; viene, inoltre, proposto un grafo nel quale vengono mostrati tutti gli attributi relativi all'evento analizzato o ad eventi correlati. Un esempio di grafo è mostrato in Figura 4.9, nel quale si può vedere come l'evento Emotet sia collegato con molti attributi.

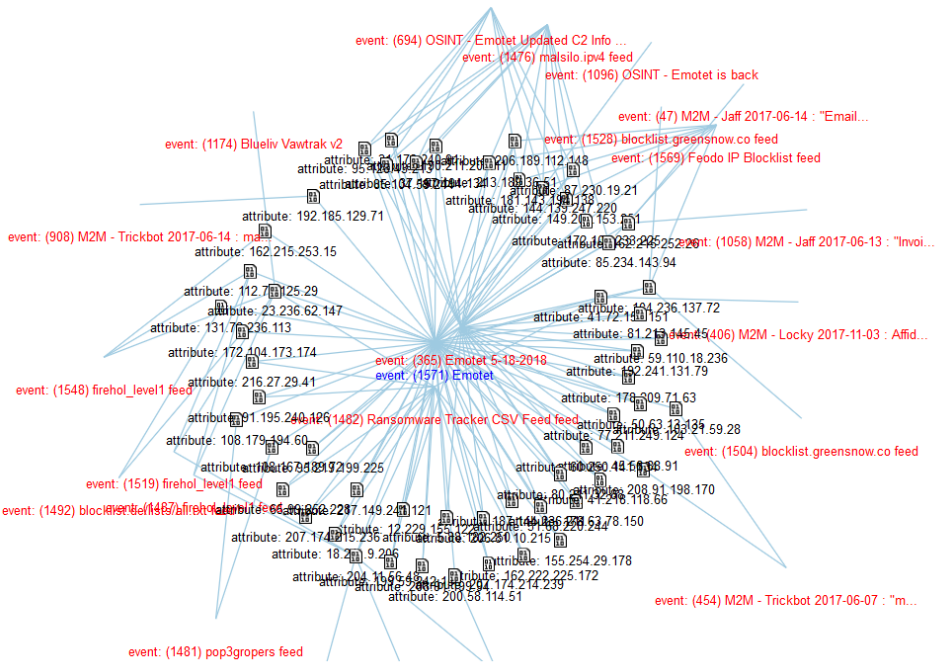

Figura 4.9. Grafo degli attributi correlati ad un evento

Si è creato poi un collegamento tra questa fonte di threat intelligence e gli incidenti di sicurezza monitorati dal SOC.

4.2.3 Whois

Whois è un protocollo di rete che consente, mediante l'interrogazione di appositi database, di stabilire a quale Internet Provider appartenga un determinato indirizzo IP o uno specifico DNS. In Whois vengono solitamente mostrate anche informazioni riguardanti l'intestatario, la data di registrazione e la data di scadenza di un dominio.

In Figura 4.10 viene presentato un esempio di risultato di esecuzione di Whois, cercando di avere più informazioni relative al dominio di Wikipedia. Dalla ricerca effettuata si possono vedere le seguenti informazioni:

```
ebdev@eb-dev:~$ whois wikipedia.it

*******************************************************************
* Please note that the following result could be a subgroup of    *
* the data contained in the database.                             *
*                                                                 *
* Additional information can be visualized at:                    *
* http://web-whois.nic.it                                         *
* Privacy Information: http://web-whois.nic.it/privacy            *
*******************************************************************

Domain:             wikipedia.it
Status:             ok
Signed:             no
Created:            2003-03-04 00:00:00
Last Update:        2019-07-10 00:53:45
Expire Date:        2020-06-24

Registrant
  Organization:     Associazione Wikipedia Italia
  Address:          Via Flaming, 49
                    Roma
                    00191
                    RM
                    IT
  Created:          2007-03-01 10:41:48
  Last Update:      2010-08-20 12:50:36

Admin Contact
  Name:             hidden
  Organization:     hidden

Technical Contacts
  Name:             hidden
  Organization:     hidden

Registrar
  Organization:     Yepa S.r.l.
  Name:             YEPA-REG
  DNSSEC:           no


Nameservers
  ns0.yepa.com
  ns1.yepa.com
```

Figura 4.10. Risultato ottenuto cercando informazioni con Whois

- *il dominio;*
- *la data di creazione;*
- *la data dell'ultimo aggiornamento;*
- *l'organizzazione che gestisce il dominio;*
- *il nameserver.*

Whois è un servizio stand alone, di cui non è stata necessaria nessuna configurazione. In seguito si è creato un collegamento tra questa fonte di threat intelligence e gli incidenti di sicurezza monitorati dal SOC.

4.2.4 T-Pot

Come già spiegato nel Capitolo 1, un honeypot è un programma con lo scopo di subire exploit. Esso espone delle vulnerabilità con l'intenzione di attirare più malintenzionati possibili, affinchè si possano studiare ed apprendere le nuove tattiche di attacco.

Tale tecnologia viene utilizzata, anche, come fonte di threat intelligence. T-Pot [6] è un esempio di honeypot avanzato; esso è un server Debian in cui sono presenti

più honeypot racchiusi nei propri docker. Questa struttura permette di eseguire più honeypot nella stessa interfaccia di rete, mantenendo basso l'ingombro della stessa e vincolando ogni honeypot all'interno del proprio ambiente virtuale.

I principali honeypot presenti all'interno di T-Pot sono:

- *Conpot:* è un honeypot Industrial Control System (ICS) con il fine di raccogliere informazioni sui metodi degli avversari che prendono di mira i sistemi di controllo industriali.
- *Dionaea:* ha come obiettivo di intrappolare il malware che sfrutta le vulnerabilità esposte e di ottenere una copia.
- *Honeytrap:* ha come scopo di osservare gli attacchi contro i servizi TCP e UDP.
- *Cowrie:* è un honeypot SSH e Telnet progettato per registrare gli attacchi di forza bruta e l'interazione dell'aggressore con la shell dell'honeypot.
- *Ciscoasa:* è un honeypot progettato per il rilevamento della vulnerabilità di Cisco ASA, che è stata resa pubblica (CVE-2018-0101).

Durante lo svolgimento del tirocinio, T-Pot è stato installato e collocato nella rete del Security Operation Center, al fine di ottenere informazioni da possibili attacchi interni. L'installazione è stata tenuta nascosta al gruppo dei Penetration Tester, al quale in seguito è stato chiesto di effettuare una scansione di vulnerabilità della rete interna.

In Figura 4.11 viene presentato il risultato della scansione dove sono illustrati gli honeypot coinvolti ed il numero di attacchi subiti. Inoltre, vengono mostrate anche le porte che sono state sfruttate per eseguire tale scansione.

Nella Figura 4.12, viene presentato l'attacco che ha subito l'honeypot Cowrie. Si può notare come quest'utlimo abbia subito 1.513 attacchi provenienti da 3 IP diversi, sfruttando i due protocolli di rete, SSH e Telnet, che esponeva, e le due porte, 22 e 23, anch'esse esposte.

Figura 4.11. Dashboard principale di T-Pot

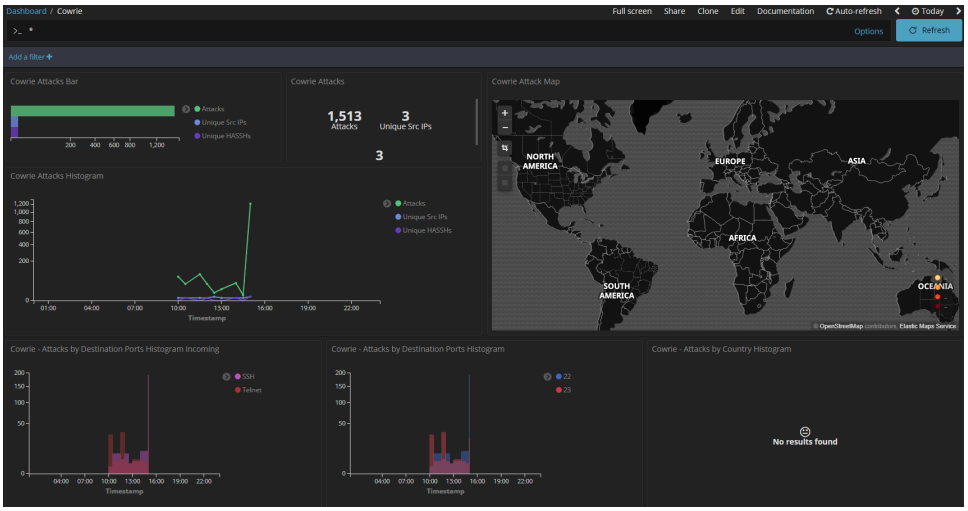

Figura 4.12. Dashboard dell'honeypot Cowrie

5

Configurazione del SOAR ed implementazione delle integrazioni

Nella prima parte di questo capitolo verrà descritto cosa è Resilient, quali vantaggi può portare all'interno del Security Operation Center e come è stato messo in comunicazione con il SIEM QRadar. Nella seconda parte verrà descritto come sono state implementate le integrazioni per collegare le fonti di threat intelligence con Resilient.

5.1 Il SOAR Resilient

Le organizzazioni, a causa della mancanza di personale formato, competenze e budget nel campo della Cybersecurity, si stanno spingendo l'utilizzo del Security Orchestration Automation and Response (SOAR), Figura 5.1.

Tale tecnologia accellera e affina drasticamente la risposta, combinando l'orchestrazione dell'Intelligenza Artificiale e, di quella umana ed automatizzando i processi.

Figura 5.1. Funzionalità orchestrate dal SOAR

Allo scopo di sopperire alla carenza di personale nelle operazioni di sicurezza, si ha la crescente necessità di automatizzare le attività ripetibili, snellire i flussi di lavoro ed orchestrare le attività di sicurezza. Inoltre, le organizzazioni hanno bisogno di poter dimostrare al management, di avere la capacità di ridurre l'impatto di incidenti inevitabili.

L'obiettivo del SOAR è di fronteggiare le difficoltà principali di un SOC; queste possono essere così riassunte:

- *volume e severità degli attacchi in costante crescita;*
- *complessità delle regolamentazioni;*
- *persistente carenza di competenze;*
- *complessità dei processi interni al SOC.*

Resilient è la piattaforma SOAR di IBM, leader per l'orchestrazione e l'automazione dei processi di risposta agli incidenti, utilizzata da Cybertech. Le organizzazioni, che operano nell'ambito della sicurezza, possono ridurre significativamente il loro tempo medio per trovare, rispondere e rimediare agli incidenti usando tale piattaforma.

Quest'ultima è di rapida e facile integrazione con i tool ed i processi esistenti, permettendo di creare un unico hub avanzato allo scopo di guidare un'azione veloce ed intelligente (Figura 5.2). Le avanzate capacità di orchestrazione della piattaforma, consentono una risposta adattiva alle complesse minacce informatiche.

Figura 5.2. Capacità di Resilient di accentrare più funzioni in un unico hub

Nel contesto di un SOC distribuito ed eterogeneo, come quello di Cybertech, il SOAR è l'arma vincente per ridurre i tempi di rilevamento e di risposta ad una minaccia. Esso è in grado di orchestrare tutti i processi interni del SOC, nonostante

i suoi livelli siano distribuiti in diverse nazioni europee; riesce facilmente a rimanere conforme a tutte le regolamentazioni, avendo in carico anche dei clienti operanti in settori produttivi diversi.

Resilient è in grado di portare vantaggi ai diversi ruoli interni di un'organizzazione. Nel seguito, ecco una lista di tali vantaggi:

- *Chief Information Security Officer (CISO):* Fornisce accesso e visibilità al programma di risposta agli incidenti, tramite dashboard e reportistica. Fornisce una stima della spesa per la sicurezza, misurabile in termini di tempo e valore. Aumenta il Return on Investment (ROI) degli strumenti di sicurezza e dimostra il valore della sicurezza per l'azienda.
- *SOC Manager:* Misura e migliora la produttività del SOC. Adatta automaticamente il processo di risposta all'attacco. Applica gli SLA e migliora il tempo medio di risoluzione. Aumenta l'efficacia del personale con strumenti che lo aiutano a concentrarsi sui compiti giusti, affrontando il deficit di competenze. Dimostra la coerenza dell'esecuzione della risposta in tutti i reparti.
- *Analisti:* Aiuta gli analisti a concentrarsi sull'indagine e sulla risposta, invece di cercare informazioni tra gli strumenti a loro disposizione. Automatizza le attività di triage e di arricchimento.
- *Organizzazione:* Migliora la responsabilità dimostrando cosa è stato fatto dopo l'incidente per correggere la situazione. Registra le prestazioni in termini di tempo di rilevamento e di risposta. Produce dei documenti comprovanti il rispetto delle norme e dei regolamenti. Arruola diverse unità di business nel processo di risposta agli incidenti.

5.1.1 Architettura Managed Security Service Provider di Resilient

Nel contesto aziendale in cui è stato svolto il tirocinio, con l'aumentare del numero dei clienti è nata l'esigenza di avere una piattaforma SOAR in grado di gestire, da una postazione centralizzata, le singole configurazioni dei clienti.

Con l'ultima release del 2019, Resilient ha messo a disposizione un plug-in specifico per questa funzionalità.

L'add-on di Resilient Managed Security Service Provider (MSSP) consente di gestire più organizzazioni figlie da una singola organizzazione di configurazione padre.

Ogni personalizzazione o integrazione implementata, in una piattaforma Resilient con l'add-on MSSP, deve essere distribuita all'organizzazione di configurazione; quest'ultima in automatico effettuerà il deployment delle modifiche ad ogni organizzazione figlia. Il flusso del deployment di una integrazione è mostrato in Figura 5.3.

Prima di passare in produzione è stato effettuato un periodo di testing della release di Resilient con l'add-on MSSP.

Essendo Resilient una piattaforma scritta completamente in Python, per simulare le singole organizzazioni figlie, è stato utilizzato il modulo `venv` di Python.

Questo modulo fornisce il supporto per la creazione di ambienti virtuali leggeri con le proprie directory, isolate dalla directory del sistema. Ogni ambiente virtuale

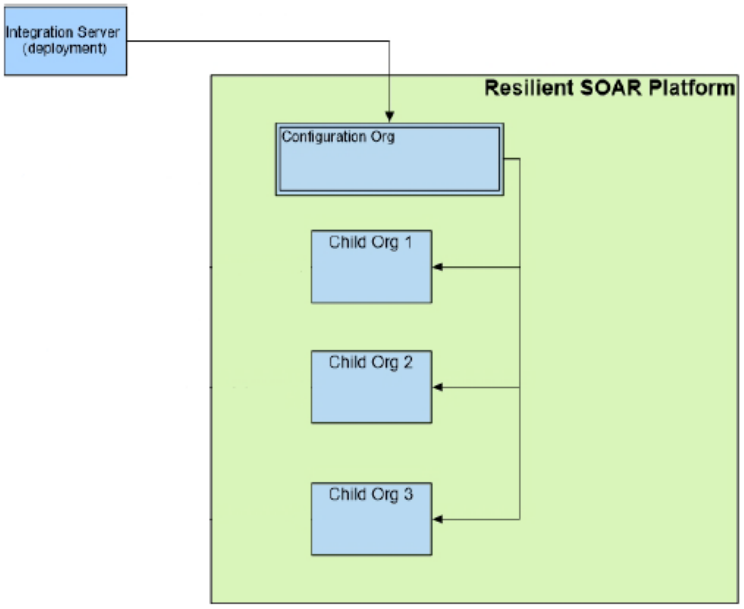

Figura 5.3. Flusso del deployment alle singole organizzazioni

ha il proprio binario Python, che corrisponde alla versione del binario utilizzata per creare il virtualenv e può avere il proprio set indipendente di pacchetti Python installati nella directory.

Una volta creati due ambienti Python isolati, passiamo alla creazione dell'architettura MSSP, utilizzando i comandi messi a disposizione da Resilient.

Per usufruire della funzionalità MSSP di Resilient, bisogna inizialmente determinare l'organizzazione di configurazione padre. Per crearla, eseguiamo il comando perchè nella Riga 1 del Listato 5.1.

Definita l'organizzazione padre, con nome "MSSP Config Org" e tipologia "configuration", passiamo alla creazione delle organizzazioni figlie, dipendenti da quest'ultima.

Nelle Righe 2, 3 e 4 del Listato 5.1 sono state create tre organizzazioni figlie con i seguenti nomi, "MSSP Global Org", "Client 1" e "Client 2", tutte dipendenti dall'organizzazione "MSSP Config Org".

L'organizzazione "MSSP Global Org", con tipologia "global_dashboard", viene utilizzata dal SOC manager per avere la visione di come vengono gestite le organizzazioni figlie, "Client 1" e "Client 2", utilizzando delle dashboard configurabili ed interrogabili.

Finita l'architettura MSSP, nella Riga 6 del Listato 5.1, viene creato l'utente "Integration User", il quale può effettuare modifiche all'organizzazione "MSSP Config Org" e fare il deployment di queste ultime in tutte le organizzazioni figlie.

```
1    sudo resutil neworg -name "MSSP Config Org" -configtype configuration
2    sudo resutil neworg -name "MSSP Global Org" -configtype global_dashboard -parentorg "MSSP Config Org"
3    sudo resutil neworg -name "Client 1" -configtype child -parentorg "MSSP Global Org"
4    sudo resutil neworg -name "Client 2" -configtype child -parentorg "MSSP Global Org"
5
6    sudo resutil newuser -email integration.user@cybertech.eu -first Integration -last User -org "MSSP Config Org"
```

Listato 5.1. Creazione dell'architettura MSSP in Resilient

Completata l'installazione e la configurazione del SOAR Resilient, procediamo alla creazione del collegamento tra tale piattaforma ed il SIEM QRadar.

5.1.2 Creazione del template per l'escalation delle offenses

L'obiettivo del SOAR è quello di concentrare tutte le informazioni utili, per gli analisti, in un'unica piattaforma. Dovendo simulare anche in QRadar un ambiente distribuito, sono stati creati due domain differenti, ai quali arrivano informazioni da due log source diversi. I domain creati sono "Customer1" e "Customer2".

Resilient, per prima cosa, è stato messo in collegamento con QRadar. Essendo entrambi software di proprietà di IBM, era gia prevista un'integrazione installabile di Resilient in QRadar.

Installato il pacchetto di integrazione, si è creato il template "Escalation Template QRadar", grazie al quale viene effettuata una traduzione dei singoli campi di una offense di QRadar. In un incidente di Resilient. Nella Figura 5.4 viene presentato il template selezionato per l'escalation automatica delle offense in Resilient.

Prima di completare il collegamento tra il SIEM QRadar ed il SOAR Resilient, è necessario creare il mapping tra i domain creati in QRadar e le organizzazioni presenti in Resilient.

Come viene presentato in Figura 5.5, sono stati creati due legami: uno tra il domain "Customer1" di QRadar e l'organizzazione "Client1" di Resilient e l'altro tra "Customer2" e "Client2".

Completate tali configurazioni, gli analisti non avranno più bisogno di monitorare i clienti utilizzando QRadar, ma possono farlo utilizzando il SOAR Resilient; il quale verrà integrato con delle fonti di threat intelligence.

5.2 Sviluppo delle integrazioni

Un'integrazione, o funzione, in Resilient è un componente del workflow, che chiama un codice remoto. Un esempio di workflow viene presentato in Figura 5.6.

Ogni funzione racchiude i suoi compiti in un singolo blocco del workflow. La piattaforma Resilient invia i dati al componente remoto; questo esegue l'attività e, successivamente, restituisce i risultati al flusso di lavoro. Tali risultati possono essere gestiti tramite script e da altre funzioni del workflow per orchestrare dinamicamente le attività di risposta agli incidenti.

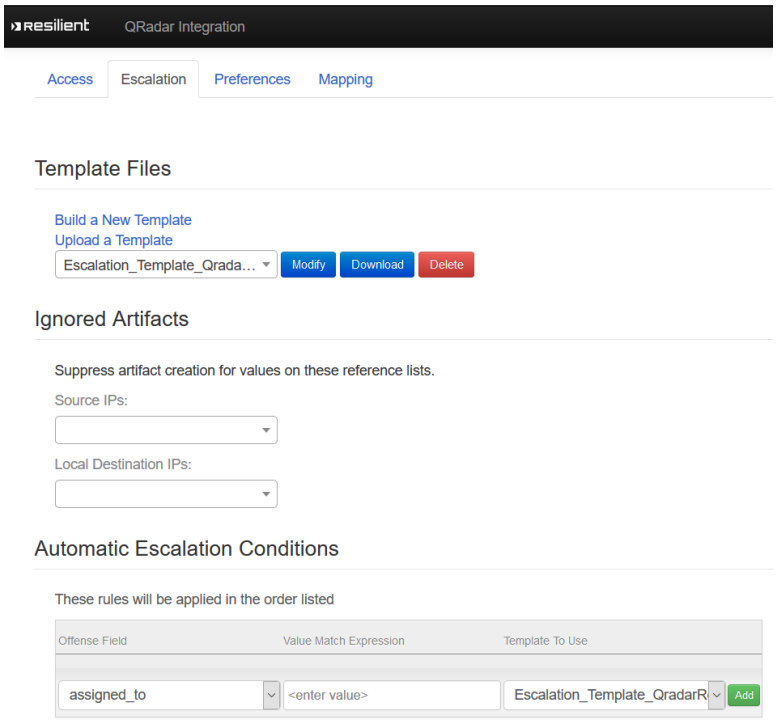

Figura 5.4. Template per l'escalation automatica delle offenses in Resilient

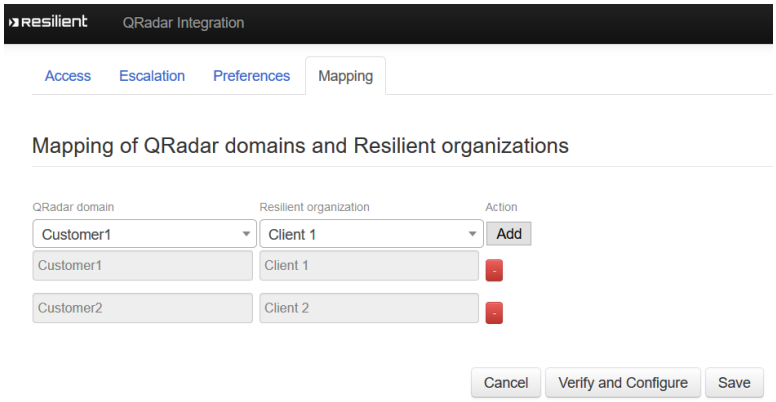

Figura 5.5. Mapping tra i domini di QRadar e le organizzazioni di Resilient

Una funzione ha uno o più ingressi e fornisce un risultato in JSON. Nella sua forma più semplice, una funzione viene dapprima aggiunta al workflow e poi si inseriscono manualmente i valori per ciascuno dei suoi campi di input.

La funzione, quando viene attivata dal workflow, invia i valori di input al codice remoto tramite una richiesta POST e attende un risultato. L'input e l'output della funzione vengono gestiti, rispettivamente, dal pre-process e dal post-process

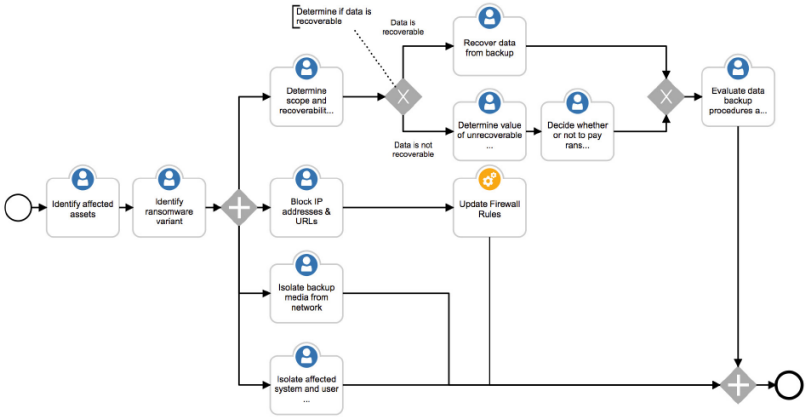

Figura 5.6. Esempio di un workflow in Resilient

script di Resilient. Il flusso delle operazioni dell'attivazione di una funzione viene rappresentato in Figura 5.7.

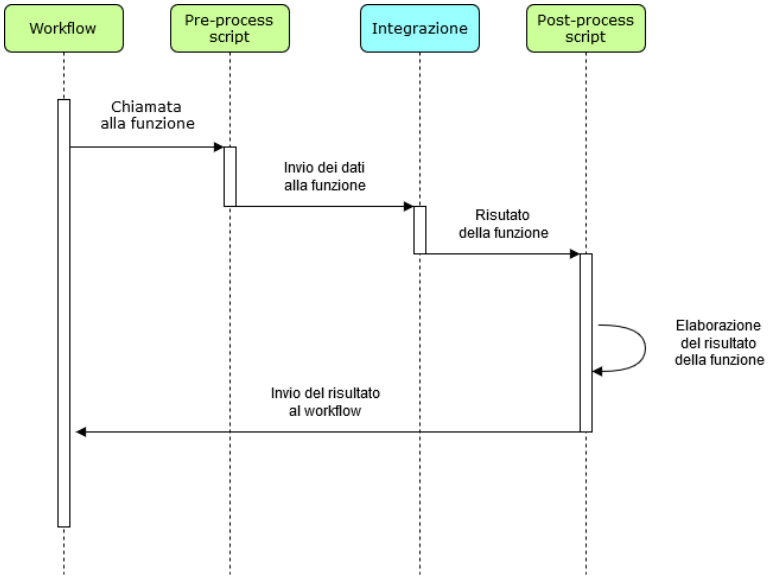

Figura 5.7. Gestione del flusso dell'attivazione di una funzione

In tale Figura 5.7 sono indicati, con dei rettangoli verdi, i componenti interni a Resilient, mentre in azzurro viene mostrato il codice remoto.

Uno script di pre-process è uno script di sola lettura, che viene utilizzato per impostare dinamicamente il valore di uno o più campi di input della funzione.

È possibile utilizzare lo script per recuperare il valore corrente di una proprietà e per fornire successivamente tale valore alla funzione. Uno script di pre-process non

può eseguire certe attività, come la modifica dei valori degli incidenti o l'aggiunta di artefatti.

È possibile utilizzare il risultato della funzione in uno script di post-process, il quale esegue un'attività in risposta al risultato fornito dalla funzione. Lo script può modificare i valori degli incidenti, aggiungere artefatti, righe al database e altro ancora.

Questo è lo schema da seguire per implementare una nuova funzione in Resilient. Tale struttura non permette di eseguire codice proprio all'interno della piattaforma, ma obbliga a far passare l'esecuzione attraverso i due filtri di pre-process e post-process.

Nel seguito, verranno descritte le funzioni implementate per connettere Resilient con le fonti di threat intelligence, descritte nel Capitolo 4.

Essendo il codice delle integrazioni utilizzato in un ambiente di produzione, per motivi di privacy, non sarà possibile descrivere nel dettaglio tutte le integrazioni.

5.2.1 Integrazione con Virustotal

L'integrazione con la threat intelligence Virustotal è stata implementata in collaborazione con gli sviluppatori di Cybertech.

La classe `VirusTotalFunction`, mostrata nel Listato 5.2, ha quattro metodi: `__init__`, `_init_virustotal_api`, `_virustotal_function` e `parse_results`.

Il primo metodo stabilisce il collegamento tra Resilient e la funzione di Virustotal. Il secondo, valida i campi necessari per utilizzare le API della threat intelligence. Il metodo `_virustotal_function` salva i dati che provengono dal pre-process script di Resilient in variabili locali. Le informazioni ricevute in input da Resilient sono l'incident id, gli artifact e gli attachment legati all'incidente che si vuole analizzare. Le tipologie di input possono essere file, URL, IP, sha256, domini e hash.

Tale metodo esegue anche la ricerca su Virustotal e salva il risultato in un dizionario chiamato `results`. Infine l'ultimo metodo, `parse_results`, effettua il parser della risposta di Virustotal e la restituisce in formato JSON.

```
1  class VirusTotalFunction:
2
3      def __init__(self, opts): ...
4
5      def _init_virustotal_api(self): ...
6
7      def _virustotal_function(self, event, *args, **kwargs): ...
8
9      def parse_results(self, results, callback, start_time): ...
```

Listato 5.2. Codice della funzione di Virustotal

Per richiamare l'integrazione di Virustotal in un workflow, è necessario configurare i suoi pre-process e post-process script.

Lo script di pre-process viene presentato nella Figura 5.8. Esso crea un dizionari `typeLookup` contenente tutti i possibili campi presenti in un incident di Resilient.

In seguito, "incident.id", "artifact.id" ed "artifact.value", vengono inviati all'integrazione.

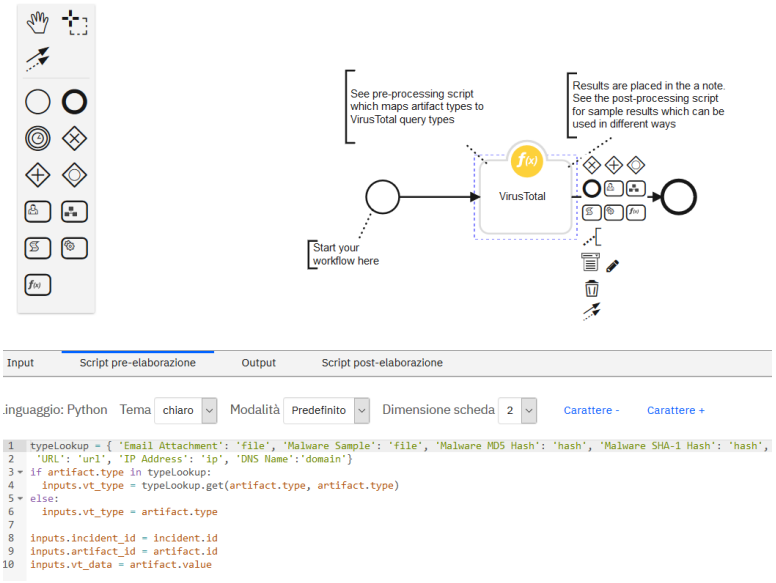

Figura 5.8. Pre-process script della funzione di Virustotal

Una volta inviati i dati in input alla funzione, e una volta effettuata le ricerca su Virustotal, è necessario gestire il risultato ottenuto per renderlo disponibile in un workflow.

Lo script di post-process riceve il dizionario `results` e, se in quest'ultimo il valore della chiave "positives" è diverso da "None", viene creata una variabile `msg`, contenente la stringa, con il risultato esaminato dal parse, della ricerca su Virustotal.

Infine nelle note dell'incidente viene aggiunta questa stringa, in modo tale che gli analisti, quando devono effettuare le analisi di un incidente, hanno già le informazioni provenienti da Virustotal.

5.2.2 Integrazione con MISP

L'integrazione implementata per contattare la threat intelligence MISP, ha come scopo quello di cercare, all'interno di questa piattaforma, degli attributi presenti negli artifact di un incidente.

La classe `MispFunction` ha il metodo `misp_search_attribute`, il quale utilizzando le API e l'URL di MISP, effettua una ricerca negli eventi della threat intelligence.

La ricerca viene effettuata nella Riga 11 del Listato 5.3. Se la ricerca va a buon fine, il risultato viene inserito all'interno del dizionario `results` (righe 13-17).

```
1   class MispFunction:
2       def misp_search_attribute(self, event, *args, **kwargs):
3           try:
4               API_KEY = get_config_option("API_KEY_MISP")
5               URL = get_config_option("URL_MISP")
6
7               search_attribute = kwargs.get("misp_attribute_value")
```

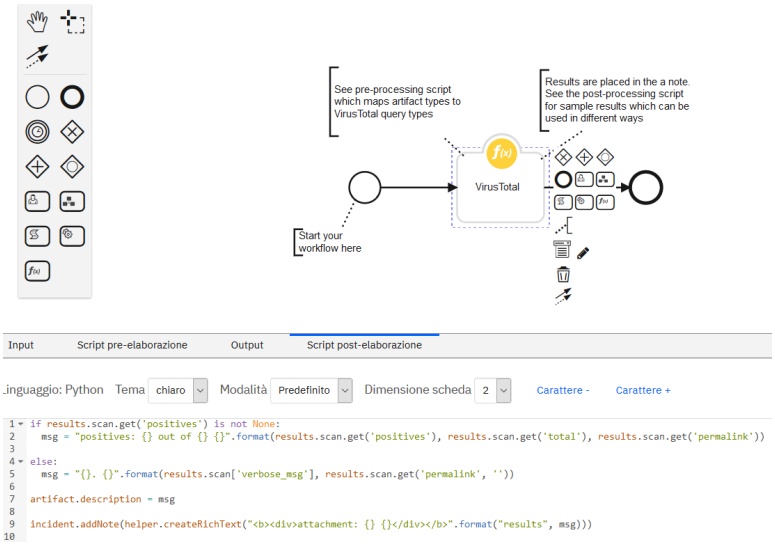

Figura 5.9. Post-process script della funzione di ViruaTotal

```
            misp_client = misp_helper.get_misp_client(URL, API_KEY)

            results = {}
            search_results = misp_helper.search_misp_attribute(misp_client, search_attribute)

            if search_results['search_status']:
                results['success'] = True
                results['content'] = search_results['search_results']
                misp_tags = misp_helper.get_misp_attribute_tags(misp_client, search_results['search_results'])
                results['tags'] = misp_tags

            else:
                results['success'] = False

        except Exception:
            yield FunctionError()
```

Listato 5.3. Codice della funzione di MISP

Come già detto in precedenza, per eseguire il codice esterno, bisogna necessariamente utilizzare i due filtri messi a disposizione da Resilient, ovvero il pre-process ed il post-process script.

Il pre-process della funzione del MISP, viene presentato in Figura 5.10. Come input alla funzione vengono trasmessi i valori presenti negli artifact dell'incidente.

Il risultato dell'integrazione del MISP viene gestito dal post-process script mostrato in Figura 5.11.

La risposta della ricerca viene scritta nel dizionario `results`. Se il valore della chiave `success` del dizionario `results` è posto a "False", viene aggiunta la stringa "No matching attribute found" alla descrizione dell'incidente. Se questo avviene, all'interno del MISP, non sono contenuti eventi utili per analizzare l'incidente.

Diversamente, utilizzando un ciclo for, viene scorso tutto il dizionario `results` ed il suo contenuto viene salvato nella lista `matched`.

Infine, nelle note dell'incidente, viene aggiunto il contenuto della lista, in modo tale che gli analisti, quando devono effettuare le analisi di un incidente, hanno già le informazioni provenienti dal MISP.

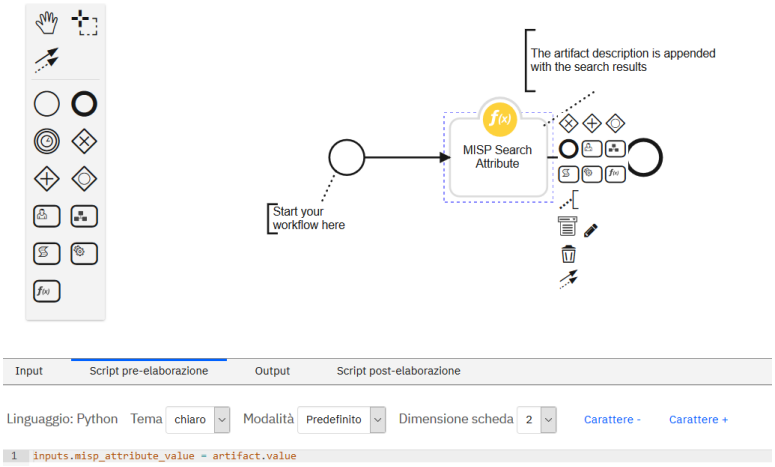

Figura 5.10. Pre-process script della funzione di MISP

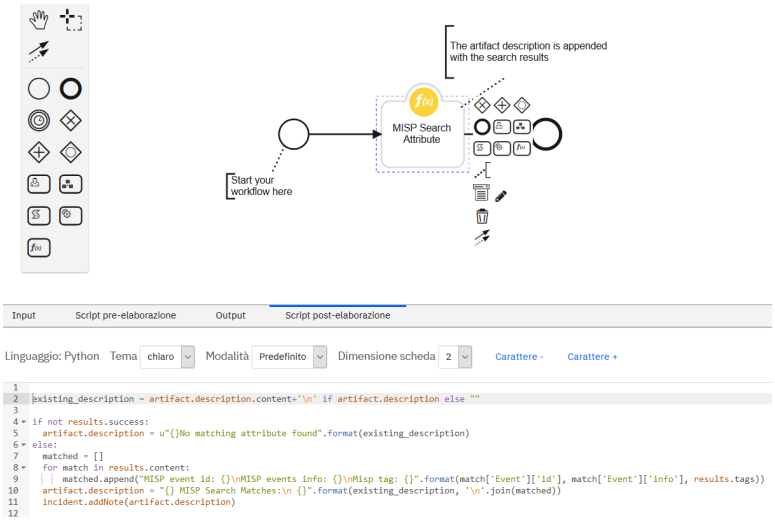

Figura 5.11. Post-process script della funzione di MISP

5.2.3 Integrazione con Whois

L'integrazione con la threat intelligence Whois è stata implementata in collaborazione con gli sviluppatori di Cybertech.

La funzione con cui contattare il database Whois è mostrata nel Listato 5.4. Quest'ultima è composta da due classi: `PayloadWhois` e `WhoisFunction`.

La prima classe ha due metodi: `__init__` e `as_dict`. Essa racchiude il payload, contenente la risposta di Whois, il quale ritorna in Resilient ed è disponibile al post-process script.

La seconda classe, `WhoisFunction`, ha due metodi: `__init__` e `whois_query`.

```
class PayloadWhois:

    def __init__(self, inputs): ...

    def as_dict(self): ...

class WhoisFunction:

    def __init__(self, opts): ...

    def whois_query(self, event, *args, **kwargs): ...
```

Listato 5.4. Codice della funzione di Whois

Il primo metodo crea la connessione tra Resilient e la funzione di Whois. Invece il metodo `whois_query` viene utilizzato per eseguire una query direttamente nel server Whois, così da raccogliere informazioni su un IP o un URL ricevuto in input. Il risultato della query viene salvato nel dizionario `results`, che, in seguito, verrà gestito dal post-process script.

Per richiamare l'integrazione di Whois in un workflow è necessario configurare i suoi pre-process e post-process script.

Il pre-process script di Whois viene presentato in Figura 5.12. Come input alla funzione vengono passati tutti i valori presenti negli artifact dell'incidente.

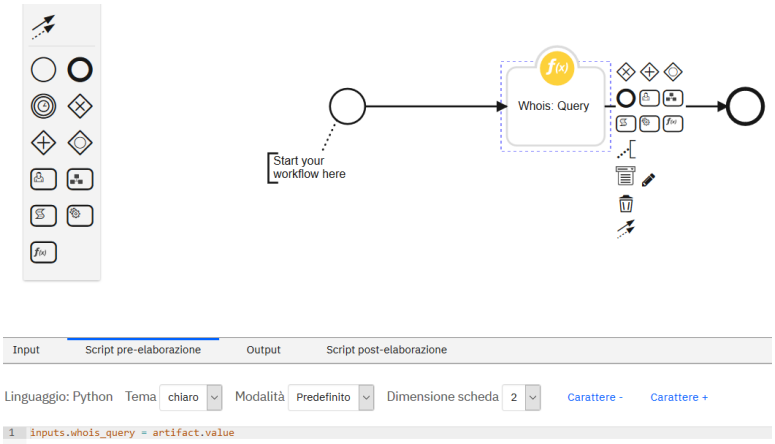

Figura 5.12. Pre-process script della funzione di Whois

Il risultato dell'integrazione del Whois viene gestito dal post-process script mostrato in Figura 5.13. Se il valore della chiave "success" del dizionario `results` è posto a "True", viene salvata la stringa contenente il risultato della query nella variabile "noteText". Al contrario, se il valore è posto a "False", nella variabile "noteText" viene salvata la stringa "No results found". In entrambi i casi, nelle note dell'incidente viene aggiunto il contenuto della variabile, in modo tale che gli analisti, quando devono effettuare le analisi di un incidente, hanno già le informazioni provenienti dal Whois.

Prima dell'installazione e configurazione del SOAR, gli analisti di Cybertech, per effettuare un'analisi, dovevano cercare le informazioni relative all'incidente nelle

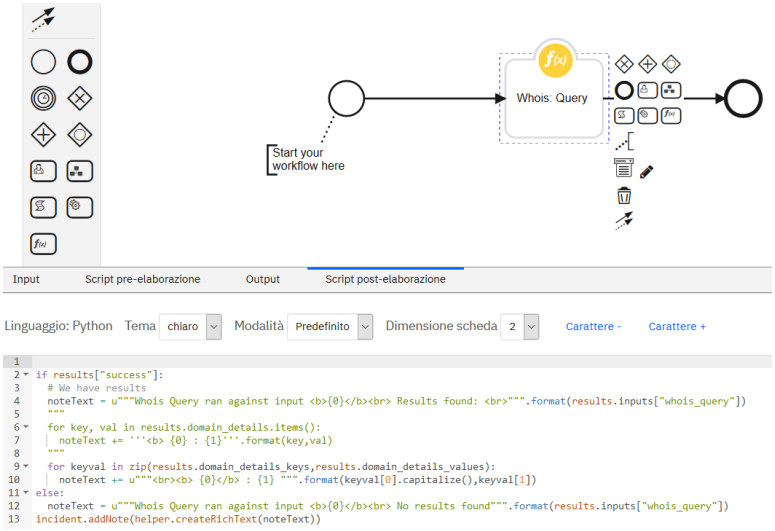

Figura 5.13. Post-process script della funzione di Whois

varie fonti di threat intelligence, appuntarsele, e poi riportarle in una piattaforma di ticketing.

Effettuata l'installazione del SOAR Resilient, ed effettuata la sua integrazione con il SIEM QRadar e con le diverse fonti di threat intelligence, gli analisti hanno in automatico a loro disposizione, in unica piattaforma, le informazioni provenienti dalle fonti di threat intelligence integrate con Resilient.

Nel capitolo successivo verrà descritto come è stato implementato un workflow per la gestione di un incidente informatico, al cui interno vengono richiamate le funzioni descritte in questo capitolo.

6

Implementazione di un workflow automatico ed ottimizzazione dei tempi di risposta

Nella prima parte di questo capitolo verranno descritte le potenzialità di un workflow e come viene implementato. Nella seconda parte si mostrerà come è stato ridotto il tempo di risposta di un incidente grazie all'utilizzo del SOAR.

6.1 Implementazione di un workflow automatico in Resilient

Gli analisti del SOC di Cybertech, una volta installato e configurato il SOAR, non perdono tempo nel cercare, nelle piattaforme di threat intelligence, informazioni utili allo scopo di arricchire una offense. Infatti, essi possono usufruire di Resilient, collegato con le tecnologie mostrate in Figura 6.1, il quale effettua delle ricerche in automatico di informazioni relative ad un incidente.

Tutte le offense di QRadar, tramite il template illustrato nel Capitolo 5, vengono inviate automaticamente a Resilient, il quale, nel suo database, crea un incidente con le stesse informazioni contenute nelle offense.

Le regole che gli analisti generano in QRadar vengono assegnate ad una specifica tipologia di incidente la quale, tramite il template per l'escalation automatica, viene trasmessa a Resilient.

Ad esempio, la regola "Potential Botnet Emotet Activity", presentata nel Capitolo 4, è stata assegnata alla tipologia "Malware".

Per guidare gli analisti durante un incidente informatico, Resilient mette a disposizione i workflow.

Un workflow è un insieme di attività, progettato graficamente, che consente di creare un insieme complesso di istruzioni. I flussi di lavoro permettono di implementare sofisticati processi di risposta, che possono essere invocati da condizioni presenti in un incidente di Resilient, come ad esempio, la sua tipologia.

Inoltre esso permette di definire sequenze di attività umane, condizioni logiche ed operazioni automatiche.

Gli analisti, in Resilient, possono utilizzare delle regole per invocare i flussi di lavoro quando è opportuno, così da mettere in atto una risposta logica in base alla tipologia dell'incidente.

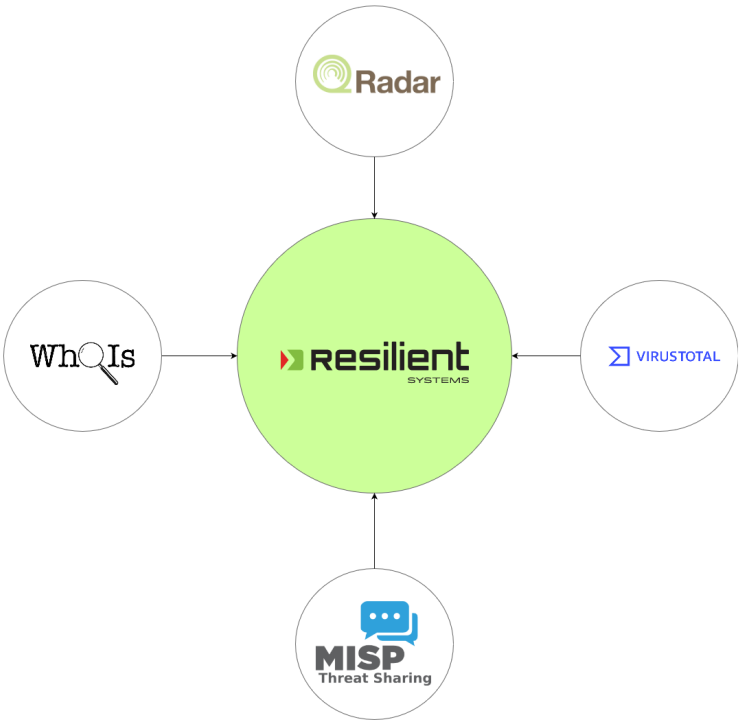

Figura 6.1. Configurazione finale del SOAR Resilient

Ad esempio, ogni volta che un incidente ha come tipologia “Malware”, scatta il workflow “Malware response”.

I flussi di lavoro possono includere le seguenti componenti: gateway parallelo, gateway condizionale, altri flussi di lavoro, timer, task dell’analista e funzioni.

L’implementazione di un workflow, in Resilient, ha diversi obiettivi:

- *Velocità:* raccoglie le informazioni in automatico, non appena viene generato un incidente, al fine di rendere queste, immediatamente disponibili agli analisti.
- *Riduzione degli errori umani:* effettua le ricerche nelle fonti di threat intelligence, evitando errori di distrazione o di battitura da parte degli analisti.
- *Linee guida:* fornisce, all’analista meno esperto, delle linee guida, progettate dagli analisti con più esperienza. Risolve il problema della mancanza di personale formato.

Durante il tirocinio, è stato implementato il workflow “Malware response” per la gestioni di incidenti, associati alla tipologia “Malware”. Tale flusso di lavoro è composto da quattro fasi:

1. *fase di engage;*
2. *fase di analisi;*
3. *fase di risposta;*
4. *fase di post-incident.*

Queste saranno esaminate in dettaglio nelle prossime sottosezioni.

6.1.1 Fase di engage

La fase di engage, mostrata in Figura 6.2, è composta dalle tre funzioni implementate nel Capitolo 5, rappresentate con rettangoli gialli, da sei task che gli analisti devono completare in questa fase, raffigurati con rettangoli blu e da un timer.

Le funzioni, descritte nel Capitolo 5, hanno lo scopo di ottenere in automatico tutte le informazioni dell'incidente, provenienti dalle fonti di threat intelligence, integrate con la piattaforma SOAR.

La threat intelligence Virustotal restituisce il risulato della ricerca in score. Il punteggio serve all'analista per comprendere se il file, l'URL, l'IP, lo sha256, i domini e l'hash inviati siano malevoli oppure no. L'integrazione, oltre allo score, riporta il link della ricerca in Resilient, permettendo all'analista di verificare, se vuole, il risultato riportato.

La funzione "MISP Search Attribute" contatta la piattaforma MISP, in cerca di eventi con gli IoC dell'incidente preso in analisi. Se il risultato della ricerca è positivo, in Resilient viene riportato il livello della minaccia cercata e l'ID dell'evento correlato in MISP.

L'integrazione con la threat intelligence Whois, restituisce il risultato della query effettuata nel suo server. In Resilient verranno riportati, la data di quando sono stati eseguiti gli ultimi aggiornamenti in quel dominio, il nome del server, lo status, la nazione e la regione.

Passando ai task manuali, che gli analisti devono svolgere, troviamo:

1. *Initial Triage:* l'analista si assegna l'incidente, in modo tale che nessun altro analista prenda in carico lo stesso. Questo serve, inoltre, a prendersi la responsabilità nella chiusura di un incidente.
2. *Interview key individual:* si controlla se il cliente sotto monitoraggio abbia segnalato qualcosa di anomalo nella propria workstation o nella casella postale.
3. *Determine if illegal activity is involved:* l'analista controlla la sezione delle note dell'incidente. In questa sezione trova i risultati ottenuti dalle fonti di threat intelligence.
4. *Determine if inappropriate internal involvement:* l'analista, effettuata una prima visione del problema, cerca di capire se una possibile minaccia possa essersi diffusa in altre macchine interne.
5. *Ensure appropriate evidence collection and preservation:* nella sezione note, dove già sono contenute le informazioni provenienti dalle fonti di threat intelligence, l'analista scrive il resoconto della fase di engage.
6. *Notify internal management chain:* vengono riportate al SOC manager, tramite e-mail, tutte le informazioni ottenute in questa fase. Questo task serve. anche, per tenere traccia delle fasi che precedono la chiusura di un incidente.

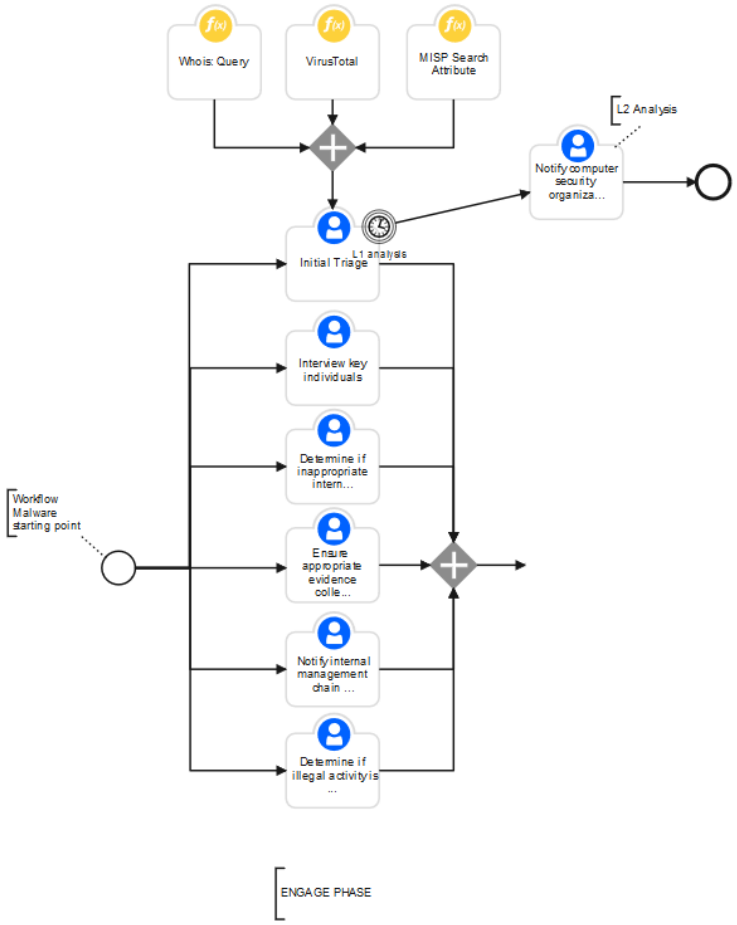

Figura 6.2. Engage phase del workflow “Malware response”

Se un incidente non viene preso in carico entro un determinato tempo stabilito, il timer fissato nel task “Initial Triage” scala l’incidente al SOC manager, il quale, successivamente, assegnerà l’incidente ad un analista.

Una volta completati tutti i task di questa fase si può passare alla fase successiva.

6.1.2 Fase dell’analisi

La fase dell’analisi, mostrata in Figura 6.3, inizia con un gateway condizionale, nel quale l’analista deve etichettare se l’incedente sia un falso positivo oppure no. Nel

caso in cui l'incidente verrà etichettato come falso positivo, esso verrà chiuso come tale; altrimenti si proseguirà nel flusso di lavoro. L'analista, per completare questa fase deve svolgere cinque attività:

1. *Analyze network traffic for malware activity:* l'analista effettua un'analisi del traffico di rete, in entrata ed in uscita, generato dalla macchina coinvolta nell'incidente.
2. *Analyze malware infected system:* viene effettuata un'analisi della macchina infettata dal malware e vengono controllati i suoi registri ed i suoi log di sistema.
3. *Review the output and status of anti-virus software:* l'analista effettua una scansione con l'anti-virus presente nella macchina e controlla se è stato disabilitato oppure no.
4. *Create backup of affected system:* viene effettuato un backup della macchina allo scopo di svolgere un'analisi più approfondita ed, infine, salvare i documenti presenti in essa.
5. *Disconnect or isolate malware infected system:* la macchina vittima viene disconnessa dalla rete, in modo tale che il malware rimanga confinato nella stessa.

I timer, nei tre task sequenziali, servono per non far bloccare l'analisi dell'incidente in questa fase. Completati tutti i task della fase dell'analisi passiamo alla fase della risposta.

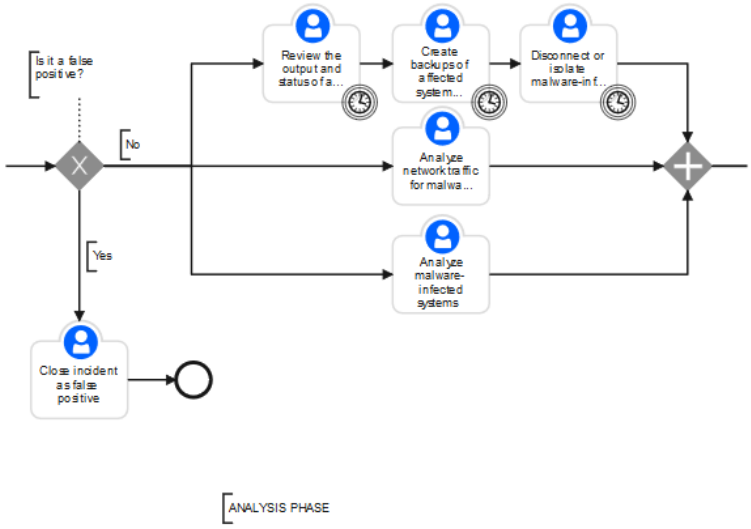

Figura 6.3. Analysis phase del workflow "Malware response"

6.1.3 Fase della risposta

La fase della risposta, mostrata in Figura 6.4, è formata da quattro task:

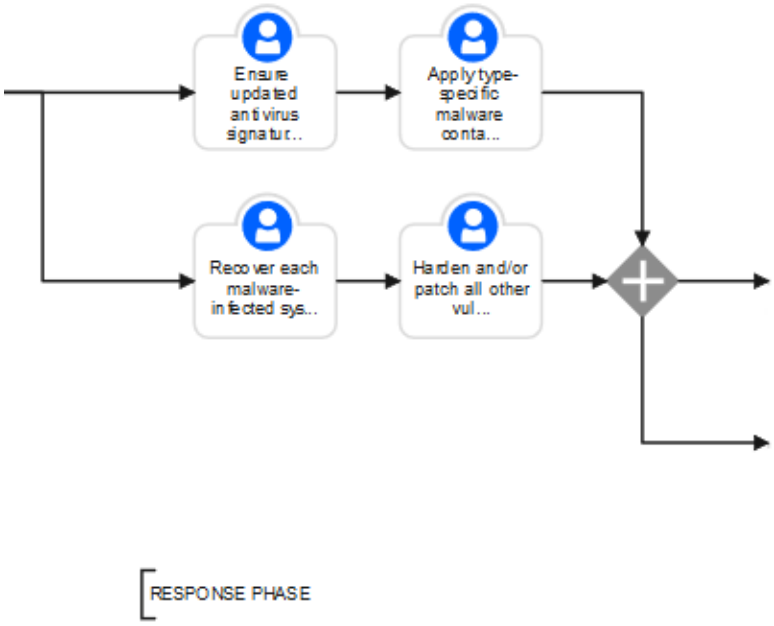

Figura 6.4. Response phase del workflow “Malware response”

1. *Ensure update anti-virus signatures are deployed:* confermato il malware, l’analista deve distribuire la firma di esso alle macchine di tutti i clienti.
2. *Recover each malware infected system:* l’analista deve eseguire delle attività di recupero della macchina infetta; nell’ambito di questa attività, è necessaria la formattazione della stessa.
3. *Apply type specific malware containment measures:* in base al comportamento del malware, vengono effettuate delle diverse misure di contenimento, ad esempio, se siamo in presenza di un attacco Distributed Denial of Service (DDoS), vengono messi in blacklist tutti gli IP, che hanno inondato di richieste la macchina vittima.

4. *Harden and/or patch all other vulnerable systems:* nota la vulnerabilità sfruttata dall'attacco, viene eseguito un aggiornamento, allo scopo di non subire lo stesso tipo di attacco in altre macchine.

Terminata questa fase si procede con l'ultima fase del workflow.

6.1.4 Fase del post-incident

La fase della risposta, mostrata in Figura 6.5, è formata da cinque task:

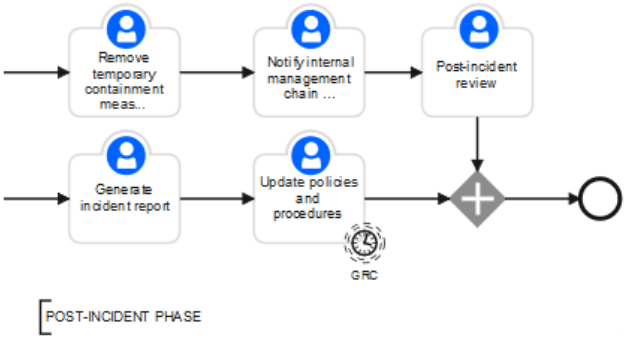

Figura 6.5. Post-incident phase del workflow "Malware response"

1. *Remove temporary containment measure:* vengono tolte temporaneamente le misure di contenimento effettuate nella fase precedente. La rete coinvolta nell'incidente viene mantenuta sotto osservazione.
2. *Notify internal management chain:* la conclusione dell'incidente viene riportata al SOC manager, il quale provvederà ad informare il cliente, coinvolto nell'incidente, di tutte le attività svolte dal SOC.
3. *Generate incident report:* viene generato un report dove vengono scritte le attività svolte dall'analista, dall'assegnazione dell'incidente alla sua chiusura.
4. *Post-incident review:* l'analista, concluse formalmente le attività, informa gli altri analisti. Esso riferisce il modo in cui è stato gestito l'attacco e quali dettagli dell'incidente sono stati utili per capire che non fosse un falso positivo.
5. *Update policies and procedures:* vengono aggiornate le regole e le procedure, in modo tale da migliorare il rilevamento e l'analisi di un incidente simile a quello gestito.

Il workflow completo viene rappresentato in Figura 6.6. Nella sezione successiva verrà mostrato un esempio di gestione di un incidente reale utilizzando questo flusso di lavoro.

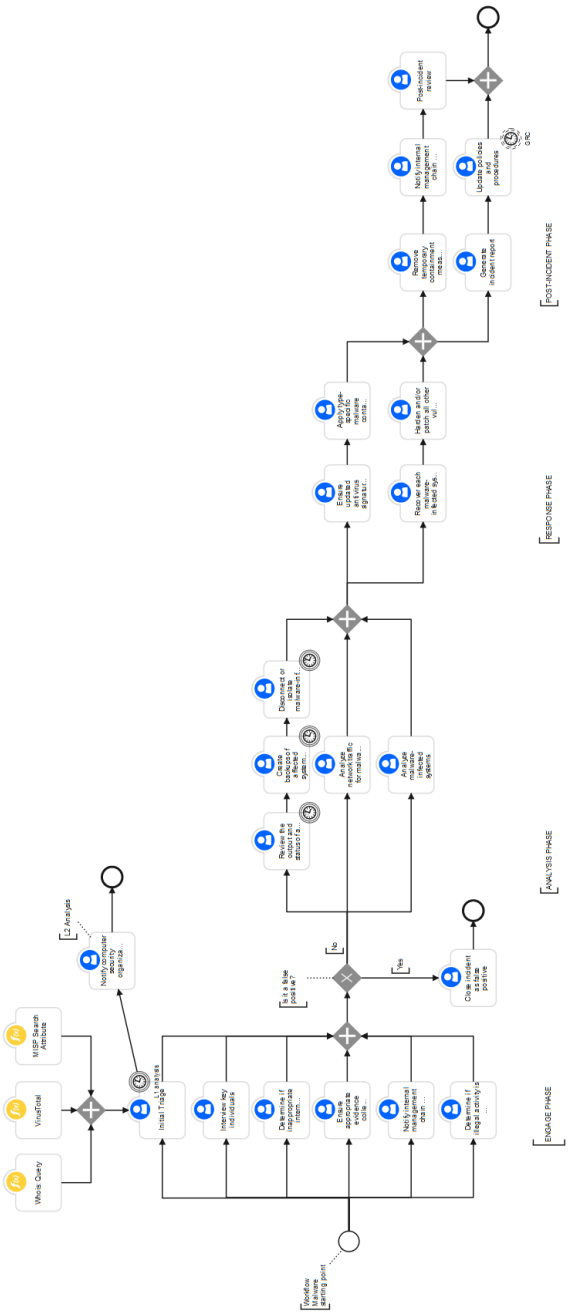

Figura 6.6. Workflow per la gestione di un incidente di tipo Malware

6.2 Ottimizzazione dei tempi di risposta di un incidente

Completato il workflow con le integrazioni delle funzioni ed i task accordati insieme al SOC manager, inizia la fase di testing.

Per simulare un incidente reale è stato utilizzato un tool, implementato dagli sviluppatori di Cybertech, che invia i log, relativi ad una offense già analizzata, al SIEM QRadar. Al fine di collaudare il flusso di lavoro, è stato imitato un incidente relativo al malware Emotet, descritto nel Capitolo 4.

Inviati i log a QRadar, si sono generate delle offense, rappresentate in Figura 6.7.

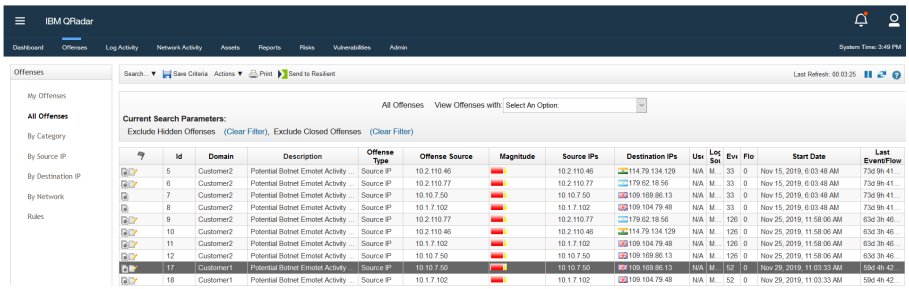

Figura 6.7. Offense generate dalla regola Emotet

Prendiamo in analisi l'offense con ID 17; i dettagli di questa vengono mostrati in Figura 6.8. Sono presenti la descrizione dell'incidente "Potential Botnet Emotet Activity", l'IP della macchina vittima "10.10.7.50" e l'IP malevolo contattato "109.169.86.13".

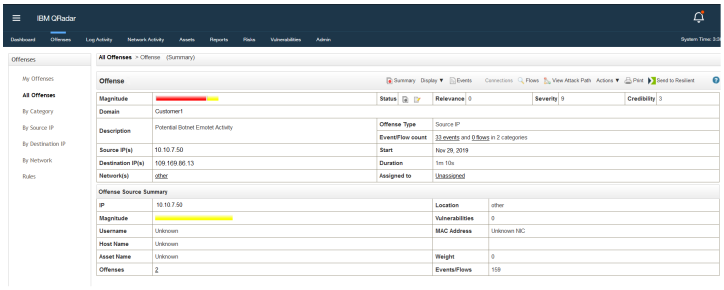

Figura 6.8. Dettagli di una offense generata dalla regola Emotet

Essendo stato messo in collegamento Resilient con QRadar, tutti i dettagli di questa offense vengono inviati in automatico alla piattaforma SOAR.

In Figura 6.9, viene mostrato l'incidente di Resilient con ID 2195, correlato alla offense di Qradar con ID 17.

Figura 6.9. Incidente contenente i dettagli della offense di QRadar

Tra tutti i dettagli viene inviata, anche, la tipologia "Malware" della offense relativa ad Emotet.

Quando l'incidente viene salvato nel database di Resilient, avendo creato in quest'ultimo la regola, "ogni volta che un incidente ha come tipologia Malware, scatta il workflow Malware response", si attiva automaticamente il flusso di lavoro descritto nella prima sezione di questo Capitolo.

Vengono generati automaticamente i task, che gli analisti dovranno svolgere (Figura 6.10), e vengono scritte, nelle note dell'incidente, le informazioni raccolte dalle threat intelligence, integrate con il SOAR.

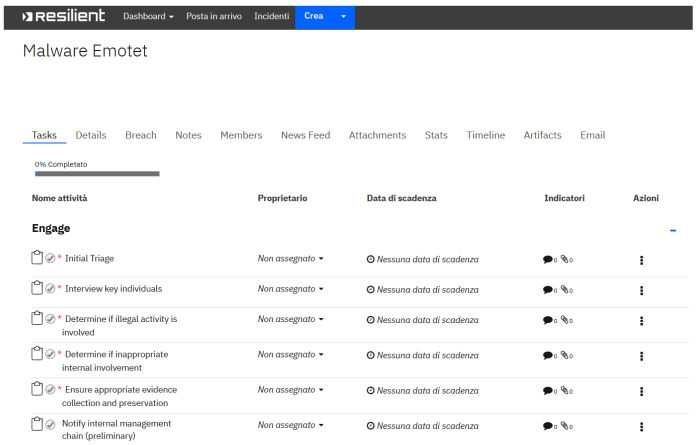

Figura 6.10. Creazione automatica dei task da seguire

Le informazioni presenti nella sezione relativa alle note, mostrate in Figura 6.11, riguardano alle fonti di threat intelligence integrate.

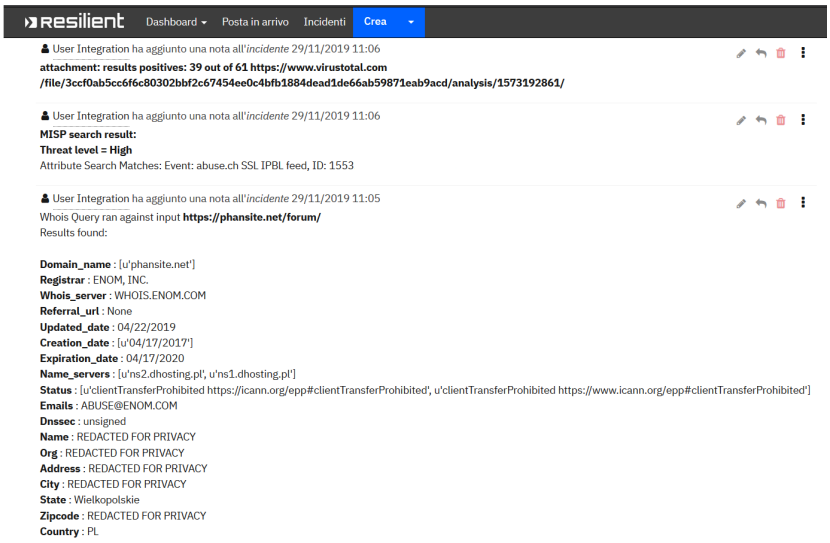

Figura 6.11. Risulato delle threat intelligence integrate

Virustotal riporta il punteggio dell'analisi effettuata nell'IP di destinazione ed il link della ricerca effettuata. MISP restituisce il livello di minaccia presente nella piattaforma e l'ID dell'evento associato. Whois riferisce i dettagli relativi al dominio contattato.

L'analista dovrà svolgere manualmente tutti i task presenti nelle fasi del workflow, descritti nella sezione precedente. Completate tutte le attività e le varie comunicazioni, in Resilient si avrà la situazione mostrata in Figura 6.12.

Completato il flusso di lavoro, l'analista chiude l'incidente con una risoluzione riportata nelle note.

Per la valutazione dei tempi del workflow, sono state effettuate due diverse tipologie di misurazione, ovvero:

- *i tempi di valutazione di un incidente;*
- *i tempi della chiusura di un incidente.*

Per la realizzazione di entrambe, sono stati coinvolti in totale dieci analisti. I tempi sono stati presi disponendo gli analisti in coppie; un elemento della coppia utilizzava Resilient mentre l'altro no. La valutazione è stata svolta sottoponendo a tutti e dieci la stessa offense.

La prima misurazione prende il tempo da quando l'offense viene generata a quando l'analista stabilisce se è un falso positivo oppure no.

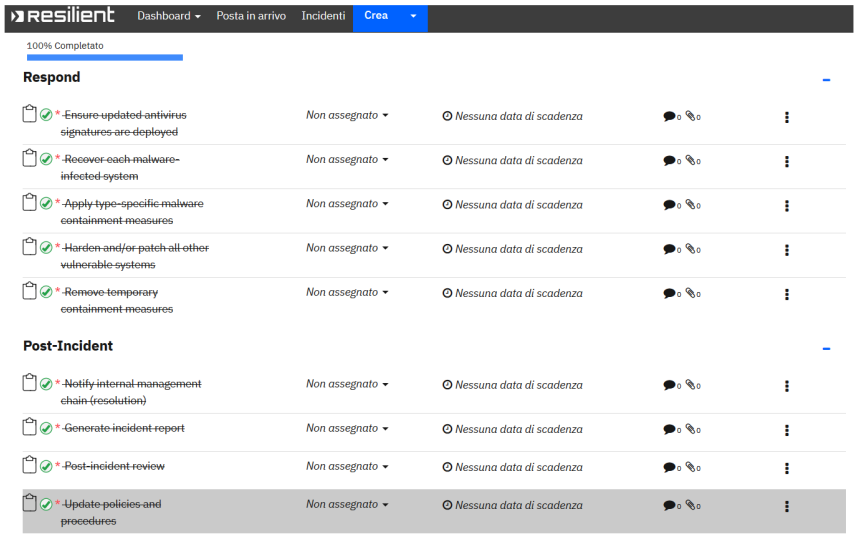

Figura 6.12. Completamento di tutti i task

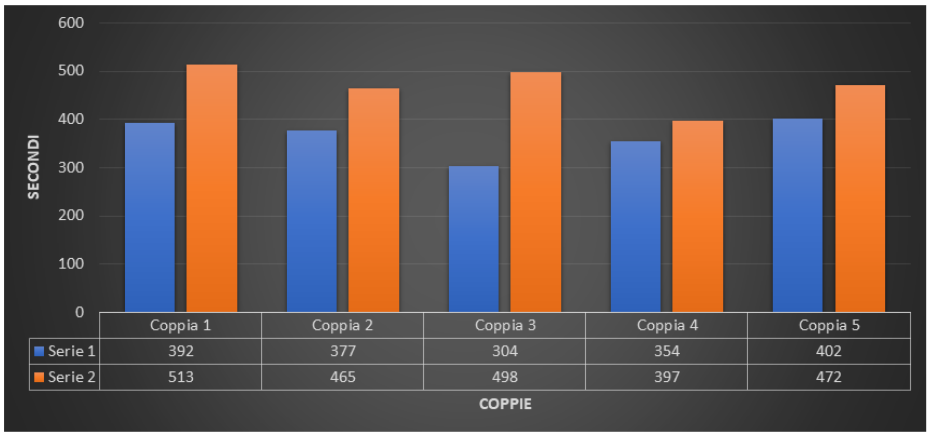

Figura 6.13. Differenza dei tempi per l'analisi di un incidente

I tempi delle coppie sono riportati nel grafico in Figura 6.13.

Le colonne in blu si riferiscono agli analisti che hanno utilizzato il SOAR; le colonne in arancione sono relative a quelli che non lo hanno utilizzato.

Gli analisti che non usufruiscono di Resilient perdono circa 200 secondi per

raccogliere le informazioni dalle fonti di threat intelligence e per scriverle in un unico punto.

Utilizzando Resilient si nota che il tempo per stabilire se un incidente è da considerare falso positivo oppure no si riduce di circa 100 secondi.

Nei tempi misurati, sono comprese le tempistiche di valutazione soggettive degli analisti.

La seconda misurazione prende il tempo da quando l'offense viene generata a quando l'analista chiude l'incidente. I tempi delle coppie sono riportati in Figura 6.14.

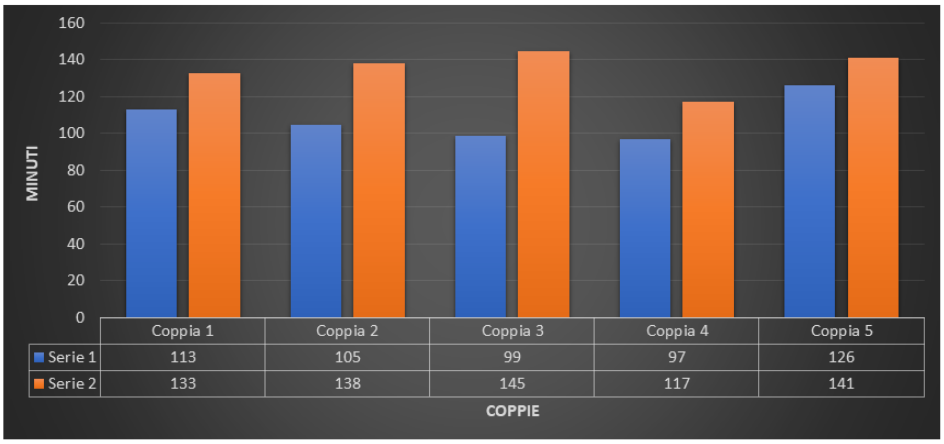

Figura 6.14. Differenza dei tempi per la chiusura di un incidente

Utilizzando il SOAR, si evidenzia che il tempo per chiudere un incidente si riduce, in media, di circa 25 minuti.

Le misurazioni sono state calcolate effettuando un'analisi di un incidente potenzialmente dannoso. Nella valutazione delle tempistiche, è necessario considerare, anche, i diversi livelli di competenza degli analisti.

In questo capitolo è stato descritto come implementare un workflow per la gestione di un incidente reale, è stato testato il funzionamento di questo ed infine vengono confrontate le tempistiche di analisi, di un incidente grave, utilizzando il SOAR Resilient oppure no.

7

Discussione

In questo capitolo verranno valutati i punti di forza, di debolezza, le opportunità e le minacce relative all'installazione e alle implementazioni effettuate in Resilient. Successivamente verranno descritte le lezioni apprese.

7.1 SWOT Analysis delle automatizzazioni tramite Resilient

L'analisi SWOT, conosciuta anche come matrice SWOT (Figura 7.1), è uno strumento di pianificazione strategica usato per valutare i punti di forza (Strengths), le debolezze (Weaknesses), le opportunità (Opportunities) e le minacce (Threats) di un progetto, di un'impresa o di ogni altra situazione in cui un'organizzazione o un individuo debba prendere una decisione per il raggiungimento di un obiettivo. L'analisi può riguardare l'ambiente interno, analizzando punti di forza e di debolezza, o esterno, analizzando minacce ed opportunità.

Figura 7.1. Diagramma della matrice SWOT

7.1.1 Punti di forza

IBM Resilient è la piattaforma leader per l'orchestrazione e l'automazione dei processi di risposta agli incidenti. Tale tecnologia si integra rapidamente con altre piattaforme ed altre tecnologie, già esistenti in un SOC, consentendo ad un unico hub intelligente di guidare un'azione rapida ed efficente. Le avanzate capacità di orchestrazione della piattaforma consentono una risposta adattiva alle complesse minacce informatiche.

Sicuramente uno dei punti di forza è la facilità di installazione e configurazione della piattaforma. Dopo l'installazione e la configurazione è stato possibile, fin da subito, effettuare l'escalation automatica delle offense del SIEM QRadar in Resilient, senza incorrere in problemi di traduzione dalle offense del SIEM agli incident del SOAR.

Non sono stati rilevati ritardi considerevoli dalla creazione delle offense alla generazione degli incident.

Un altro punto di forza è dato dalla possibilità di integrare Resilient con molteplici fonti di threat intelligence, che consente di raccogliere, da un bacino sempre più grande, informazioni relative a minacce mondiali.

Un'altra qualità che contraddistingue Resilient dalle altre piattaforme SOAR è l'add-on MSSP, con cui poter configurare, da un'organizzazione principale, tutte le organizzazioni dei clienti tramite cui creare facilmente workflow dinamici.

È stato possibile ottenere dei risultati concreti grazie alle macchine ed ai log messi a disposizione da Cybertech. L'obiettivo di questo lavoro di tesi era quello di riuscire ad automatizzare dei processi ripetitivi, così da ottimizzare i tempi di risoluzione di un attacco. Tramite Resilient si è riusciti a:

- raccogliere, in un'unica piattaforma, più informazioni provenienti da diverse fonti di threat intelligence;
- automatizzare il processo di enrichment di un incidente;
- implementare un flusso di lavoro allo scopo di guidare gli analisti verso la risoluzione di un incidente di tipo Malware.

7.1.2 Punti di debolezza

Per poter utilizzare queste tecnologie è necessario, ovviamente, avere la licenza di IBM Resilient, avente un costo non sostenibile per molte aziende operanti nell'ambito della Cybersecurity. Essendo il codice adattato ai requisiti di tale piattaforma, le funzioni implementate possono essere utilizzate soltanto in essa.

Allo scopo di effettuare tali implementazioni è necessaria una conoscenza approfondita dell'architettura di Resilient, delle sue componenti e della metodologia utile per sviluppare una propria integrazione.

7.1.3 Opportunità

L'opportunità offerta da queste implementazioni riguarda la riduzione dei tempi di risposta, liberando gli analisti dai task ripetitivi.

Di conseguenza, fornendo loro maggior tempo, possono concentrarsi e focalizzarsi sull'analisi di un incidente.

7.1.4 Minacce

Una minaccia reale di queste implementazioni è dovuta al codice stesso. Infatti, se fosse presente un errore di programmazione, essendo del codice proprietario, potrebbe restituire dei risultati errati ed indurre l'analista a trarre delle conclusioni sbagliate.

Un altro aspetto da tenere in considerazione è presente nello sviluppo dei workflow. Infatti, se non vengono considerate delle situazioni reali, a cui il SOC deve sottostare per rispettare gli SLA stabiliti con i clienti, durante la progettazione del flusso di lavoro, si rischia di incorrere in sazioni economiche.

7.2 Lezioni apprese

L'obiettivo di questo elaborato è stato quello di installare Resilient, collegarlo con il SIEM utilizzato dal SOC di Cybertech, implementare delle funzioni nella piattaforma, allo scopo di integrare le fonti di threat intelligence nella stessa. Successivamente è stato implementato un flusso di lavoro utile alla gestione di un incidente di tipo Malware.

Le procedure o le azioni più significative, che hanno permesso di raggiungere tali obiettivi, sono riassunte qui di seguito.

Innanzitutto bisogna comprendere le nozioni fondamentali di sicurezza informatica e le funzioni che svolge il SOC; in particolare gli argomenti appresi sono i seguenti:

- le funzioni, gli obiettivi e la strutturazione gerarchica di un SOC;
- i software QRadar, Resilient e le fonti di threat intelligence;
- le fasi di analisi di un incidente;
- i processi interni per la risoluzione delle diverse tipologie di attacchi;
- la gestione di incidenti gravi, con escalation dal primo al terzo livello del SOC.

Successivamente, collaborando con analisti, sviluppatori e SOC manager di Cybertech, si sono effettuate l'implementezione delle funzioni e del workflow, che hanno coinvolto il maggior numero di risorse, in quanto è stata necessaria una conoscenza approfondita di Resilient e del modo in cui integrare il codice esterno nella piattaforma.

8

Conclusioni

In questa tesi è stato presentato lo sviluppo di funzioni automatiche, utilizzando il Security Orchestration Automation and Response, per la riduzione dei tempi nei processi del Security Operation Center di Cybertech.

Nella prima parte, si è analizzata l'evoluzione delle minacce cyber nel panorama mondiale e si è visto come la Cybersecurity si sia sviluppata di conseguenza. In seguito alla crescente richiesta di sicurezza, si sono esaminati il progetto e la visione di Cybertech nella realizzazione di un Security Operation Center. Successivamente si sono delineate le componenti tecnologiche e le fasi operative indispensabili per il funzionamento di qualisasi SOC e si è visto come quest'ultimo sia organizzato gerarchicamente in tre livelli. In aggiunta, sono state descritte le caratteristiche che rendono il SOC di Cybertech distribuito ed eterogeneo e si sono illustrate le piattaforme ed i software che quest'ultimo utilizza.

Di seguito sono state descritte l'installazione e la configurazione della piattaforma Resilient e si è visto come sono stati messi in collegamento il SIEM QRadar ed il SOAR. In tale piattaforma, si sono implementate delle funzioni per effettuare l'enrichment automatico di un incidente ed è stato definito un workflow per guidare l'analista nella gestione di un incidente di tipo malware. Infine, si sono misurate, effettuando dei test, le tempistiche di risposta di un incidente senza e con l'utilizzo di Resilient.

I risultati hanno mostrato un'ottimizzazione dei tempi di risposta quando veniva impiegata la tecnologia SOAR. Contrariamente a quanto si possa pensare, prima di effettuare l'installazione del SOAR bisogna comprendere le esigenze del SOC. Inoltre tale tecnologia ha un costo sia di licenza che di risorse non sottovalutabile. La scelta dell'installazione dipenderà soprattutto dagli SLA stabiliti con i propri clienti. Se perdere in media 25 minuti durante un'analisi non comporta nessuna sanzione, il SOAR si rivela un costo inutile da sostenere.

Il lavoro esaminato in questo elaborato descrive la fase iniziale dell'utilizzo della tecnologia SOAR in un SOC e, come tale, deve evolversi ed innovarsi.

Le implementazioni future, in Resilient, prevederanno le integrazioni con più fonti di threat intelligence, in modo tale da avere un bacino più ampio di IoC, utili per lo svolgimento delle analisi degli incidenti.

Altre implementazioni prevederanno l'automatizzazione, da parte degli analisti, di processi ripetitivi, come inviare e-mail o creare dei report una volta conlcusa

l'analisi.

In un futuro non troppo lontano, gli sviluppi riguarderanno l'applicazione dell'Intelligenza Artificiale per aiutare gli analisti; ad esempio, si potrebbero applicare algoritmi di machine learning per la riduzione del numero dei falsi positivi e per rivelare casi simili già analizzati in precedenza, con la stessa gestione di chiusura dell'incidente.

Riferimenti bibliografici

1. Syrus Agency. *General Data Protection Regulation, diritto all'oblio*. 2018.
2. Cert-Pa. *Emotet, il trojan bancario si evolve ed irrompe minacciosamente*. Cert-Pa, 2018.
3. Pratyusa K. Manadhata and Jeannette M. Wing. *An Attack Surface Metric*. 2011.
4. Martina Petrucci Marta Cogode. *Il cybersecurity act: i vantaggi del nuovo regolamento europeo di certificazione della cyber-sicurezza per le tecnologie dell'informazione e della comunicazione*. 2019.
5. Paolo Giudice Andrea Piazza Giovanni Reccia Nunzia Ciardi, Corrado Giustozzi. *Rapporto Clusit 2019*. 2019.
6. Telekom Security on Github. *T-Pot - The All In One Honeypot Platform*.
7. Tim Grance Karen Scarfone Paul Cichonski, Tom Millar. *Computer Security Incident Handling Guide*. NIST, 2012.