ALMA MATER STUDIORUM – UNIVERSITÀ DI BOLOGNA
CAMPUS DI CESENA

Dipartimento di Informatica – Scienza e Ingegneria
Corso di Laurea Triennale in Ingegneria e Scienze Informatiche

Analisi di integrazione su sistemi di Intrusion Detection e Incident Handling in ambito enterprise

Tesi di laurea in
Reti di Telecomunicazione

Relatore
Prof. Franco Callegati

Candidato
Pietro Mazzini

Correlatore
Dott. Alessandro Molari

Terza Sessione di Laurea
Anno Accademico 2019-2020

Sommario

Questa tesi ha l'obiettivo di presentare un sistema di Intrusion Detection, Incident Handling e Response nei suoi processi produttivi, organizzativi e manageriali e in quelli puramente pratici ed implementativi.

Il nome di questo progetto è OSSIHR [1] (Open Source System for Incident Handling and Response).

0.1 Struttura della tesi

La tesi è composta da quattro capitoli.

Il capitolo 1 contiene un'introduzione ai concetti, alle sigle ed ai processi che caratterizzano le discipline di Intrusion Detection, Incident Handling e Incident Management.

Nel capitolo 2 è analizzato lo stato dell'arte sulla materia e vengono definiti i meccanismi di un sistema di Incident Handling che possa essere adottato in ambito enterprise. Le integrazioni dei software che sono stati utilizzati e l'architettura di OSSIHR sono documentati ed approfonditi nel capitolo 3.

I margini di miglioramento e le criticità del sistema in oggetto sono evidenziate nel capitolo 4 che include anche uno studio di paragone fra il sistema open source proposto ed altri sistemi closed source.

Ad Alice e Franco, i miei genitori, che mi hanno dato la possibilità di arrivare fin qui sorreggendomi nei momenti di difficoltà.

Indice

Capitolo 1

Introduzione

1.1 CSIRT: Computer Security Incident Response Team

L'acronimo CSIRT indica "un gruppo di lavoro o un'organizzazione che fornisce servizi e supporto per prevenire, gestire e rispondere a problematiche di sicurezza inerenti i sistemi informatici" [2].

In relazione alla qualità ed al livello del servizio erogato si classificano tre tipologie di CSIRT in ordine crescente: **security teams**, **internal CSIRTs** e **coordinating CSIRTs**

- In un security team il personale disponibile (amministratori di sistema, di rete e di sicurezza) gestisce gli eventi di sicurezza in maniera isolata, in aggiunta alle mansioni e responsabilità di base.

- Un internal CSIRT è composto da professionisti ai quali viene assegnata specificamente la responsabilità e l'incident handling, cioè il processo di gestione di un attacco informatico. Questo CSIRT è parte integrante dell'organizzazione aziendale. Per esempio la Siemens commercial organization è il committente del Siemens Computer Emergency Response Team.

- Un coordinating CSIRT coordina la gestione delle problematiche e delle vulnerabilità e la trasmissione delle informazioni tra le organizzazioni interne ed esterne all'azienda attivate nel processo di incident handling (differenti CSIRT, venditori, esperti di sicurezza e forze dell'ordine).

1.2 Incident management, handling e response

1.2.1 Incident handling

Un incident è un evento che potrebbe determinare una perdita di informazioni o un disservizio relativo alle operazioni ed alle funzioni svolte da un'azienda. L'incident handling è il procedimento attivato per gestire e risolvere i problemi di sicurezza a livello informatico. Questo processo definisce le attività atte a identificare, analizzare e correggere eventuali incident, prevenendo la possibilità che si ripropongano.

L'incident handling include quattro principali processi [3]:

- "detecting and reporting": ricezione ed analisi delle informazioni relative agli eventi, report di incident e alert;
- "triage": classificazione ed assegnazione di priorità agli incident;
- "analysis": inquadramento su ciò che è accaduto, su quale impatto o danno ha arrecato al sistema e sui processi di risoluzione o mitigazione che devono essere adottati;
- "response": attivazione di procedure volte a risolvere o mitigare un incident, coordinare e diffondere informazioni ed implementare strategie per evitare che l'incident si verifichi una seconda volta. L'incident response rappresenta l'atto conclusivo dell'incident handling.

1.2.2 Incident management

Come è rappresentato nella fig. 1.1, il termine "incident management" include tutti i servizi che un CSIRT può offrire ad un committente, in aggiunta all'incident handling.

Oltre a rispondere ad un ipotetico problema di sicurezza, l'incident management promuove attività volte a prevenire gli incident, fornendo linee guida contro potenziali rischi e minacce. Ad esempio fanno parte di queste attività l'identificazione precoce delle vulnerabilità nel software e la formazione degli utenti/dipendenti in tema di sicurezza informatica.

1.2.3 Intrusion detection

Si definisce intrusion detection il monitoraggio del sistema informatico al fine di rilevare precocemente minacce, violazioni di policy di sicurezza dei computer o individuare non conformità nelle configurazioni di sicurezza [4].

Si possono identificare diverse cause di incident quali malware (worms, spyware...), soggetti che violano i sistemi mediante Internet, utenti autorizzati che abusano dei loro privilegi o tentano di acquisirne altri ai quali non potrebbero accedere. Alcuni alert sono di natura colposa, altri invece sono incidentali o casuali.

Un Intrusion Detection System (IDS) è un software che automatizza il processo di intrusion detection, allertando il gruppo di professionisti che si occupa della sicurezza. Un Intrusion Prevention System (IPS) è un software che alle capacità di un Intrusion Detection System aggiunge quella di bloccare o risolvere alcuni incident.

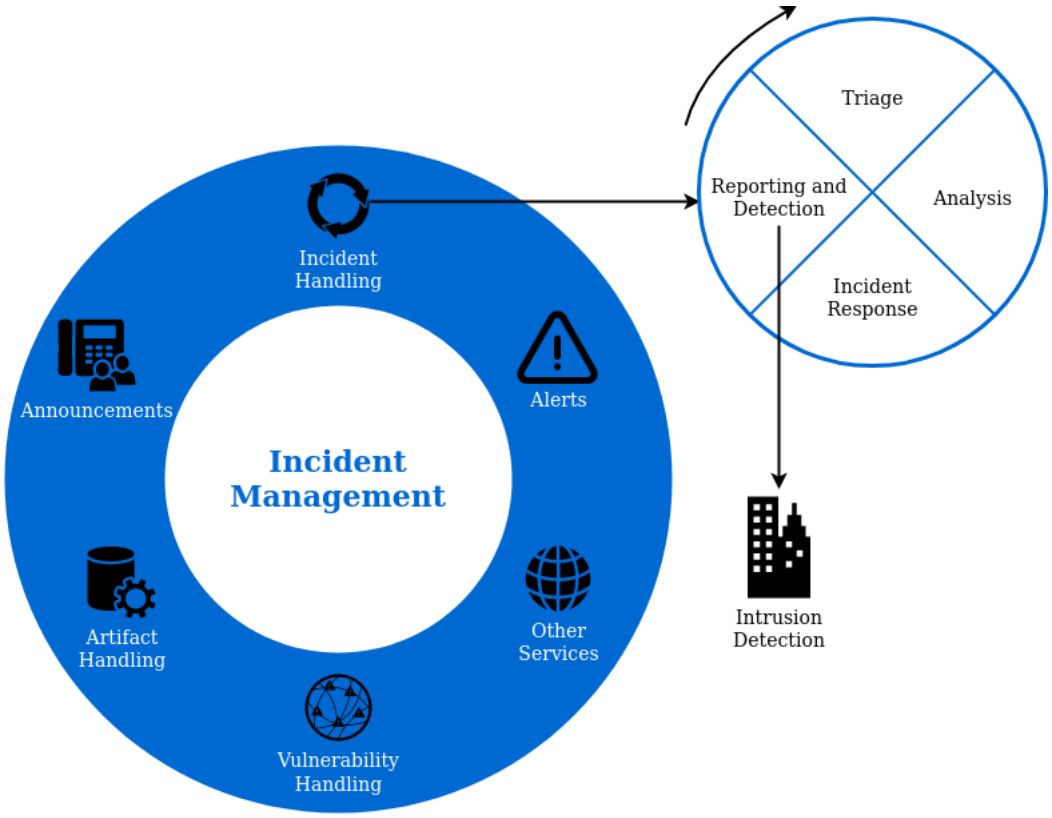

Figura 1.1: Correlazione ed integrazione tra Incident Management, Handling, Response e Intrusion Detection.

Capitolo 2

Stato dell'Arte

2.1 Servizi gestiti dai CSIRT

I CSIRT possono offrire tre categorie di servizi come visibile nella tabella 2.1 [5].

Servizi reattivi	**Servizi proattivi**	**Servizi di gestione della qualità della sicurezza**
Alert e warning Incident handling - Analysis - Response on site - Response support - Response coordination Vulnerability handling - Analysis - Response - Response coordination Artifact handling - Analysis - Response - Response coordination	Announcements Technology watch Security audits or assesments Configuration and maintenance of security tools, applications, infrastructures and services Developement of security tools Intrusion detection services Security-related information dissemination	Risk analysis Business continuity and disaster recovery planning Security consulting Awareness building Education/training Product evaluation or certification

Tabella 2.1: Servizi gestiti dai CSIRT.

Di seguito si analizzano in dettaglio le categorie e sottocategorie sopracitate.

- Servizi reattivi: si tratta di *procedure attivate da un evento* o da una richiesta, come per esempio il report di un host compromesso, la diffusione di codice malevolo, vulnerabilità nel software o una notifica generata da un IDS o un sistema di logging. Queste attività rappresentano la parte principale del lavoro di un CSIRT.

- Servizi proattivi: questi servizi forniscono assistenza ed informazioni per la preparazione, protezione e messa in sicurezza dei sistemi del committente *prima che si verifichi un attacco o un problema*. La qualità di questo servizio è definita dal numero di incident anticipati ed evitati.

- Servizi di gestione della qualità della sicurezza: questi servizi mirano a *migliorare le performances nei procedimenti di sicurezza aziendale*.

2.1.1 Servizi reattivi

Sono compresi in questa categoria il servizio di alert e warning, l'incident handling, il vulnerability handling e l'artifact handling. Tutte queste attività si sviluppano in risposta ad un attacco o ad un'intrusione.

Alert e warning

Consiste nel diffondere dati ed informazioni che descrivono l'attacco di un intruso, le vulnerabilità di sicurezza, la presenza di malware o abusi informatici, fornendo qualsiasi aiuto per gestire il problema risultante. L'alert o il warning inviati al personale aziendale contengono linee guida per proteggere o ripristinare i sistemi infetti.

Incident handling

Come già espresso nella sezione 1.2.1 le attività di detecting, triaging, analyzing e responding sono parte fondante dell'incident handling. Nell'insieme questo servizio può includere le seguenti azioni:

- assumere provvedimenti per proteggere sistemi e reti minacciate da azioni di intrusione;

- fornire soluzioni e strategie di mitigazione ad alert ed incident;

- indagare sull'attività dell'intruso in altre parti della rete;

- filtrare ed analizzare il traffico di rete;
- riparare i sistemi e rimetterli in produzione.

Detect Questa fase consiste nella rilevazione di possibili incident ed è svolta principalmente in automatico da IDS, SIEM (Security Information and Event Management, simili agli IDS), antivirus e software di file integrity checking; questi ultimi possono rilevare i cambiamenti apportati ad importanti file mediante il calcolo dei checksum.

Triage L'assegnazione di priorità agli incident è il punto cruciale dell'intero processo di incident handling. I fattori da considerare per eseguire correttamente questo lavoro sono l'impatto funzionale, quello sull'informazione e la recuperabilità da un incident [6].

- *Impatto funzionale*: gli incident che hanno come obiettivo i sistemi del reparto tecnologico interessano tipicamente le funzionalità commerciali che questi sistemi offrono; il risultato è un impatto negativo sugli utenti del sistema stesso. Gli addetti alla sicurezza devono considerare come l'incident influirà sulle funzionalità del sistema attaccato ed anche i problemi futuri che questo incident genererebbe se non arginato per tempo.
- *Impatto sull'informazione*: gli incident potrebbero interessare la confidenzialità, l'integrità e la disponibilità delle informazioni aziendali. Ad esempio un agente malevolo potrebbe esfiltrare informazioni sensibili. Gli addetti alla sicurezza devono considerare come questa fuga di informazioni impatterà sull'organizzazione e sulle organizzazioni partner.
- *Recuperabilità da un incident*: la dimensione dell'incident ed il tipo di ambiti interessati determinano il tempo e le risorse necessarie per risolvere il problema. Gli addetti alla sicurezza devono considerare lo sforzo necessario per risolverlo e valutarne i benefici conseguenti. In alcuni casi rimediare all'incident non è possibile o sarebbe inutile a meno che non impedisca che un problema analogo si verifichi nuovamente. In altri casi un incident potrebbe richiedere più risorse di quante l'organizzazione abbia a disposizione.

Analysis Rappresenta l'analisi di tutte le informazioni disponibili compreso le prove a sostegno o gli artefatti collegati ad un incident o ad un evento. Questa attività include l'analisi del flusso di rete, del funzionamento degli host e dei log delle applicazioni, dei tool utilizzati dall'intruso, del codice malevolo e di qualsiasi altra informazione utile alla risoluzione del problema. Identificare la portata, il

campo e la natura dell'incident, l'entità del danno causato e le possibili strategie di risposta o soluzioni alternative sono gli obiettivi di questa fase. Il CSIRT valuta possibili correlazioni tra i vari incident e determina andamenti analoghi, schemi ricorrenti o tracce distintive dell'intruso.

Due sottopratiche utilizzate nel contesto dell'incident analysis sono la *forensic evidence collection* e il *tracking*. La prima consiste nella raccolta, la conservazione, la documentazione e l'analisi di prove relative ad un sistema compromesso al fine di rilevarne i cambiamenti e ricostruire la cronologia degli eventi che ha portato alla sua compromissione. Prevede le pratiche di clonazione di hard disk delle macchine infette, i controlli riguardanti i cambiamenti subiti dai sistemi (es. installazione/rimozione di programmi, file, servizi e utenti), la verifica dei processi in esecuzione, delle porte aperte e la scansione dei sistemi in cerca di malware e strumenti di intrusione. Questo processo deve rispettare i criteri di validità e di integrità imposti dalla legge.

Il tracciamento dell'origine di un'intrusione, l'identificazione dei sistemi ai quali l'intruso ha avuto accesso ed i metodi utilizzati compongono il tracking. Solitamente questa attività viene eseguita dal CSIRT in collaborazione con enti esterni quali per esempio le forze dell'ordine e gli Internet Service Providers (ISP).

Response Si divide in tre categorie, in base al tipo di coinvolgimento.

- *On site*: il CSIRT fornisce assistenza sul campo per aiutare i committenti a risolvere un incident, analizza fisicamente i sistemi interessati e conduce le operazioni di riparazione e ripristino. Se la postazione di lavoro del CSIRT non è nello stesso luogo dell'azienda del committente i membri del CSIRT dovranno spostarsi fisicamente nel sito di interesse per attuare la strategia di risposta.

- *Support*: il CSIRT assiste e guida a distanza le vittime dell'attacco nel ripristino dei sistemi utilizzando il telefono, la posta elettronica o fornendo documentazione idonea.

- *Coordination*: il CSIRT coordina vari gruppi di lavoro per conseguire la fase di response. Fra questi sono compresi le vittime dell'attacco, gli altri siti coinvolti ed eventualmente gli enti che forniscono supporto informatico alle vittime (come gli ISP, altri CSIRT e amministratori di sistema e di rete). La necessità di un supporto legale porterà ad una collaborazione con i rappresentanti legali dell'azienda, con il reparto delle risorse umane e con quello delle relazioni con il pubblico, fino ad includere anche le forze dell'ordine.

Vulnerability handling

Include la ricezione di informazioni e report riguardanti eventuali vulnerabilità hardware e software, i loro effetti e lo sviluppo di strategie di risposta per la loro rilevazione e risoluzione. Il servizio viene suddiviso in tre categorie in base al tipo di attività svolte e di assistenza fornita: analysis, response e response coordination.

- *Analysis*: il CSIRT esegue analisi di vulnerabilità hardware e software al fine di identificare dove è collocata la criticità e come potrebbe essere sfruttata. Fanno parte di questo processo la review di codice sorgente, l'utilizzo di un debugger per determinare in che linea di codice il problema emerge ed il tentativo di riprodurre la falla su un sistema di test.

- *Response*: questo servizio formula una risposta utile a mitigare o riparare una vulnerabilità, sviluppando patch o applicando fix. La notifica ai membri aziendali della strategia di mitigazione adottata è una pratica consigliabile.

- *Response coordination*: il CSIRT comunica la vulnerabilità rilevata alle diverse parti dell'azienda committente, trasmette informazioni su come ripararla o mitigarla e, di seguito, verifica la corretta applicazione della strategia di risposta. Le attività includono l'assistenza nell'analisi o nel report di una vulnerabilità, la coordinazione nel rilascio dei corrispondenti documenti o patch e la sintesi delle analisi fatte da differenti gruppi. A queste attività di base potrebbero aggiungersi il mantenimento di un archivio pubblico o privato di vulnerabilità note e la corrispondente strategia di risposta.

Artifact handling

Un artefatto è un file trovato in un sistema sottoposto ad un attacco.

Gli artefatti possono includere virus, trojan horse, worms, exploit scripts e rootkits. L'artifact handling studia la natura, il funzionamento e lo scopo degli artefatti, con l'obiettivo di sviluppare una strategia di risposta e di difesa nei confronti dello stesso. Come per il vulnerability handling, anche in questo caso riferendosi al tipo di attività eseguita si possono riconoscere le tre modalità di servizio precedentemente citate.

- *Analysis*: il CSIRT esamina a basso livello ogni artefatto trovato nel sistema. L'analisi effettuata potrebbe portare all'identificazione del tipo e della struttura del file mediante la comparazione con artefatti noti e/o la pratica di reverse engineering.

- *Response*: questo servizio definisce le azioni da effettuare per rilevare e rimuovere gli artefatti dal sistema e per prevenire la loro installazione. Questo

risultato può essere ottenuto creando delle signatures ed aggiungendole al software antivirus o all'IDS.

- *Response coordination*: consiste nella sintesi e nella condivisione con altri ricercatori, CSIRT ed esperti di sicurezza dei risultati delle analisi e delle strategie di risposta inerenti gli artefatti. È importante mantenere un archivio pubblico di artefatti conosciuti, del loro impatto e della loro strategia di risoluzione: ciò risulta molto utile per la creazione di una artifact intelligence.

2.1.2 Servizi proattivi

Sono i servizi preventivi pensati per migliorare l'infrastruttura ed i processi di sicurezza di un committente prima che un incident avvenga. Tra questi annoveriamo numerose procedure di seguito descritte.

Announcements

Sono alert d'intrusione, warning di vulnerabilità e avvisi di sicurezza. Questi servizi abilitano i committenti a correggere eventuali criticità dei propri sistemi e reti, prima che possano essere sfruttate.

Tecnhnology watch

È il monitoraggio che il CSIRT attiva sulle nuove tecnologie sviluppate, sull'attività degli intrusi e le tendenze collegate al fine di identificare future minacce. Gli ambiti analizzati possono includere le decisioni legislative, le minacce sociopolitiche e le tecnologie emergenti. Il risultato di questo servizio è la produzione di linee guida, annunci e suggerimenti mirati alla risoluzione di problemi dal medio al lungo termine. Si ottiene quindi un servizio di intelligence/raccolta informazioni.

Security audits or assessments

Rappresenta l'analisi dettagliata dell'infrastruttura di sicurezza di un'azienda o ente e può includere anche una revisione delle pratiche di sicurezza a livello organizzativo. Esistono vari tipi di assessments applicabili.

- Revisione dell'infrastruttura: è la procedura manuale di revisione dell'hardware, delle configurazioni software, dei router, del firewall, dei server, e dei dispositivi desktop per assicurarsi che siano conformi alle politiche e alle pratiche di sicurezza dell'azienda.

- Revisione delle best practice: consiste nell'intervistare gli impiegati e gli amministratori di sistema e di rete per determinare se le pratiche di sicurezza che seguono sono conformi a quelle definite dall'azienda.

- Scansione: è il processo che determina quali sistemi e reti sono vulnerabili mediante l'ausilio di scanner di vulnerabilità.

- Penetration testing: rappresenta il test della sicurezza di un infrastruttura simulando attacchi ai suoi sistemi e reti. Possono essere inclusi in questa pratica attacchi effettuati di persona mediante ingegneria sociale oltre che aggressioni informatiche.

Per realizzare dei security audits è necessaria l'approvazione dei dirigenti aziendali. Alcuni di questi approcci potrebbero essere proibiti da politiche aziendali, altri potrebbero avere implicazioni legali. Le attività che superano i limiti geografici (es: nazionale, statale, provinciale...) potrebbero essere soggette a legislazione differente. Lo sviluppo di protocolli di security assessment e la formazione continua della squadra che si occupa di questo lavoro sono di estrema importanza. Questo servizio potrebbe anche essere affidato ad aziende esterne.

Configuration and maintenance of security tools, applications, infrastructures, and services

Comprende la definizione di linee guida centrate sulla configurazione ed il mantenimento di tool, delle applicazioni ed in generale della sicurezza dell'ambiente informatico utilizzato. Oltre a ciò il CSIRT deve curare la produzione di aggiornamenti e la manutenzione dei servizi di sicurezza (quali IDS, sistemi di monitoraggio di rete, firewall, virtual private networks). Il CSIRT ha anche il ruolo di notificare qualsiasi problema o vulnerabilità riguardante i software utilizzati ai membri del gruppo di management aziendale.

Development of security tools

Questo attivtià prevede lo sviluppo di strumenti software necessari per il committente o per il CSIRT stesso (per esempio lo sviluppo di patch di sicurezza per software custom utilizzato dall'azienda o di strumenti che estendono le funzionalità di già esistenti sistemi di anti-intrusione quali IDS o vulnerability scanner).

Intrusion detection services

I CSIRT che svolgono questo servizio effettuano la review dei log degli IDS, inizializzano la response per ogni evento sopra una certa soglia di pericolosità o inoltrano

gli alert ad un altro dipartimento seguendo gli accordi di servizio. Questo lavoro potrebbe risultare complicato per la grande mole di dati raccolti da analizzare; per questo motivo in molti casi vengono utilizzati strumenti specializzati per sintetizzare e interpretare le informazioni identificando falsi allarmi, attacchi o eventi di rete.

Security-related information dissemination

Questo servizio che deve fornire ai committenti un archivio facilmente consultabile e ricco di informazioni utili per il miglioramento della sicurezza aziendale, include:

- linee guida per il report di informazioni al CSIRT e suoi contatti
- alert, warning, e altri annunci
- documentazione relative alle pratiche adottate
- guida generale alla sicurezza dei computer aziendali
- politiche e procedure
- informazioni sullo sviluppo di patch e la loro distribuzione
- statistiche sugli incident

Questo archivio è mantenuto dal CSIRT o da altre parti dell'organizzazione e può conservare anche informazioni di terzi (altri CSIRT, aziende, ed esperti di sicurezza).

2.1.3 Servizi di gestione della qualità della sicurezza

Questi servizi sono utilizzati per migliorare la sicurezza generale di un'azienda e non sono garantiti esclusivamente dai CSIRT. Il valore aggiunto che un CSIRT può determinare è dovuto ai servizi reattivi e proattivi precedentemente applicati.

Le seguenti descrizioni spiegano come l'esperienza dei CSIRT può migliorare ognuno di questi servizi di gestione della qualità della sicurezza.

Risk analysis

I CSIRT che operano in questo servizio possono fornire assistenza mediante attività di analisi del rischio mirate a perfezionare i nuovi sistemi ed i processi aziendali o valutare minacce e attacchi contro i sistemi e le risorse dei committenti.

Business continuity and disaster recovery planning

Le raccomandazioni dei CSIRT riguardo alle modalità di risposta agli incident possono assicurare la continuità delle operazioni aziendali.

Security consulting

Un CSIRT potrebbe essere chiamato in causa per il suggerimento o l'identificazione dei requisiti per l'acquisto, l'installazione, o la messa in sicurezza di nuovi sistemi, dispositivi di rete, software o processi aziendali.

Awareness building

I CSIRT possono aiutare in modo considerevole gli utenti non solo migliorando la comprensione dei problemi di sicurezza ma anche aiutando ad eseguire in maniera più sicura le operazioni giornaliere. Questo può ridurre il verificarsi di attacchi e aumentarne le probabilità di segnalazione da parte dei dipendenti, riducendo i tempi di ripristino e le eventuali perdite.

Per migliorare la consapevolezza dei committenti i CSIRT producono articoli, poster, newsletter o altro materiale informativo atto a spiegare le pratiche di sicurezza e fornire consigli sulle precauzioni da prendere. Questa attività include l'organizzazione di seminari e di aggiornamenti sulle più recenti procedure di sicurezza e le potenziali minacce. È di estrema importanza e qualità che il CSIRT coinvolto in questa fase produca report per i gruppi di management, non solo per discutere sullo stato dell'azienda ma anche per consigliare i dirigenti sull'adozione di idonee precauzioni di sicurezza.

Education/training

Il training consiste nell'educare i committenti sulle problematiche di sicurezza dei computer mediante seminari, laboratori, corsi e guide. Gli argomenti includono linee guida su come segnalare un incident, sui metodi di risposta appropriati, sugli strumenti di risposta, sui metodi di prevenzione, sull'educazione riguardo l'ingegneria sociale, lo SPAM e i virus e altre informazioni necessarie a proteggere, rilevare, segnalare e rispondere a incident di sicurezza.

Product evaluation or certification

Il CSIRT deve effettuare valutazioni e certificazioni su strumenti, applicazioni o altri servizi per assicurare la sicurezza del sistema e la sua conformità alle pratiche organizzative di sicurezza dell'azienda.

Capitolo 3

Componenti di OSSIHR ed integrazione

Il sistema oggetto di questa tesi prende il nome di OSSIHR (Open Source Software for Incident Handling and Response).

3.1 Componenti

OSSIHR è un agglomerato di vari software gratuiti ed open source che, integrandosi, forniscono funzioni utili per il processo di incident handling.

I software principali che compongono OSSIHR attualmente sono sette:

1. Wazuh [7], [8]
2. OwlH [9]
    - Moloch [10]
    - Suricata [11]
    - Zeek [12]
3. Elastic Stack [13]
    - Elasticsearch [14]
    - Kibana [15]
    - Beats [16]
4. AIL-Framework [17]
5. Cortex [18]

6. MISP [19]

7. TheHive [18]

3.1.1 Wazuh

Wazuh è un Host Intrusion Detection System (HIDS) che si occupa di threat detection, security monitoring, incident response e regulatory compliance. Può essere utilizzato per monitorare gli endpoint, i servizi cloud ed i container e per aggregare ed analizzare dati da sorgenti esterne.

I due componenti che costituiscono il cuore di Wazuh sono gli *agent* ed il *manager*. Gli agent sono software che vengono installati sulle macchine da monitorare ed inviano le informazioni raccolte al manager che ha il compito di analizzarle ed archiviarle.

Wazuh fornisce le seguenti funzionalità:

- *security analytics* → raccolta, aggregazione, indicizzazione ed analisi delle informazioni di sicurezza aiutando a rilevare intrusioni, minacce ed inadeguatezze;

- *intrusion detection* → scansione delle macchine da monitorare in cerca di malware, rootkit ed anomalie. Possono essere rilevati file e processi nascosti, listener di rete non registrati o inconsistenze nelle risposte alle system call. È inoltre eseguita un'analisi sulle intrusioni mediante un approccio signature-based, in cerca di Indicator Of Compromise (IOC, elementi che con alta probabilità indicano un'intrusione informatica);

- *log data analysis* → salvataggio e successiva analisi dei log dei sistemi operativi e delle applicazioni mediante un approccio rule-based. In questo modo vengono rilevati errori di sistema o delle applicazioni, configurazioni errate, attività malevole, violazione di politiche, ecc;

- *file integrity monitoring* → monitoraggio del file system rilevando cambiamenti nel contenuto, nei permessi e nelle proprietà dei file. Vengono inoltre identificati gli utenti e le applicazioni usate per creare o modificare i file stessi;

- *inventory management* → controllo in tempo reale dei software installati e dei processi in esecuzione sugli endpoint sorvegliati;

- *vulnerability detection* → raccolta di informazioni sui software installati. I dati ottenuti vengono poi comparati con dei database di Common Vulnerabilities and Exposure (CVE) al fine di identificare i programmi vulnerabili;

- *configuration assessment* → monitoraggio delle configurazioni di sistema e delle applicazioni per accertare che siano coerenti con le politiche di sicurezza stabilite;

- *incident response* → produzione di contromisure alle minacce. È possibile bloccare automaticamente l'accesso ad un sistema quando determinati criteri sono riconosciuti o eseguire a distanza comandi sulle macchine monitorate;

- *regulatory compliance* → esecuzione di controlli di sicurezza per rientrare negli standard tecnici e industriali. Wazuh è ampiamente utilizzato dalle compagnie finanziarie per soddisfare il requisito di Payment Card Industry Data Security Standard (PCI DSS). Sovrintende inoltre a molti altri standard quali per esempio GPG13 o GDPR.

- *cloud security monitoring* → monitoraggio le infrastrutture cloud a livello delle Application programming interface (API) ed applicazione di regole per valutare la configurazione dell'ambiente;

- *containers security* → controllo dei container, delle immagini, dei volumi e delle reti di Docker per rilevare minacce, vulnerabilità ed anomalie. Ad esempio vengono attivati alert nel caso in cui alcuni container siano in esecuzione in modalità privilegiata o vengano apportati cambiamenti a volumi o immagini persistenti.

3.1.2 OwlH

OwlH è un Network Intrusion Detection System (NIDS) utilizzato per gestire, analizzare e rispondere a minacce ed anomalie di rete. L'architettura di questo software prevede due componenti principali: i *node* - elementi incaricati di raccogliere ed analizzare il traffico di rete - ed il *master* - punto di gestione di tutti i node - .

OwlH fornisce numerose funzionalità:

- gestione e visualizzazione centralizzata della configurazione delle regole di sicurezza di rete e dei node;

- servizio di Software network TAP (STAP) utilizzato per raccogliere il traffico di rete da sorgenti eterogenee;

- analisi di conformità rispetto agli standard di sicurezza quali per esempio PCI-DSS;

- analisi forense del traffico di rete con l'ausilio di Moloch. Questo software si occupa di indicizzare, catalogare, graficare ed arricchire il traffico di rete giunto in input da un'interfaccia o da file pcap e, di seguito, proporlo all'utente mediante una visualizzazione semplice e di facile navigazione;
- analisi di sicurezza e monitoraggio del traffico di rete mediante Suricata e Zeek;
- integrazione con Wazuh. Quest'ultimo servizio è approfondito nella sezione 3.2

3.1.3 Elastic Stack

Elastic è uno stack software che consente di aggregare log derivanti da tutti i sistemi e dalle applicazioni di un'ipotetica azienda; inoltre offre la possibilità di analizzarli e creare visualizzazioni utili al monitoraggio dell'infrastruttura, alla risoluzione di problemi, alle analisi di sicurezza ecc.

L'Elastic stack in questione è composto dai seguenti tre software.

1. Elasticsearch: motore di ricerca ed analisi basato sul formato JSON, distribuito, scalabile e RESTful. È il cuore dell'Elastic Stack e si occupa di immagazzinare dati, generare statistiche ed effettuare ricerche.
2. Kibana: interfaccia utente che visualizza i dati salvati in Elasticsearch e "naviga" l'Elastic stack.
3. Beats: piattaforma che si occupa della spedizione di dati che vengono distribuiti da centinaia o migliaia di macchine e sistemi a Elasticsearch.

3.1.4 AIL-Framework

AIL (Analysis Information Leak) è un framework modulare pensato per analizzare potenziali leak di informazioni (leak detection) da sorgenti di dati non strutturati quali per esempio paste di Pastebin o servizi simili.

Le funzionalità principali di AIL sono:

- crawler automatico di servizi della clear net e del dark web;
- rilevamento dalle sorgenti ed estrazione di
  - codici IBAN
  - chiavi private
  - certificati

  - file codificati (base64, hex dump, schema di decodifica personalizzato)
  - Amazon AWS e Google API keys
  - indirizzi e chiavi di portafogli Bitcoin
  - numeri di telefono, email, credenziali, domini della clearnet e del deep web, hash...
  - URL e la loro locazione geografica
  - termini, set di termini e regex personalizzate;

- dashboard di statistiche e grafici relazionali;
- integrazione con MISP e TheHive (approfondita nella sezione 3.2)
- riconoscimento dei sentimenti espressi in un testo

3.1.5 Cortex

Gli observable come IP, indirizzi email, URL, domini, file o hash possono essere facilmente valutati da Cortex. Gli analisti possono automatizzare questo processo e studiare grandi quantità di observable da TheHive (approfondito nella sezione 3.1.7) o mediante le REST API di Cortex da altre piattaforme, script personalizzati o MISP (approfondito nella sezione 3.1.6). Quando usato in coppia con TheHive, Cortex facilita notevolmente il contenimento di minacce svolgendo le sue atività di active response.

Cortex mette a disposizione un'ampia varietà di analyzer e responder e permette di crearne aggiuntivi. Gli analyzer permettono di analizzare observable mediante servizi esterni (Virustotal [20], Shodan [21]...) mentre i responder danno la possibilità di eseguire operazioni personalizzate sulle macchine per rispondere agli incident.

3.1.6 MISP

Malware Information Sharing Platform (MISP) è una threat intelligence platform per acquisire, correlare e condividere informazioni relative ad attacchi, frodi finanziarie, vulnerabilità e controterrorismo.

La condivisione è la chiave per un'efficiente ed efficace rilevazione degli incident. Frequentemente le aziende sono bersaglio di attacchi che hanno caratteristiche e modalità simili; la condivisione di queste può consentire di evitare agli utenti di ripetere il lavoro già svolto da qualcun altro.

3.1.7 TheHive

TheHive è una Security Incident Response Platform scalabile strettamente integrata con MISP e Cortex.

I punti chiave di TheHive sono la collaborazione, l'elaborazione e l'azione.

- Collaborazione: vari CSIRT possono collaborare sulle investigazioni simultaneamente grazie alla funzionalità di live stream e real time information riguardanti case (incident), task, observable (file, indirizzi ip, domini ecc.) e IOC. Sono presenti notifiche che permettono di gestire, assegnare task e visualizzare un'anteprima degli alert ed eventi di MISP.

- Elaborazione: i case e i tasks associati possono essere creati usando dei template personalizzabili con l'aggiunta di metriche e campi. Gli analisti possono registrare i loro progressi e collegare ai case risorse utili alla risoluzione dell'incident.

- Azione: è possibile aggiungere observable ai case o importarli da MISP, filtrarli ed eseguire triage su di essi. TheHive sfrutta le potenzialità di Cortex e dei suoi analyzer e responder per ricavare informazioni, velocizzare il processo di incident handling e contenere le minacce. Al termine dell'investigazione è possibile esportare le informazioni acquisite su MISP e condividerle con la community.

3.2 Integrazioni

All'interno di OSSIHR possiamo distinguere integrazioni native ed integrazioni sviluppate successivamente.

3.2.1 Integrazioni native

Integrazione fra OwlH e Wazuh

Come già citato OwlH genera eventi ed alert mediante l'analisi di rete svolta da Zeek e Suricata. I risultati di questo studio sono poi convertiti e compattati in un formato riconoscibile da Wazuh tramite il componente Analyzer di OwlH.

Integrazione fra TheHive, Cortex e MISP

TheHive utilizza gli analyzer e i reponder di Cortex per arricchire i case con informazioni sugli observable collegati e per effettuare una risposta immediata dal pannello di controllo dell'intero sistema (la dashboard di TheHive).

TheHive interagisce con MISP per ricevere dalla community eventuali alert sulle nuove minacce che potrebbero interessare il sistema aziendale. Allo stesso modo la singola azienda può contribuire alla sicurezza di altri enti ed organizzazioni, condividendo i case gestiti e gli observable collegati ad essi.

Cortex e MISP cooperano nella raccolta di informazioni sugli observable. L'utilizzo di opportuni analyzer consente a Cortex di sfruttare MISP per cercare informazioni su observable noti ed a MISP di analizzare observable sconosciuti, mediante Cortex.

Integrazione fra AIL-Framework, TheHive e MISP

AIL può condividere con la community i leak di dati rilevati mediante l'integrazione con MISP ed esportarli sotto forma di alert o case sulla dashboard di TheHive, manualmente o automaticamente.

Integrazione fra Cortex e Wazuh

Cortex si interfaccia con i Wazuh agent attraverso un modulo specifico dei responder; in questa maniera riesce ad attivare procedure volte a contenere attacchi, eseguendo operazioni in tempo reale sulle macchine aggredite.

Integrazione fra OwlH e Moloch

I flussi di rete catturati da OwlH possono essere condivisi con Moloch in due modi. Il primo consiste nel salvare il traffico catturato in file pcap e, sfruttando cartelle condivise, inviarli a Moloch che potrà interpretarli. Il secondo metodo è da preferire perché più performante: il traffico catturato da OwlH viene inoltrato ad un interfaccia di rete collegata a Moloch, consentendo a quest'ultimo di interpretare le informazioni in ingresso.

3.2.2 Integrazioni sviluppate

Integrazione fra Wazuh e TheHive

Usufruendo del componente wazuh2thehive ([22] fork di [23]) Wazuh esporta su TheHive gli alert che rispettano specifici requisiti. Questa integrazione è mediata dal componente integrator di Wazuh [24] che permette di eseguire uno script ogni volta che un alert è rilevato. Allo script in questione vengono trasmessi come argomenti l'URL, l'API key del servizio da integrare (TheHive in questo caso) e l'alert registrato.

Successivamente wazuh2thehive esegue le seguenti operazioni:

1. filtraggio degli alert valutando la soglia di severity impostata dall'utente;
2. estrazione degli observable (indirizzi ip, domini e url);
3. conversione della severity dalla scala di Wazuh a quella di TheHive;
4. creazione dell'alert appena convertito su TheHive mediante la libreria TheHive4Py, wrapper delle API di TheHive su Python.

La prima versione dello script inserisce nella descrizione degli alert di TheHive la quasi totalità dei campi di Wazuh, formattandoli sotto forma di tabelle mediante il linguaggio di markup "Markdown" (fig. 3.1).

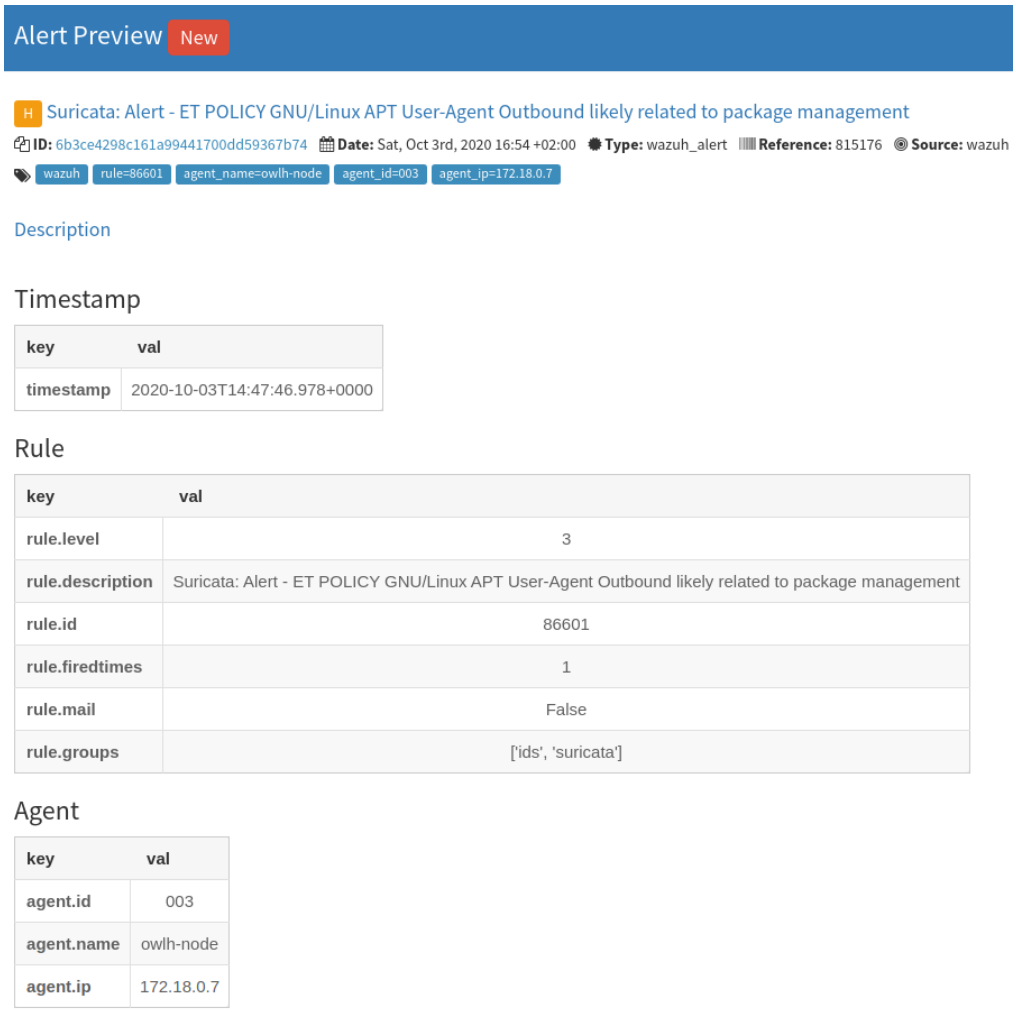

Figura 3.1: Esempio di alert di Wazuh esportato su TheHive.

Questa operazione viene effettuata perché TheHive definisce un alert sfruttando pochi campi essenziali, a differenza di Wazuh che ne utilizza molteplici.

Tale metodo di conversione è stato successivamente accantonato poiché gli alert risultanti sarebbero stati difficilmente manipolabili da un sistema informatico. Uno studio attento ed approfondito sui campi degli alert di Wazuh, su come vengono generati e la successiva catalogazione dei medesimi [25] ha portato ad una soluzione alternativa: creare una corrispondenza uno ad uno tra i campi di Wazuh e quelli di TheHive, sfruttando i custom fields messi a disposizione da quest'ultimo.

Alert aggregator

La soluzione appena descritta è stata adottata a seguito della teorizzazione del componente Alert aggregator: questo esegue l'analisi degli alert e dei case presenti in TheHive mediante algoritmi di machine learning, al fine di aggregare automaticamente gli alert in case opportuni.

Capitolo 4

Valutazione del progetto e considerazioni conclusive

OSSIHR è conforme alle linee guida ed ai suggerimenti della letteratura specializzata che costituisce il riferimento teorico in materia di incident handling. Questo progetto rappresenta un supporto consistente per il lavoro di uno CSIRT poiché incorpora le funzionalità di un HIDS, di un NIDS e di un sistema di incident handling, leak detection e network analysis.

Le tecnologie di OSSIHR sono tuttora in fase di sviluppo, migliorabili ed adattabili ad un utilizzo in ambiti più estesi e complessi. Inoltre il componente Alert aggregator non è ancora stato implementato, anche se è già stato teorizzato il suo funzionamento.

4.1 Analisi di comparazione

In questa sezione è riportata un'analisi di comparazione tra OSSIHR ed altri progetti closed source. Come si evince dalla tabella 4.1, sono state prese in considerazione le funzionalità di seguito elencate, in parte già illustrate nei capitoli precedenti.

- File Integrity Monitoring (FIM)
- Inventory management
- Log collection and retention: mantenimento per un periodo di tempo indefinito dei log di rete e di quelli di sistema.
- Vulnerability assessment: pratica analoga alla vulnerability detection spiegata nella sezione 3.1.1.

- Network analytics and response

- Endpoint detection and response: unione delle funzioni di intrusion detection ed incident response definite nella sezione 3.1.1.

- Deception: creazione e diffusione di false password, file e host per disorientare eventuali attaccanti.

- User behavior analytics: profilazione e monitoraggio delle attività degli utenti per rilevare azioni anomale, mediante uno studio comportamentale.

- Attacker behaviour analysis: profilazione e monitoraggio delle attività intrusive per bloccare all'origine operazioni malevole.

- Pre-set remediation: set di strumenti predefiniti che pongono rimedio in modo automatico a singoli alert.

- Custom remediation: meccanismo analogo al precedente ma personalizzabile.

- Automated playbooks: sequenze ordinate di pre-set e custom remediation al fine di risolvere un incident.

- Leak detection: attività precedentemente citata nella sezione 3.1.4 che può essere esercitata su fonti provenienti dalla clear net (internet) e dal deep web.

- Policy assessment: pratica equivalente alla configuration assessment definita nella sezione 3.1.1.

- Threat intelligence: metodologia di scambio di informazioni riguardanti minacce informatiche note.

- Email protection: rilevamento di file malevoli ricevuti via email e protezione dai medesimi.

Sistema → *Funzionalità* ↓	**OSSIHR**	**Rapid7**	**Cynet**	**RSA SecOps**	**Symantec**	**Cisco**
FIM	×	×	×		×	×
Inventory management	×	×	×	×	×	×
Log collection and retention	×	×	×	×	×	×
Vulnerability assessment	×	×	×	×		
Antivirus	≈	×	×	×	×	×
Network analytics and response	×	×	×	×	×	×
Endpoint detection and response	×	×	×	×	×	×
Deception		×	×		×	×
User behavior analytics		×	×	×	×	×
Pre-set remediation		×	×	×		×
Custom remediation		×	×	×		
Automated playbooks		×	×	×		
Attacker behaviour analysis		×			×	×
Dynamic and live dashboards	×	×	×	×	×	×
Leak detection (clearnet)	×	×				
Leak detection (deep web)	×					
Policy assessment	×	×		×	×	
Threat intelligence	×	×		×	×	×
Email protection			×		×	×

Tabella 4.1: Confronto fra OSSIHR e le alternative closed source.

Analizzando la tabella 4.1 e confrontando le funzionalità con quelle di altri progetti concorrenti closed source si può affermare che, attualmente, OSSIHR non rappresenta un'alternativa solida e competitiva.

Tuttavia, poiché questo progetto è open source, i margini di miglioramento appaiono ampi e le possibilità di estensione e personalizzazione molteplici.

L'antivirus è uno dei componenti che necessitano di essere migliorati perché non risulta ancora sufficientemente performante. Infatti Wazuh delega questa funzione a software antivirus di terze parti mentre molti concorrenti forniscono un loro sistema di difesa.

Inoltre sarebbe importante aggiungere ad OSSIHR le funzionalità mancanti di deception, di email protection, le pre-set e custom remediation e gli automated playbooks. Questi servizi andrebbero inseriti sviluppando appositi software o integrando tecnologie già esistenti.

L'accesso gratuito al sistema OSSIHR consente anche ad aziende di piccole dimensioni di allestire un impianto difensivo adeguato. Conseguentemente aumentano le possibilità di estensione del software poiché le aziende stesse sono motivate a contribuire e a migliorare il progetto.

In conclusione si può affermare che OSSIHR risulta un progetto in evoluzione, in grado di stimolare le capacità creative degli sviluppatori e degli analisti di sicurezza e l'interesse dei potenziali utenti utilizzatori.

Ringraziamenti

È mia premura ringraziare il Professor Franco Callegati, relatore della tesi, per aver creduto in questo progetto.

Grazie di cuore ad Alessandro Molari, correlatore nonché presidente di Cyberloop, l'azienda presso la quale ho svolto il tirocinio. Mediante il suo aiuto, le sue direttive ed i suoi preziosi consigli sono riuscito a concretizzare questo lavoro.

La mia gratitudine e la mia stima vanno inoltre ad Edoardo Rosa, figura di riferimento in ambito lavorativo e morale ed amico fidato. Sono inoltre riconoscente verso Fabrizio Margotta e Franco Righetti, compagni di corso, per il loro sostegno ed il proficuo confronto nello studio universitario.

Non posso non citare tutti gli amici, la mia ragazza Chiara ed il gruppo di sicurezza informatica CesenaSecurity di cui faccio parte e che mi aiuta nella crescita culturale e professionale.

Infine un'attenzione particolare la esprimo verso i miei genitori per quanto fanno per rendermi felice, per l'esempio di dedizione al lavoro e per le possibilità che mi offrono di coltivare le mie passioni ed esprimere la mia personalità.

Concludo riassumendo la mia esperienza universitaria triennale con una parola che nel gergo conviviale della mia compagnia esprime un avvenimento positivo: **devastante**!

Bibliografia

[1] Projects · CyberLoop / Tesi-Tirocini / Pietro-Mazzini / OSSIHR-PoC · GitLab, Ott 2020. https://gitlab.com/cyberloop/tesi-tirocini/pietro-mazzini/ossihr-poc.

[2] Chris Alberts, Audrey Dorofee, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. Defining Incident Management Processes for CSIRTs. Technical report, Carnegie Mellon University, 2014. Pages 1-5.

[3] ENISA. Good Practice Guide for Incident Management, 2010. Page 34.

[4] Karen Scarfone and Peter Mell. Intrusion Detection and Prevention Systems. *Securing the Information Infrastructure*, pages 2–1, 2011.

[5] Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle, and Mark Zajicek. Organizational Models for Computer Security Incident Response Teams (CSIRTs). *SEI Digital Library*, pages 13–24, 2003.

[6] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone. NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide Recommendations. *NIST Special Publication*, page 32, 2012.

[7] Wazuh · The Open Source Security Platform, Ott 2020. https://wazuh.com/.

[8] Wazuh 3.13 documentation, Ott 2020. https://documentation.wazuh.com/3.13/index.html.

[9] Owlh official website, Ott 2020. https://www.owlh.net/.

[10] Moloch official website, Ott 2020. https://molo.ch/.

[11] Suricata — Open Source IDS / IPS / NSM engine, Ott 2020. https://suricata-ids.org/.

[12] The Zeek Network Security Monitor, Ott 2020. https://zeek.org/.

[13] What is the ELK Stack?, Ott 2020. https://www.elastic.co/what-is/elk-stack.

[14] Elasticsearch: The Official Distributed Search & Analytics Engine — Elastic, Ott 2020. https://www.elastic.co/elasticsearch/.

[15] Kibana: Explore, Visualize, Discover Data — Elastic, Ott 2020. https://www.elastic.co/kibana.

[16] Beats: Data Shippers for Elasticsearch — Elastic, Ott 2020. https://www.elastic.co/beats.

[17] CIRCL/AIL-framework: AIL framework - Analysis Information Leak framework, Ott 2020. https://github.com/CIRCL/AIL-framework.

[18] TheHive Project, Ott 2020. https://thehive-project.org/.

[19] MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing (formely known as Malware Information Sharing Platform), Ott 2020. https://www.misp-project.org/.

[20] Virustotal - Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community, Ott 2020. https://www.virustotal.com/gui/.

[21] Shodan - The search engine for the Internet of Things, Ott 2020. https://www.shodan.io/.

[22] Projects · CyberLoop / Tesi-Tirocini / Pietro-Mazzini / wazuh2thehive · GitLab, Ott 2020. https://gitlab.com/cyberloop/tesi-tirocini/pietro-mazzini/wazuh2thehive.

[23] crow1011. crow1011/wazuh2thehive, Ott 2020. https://github.com/crow1011/wazuh2thehive.

[24] How to integrate external software using Integrator · Wazuh · The Open Source Security Platform, Ott 2020. https://wazuh.com/blog/how-to-integrate-external-software-using-integrator/.

[25] Projects · CyberLoop / Tesi-Tirocini / Pietro-Mazzini / wazuh2thehive / wazuh-alerts-fields · GitLab, Ott 2020. https://gitlab.com/cyberloop/tesi-tirocini/pietro-mazzini/wazuh2thehive/-/blob/master/doc/wazuh_alerts_fields.md.