Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea Triennale in Informatica

MONITORAGGIO DELLA SICUREZZA INFORMATICA MEDIANTE IL MODELLO SIEM IN UNA ORGANIZZAZIONE COMPLESSA: LA REGIONE EMILIA-ROMAGNA

Tesi di Laurea in Sicurezza

Relatore:
Chiar.mo Prof.
OZALP BABAOGLU

Presentata da:
FABIO BUCCIARELLI

Sessione III
Anno Accademico 2010/11

Introduzione

La sicurezza costituisce un elemento sempre più importante nell'ambito di aziende e pubblica amministrazione, soprattutto in seguito alla sempre maggior interconnessione tra i sistemi e all'aumento dei servizi Internet. Per questo motivo negli ultimi anni si è assistito ad un proliferare di sistemi di sicurezza, passando da un modello basato su pochi dispositivi posti sul perimetro della rete, ad un modello di sicurezza distribuita, in cui tutti gli end point della rete collaborano alla sicurezza.

Il continuo aumento del numero e dell'assortimento dei dispositivi di sicurezza presenti in azienda, e in generale l'aumento della complessità del sistema informativo aziendale fa sì che che i team dedicati alla sicurezza siano alle prese con un flusso di eventi continuamente crescente e spesso ingestibile. Gli amministratori di sicurezza, di sistema e di rete, sotto la cui responsabilità ricade tradizionalmente l'analisi dei log, considerano tale attività come un'attività a bassa priorità, noiosa e poco produttiva rispetto al dispendio di tempo ed energia richiesti. Questo è in parte motivato dal fatto che su milioni di log prodotti giornalmente, solo poche decine hanno un interesse reale e senza strumenti automatici è impossibile distinguerli dal rumore di fondo.

La necessità di rilevare prontamente eventuali attacchi e violazione delle policy, il rispetto di normative e di "best practice" sulla sicurezza delle informazioni rendono indispensabile la presenza di un'infrastruttura di log management robusta e affidabile, che automatizzi anche alcune operazioni di analisi impossibili da svolgere a mano.

L'attività di questa tesi si concentra sulla gestione dei log di sicurezza aziendali secondo il modello System Information and Event Management (SIEM), considerato come strumento di monitoraggio della sicurezza privilegiato su cui basare l'attività di un Security Operation Center (SOC).

Viene analizzato come caso di studio il sistema di monitoraggio della sicurezza implementato presso la Regione Emilia-Romagna, realizzato sotto la diretta responsabilità del candidato nell'ambito della propria attività lavorativa presso tale Ente.

La prima parte tratta da un punto di vista generale la gestione dei log di sicurezza secondo il modello SIEM. Il capitolo 1 introduce gli scopi, le problematiche e i modelli di gestione dei log di sicurezza. Il capitolo 2 descrive l'architettura e le componenti di un SIEM. Il capitolo 3 descrive l'architettura e le specificità di Arcsight ESM, il SIEM utilizzato dalla Regione Emilia-Romagna.

La seconda parte descrive il processo di realizzazione del sistema di monitoraggio presso la Regione Emilia-Romagna. Il capitolo 4 descrive la gestione della sicurezza informatica presso tale ente. Il capitolo 5 descrive i passi seguiti nella realizzazione del sistema, la definizione del modello, l'interconnessione con il database degli asset, la definizione di regole per la rilevazione di eventi di interesse.

A Serena, Chiara, Daniele, Stefano, Filippo

Indice

Elenco delle figure

Elenco delle tabelle

Parte I

Gestione dei log mediante un System and Event Management

Capitolo 1

La gestione dei log di sicurezza

1.1 Introduzione

Con il termine log si intende un record di eventi che si verificano all'interno dei sistemi e delle reti di un'organizzazione. I log sono composti da entries; ogni entry contiene informazioni relative ad uno specifico evento che si è verificato all'interno di un sistema o di una rete. In origine i log erano usati soprattutto per la risoluzione dei problemi, ma attualmente i log espletano varie funzioni all'interno delle organizzazioni, come l'ottimizzazione delle prestazioni dei sistemi e delle reti, la registrazione delle azioni degli utenti, l'investigazione sulle attività malevole. Molti di questi log contengono informazioni relative alla sicurezza dei sistemi; esempi di questo tipo di log sono gli audit log, che tengono traccia dei tentativi di autenticazione degli utenti e i log dei dispositivi di sicurezza, che registrano possibili attacchi.

In seguito all'aumento del numero di dispositivi connessi alla rete e all'aumento delle minacce a tali sistemi, il numero di log è andato via via aumentando, fino a richiedere un vero e proprio processo di log management. Con *log management* si intende il processo di generazione, trasmissione, memorizzazione, analisi e messa a disposizione dei log di sicurezza.

Con *infrastruttura di log management* si intende l'insieme di hardware, software, reti e media utilizzati per il log management.

1.2 Tipologie di log di sicurezza

Le varie tipologie di sistemi presenti all'interno di un'organizzazione producono log che contengono diverse tipologie di informazioni. Alcune tipologie di log sono più indicate di altre ai fini di indivuare attacchi, frodi e usi inappropriati. Per ogni tipo di situazione, certi log sono più pertinenti di altri nel contenere

informazioni dettagliate sulle attività in questione. Altri tipi di log contengono informazioni meno dettagliate, ma sono comunque utili per correlare i log con quelli del tipo principale. Per esempio, un sistema di intrusion detection può rilevare comandi malevoli inviati ad un server da un host esterno: questa sarà la fonte primaria di informazioni. Può essere quindi utile cercare all'interno dei log di un firewall altre connessioni tentate dallo stesso IP sorgente: questa sarà la fonte secondaria di informazione sull'attacco.

1.2.1 Software di sicurezza

All'interno delle organizzazioni sono presenti diversi dispositivi di sicurezza che hanno lo scopo di evidenziare e di proteggere da attività malevole. Occorre partire da queste tipologie di log nella realizzazione di un'infrastruttura di log management.

Descriviamo brevemente scopi e caratteristiche delle principali tipologie di dispositivi di sicurezza, al fine di comprendere che tipo di informazioni è possibile estrarne.

- **Firewall**. I firewall sono dispositivi che, basandosi su policy definite più o meno complesse, bloccano o permettono il passaggio di traffico di rete. Generalmente viene generato un record di log per ogni pacchetto o per ogni sessione del traffico di rete che attraversa il firewall, con la policy che viene applicata.

- **Sistemi AntiMalware**. I software antimalware più comuni sono i software antivirus. Tipicamente registrano tutte le istanze di malware, file e sistemi disinfestati e file messi in quarantena. In più, i software antivirus possono anche registrare quando vengono effettuate scansioni alla ricerca di malware e quando viene fatto l'update del database delle signature.

- **Sistemi di Intrusion Prevention e Intrusion Detection**. I sistemi di Intrusion Detection e Intrusion Prevention hanno lo scopo di segnalare (Intrusion Detection) e/o di bloccare (Intrusion Prevention) eventuali attacchi alle reti o ai sistemi, generalmente basando il riconoscimento su signature e/o anomalie nel comportamento. I log registrano informazioni sui sospetti tentativi di attacco e sulle azioni intraprese per bloccarli.

- **Virtual Private Network software**. Le VPN garantiscono l'accesso remoto in modalità sicura alle risorse aziendali. I log di tali sistemi contengono generalmente tentativi di autenticazioni, sia falliti che andati a buon fine, durata e provenienza delle connessioni, le risorse a cui l'utente ha avuto accesso.

- **Web Proxy**. I web proxy sono sistemi che fungono da intermediari nell'accesso alle risorse web, mantenendo una cache locale delle pagine web e restringerndo l'accesso ad alcune risorse web basandosi su policy definite, proteggendo così la rete dell'organizzazione. I log registrano gli url a cui gli utenti hanno avuto accesso attraverso il web proxy.

- **Sistemi di autenticazione.** Tipicamente directory server, radius server e server di single sign on, registrano le autenticazioni andate a buon fine e i tentativi di autenticazione falliti, con lo username dell'utente, il timestamp, il sistema di provenienza.

- **Software per la gestione delle vulnerabilità.** In questa categoria sono compresi i software per la gestione delle patch di sicurezza e i software per il vulnerability assessment. I log contengono la storia delle patch installate e lo stato delle vulnerabilità di ogni host.

Esempi di log di sistemi di sicurezza sono mostrati nella figura 1.2.1.

1.2.2 Sistemi operativi

Anche i sistemi operativi presenti su server, workstation e apparati di rete producono log significativi dal punto di vista della sicurezza, appartenenti alle categorie di seguito elencate. I log dei sistemi operativi contengono inoltre log dei software di sicurezza e delle applicazioni installate sul sistema: tali log rientrano nelle tipologie trattate al paragrafo precedente e al paragrafo successivo.

- **Eventi di sistema.** Gli eventi di sistema sono azioni svolte dai singoli componenti dei sistemi operativi. Tipicamente vengono registrati gli eventi falliti e gli eventi più significativi che hanno avuto successo. Alcuni sistemi operativi permettono all'amministratore di definire i tipi di eventi di cui tenere traccia. I log contengono un timestamp, il nome del sistema e altre informazioni che possono variare enormemente da sistema a sistema, come descrizione dell'evento, stato, codici di errore.

- **Audit Record.** Contengono eventi relativi alla sicurezza, come tentativi di autenticazione andati a buon fine o falliti, utilizzo di privilegi amministrativi da parte dell'utente, accesso a file critici, modifica di policy di sicurezza, creazione, modifica, cancellazione di account e variazione nella composizione di gruppi. Gli amministratori dei sistemi operativi in genere possono specificare quali tipi di eventi possono essere soggetti ad audit e se tenere traccia di alcune azioni andate a buon fine o fallite.

I log del sistema operativo sono importanti soprattutto nel caso di attacchi verso un host specifico. Se per esempio da parte di un software di sicurezza viene segnalato un'attività sospetta, sui log del sistema operativo possono essere trovati maggiori dettagli sull'attività segnalata. La maggior parte dei sistemi operativi produce log in formato syslog, mentre, altri, come per esempio Microsoft Windows, utilizzano un formato proprietario.

Un esempio di log di sistemi operativi sono mostrati nella figura 1.2.2.

1.2.3 Applicazioni

Le applicazioni, usate all'interno delle organizzazioni per memorizzare, accedere e manipolare i dati usati dai processi di business, possono generare i loro log o

utilizzare le funzionalità di log del sistema operativo. Le informazioni contenute all'interno dei log cambiano enormemente a seconda del tipo di applicazione. Di seguito vengono elencati tipologie di informazioni che possono essere contenute all'interno dei file di log di applicazioni e che possono riguardare il monitoraggio della sicurezza.

- **Richieste del client e risposte del server.** Possono essere molto utili per ricostruire sequenze di eventi e il loro esito, in caso di investigazione sugli incidenti, nelle operazioni di audit e in fase di verifiche sulle conformità alle policy.
- **Informazioni su account.** Contengono informazioni come tentativi di autenticazione che hanno avuto successo o che sono falliti, modifiche sugli account, uso di privilegi. Possono essere utilizzati per individuare attacchi di forza bruta o escalation di privilegi e per verificare chi ha utilizzato l'applicazione e in quali momenti.
- **Informazioni sull'uso.** Contengono informazioni come il numero di transazioni in un certo periodo di tempo e la grandezza delle transazioni. Possono essere utilizzati per alcuni tipi di monitoraggio, quando si verificano variazioni significative rispetto al normale utilizzo.
- **Azioni significative.** Contengono informazioni come l'avvio o lo stop dell'applicazione, errori dell'applicazione o le principali modifiche nella configurazione. Possono essere utilizzate per verificare le compromissioni della sicurezza e malfunzionamenti.

Un esempio di log di un web server è mostrato nella figura 1.2.3.

Tali log sono importanti soprattutto in caso di incidenti che coinvolgono le applicazioni; spesso però sono in formato proprietario, cosa che rende difficile il loro utilizzo.

1.3 Gli scopi

Gli scopi che ci si prefigge nell'implementazione di un'infrastruttura di log management all'interno di un'azienda sono sostanzialmente due:

- il monitoraggio della sicurezza dei propri asset, che vanno protetti da tutti gli attacchi a cui possono essere soggetti;
- la conformità alle normative che regolano la sicurezza e la privacy.

Se sicurezza informatica vuole dire garantire la confidenzialità, l'integrità e la disponibilità del dato, come ci insegna qualsiasi manuale di sicurezza informatica, i due punti precedenti vanno declinati sul modello di business della singola azienda. Occorre quindi partire da un'analisi dei rischi, nella quale si cerca di capire qual è il valore dei singoli asset, quali sono le principali minacce a cui sono soggetti, la probabilità che si concretizzino, ottenendo così una valutazione del

rischio. Il modello di business dell'organizzazione è anche il punto da cui partire per definire quali sono le leggi, le normative, gli standard o semplicemente le best pratice relative alla privacy e alla sicurezza informatica che l'organizzazione è tenuta a rispettare.

1.3.1 Monitoraggio della sicurezza

1.3.1.1 L'analisi dei rischi

Differenti tipi di organizzazione hanno differenti tipi di dati da proteggere, a seconda di come è configurato il loro business. Un sistema di monitoraggio della sicurezza, e ancor più in generale il processo di messa in sicurezza del sistema informativo di un'organizzazione, per poter essere efficace deve partire da *un'analisi dei rischi.* L'analisi dei rischi può essere scomposto nelle seguenti fasi:

- identificazione o classificazione degli asset da proteggere;
- identificazione delle minacce a cui sono soggetti gli asset;
- identificazione delle vulnerabilità;
- stima delle probabilità di sfruttamento;
- valutazione del rischio.

Identificazione o classificazione degli asset da proteggere In questa fase occorre fare un inventario di tutti gli asset. Con *asset* si intende una risorsa informativa che può essere un dato, un software, un hardware. In particolare tale inventario dovrebbe definire, per gli asset censiti, dati come tipo di risorsa (dato, hardware, software, ...), criticità, proprietà delle informazioni, posizione fisica o logica, numero di inventario (in caso di asset fisico), informazioni relativi a contratti di manutenzione per l'asset, relazione con asset di altri tipi (es. un server con le applicazioni in esecuzione su di esso).

Al fine poi della protezione delle risorse il dato più importante è quello della criticità; il valore della criticità deve essere ricavato, soprattutto per quel che riguarda le risorse informative, a partire dalle caratteristiche del proprio business confrontate con gli obiettivi primari della sicurezza, confidenzialità, integrità e disponibilità. La classificazione degli asset dovrebbe avvenire proprio a partire dalla criticità.

Identificazione delle minacce a cui sono soggetti gli asset Le minacce possono essere di diversi tipi, che devono essere considerati in relazione alle caratteristiche dell'organizzazione. Queste vanno valutate sia in termini di locazione geografica, sia (e soprattutto) in riferimento alle attività e al modello di business. Per esempio, una banca sarà maggiormente esposta a minacce di tipo volontario di quanto non lo sia una catena di ristoranti.

Ognuno dei modi in cui una risorsa può essere danneggiata, alterata, rubata, distrutta o resa inaccessibile, costituisce una minaccia. Tra questi modi bisogna considerare sia quelli volontari che involontari, senza dimenticare le catastrofi, quali incendi, terremoti e inondazioni.

Identificazione delle vulnerabilità (vulnerability assessment) Con vulnerabilità si intende una o più situazioni particolari o debolezze che possono essere sfruttate affinché le minacce si concretizzino. Considerando le varie minacce (che possono essere anche di tipo misto), è possibile determinare quali vulnerabilità possono essere sfruttate. Le vulnerabilità sono, in generale, dovute a errori o trascuratezza di gestione: una configurazione superficiale, un bug del software, una versione non aggiornata dell'antivirus e così via.

Stima della probabilità di sfruttamento Il passaggio successivo consiste nella determinazione della probabilità con cui una vulnerabilità possa essere sfruttata. Questa probabilità è ottenuta tenendo conto delle misure di sicurezza già adottare all'interno dell'organizzazione e della probabilità che qualcuno o qualcosa le aggiri.

Valutazione del rischio Terminate le quattro fasi illustrate precedentemente, attraverso un lavoro di sintesi si arriverà alla valutazione del rischio, che può essere sia di tipo qualitativo che quantitativo, includendo, per esempio, valori numerici del rischio espressi in percentuale del fatturato.

1.3.1.2 Vulnerabilità e minacce

Per poter operare un efficace monitoraggio della sicurezza, occorre tenere conto delle vulnerabilità dei propri sistemi; sarebbe auspicabile trovare la maniera di inserire i report dei vari vulnerability assessment effettuati all'interno del sistema di log management, per automatizzare il processo di identificazione di possibili attacchi.

Di seguito vengono analizzati alcune delle principali vulnerabilità che possono essere presenti all'interno dell'organizzazione.

Protocolli vulnerabili I protocolli che regolano la comunicazione tra computer sono stati pensati parecchi anni fa e con una minima attenzione alle problematiche della sicurezza. Alcuni di questi protocolli contengono vulnerabilità note e alcuni di questi sono stati sostituiti con versioni più sicure. Per eliminare tali vulnerabilità occorrerebbe definire delle policy che non permettano l'uso di protocolli vulnerabili. Sistemi che individuino tali protocolli sul loro segmento di rete, come router o IDS che siano configurati per inviare i loro log al sistema di log management, permettono di segnalare l'uso di protocolli vulnerabili non consentiti dalle policy.

Errori di configurazione Gli errori di configurazione possono introdurre vulnerabilità su sistemi altrimenti sicuri. Tali errori possono essere frutto di sviste da parte di amministratori, mentre a volte possono essere appositamente commessi da parte di utenti che intendono svolgere attività malevole senza essere scoperti. Esempi comuni di errori di configurazione possono essere l'attivazione o la disattivazione di servizi, la modifica di configurazione di servizi che vengono resi meno sicuri. Il sistema di log management può essere utilizzato per monitorare i servizi attivi sui sistemi e per ricevere i log di sistemi di controllo dell'integrità.

Errori degli utenti Molte vulnerabilità vengono introdotte nei sistemi da parte degli utenti che, sia perché non sono adeguatamente formati sulle possibili minacce, o perché giudicano eccessive le policy di sicurezza, possono tenere dei comportamenti o commettere errori che mettano a repentaglio la sicurezza della rete e del sistema informativo dell'organizzazione. Esempi di comportamenti di questo tipo sono l'installazione di software non autorizzato, la navigazione su siti di dubbia reputazione, il desiderio di accedere a documenti riservati, la navigazione su siti contenuti in email che sono in realtà attacchi di phishing. Al di là del fatto che la contromisura più efficace a questo tipo di vulnerabilità è la formazione continua degli utenti, questi comportamenti, se il sistema di log management è opportunamente configurato, possono essere monitorati.

Minacce interne ed esterne Passando dal campo delle vulnerabilità a quello delle intenzioni malevole, le reti aziendali sono normalmente meno protette verso gli attacchi provenienti dall'interno rispetto a quelli provenienti dall'esterno. Il motivo principale è che molte reti sono costruite puntando i sistemi di sicurezza verso l'esterno, là dove si pensa vengano la maggior parte delle minacce. Le statistiche dicono invece che la maggior parte degli attacchi proviene dall'interno; per questo motivo nelle misure di sicurezza occorre sempre tenere presente tali minacce.

Come contromisure alle minacce interne, occorre sempre tenere conto del principio del minimo privilegio, cercando di fare in modo di concedere a ciascun utente i minimi privilegi che gli permettano di svolgere la sua attività. Le tecniche per limitare le possibilità che utenti alterino la sicurezza dei sistemi e/o per rilevare possibili azioni malevole sono:

- separazione dei privilegi;
- rotazione delle attività;
- definizione di access control list (ACL) secondo il principio del minimo privilegio;
- implementare l'auditing su dati critici, applicazioni, configurazioni e log dei sistemi.

Le minacce esterne sono generalmente più facili da rilevare, in quanto esistono apparati di sicurezza in grado di segnalare attacchi provenienti dall'esterno.

Tale rilevazione è più facile nel caso di attacchi operati con tool automatici, che lasciano molte più tracce e generano più "rumore", rispetto ad attacchi manuali mirati.

1.3.1.3 Riconoscimento degli attacchi

La maggior parte degli attacchi, di qualsiasi tipo, lasciano tracce all'interno dei log di uno o più sistemi. Una volta che questi log sono arrivati al sistema di log management, il team di sicurezza può comprendere che qualcosa di sospetto sta accadendo.

Di seguito viene presentato un sommario di alcuni eventi contenuti in un attacco e che possono essere identificabili e alcuni modi in cui può essere configurato il sistema di log management per identificarli rapidamente.

Scansione e riconoscimento Normalmente la fase preliminare di ogni attacco prevede la scansione della rete per identificarne la topologia, i sistemi che ne fanno parte e la presenza di eventuali servizi vulnerabili. Tale attività si compone normalmente di due fasi, una fase di *fingerprinting*, durante la quale l'attaccante cerca di identificare la struttura del sistema IT, le sottoreti IP e i sistemi di tali sottoreti, e la fase di *footprinting*, nella quale l'attaccante cerca di identificare la natura dei nodi individuati durante la fase precedente, sistema operativo, servizi attivi e relative versioni, livello di patching; ciò allo scopo di individuare all'interno della rete i sistemi più appetibili, o per la rilevanza dei dati contenuti, o per la presenza di vulnerabilità che permettano facilmente di prenderne possesso.

Durante tale fase, soprattutto se svolta con tool automatici, avremo, nell'arco di un periodo di tempo limitato, una certa quantità di pacchetti provenienti da un unico indirizzo IP verso molti indirizzi della rete o verso molte porte tcp e udp di un singolo target. L'attaccante può svolgere la scansione e il riconoscimento in maniera manuale, diradando la frequenza dei pacchetti e utilizzando più indirizzi IP sorgenti, rendendo l'identificazione di questo tipo di attività più complicata.

Malware Una volta che l'attaccante ha un'idea della topologia della rete ed ha identificato uno o più sistemi target che espongono vulnerabilità o che sono appetibili, la fase successiva può essere quella di installare malware sui sistemi target nella speranza di comprometterli. Questa fase può avvenire anche direttamente, saltando la fase di scansione e riconoscimento, per esempio attraverso attacchi automatici fatti da un worm che cerca di propagarsi.

Esempi di malware sono i virus e i worm. I virus si iniettano all'interno del codice eseguibile e una volta che il codice eseguibile viene lanciato, il codice del virus viene eseguito con i privilegi dell'utente che lo ha lanciato. Normalmente il virus replica sé stesso, oltre ad eseguire le attività malevole definite all'interno del suo codice.

I worm sono un tipo malware che si auto-propaga e che sfrutta vulnerabilità note all'interno di applicazioni o servizi. Una prevenzione per i worm è l'installazione tempestiva delle patch di sicurezza sui sistemi.

I malware vengono rilevati dai sistemi antivirus, che devono essere configurati per inviare i log al sistema di log management. All'interno del sistema di log management, occorre essere in grado di rilevare la presenza dello stesso malware su diversi sistemi o l'individuazione di un malware che l'antivirus non è in grado di eliminare.

IP spoofing Molti attacchi provenienti dall'esterno vengono fatti in modo da presentarsi come provenienti da IP appartenenti alla rete interna (ip spoofing dall'esterno), in generale IP privati. Alla stessa maniera, un malintenzionato che si trova su una rete interna privata, può generare pacchetti con IP sorgente pubblico, diretti verso l'esterno (ip spoofing dall'interno). In entrambi i casi il firewall dovrà bloccare tale tipo di pacchetti e inviare i log di tali blocchi al sistema di log management.

Denial-of-service distribuito (DDoS) In questo attacco, molti IP sorgenti diversi inviano pacchetti ad un singolo indirizzo IP ad una tale frequenza che il sistema sotto attacco, cercando di soddisfare queste false richieste, finisce per non rispondere più alle richieste di servizio lecite. Questo tipo di attacco è difficile da individuare; il sistema migliore sono le segnalazioni di sistemi IDS basati sull'analisi delle anomalie di comportamento, eventualmente correlate con segnalazioni di utenti.

Buffer overflow e attacchi di SQL injection Sono attacchi che sfruttano vulnerabilità causate da errori di programmazione nelle applicazioni, in particolare la mancata validazione dell'input dell'utente. Gli attaccanti possono sfruttare tali vulnerabilità per ottenere l'accesso a sistemi o a database. A parte la necessità di eliminare preventivamente vulnerabilità di tale tipo, attraverso processi di vulnerability assessement o di auditing del codice, tentativi di attacco di tale tipo possono essere individuati attraverso l'analisi dei log degli application server, che segnalano eventuale input dell'utente rigettato. Anche i sistemi IDS contengono le signature di molti di questi attacchi.

Attacchi di forza bruta alle password Un malintenzionato potrebbe tentare di ottenere l'accesso ad un sistema o ad un'applicazione provando diverse combinazioni di password, generalmente con l'aiuto di apposite applicazioni. Una contromisura a questo tipo di minaccia può essere quella di bloccare temporaneamente un account dopo un certo numero di errori di autenticazione, anche se tale contromisura può rendere vulnerabili ad attacchi di denial of service. Attacchi di questo tipo possono essere rilevati attraverso il monitoraggio dei log dei sistemi di autenticazione.

Attacchi ai sistemi IPS/IDS I sistemi IPS/IDS sono un componente fondamentale del monitoraggio della sicurezza. È bene monitorare i pacchetti diretti a tali sistemi, in quanto normalmente non esistono pacchetti destinati ai sistemi IPS/IDS, se non provenienti dai sistemi di management.

Nel caso un attacco sia andato a buon fine, l'attaccante provvederà a nascondere le sue tracce, in modo da poter continuare indisturbato a svolgere le sue attività.

Di seguito viene presentato un sommario delle modalità con cui un attaccante può procedere a tale scopo.

Disattivazione degli aggiornamenti di sistema operativo Al fine di mantenere la vulnerabilità appena sfruttata, l'attaccante potrebbe disabilitare l'installazione delle patch di sistema, che rimuovono le vulnerabilità note. Occorre tenere costantemente monitorata l'installazione delle patch di sicurezza. Un'altra tecnica più sofisticata consiste nella modifica delle impostazioni per la risoluzione dei nomi per far puntare il sistema compromesso ad un server DNS sotto il controllo dell'attaccante. In questa maniera gli aggiornamenti di sicurezza verranno scaricati da un sito sotto il controllo dell'attaccante. Occorre monitorare le connessioni dirette alla porta 53 di indirizzi IP diversi dai server DNS legittimi. Un'altra tecnica con le stesse finalità consiste nel modificare il file hosts locale al sistema compromesso: occorre tenere modificate tutte le modifiche al file hosts dei sistemi.

Disattivazione degli aggiornamenti del software antivirus e antispyware Al fine di evitare che il malware installato venga rilevato, l'attaccante potrebbe impedire al sistema di connettersi ai server da cui vengono scaricate le signature e gli aggiornamenti per i software antivirus e antispyware. Anche in questo caso occorre monitorare gli aggiornamenti dei sistemi, le connessioni aperte verso la porta 53 di indirizzi IP diversi dai server DNS legittimi.

Disattivazione del forwarding dei log al sistema di log management L'attaccante, al fine di disperdere le proprie tracce, potrebbe disabilitare il forwarding dei log verso il sistema di log management. Occorre monitorare, sul sistema di log management, se i sistemi interrompono la trasmissione dei log.

Modifica alle configurazioni dei sistemi Allo scopo di aprire nuove backdoor e assicurarsi la possibilità di accedere nuovamente al sistema, l'attaccante potrebbe effettuare modifiche alla configurazione del sistema compromesso. Queste modifiche possono essere rilevate da tool di verifica dell'integrità. I log di tali sistemi possono essere inviati al sistema di log management.

Installazione di nuovi servizi e disattivazione di altri servizi Allo scopo di aprire nuove backdoor e assicurarsi la possibilità di accedere nuovamente al sistema, l'attaccante potrebbe avviare servizi esistenti o installare nuovi servizi. Potrebbe inoltre arrestare o disabilitare servizi legati alla sicurezza del sistema. Anche in questo caso occorre rilevare le modifiche alle configurazioni dei sistemi, inviando i riscontri al sistema di log management.

Inoltre l'attaccante, dopo essersi nascosto, avrà necessità di installare dei tool e malware che gli permettano di operare un controllo maggiore sulla rete dell'organizzazione. A tale scopo provvederà a fare un download di rootkit o collezione di malware da installare all'interno della rete compromessa.

Di seguito viene presentato un elenco di tecniche usate dagli attaccanti a tale scopo.

Reset della home page di default del browser Quando un browser carica un sito web, script ed eseguibili possono essere messi in esecuzione sul sistema client. Se l'attaccante può modificare la home page di default del browser, eventuale software malevolo contenuto in tale home page verrà eseguito non appena l'utente apre il browser. Se poi la home page è costruita in modo da assomigliare a quella legittima, tale malware può essere eseguito più volte. Una protezione a questo tipo di attacco può essere quella di impostare a livello centrale la home page di default del browser.

Uso di IP che fanno parte di blacklist Gli attaccanti hanno spesso necessità di mantenere risorse raggiungibili da Internet, per ottenere i loro scopi. Alcuni server che ospitano attività malevole sono conosciuti e finiscono nelle cosiddette "black list". Ci sono parecchi siti su Internet che mantengono blacklist aggiornate e rendono tali liste disponibili per il download. Alcuni IDS hanno la possibilità di consultare e scaricare blacklist in modo da monitorare pacchetti distinati ad IP appartenenti ad esse.

Traffico anomalo Spesso le risorse esterne dell'attaccante non sono ancora state identificate e non sono ancora entrate a far parte di blacklist, oppure dopo essere entrate a far parte di blacklist l'attaccante ha spostato il server su un altro indirizzo IP. Occorre quindi monitorare la rete alla ricerca di traffico anomalo, pur diretto ad IP leciti. Esempi di questo tipo di monitoraggio possono essere upload e download di file di grandi dimensioni, traffico verso porte note per essere utilizzate da malware, traffico eccessivo verso IP di paesi da cui notoriamente arriva il maggior numero di attacchi.

Infine, una volta che l'attaccante ha una conoscenza approfondita della rete compromessa, ha individato alcuni sistemi da attaccare, ha preso possesso di tali sistemi, ha coperto le proprie tracce, si è assicurato la possibilità di continuare ad accedere, ha contattato il proprio repository esterno per il download della versione aggiornata della propria collezione di malware, avrà necessità di inviare dati all'esterno.

Di seguito verrà presentato un elenco di tecniche utilizzate in questa fase.

IRC Questo protocollo è spesso usato come mezzo di comunicazione fra l'attaccante e la sua collezione di sistemi compromessi, chiamata *zombies*. Una chat room può essere utilizzata dall'attaccante per isolarsi dai suo zombies, rimanendo così anonimo. Gli zombies possono essere istruiti per ricevere comandi

attraverso una chat room. Normalmente il protocollo IRC non è utilizzato all'interno delle organizzazioni, per cui occorre monitorare la propria rete alla ricerca di tentativi d'uso di tale protocollo.

Porte conosciute come destinazione di traffico malevolo Molti tipi di malware utilizzano porte specifiche per comunicare. Occorre monitorare il traffico diretto verso tali porte.

Protocolli inattesi/atipici Il traffico e i protocolli usati all'interno della rete di un'organizzazione rientrano spesso in una lista standard e predicibile. Occorre monitorare l'uso di protocolli e destinazioni che non rientrano in tale lista.

1.3.2 Compliance alle normative

Negli ultimi anni, in seguito all'aumento del numero dei dati trattati, si è assistito ad un aumento della consapevolezza da parte delle organizzazioni dell'importanza delle informazioni trattate, e quindi della loro protezione, per il raggiungimento degli obiettivi di business. Vi è quindi, da parte delle organizzazioni, una crescente esigenza di "compliance", ovvero di predisporre processi e modalità di gestione delle informazioni, che abbiano adeguati requisiti di riservatezza, tracciabilità e protezioni, richieste dalle leggi vigenti, ma anche da standard internazionali, da "best practice" e policy interne all'organizzazione.

Limitandoci all'aspetto delle normative, uno dei motivi che negli ultimi anni hanno portato molte organizzazioni alla creazione di infrastrutture di log management è l'introduzione di leggi che hanno lo scopo di regolare la protezione delle informazioni da parte delle organizzazioni, al fine di prevenire eventuali danni ad individui e ad altre organizzazioni. Un tratto comune di queste normative è l'introduzione dell'obbligo di controllo sulla sicurezza dei sistemi IT e dell'obbligo di documentare le misure e le procedure di sicurezza adottate.

Alcune normative, per lo più riguardanti gli operatori finanziari, prevedono esplicitamente forme di log management. L'unica normativa italiana che prevede esplicitamente la raccolta e la gestione di log è il "Provvedimento del Garante per la Protezione dei Dati Personali relativo agli Amministratori di Sistema", ma occorre considerare che organizzazioni che operano sul mercato bancario e finanziario internazionale sono tenute a rispettare standard e best practice internazionali.

Di seguito vediamo più in dettaglio alcune di queste normative.

Il Testo Unico sulla Privacy (Dlgs196/2003) Il Codice in materia di dati personali, varato il 30 giugno 2003 ed entrato in vigore il 1° gennaio 2004, riunisce tutti i provvedimenti normativi connessi con la protezione dei dati personali varati precedentemente. Il testo unico introduce (allegato B) un Disciplinare Tecnico in materia di misure minime di sicurezza. La novità più importante introdotta dal testo unico consiste nell'obbligo di creare una catena di comando

formalizzata, dedicata a garanzia della privacy, in cui vengono definiti, per ciascun trattamento di dati, ruoli specifici (Titolare del trattamento, Responsabile, Incaricato) a cui corrispondono compiti e responsabilità definite. Vengono inoltre introdotte le cosiddette misure minima di sicurezza relative al trattamento di dati personali con strumenti elettronici:

- autenticazione informatica;
- adozione di procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;
- aggiornamento periodico dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti dei dati, ad accessi non consentiti e a determinati programmi informatici;
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- tenuta di un aggiornato documento programmatico sulla sicurezza;
- adozione di tecniche di cifratura o di codici identificativi per determinati trattamentidi dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari (dati sensibili).

Di rilevante per l'ambito qui trattato vi è l'esigenza di identificare in maniera certa gli incaricati di ciascun trattamento quando questi accedono ai dati e ai sistemi che li contengono. Ciò porta a prevedere un processo per l'assegnazione dei privilegi minimi per gli operatori che hanno l'esigenza di lavorare sui soli dati, per le sole operazioni previste dal proprio ruolo e necessarie per lo svolgimento delle proprie mansioni. Il requisito di poter attribuire in modo inequivocabile le azioni compiute su un dato critico al suo effettivo autore obbliga a prevedere un sistema di tracciamento, non ripudiabile, che intervenga ad ogni livello di operazione compiuta su un dato critico.

Il controllo sull'operato degli Amministratori di Sistema Il Provvedimento del Garante per la Protezione dei dati personali relativo agli Amministratori di Sistema, varato il 27 novembre 2008, le cui prescrizioni sono entrate in vigore il 15 dicembre 2009, nasce dalla constatazione che gli amministratori di sistema svolgono funzioni delicate che comportano la concreta capacità di accedere a tutti i dati che transitano sulle rete di aziende e pubbliche amministrazioni. Le ispezioni effettuate nel corso degli anni da parte dell'Autorità Garante hanno messo in luce in diversi casi una scarsa consapevolezza da parte delle organizzazioni di qualsiasi dimensione del ruolo svolto dagli amministratori di sistema e una sottovalutazione dei rischi che possono derivare da un'attività

di questo tipo svolta senza il necessario controllo. Per questo motivo il Garante ha deciso di prescrivere l'adozione di specifiche misure tecniche e organizzative che agevolino la verifica sulla sua attività da parte di chi ha la titolarità delle banche dati e dei sistemi informatici.

Il provvedimento del Garante prescrive che l'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti di dati personali. Inoltre devono essere adottati strumenti idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Ciascuna organizzazione dovrà conservare in un documento gli estremi identificativi degli amministratori di sistema e l'elenco delle funzioni loro attribuite. Dovranno essere infine valutate con attenzione esperienza, capacità e affidabilità della persona chiamata a ricoprire il ruolo di amministratore di sistema, che deve essere in grado di garantire il pieno rispetto della normativa in materia di protezione dei dati personali, compreso il profilo della sicurezza.

Il Payment Card Industry Data Security Standard (PCI DSS) Lo standard Payement Card Industry (PCI) Data Security Standard (DSS) regolamenta le modalità di realizzazione e di protezione dei sistemi di pagamento e delle carte che vengono utilizzate nell'ambito dei circuiti di pagamento. Questo standard si applica a tutte le infrastrutture di rete, server, sistemi di messaggistica e applicazioni utilizzate all'interno di ambienti dove sono conservati dati relative alle carte di credito o debito.

Lo standard contiene specifiche per 12 aree di controllo separate:

1. provvedere all'installazione e manutenzione di firewall;

2. non utilizzare dati di default forniti dal venditore come password di sistema;

3. proteggere i dati di un proprietario di card che siano stati memorizzate in un sistema di storage aziendale;

4. criptare i dati del possessore di card quando vengono trasmessi su qualsiasi tipo di rete;

5. utilizzare e aggiornare con regolarità il software delle applicazioni antivirus;

6. sviluppare e mantenere adeguatamente il sistema di sicurezza e le applicazioni;

7. limitare l'accesso in aderenza al concetto di need-to-know, ovvero concederlo esclusivamente a coloro che hanno ottimi motivi;

8. assegnare un ID univoco a ogni persona che abbia accesso ai computer interessati alla gestione o alla trasmissione dei dati di un proprietario di card;
9. limitare l'accesso ai dati di un proprietario di card anche dal punto di vista fisico;
10. *effettuare il tracciamento e il monitoraggio di tutti gli accessi alle risorse e ai dati dei proprietari delle card*;
11. effettuare regolarmente il test sia del sistema di sicurezza che dei singoli processi;
12. mantenere e aggiornare costantemente una policy che indirizzi il tema della sicurezza delle informazioni.

1.4 Le strategie

Una strategia di log management adeguata alle esigenze dell'organizzazione prevede i passi di seguito elencati.

- **Centralizzare nel sistema di log managementi tutti gli eventi rilevanti**. Una volta definiti gli eventi rilevanti per la propria organizzazione, occorre far sì che tali eventi siano registrati all'interno di un sistema centralizzato, dopo averli sottoposti a filtraggio, aggregazione e normalizzazione. Solo gli eventi provenienti dai sistemi giudicati rilevanti debbono essere raccolti.
- **Definire l'ambito di applicazione**. Occorre documentare quali sono i sistemi rilevanti ai fini del monitoraggio della sicurezza o del rispetto alle normative. Occorre definire quali sono le reti e gli asset interni che fanno parte di una rete protetta. Occorre, infine, produrre un documento che definisca dove sono registrati gli eventi e il periodo di conservazione per ogni tipologia di log.
- **Revisione tempestiva dei log**. Definire quali sono gli *Eventi di interesse*, ovvero gli eventi che possono costituire una minaccia, tenendo conto che, dei milioni di log prodotti giornalmente, meno dell'1% rappresenta una minaccia. Occorre definire dei *Service Level Agreement* (SLA) e delle *Standard Operating Procedures* (SOPs) per ogni tipo di evento di interesse, stabilendo l'intervallo di tempo affinché l'evento venga evidenziato e una procedura da seguire per ogni evento di interesse. Occorre infine schedulare la produzione di report degli eventi chiave dei dispositivi di sicurezza.
- **Creare un percorso di audit degli eventi di interesse**. Occorre mantenere un percorso di audit sicuro per provare come gli eventi di interesse siano stati gestiti e risolti. Documentare come ogni evento di interesse sia stato gestito attraverso le SOPs e rispettando gli SLA.

1.5 Le sfide

La gestione dei log all'interno delle organizzazioni presenta diverse sfide, che si possono riassumere con la considerazione che le risorse per la gestione dei log sono sempre meno e meno preparate, mentre il numero e la varietà dei log è in aumento. Vediamo più in dettaglio quali sono le problematiche.

1.5.1 Gestione e registrazione dei log

I log sono prodotti e risiedono su molti host all'interno dell'organizzazione, rendendo necessaria l'implementazione di un sistema di log management. Una stessa sorgente di log può inoltre generare molteplici log, per esempio un'applicazione può registrare gli eventi di autenticazione in un log e l'attività di rete in un'altra.

Ogni sorgente di log registra solo alcune informazioni all'interno dei propri log, come l'indirizzo IP dell'host e lo username. Per efficienza, spesso la sorgente di log registra solo la parte di informazione ritenuta più importante. Questo può rendere difficile registrare gli eventi provenienti da diverse sorgenti (ad esempio la sorgente 1 registra l'indirizzo IP, ma non lo username e viceversa). Ogni tipo di log può inoltre rappresentare i valori in maniera diversa.

Ogni sorgente di log registra eventi associando un timestamp basato sul suo orologio interno. Se l'orologio interno non è preciso, l'evento verrà registrato con un timestamp non preciso, che in fase di analisi dei log potrebbe portare che una certa sequenza di eventi si sia svolta con un ordine diverso da quanto avvenuto realmente.

Molte sorgenti di log usano diversi formati, come campi separati da virgola, campi separati da tabulazioni, database, syslog, snmp, file xml, file binari. Alcuni formati di log sono pensati per essere letti da umani, altri no. Alcuni log, come le trap snmp, non sono pensati per la memorizzazione in un file, ma per la trasmissione via rete ad altri sistemi.

Formati e contenuti inconsistenti rappresentano un problema in fase di revisione dei log, in quanto occorre comprendere il significato di tutti i campi dati in tutti i log. Per facilitare l'analisi dei log, occorre implementare sistemi automatici per convertire log che hanno contenuti e formati differenti verso un formato standard con una rappresentazione coerente dei campi dati.

1.5.2 Protezione dei log

I log provenienti dai diversi sistemi dell'organizzazione possono contenere dati delicati dal punto di vista della sicurezza o della privacy, come password di utenti, dati relativi alla navigazione o alle mail. Occorre quindi che i log siano protetti adeguatamente sia durante la trasmissione che durante la registrazione, sia dal punto di vista della confidenzialità che dell'integrità. I log infatti non devono essere alterabili, per esempio da parte di malintenzionati che vogliano coprire le loro tracce.

Occorre inoltre garantire la disponibilità dei dati. Per esempio molti sistemi sono configurati in modo che i file di log abbiano una dimensione massima e che, raggiunta tale dimensione, i file di log siano sovrascritti. Per garantire il rispetto delle policy di retention, le organizzazioni devono conservare i log per un periodo di tempo maggiore rispetto a quello di persistenza sui sistemi di origine.

1.5.3 Analisi dei log

All'interno della maggior parte delle organizzazioni, gli amministratori di sistema e di rete sono stati tradizionalmente responsabili dell'analisi dei log, studiando i log per identificare eventi di interesse. L'analisi dei log è spesso stata trattata come attività a bassa priorità da amministratori e dal management, perché altre attività degli amministratori necessitavano di risposte più rapide.

Gli amministratori che effettuano l'analisi dei log spesso non ricevono formazione adeguata per effettuare l'analisi efficacemente ed efficientemente, particolarmente per quel che riguarda la prioritarizzazione. Inoltre molti amministratori non hanno a disposizione tool che siano efficaci nell'automatizzazione dei processi di analisi. Molti di questi tool sono particolarmente efficaci nel trovare pattern che gli umani non possono vedere facilmente, come la correlazione di eventi da diverse sorgenti che si riferiscono allo stesso evento. Un altro problema consiste nel fatto che molti amministratori considerano l'attività di analisi dei log noiosa e poco proficua rispetto al tempo richiesto. L'analisi dei log è spesso trattata come reattiva, spesso fatta dopo che un problema è stato già identificato mediante altri mezzi, piuttosto che proattiva, per identificare problemi imminenti. Tradizionalmente, la maggior parte dei log non viene analizzata in realtime.

1.6 I modelli

1.6.1 Il modello Syslog

In una infrastruttura di log management basata sul modello syslog, ogni sorgente produce log dello stesso formato e utilizza lo stesso meccanismo per trasferire i log a un server syslog remoto. Syslog fornisce un semplice framework per la generazione, lo storage e il trasferimento dei log, che ogni sistema operativo, software di sicurezza o applicazione può utilizzare, se è progettato per poterlo fare. Molte sorgenti di log usano syslog come formato nativo oppure offrono la possibilità di convertire i log dal loro formato nativo a syslog.

Lo standard syslog consente di operare una classificazione del messaggio, al fine di di stabilirne la tipologia e la priorità, basandosi su due attributi: la *facility* e la *severity*. La facility rappresenta la tipologia del messaggio, per esempio messaggio del kernel, messaggio di autorizzazione, di sicurezza, applicativo. La severity può assumere un valore compreso fra 0 (emergency) e 7 (debug).

Il formato syslog è pensato per essere molto semplice e prevede che ogni messaggio sia formato da 3 parti: la prima parte contiene la facility e la severity, descritte sopra, in formato numerico, la seconda parte contiene il timestamp e il nome host (o l'indirizzo IP) del sistema che ha generato l'evento e la terza parte è il contenuto del messaggio. Non ci sono campi standard definiti per syslog e l'unica possibilità di classificazione è quella basata su severity e faciltiy: solo mediante questi attributi è possibile decidere come trattare e come fare il forward dei log.

Lo storage dei log syslog può essere effettuato utilizzando file di testo locali al sistema che li ha generati oppure può essere effettuando un forward verso uno o più sistemi centralizzati.

Lo standard syslog è stato progettato in tempi in cui la sicurezza dei log non era oggetto di molta considerazione, per cui presenta alcuni aspetti critici. In primo luogo il protocollo di trasporto utilizzato da syslog per la trasmissione sulla rete è l'UDP, protocollo senza connessione che non garantisce la consegna dei pacchetti. In secondo luogo, il server syslog che raccoglie messaggi via rete non effettua nessuna forma di autenticazione, per cui qualsiasi sistema può inviare messaggi al server syslog, senza nessun ulteriore controllo. In terzo luogo, i log trasmessi via rete da syslog viaggiano in chiaro ed è quindi possibile intercettarli. Alcune implementazioni di syslog presentano soluzioni a uno o più di questi problemi, per esempio utilizzando TCP invece che UDP, utilizzando TLS per crittografare i dati sulla rete e così via, basate su una proposta di standard l'RFC 3195, che ha lo scopo di migliorare la sicurezza di syslog, oppure anche soluzioni non previste dall'RFC 3195, come la memorizzazione dei log su database. Queste implementazioni, tuttavia, non sono supportate da tutti i sistemi.

1.6.2 Il modello SIEM

Il modello System Information and Event Management (SIEM), pur non essendo standardizzato prevede maggiori funzionalità rispetto al modello syslog e prevede un'infrastruttura più complicata, contenente uno o più server che permettono l'analisi dei log, un database, strumenti per la correlazione degli eventi, uno o più database server per lo storage dei log, strumenti sofisticati per la ricerca e la reportistica.

Essendo il modello SIEM l'oggetto di questa tesi, alla descrizione dettagliata della sua architettura è dedicato tutto il capitolo 2.

```
FIREWALL:

1:15:02 ctl craig.phoneboy.com >daemon sys_message:
installed defaultfilter; product:  VPN-1 & FireWall-1;

1:15:02 ctl craig.phoneboy.com >daemon sys_message:
The eth-s3p1c0 interface is not protected by
the anti-spoofing feature.
Your network may be at risk; product:  VPN-1 & FireWall-1;

1:15:02 ctl craig.phoneboy.com >daemon sys_message:
The eth-s2p1c0 interface is not protected by
the anti-spoofing feature.
Your network may be at risk; product:  VPN-1 & FireWall-1;

1:15:02 ctl craig.phoneboy.com >daemon sys_message:
The eth-s1p1c0 interface is not protected by
the anti-spoofing feature.
Your network may be at risk; product:  VPN-1 & FireWall-1;

1:43:20 ctl craig.phoneboy.com >daemon sys_message:
installed phoneboy-traditional; product:  VPN-1 & FireWall-1;

1:43:20 craig.phoneboy.com >daemon cp_message:
Parameter 'Connections hash table size' changed from
65536 to 32768;

12:34:08 drop craig >eth-s2p1c0 product:
VPN-1 & FireWall-1; src:  Alpha-Cluster-Inside.foo.com;
s_port:  IKE; dst:  craig; service:  876; proto:  udp; rule:  5;
12:48:17 accept craig >eth-s1p1c0 product:
VPN-1 & FireWall-1; src:  cartman.phoneboy.com; s_port:  2343;
dst:  craig; service:  https; proto:  tcp; rule:  1;

INTRUSION DETECTION SYSTEM:

11/06/04-00:32:05.706661 {ICMP}
192.168.206.129 -> 192.168.100.5 [**] [1:469:3] ICMP
PING NMAP [**] [Classification:  Attempted Information Leak]
[Priority:  2] [Xref =>
http://www.whitehats.com/info/IDS162]

11/06/04-00:32:10.896823 {ICMP}
192.168.206.129 -> 192.168.100.5 [**] [1:469:3] ICMP
PING NMAP [**] [Classification:  Attempted Information Leak]
[Priority:  2] [Xref => http://www.whitehats.com/info/IDS162]
```

Figura 1.2.1: Esempi di log di sistemi di sicurezza

```
Oct 15 18:19:08 localhost audispd:  node=prx01
type=ANOM_PROMISCUOUS msg=audit(1318695548.187:3561):
dev=eth0 prom=0 old_prom=256 auid=10000 ses=500

Oct 15 18:19:08 localhost audispd:  node=prx01 type=SYSCALL
msg=audit(1318695548.187:3561):  arch=c000003e syscall=3
success=yes exit=0 a0=3 a1=1 a2=13e0c020 a3=0 items=0
ppid=25014 pid=25449 auid=10000 uid=77 gid=77 euid=77
suid=77 fsuid=77 egid=77 sgid=77 fsgid=77 tty=pts0 ses=500
comm="tcpdump" exe="/usr/sbin/tcpdump"
subj=user_u:system_r:unconfined_t:s0 key=(null)

Oct 15 18:19:08 localhost audispd:  node=prx01 type=EOE
msg=audit(1318695548.187:3561):
Oct 15 18:21:29 localhost kernel:
device eth0 entered promiscuous mode

Oct 15 18:21:29 localhost audispd:  node=prx01
type=ANOM_PROMISCUOUS msg=audit(1318695689.232:3562):
dev=eth0 prom=256 old_prom=0 auid=10000 ses=500

Oct 15 18:21:29 localhost audispd:  node=prx01 type=SYSCALL
msg=audit(1318695689.232:3562):
arch=c000003e syscall=54 success=yes exit=0
a0=3 a1=107 a2=1 a3=7fffc25fdb90
items=0 ppid=25014 pid=25980 auid=10000 uid=0
gid=0 euid=0 suid=0 fsuid=0 egid=0 s
gid=0 fsgid=0 tty=pts0 ses=500 comm="tcpdump"
exe="/usr/sbin/tcpdump"
subj=user_u:system_r:unconfined_t:s0 key=(null)
```

Figura 1.2.2: Esempio di log di sistema operativo linux

```
192.168.1.1 192.168.1.24 - - [07/Oct/2011:14:53:16 +0200]
"GET /wpad.dat
HTTP/1.1" 404 1027 "-" "-"

192.168.1.100 - - - [07/Oct/2011:15:01:52 +0200]
"GET /squidlog/usage_201109.html HTTP/1.1" 200 105266 "-"
"Mozilla/5.0 (Windows NT 6.1; rv:7.0.1)
Gecko/20100101 Firefox/7.0.1"

192.168.1.100 - - - [07/Oct/2011:15:01:52 +0200]
"GET /squidlog/ctry_usage_201109.png HTTP/1.1"
200 2478 "http://prx01/squidlog/usage_201109.html"
"Mozilla/5.0 (Windows NT 6.1; rv:7.0.1)
Gecko/20100101 Firefox/7.0.1"

192.168.1.100 - - - [07/Oct/2011:15:01:52 +0200]
"GET /squidlog/hourly_usage_201109.png HTTP/1.1"
200 2103 "http://prx01/squidlog/usage_201109.html"
"Mozilla/5.0 (Windows NT 6.1; rv:7.0.1)
Gecko/20100101 Firefox/7.0.1"

1192.168.1.100 - - - [07/Oct/2011:15:01:52 +0200]
"GET /favicon.ico HTTP/1.1" 404 1008 "-"
"Mozilla/5.0 (Windows NT 6.1; rv:7.0.1)
Gecko/20100101 Firefox/7.0.1"

192.168.1.100 - - - [07/Oct/2011:15:02:52 +0200]
"GET /calamaris/ HTTP/1.1" 200 481 "-"
"Mozilla/5.0 (Windows NT 6.1; rv:7.0.1)
Gecko/20100101 Firefox/7.0.1"

192.168.1.100 - - - [07/Oct/2011:15:02:56 +0200]
"GET /calamaris/weekly.html HTTP/1.1" 200 214903
"http://prx01/calamaris/"
"Mozilla/5.0 (Windows NT 6.1; rv:7.0.1)
Gecko/20100101 Firefox/7.0.1"

192.168.1.1 192.168.1.30 - - [07/Oct/2011:15:05:58 +0200]
"GET /wpad.dat HTTP/1.1" 404 1027 "-" "-"
```

Figura 1.2.3: Esempio di log di un web server apache

Capitolo 2

Architettura di un SIEM

Sebbene non esista uno standard che definisca l'architettura di un SIEM, è tuttavia possibile descrivere i moduli di cui solitamente si compone e le loro interazioni (vedi figura 2.0.1).

Possiamo distinguere cinque moduli: generazione di eventi, collezionamento di eventi, registrazione e immagazzinamento, analisi, monitoraggio e reporting.

Nel seguito del capitolo approfondiremo le funzioni di ognuno di questi moduli, unitamente ad una discussione sulle problematiche da affrontare e le possibili soluzioni. Verranno anche discusse le modalità di integrazione fra i diversi moduli.

2.1 Generazione

La generazione degli eventi avviene all'interno dei sistemi e delle applicazioni di cui si vogliono raccogliere i log da far pervenire al SIEM. Ad una prima analisi questo modulo sembrerebbe non fare parte del SIEM, tuttavia, considerando il SIEM come un processo piuttosto che come un sistema da acquistare ed installare, anche questo modulo rientra a tutti gli effetti nel SIEM.

Possono essere considerate due diverse famiglie di eventi generati. I generatori di dati basati su eventi (*sensori*), generano eventi corrispondenti a specifiche operazioni svolte da sistemi operativi, applicazioni, dispositivi di sicurezza e così via sulla rete. I generatori di dati basati sullo stato (*poller*), generano eventi basati sulla reazione a stimoli esterni, come un ping, dati relativi a check di integrità o demoni che hanno il compito di verificare lo stato di un certo servizio.

- **Sensori**. Sebbene nell'ambito della sicurezza informatica il tipo più noto di sensori siano gli IDS, sia network based che host based, si possono far rientrare in questa categoria la maggior parte delle tipologie di log di sicurezza elencati alla sezione 1.2, come i log di firewall, VPN, sistemi di autenticazione, i log di sistemi operativi e applicazioni, ecc.

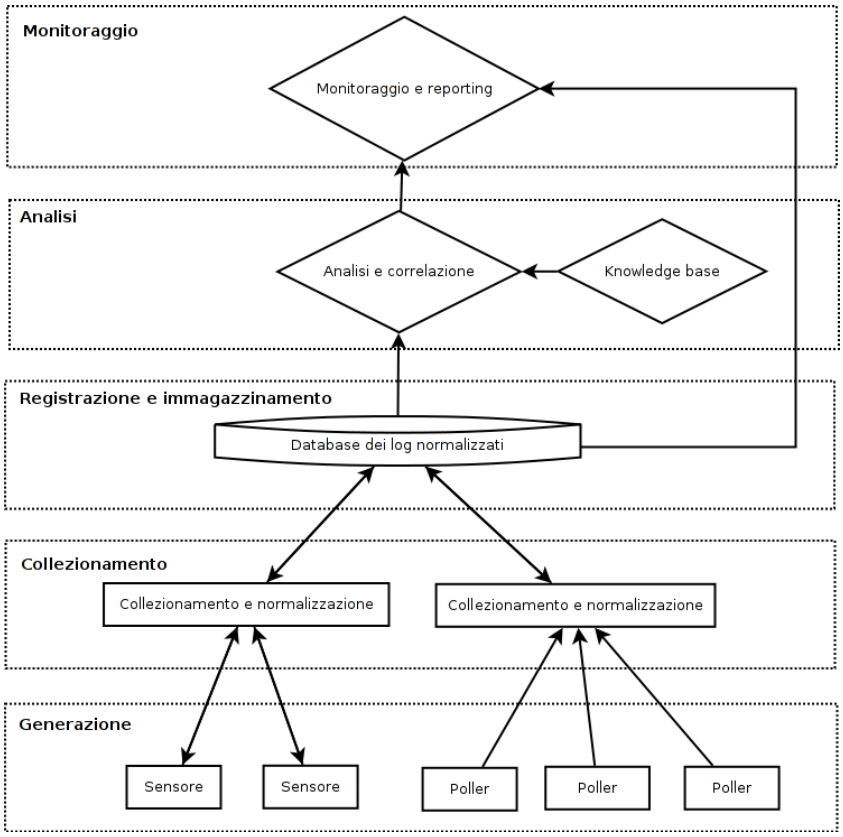

Figura 2.0.1: Macro architettura di un SIEM

- **Poller**. Lo scopo dei poller è quello di generare un evento ogni qualvolta un sistema terzo raggiunga un determinato stato. In un ambito di sicurezza, i poller sono responsabili della verifica dello stato di servizi (per rilevare la presenza di DOS) e la verifica dell'integrità.

2.2 Collezionamento

Lo scopo di questo modulo è quello di raccogliere informazioni dai diversi sensori e poller e tradurle in un formato standard, in modo da avere una base omogenea di messaggi.

Al di là dei diversi meccanismi di collezionamento utilizzati dai SIEM, esistono fondamentalmente due metodi di collezionamento. Si parla di metodo basato su agenti (*agent-based*) quando il collezionamento avviene attraverso un agente software del SIEM installato sul sistema sorgente, di metodo senza agen-

ti (*agentless*), quando il collezionamento avviene senza nessun tipo di agente installato su di esso.

- **Agentless**. Il server SIEM riceve i log dai sistemi sorgenti senza bisogno di installare su di essi nessun software particolare. Alcuni SIEM hanno la possibilità di iniziare la connessione con il sistema sorgente, utilizzando opportuni meccanismi di autenticazione, e andare a reperire ad intervalli regolari i log presenti, per esempio disponibili in un database o in un file di testo; si parla in tal caso di *metodo pull*. In altri casi i sistemi sorgente inviano loro stessi i log al SIEM, dove è presente un opportuno receiver: in tal caso si parla di *metodo push*. Esempio di questo tipo di metodo è il syslog.

- **Agent based**. Un agente software è installato sui sistemi che generano i log, allo scopo di effettuare filtraggio, aggregazione e normalizzazione per un certo tipo di log, trasmettendo poi i dati dei log normalizzati, normalmente in real-time o quasi in real-time, per l'analisi e l'immagazzinamento. Se un sistema ha diverse tipologie di log di interesse, è necessario installare più agenti.

In ognuna delle precedenti tipologie di collezionamento sono presenti vantaggi e svantaggi. Il vantaggio principale dell'approccio agentless è che non occorre installare, configurare e mantenere agenti in ogni sorgente di log. Lo svantaggio principale sta invece nel fatto che non è possibile effettuare filtraggio, aggregazione e normalizzazione a livello di sistema sorgente. Un altro possibile svantaggio è nella necessità di dotare il SIEM di credenziali valide per ogni sistema sorgente.

Normalmente i SIEM hanno metodi predefiniti per il collezionamento, il filtraggio, l'aggregazione e la normalizzazione di log di particolari sistemi o applicazioni (per esempio, server web, database relazionali, mail server, ecc.). In tali casi il SIEM sa come interpretare i vari campi presenti nel log originario (per esempio il campo numero 12 rappresenta l'IP sorgente) o determinati valori presenti nel log originario (per esempio l'evento con codice 680 in un sistema Windows rappresenta un'autenticazione fallita).

Per sistemi o applicazioni che non dispongono di metodi predefiniti i SIEM forniscono normalmente strumenti che permettono di costruirsi i propri metodi, rendendo il SIEM molto più flessibile. Naturalmente per costruire il proprio metodo di collezionamento è indispensabile conoscere il formato dei log da collezionare e dei campi disponibili all'interno del SIEM.

Scopo del modulo di collezionamento è anche quello di operare una *normalizzazione* dei log. Con normalizzazione si intende il processo che permette di trasformare i log raccolti dai diversi sistemi sorgenti nei loro formati nativi in un unico formato che sia utilizzabile all'interno del SIEM.

Come esempio, supponiamo di avere due eventi provenienti da sistemi diversi, un server Windows Server 2003 (fig. 2.2.1) e un server Linux (fig. 2.2.2) e che entambi gli eventi rappresentino un tentativo fallito di login.

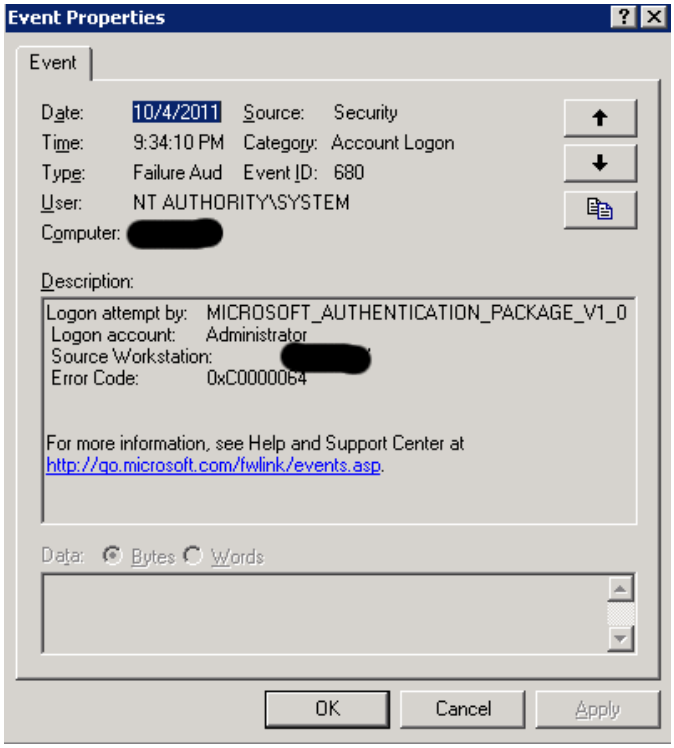

Figura 2.2.1: Evento di login fallito su Windows

```
Oct 4 21:38:34 192.168.1.1 sshd[28061]:  pam_unix(sshd:auth):
authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=localhost.localdomain user=root

Oct 4 21:38:36 192.168.1.1 sshd[28059]:
error:  PAM: Authentication failure for root from
localhost.localdomain
```

Figura 2.2.2: Evento di login fallito su Linux

Come si può vedere due diversi sistemi producono per un evento simile due log differenti. Un esempio di come potrebbero apparire i due eventi dopo il processo di normalizzazione è riportato nella tabella 2.1

Time	Device Vendor	Device Type	Event Type	Address	Host Name	User Name	Behavior
2011/10/04 21:34:10 CEST	Microsoft	Operating System	Authentication	192.168.1.2	WinHost	Administrator	Failure
2011/10/04 21:38:36 CEST	Unix	Operating System	Authentication	192.168.1.1	LinuxHost	root	Failure

Tabella 2.1: Eventi normalizzati

Altre operazioni che possono avvenire nell'ambito di questo modulo sono il *filtraggio* e l'*aggregazione*. Con filtraggio si intende la selezione, all'interno del sistema sorgente, dei log che hanno un certo interesse per la successiva registrazione e analisi e l'esclusione dei log privi di interesse. Con aggregazione si intende il consolidamento di più eventi simili in un'unica entry che abbia un campo contatore del numero di eventi.

2.3 Registrazione e immagazzinamento

Per lavorare con l'elevato numero di log che arrivano al SIEM, occorre definire un sistema di memorizzazione che permetta di conservare i log per il periodo definito allo scopo di soddisfare i requisiti normativi e di effettuare analisi storiche. Nella scelta del meccanismo di memorizzazione occorre tenere presente la facilità con cui è possibile definire query per estrarre gli eventi di interesse e la rapidità di risposta alle query definite.

Esistono tipicamente tre metodi di memorizzazione dei log: in un database, in file di testo, in file binari. Il caso di memorizzazione in un database standard è attualmente il più utilizzato, in quanto è il sistema che permette solitamente il miglior compromesso fra la necessità di utilizzare i log da parte di altre applicazioni, la necessità di eseguire facilmente le analisi, e la necessità di accedere a tali dati in maniera efficiente. I file di testo, pur permettendo l'accesso ai log da parte di altre applicazioni e di eseguire facilmente analisi, non permettono di accedere in maniera efficiente ai dati, soprattutto in presenza di archivi contenenti grandi quantità di log. Al contrario, i formati binari permettono di accedere in maniera efficiente ai dati, ma non permettono l'accesso ad altre applicazioni che non siano il SIEM stesso.

Per garantire l'integrità dei dati memorizzati, alcuni SIEM calcolano un digest sul database dei log, o sui file che contengono i log, o su ogni record contenuto nel database. Un digest è una firma che identifica univocamente

i dati, con la caratteristica che cambiando un singolo bit del dato, il digest cambia. I principali algoritmi utilizzati per il calcolo del digest sono l'MD5 e lo SHA-1. In questa maniera, se per qualche motivo i log fossero alterati il digest cambierebbe e si avrebbe la prova dell'alterazione. Un altro meccanismo per garantire l'integrità può essere la conservazione dei log su dispositivi di sola lettura.

Pur nella specificità dei vari SIEM, per ognuno dei quali la tabella dei messaggi conterrà campi diversi, è possibile individuare un insieme minimo di campi che generalmente, affinché il SIEM possa svolgere la sua funzione, fanno parte della tabella dei messaggi.

- **Time**. Contiene il timestamp in cui è avvenuto l'evento. Può essere affiancato da altri timestamp, per esempio il timestamp in cui è avvenuto il parsing dell'evento.
- **Type**. Contiene il tipo di sistema che ha generato l'evento, per esempio sistema operativo, database, firewall, ecc.
- **Category**. Contiene la tipologia dell'evento, per esempio se si tratta di un'autenticazione, di un'autorizzazione, dell'avvio di un'applicazione, ecc.
- **Severity**. Contiene il livello di pericolosità dell'evento.
- **Device**. Contiene il sistema che ha generato l'evento. Può essere diviso su più campi, contenenti per esempio l'indirizzo IP, l'hostname e il fully qualified hostname.
- **Source**. Contiene il sistema da cui è partito l'evento. Per esempio, in un login via rete, contiene un riferimento al sistema da cui l'utente ha fatto il login. Come per il device, anche in questo caso l'informazione può essere divisa su più campi.
- **Destination**. Contiene il destinatario dell'evento. Per esempio, in un login via rete, contiene un riferimento al sistema su cui l'utente ha fatto il login. Come per il device e il source, anche in questo caso l'informazione può essere divisa su più campi.
- **User**. Contiene, se esiste, l'account che ha generato l'evento. Può essere diviso in user sorgente e user destinazione per tenere conto del caso di eventi che contengano una sorgente e una destinazione.
- **Message**. Contiene un testo che descrive l'evento.

Oltre ai log, il SIEM si occuperà di registrare le statistiche e gli eventi di alert.

2.4 Analisi

2.4.1 Il Rule e il Correlation Engine

Lo scopo dell'analisi è quello di cercare eventuali anomalie all'interno dei log, per esempio per rilevare attacchi o tentativi di attacco. In un SIEM nel quale

tutti i log con una qualche rilevanza dal punto di vista della sicurezza siano centralizzati e nel quale siano presenti strumenti che permettano di operare facilmente delle ricerche per individuare eventi di interesse, tale analisi può essere operata da parte di analisti della sicurezza; questo tipo di approccio, tuttavia, è utile soprattutto in fase investigativa. Per poter operare in maniera proattiva nei SIEM esiste normalmente un componente, il *rule engine*, che permette di generare allarmi da mostrare sulla console agli operatori del SOC, oppure da inviare via mail, in base al verificarsi di determinate condizioni. Generalmente le regole vengono scritte utilizzando una qualche forma di logica booleana.

Supponiamo di voler generare un allarme ogni qualvolta un utente faccia login via rete su un server utilizzando credenziali amministrative locali e supponiamo che all'interno dell'organizzazione siano presenti server Windows e server Linux (vedi fig. 2.4.1). Normalmente dovremmo definire diversi trigger all'interno dei diversi sistemi, mentre in un SIEM, utilizzando la logica interna, è possibile definire un'unica regola basata su diverse variabili che definisca un trigger.

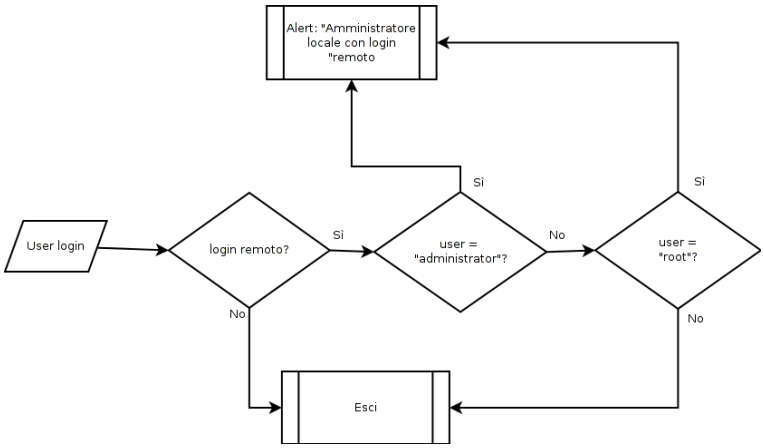

Figura 2.4.1: Regola per login amministrativo

Uno strumento più sofisticato per generare allarmi è rappresentato dal *correlation engine*, un sottoinsieme del rule engine che permette di correlare diversi eventi provenienti da diverse sorgenti creando un unico evento correlato. Tale correlazione viene operata allo scopo di semplificare l'identificazione di potenziali incidenti e le procedure di risposta.

Supponiamo di voler rilevare un attacco di forza bruta andato a buon fine verso un server, costituito da una serie di tentativi di login falliti su tale server provenienti dallo stesso IP sorgente, seguito da un tentativo di login andato a buon fine, in un certo intevallo di tempo. Supponiamo di avere una situazione come quella presente in tabella 2.2.

In una situazione reale la situazione è molto più complicata, perchè potremmo avere migliaia di eventi al secondo: chiaramente, in tale situazione, sarebbe

Time	Eventi ID	Source	Destination	Message
2011/10/04 21:34:10 CEST	**10087**	**192.168.1.2**	**10.10.10.25**	**Login failed**
2011/10/04 21:34:10 CEST	10088	192.168.1.10	10.10.10.30	Login successfull
2011/10/04 21:34:10 CEST	**10089**	**192.168.1.2**	**10.10.10.25**	**Login failed**
2011/10/04 21:34:10 CEST	10090	192.168.1.11	10.10.10.31	Login failed
2011/10/04 21:34:10 CEST	10091	192.168.1.12	10.10.10.35	Login successfull
2011/10/04 21:34:10 CEST	10092	192.168.1.12	10.10.10.36	Login successfull
2011/10/04 21:34:10 CEST	**10093**	**192.168.1.2**	**10.10.10.25**	**Login failed**
2011/10/04 21:34:10 CEST	10094	192.168.1.13	10.10.10.100	Login failed
2011/10/04 21:34:10 CEST	10095	192.168.1.13	10.10.10.110	Login failed
2011/10/04 21:34:10 CEST	**10096**	**192.168.1.2**	**10.10.10.25**	**Login successfull**

Tabella 2.2: Eventi standard in un SIEM

molto difficile rilevare manualmente un attacco di forza bruta. Il correlation engine permette, utilizzando operatori di logica booleana, di definire una regola che permetta di correlare i diversi eventi in un singlolo evento, che possa generare un allarme. Un esempio di una possibile definizione che permetta di rilevare un attacco di forza bruta è il seguente:

```
If [(failed logins >= 3) and then (Successful Login)]
   from the same source within 20 seconds =
     Possible Brute Force Compromise
```

2.4.2 La Knowledge Base

Di ausilio alla fase di analisi è anche la componente di Knowledge Base, dove viene tenuta traccia del livello globale di sicurezza dell'infrastruttura IT. Questo permette di valutare se un tentativo di intrusione su un certo sistema può effettivamente portare ad un'intrusione e il livello di criticità di tale tentativo di intrusione.

Fanno parte della componente di knowledge base il *database degli asset*, il *database delle vulnerabilità* e le *policy di sicurezza* dell'organizzazione.

Il database degli asset può essere utilizzato per definire alcuni aspetti delle configurazioni dei sistemi, il tipo di servizio garantito all'interno del sistema informativo, gli altri sistemi al quale sono correlati, i referenti; in definitiva lo scopo è quello di determinare il livello di criticità dei sistemi e l'impatto che può avere un'eventuale intrusione.

Il database delle vulnerabilità contiene informazioni relative alle violazioni della sicurezza e ai comportamenti insicuri che possono avere impatto sul livello globale di sicurezza o che possono essere utilizzate da un attaccante allo scopo di effettuare un'intrusione. Il database delle vulnerabilità può contenere i seguenti tipi di vulnerabilità:

- *vulnerabilità strutturali*, ovvero vulnerabilità presenti in software specifici, per esempio buffer overflow; questa parte del database può essere popolata attraverso report di software di vulnerability scanner;

- *vulnerabilità funzionali*, ovvero vulnerabilità che dipendono da configurazioni, comportamenti degli utenti, ecc. Un esempio di questo tipo è la presenza di un server nfs che espone delle share non adeguatamente protette di cui un eventuale malintenzionato può fare il mount, accedendo così al filesystem. Contrariamente alle vulnerabilità del tipo precedente, queste vulnerabilità dipendono fortemente dall'ambiente in cui risiedono. La parte più difficoltosa è trovare il modo per definire / formattare questo tipo di vulnerabilità in maniera tale da popolare il database;

- *vulnerabilità basate sulla topologia di rete*, incluso l'impatto delle intrusioni sulla rete e le loro conseguenze. Questa parte del database include le vulnerabilità di rete (sniffing, spoofing, ecc.) così come l'impatto del filtraggio sui path di intrusione. Questo tipo di vulnerabilità non possono essere contenute in un database, a meno che questo non supporti un minimo di modellazione topologica.

Gli aspetti principali delle policy di sicurezza che devono essere considerati sono le autorizzazioni e le procedure di testing /auditing. Questi due aspetti forniranno informazioni riguardanti i comportamenti che i sensori dovranno rilevare. Gli eventi generati (login amministrativi, portscan, ecc.) potranno essere marcati come conformi alle policy di sicurezza oppure come parte di un possibile tentativo di intrusione.

L'obiettivo finale della knowledge base è quella di valutare lo stato di sicurezza dei sistemi monitorati. Le informazioni contenute nella knowledge base possono essere processate da un apposito engine, che fornirà una lista delle vulnerabilità a cui ogni sistema è soggetto, il potenziale impatto di ogni vulnerabilità e i path di intrusione che possono sfruttare tali vulnerabilità. Tale valutazione andrà rigenerata ogni qualvolta venga trovata una nuova vulnerabilità e ogni qualvolta ci siano modifiche ai sistemi monitorati.

2.5 Monitoraggio

Il monitoraggio è il modo con cui gli operatori del SOC e gli analisti della sicurezza interagiscono con il log registrati nel SIEM.

Generalmente i SIEM hanno una console, che può essere web-based o client-server, che permette di interagire con i dati registrati sul SIEM. In generale sono presenti tre interfacce:

- interfaccia per il monitoraggio real-time: fornisce una visione real-time degli eventi che arrivano al SIEM, permettendo un filtraggio base allo scopo di isolare i messaggi di interesse. Viene usata per scopi di debugging, per analisi approfondite di eventi specifici e per la reazione ad eventi;

- 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;
- interfaccia per le analisi statistiche: fornisce dati sulle statistiche di attività di sicurezza sul corto, medio e lungo periodo.

Oltre alla console, i SIEM hanno generalmente strumenti meno operativi, a disposizione dei responsabili della sicurezza e del management aziendale. In generale sono presenti le seguenti interfacce:

- interfaccia per la valutazione dei rischi: fornisce informazioni sull'attuale livello di sicurezza delle configurazioni dei sistemi monitorati e dei software installati. Fornisce informazioni sul livello di sicurezza globale, sulle vulnerabilità e le criticità, gli scenari di intrusioni e i dettagli sulle patch e le configurazioni;
- 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;
- stato dei sistemi: fornisce un quadro sugli incidenti aperti, sistemi sotto attacco e path di intrusione attivati dagli attaccanti. Fornisce informazioni sulle procedure di reazione ed escalation messe in atto allo scopo di circoscrivere l'attacco.

Nella figura 2.5.1, alla luce di quanto detto in questo capitolo, è schematizzata un'architettura più di dettaglio di un SIEM. Sono presenti i moduli descritti all'interno del capitolo e per ognuno di essi i componenti descritti. È stato inoltre schematizzato il flusso delle informazioni e le interazioni fra i vari moduli.

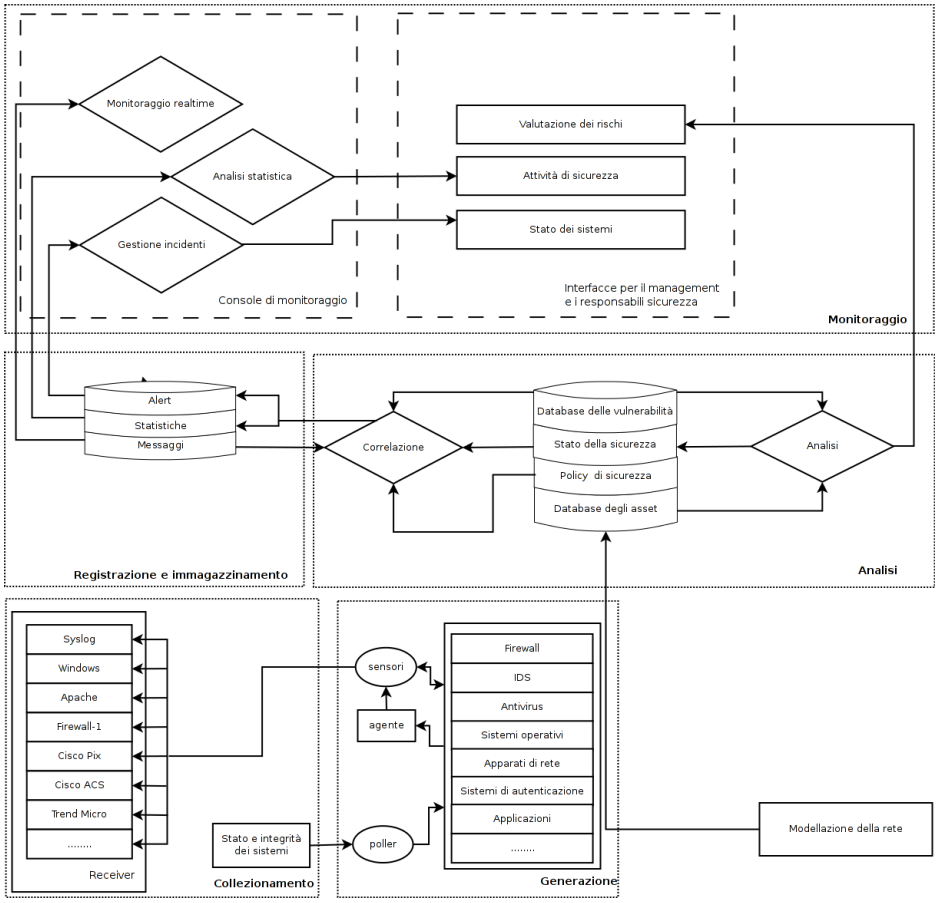

Figura 2.5.1: Architettura di dettaglio di un SIEM

Capitolo 3

ArcSight ESM

Al fine di realizzare quanto esposto nel capitolo precedente, i principali vendor hanno sviluppato soluzioni di System Information and Event Management complete, che integrano tutte le componenti dell'architettura.

Sul mercato sono presenti moltissimi prodotti con caratteristiche simili, come ad esempio: Q1 Labs QRadar, Cisco Security Mars, RSA Envision.

In questo capitolo verranno illustrate l'architettura e le caratteristiche di Arcsight Enterprise Security Manager (ESM), il prodotto utilizzato presso la Regione Emilia-Romagna per la realizzazione del sistema di monitoraggio.

3.1 Architettura di Arcsight ESM

L'Arcsight ESM consiste di diversi componenti installabili separatamente che cooperano per processare i dati degli eventi della rete di un'organizzazione. Questi componenti si connettono alla rete attraverso sensori che nella terminologia ArcSight sono denominati ESM SmartConnector. Gli SmartConnector trasformano una moltitudine di log di diversi sistemi in uno schema normalizzato che diventa il punto di partenza per le componenti di correlazione e analisi.

La figura 3.1.1 illustra i componenti dell'ESM e i componenti opzionali che gestiscono il flusso e l'analisi degli eventi e permettono il monitoraggio della rete e la risposta agli incidenti. Tali componenti verranno illustrati nel corso del capitolo, man mano che intervengono all'interno della descrizione organizzata secondo il ciclo di vita degli eventi.

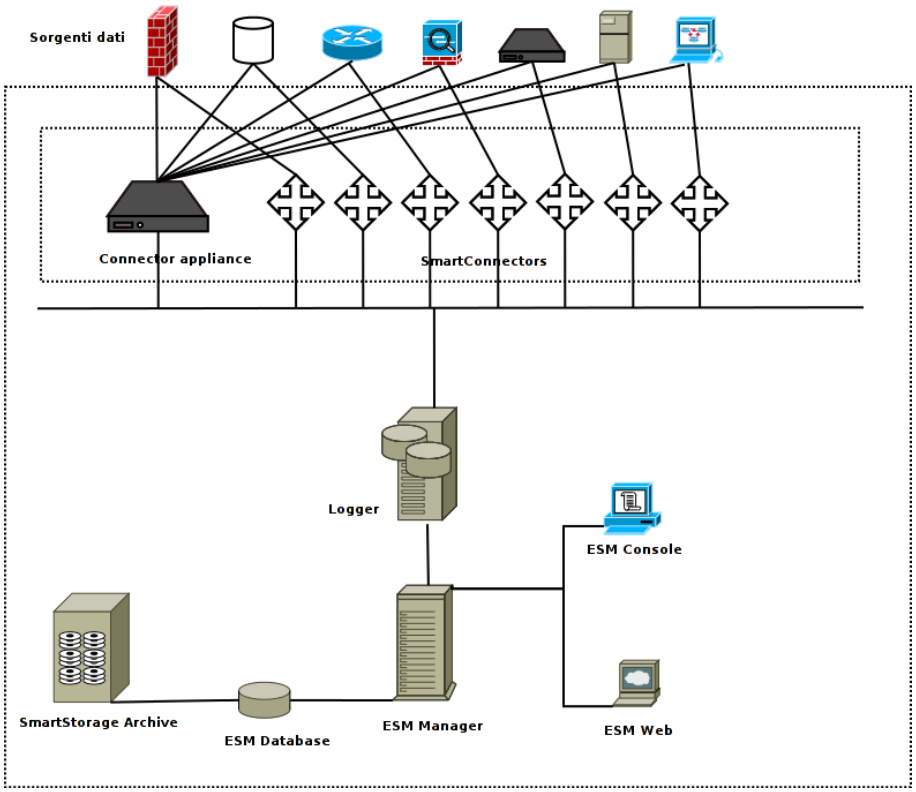

Figura 3.1.1: Architettura dell'ESM

L'ESM processa gli eventi in varie fasi, allo scopo di identificare gli eventi di interesse e operare le rispettive contromisure. La figura 3.1.2 fornisce una panoramica delle fasi principali che costituiscono il ciclo di vita di un evento attraverso l'ESM.

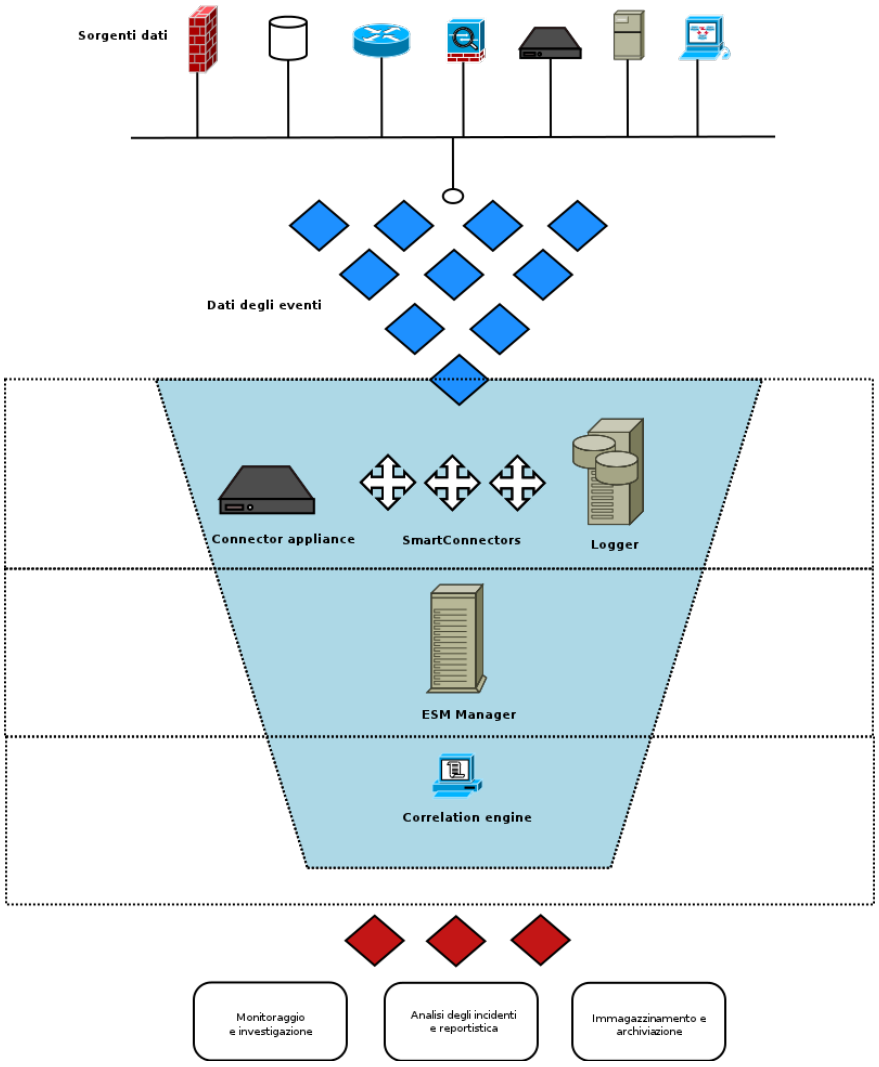

Figura 3.1.2: Ciclo di vita degli eventi nell'ESM

Appare evedente che le fasi riportate nella figura coincidono con i moduli mostrati in figura 2.1 e descritti nel capitolo 2. Nel seguito del capitolo verranno illustrate le modalità e le specificità con cui l'ESM implementa tali moduli.

3.2 Collezionamento

3.2.1 I componenti

La fase di collezionamento viene operata dagli *SmartConnector*, che possono essere installati sui sistemi sorgenti (modalità agent), oppure su server dedicati o sulla *Connector Appliance* (modalità agentless).

SmartConnector Gli SmartConnector sono l'interfaccia con i sistemi sorgenti di eventi rilevanti sulla rete dell'organizzazione. Il loro scopo è quello di collezionare eventi sulla rete. Gli eventi collezionati dagli SmartConnector sono normalizzati nel formato comune dell'ESM, descritto in seguito; gli eventi possono inoltre essere filtrati e aggregati, così da ridurre il volume inviato all'ESM Manager e migliorare l'efficienza e l'accuratezza.

Gli SmartConnector inoltre categorizzare gli eventi usando un formato facilmente leggibile e interpretabile e in modo indipendente dal sistema sorgente, sul quale poter facilmente costruire filtri, regole, report e monitoraggio nelle fasi successive.

Gli SmartConnector si occupano infine di trasmettere gli eventi all'ESM Manager.

Connector Appliance La Connector Appliance è una soluzione hardware che permette di ospitare tutti gli SmartConnector necessari in un'unico device, che contiene anche un'interfaccia utente di management per gli SmartConnector contenuti nell'appliance stessa, in server remoti dedicati, oppure installati sui sistemi sorgenti dei log, permettendo operazioni massive su tutti i tipi di connettori.

FlexConnector ArcSight fornisce SmartConnector configurati per i sistemi sorgenti più diffusi, come sistemi di intrusion prevention and detection, tool di vulnerability assessment, firewall, antivirus e antispam, sistemi operativi, web server, application server, database server, apparati di rete e così via.

Per poter integrare all'interno del SIEM anche i log di sistemi non direttamente supportati dagli SmartConnector, Arcsight fornisce anche il FlexConnector, un software development kit (SDK) che permette la creazione di SmartConnector basati su qualsiasi sorgente di log. Vengono forniti metodi per il parsing di file di testo basati su regular expression, di file di testo di tipo CSV, di tabelle di database basate su timestamp o su id.

3.2.2 I processi

Nella figura 3.2.1 sono schematizzati i processi relativi alla fase di collezionamento svolta dagli SmartConnector. I connettori normalizzano i dati nello schema dell'ESM, categorizzano gli eventi e operano filtraggio e aggregazione degli eventi per ridurre il loro volume.

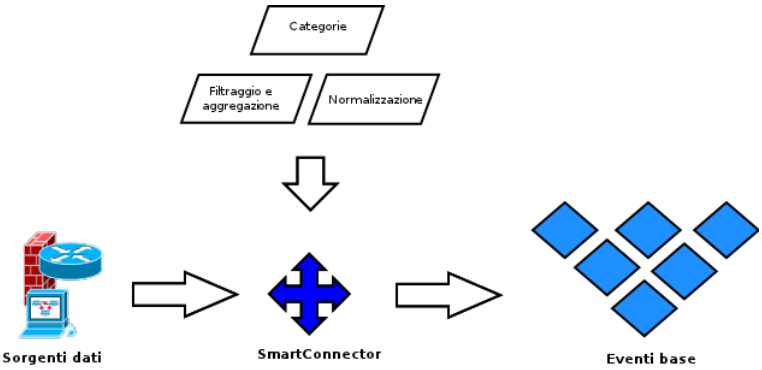

Figura 3.2.1: Collezionamento

Collezionamento e normalizzazione Il modo in cui log dei sistemi sorgenti raggiungono i connettori dipende dal tipo di sorgente; in tali casi ciò può avvenire direttamente, in altri attraverso dei concentratori (es. syslog), in alcuni casi è il connettore che si connette al sistema sorgente, in altri è il sistema sorgente che invia i log attraverso stream di rete.

La normalizzazione, come detto al paragrafo 2.2, permette, a partire da ambiente e dati non eterogenei, di estrarre informazioni omogenee e inserirle nello schema utilizzato dall'ESM. Durante il processo di normalizzazione, in base al livello di pericolo rappresentato dall'evento, assegna un valore all'attributo **Agent Severity** contenuto nello schema dell'ESM, che può assumere i valory *Very Low*, *Low*, *Medium*, *High* e *Very High*, oppure *Unknown* se il connettore non è in grado di assegnare alcun valore. Tale attributo viene utilizzato in fase di analisi per valutare la priorità di un evento.

Categorizzazione In un sistema che raccoglie eventi provenienti dalle categorie più disparate di device, è opportuno che sia presente un modello per descrivere le caratteristiche di ogni evento che viene processato, in modo che sia molto semplice comprendere il significato reale di un evento come riportato da device differenti. Questa modello aiuta, nella fase di analisi e correlazione, a scrivere regole e filtri indipendenti dal sistema che li ha generati. L'ESM fornisce un modello per descrivere gli eventi e lo SmartConnector assegna valori opportuni, secondo quanto stabilito in fase di configurazione del connettore.

Le categorie di eventi sono una serie di sei criteri che traducono il significato di un evento nel formato dell'ESM. Tali sei criteri sono centrali nella fase di analisi. L'elenco delle categorie di eventi è contenuto nella tabella 3.1

Tabella 3.1: Categorizzazione degli eventi nello schema ESM

Categoria	**Descrizione**	**Esempi**
Object	Si riferisce al tipo di oggetto che ha generato l'evento	Application Operating System Resource Router User
Behavior	Si riferisce a cosa viene fatto con l'oggetto che ha generato l'evento	Access Authentication Authorization Execute Modify
Outcome	Descrive se l'operazione descritta in Behavior ha avuto successo. Può contenere Attempt, Failure o Success. Attempt indica che l'esito dell'azione non è chiaro.	Attempt Failure Success
Technique	Descrive la natura del behavior che l'evento rappresenta. Se l'evento è considerato un attacco, identifica il metodo di attacco.	Exploit Brute force Code execution Scan Denial of service
Device Group	Molti dispositivi di sicurezza hanno diversi scopi. Per esempio, un IPS genera eventi di tipo firewall così come eventi di tipo Intrusion Detection. Il Device Group indica se un evento è di un tipo o di un altro, informazione che può essere utilizzata per effettuare query.	Assessment tool Security info manager Firewall IDS Identity Management Operating System Network equipment VPN
Significance	Indica il rischio di sicurezza relativa di un evento basato su vari elementi, incluse le informazioni dal device stesso, le informazioni inserite in fase di modellazione degli asset e i dati da altre categorie di eventi. I valori inseriti in questa categoria possono essere utilizzati dallo staff del Security Operation Center e dagli analisti di sicurezza per assegnare una priorità agli eventi.	Normal Informational Reconnaissance Suspicious Hostile Compromise

Filtraggio e aggregazione Le fasi di filtraggio e aggregazione, descritte nel paragrafo 2.2, nell'ESM sono svolte ancora dallo SmartConnector.

L'aggregazione permette di condensare in un unico evento aggregato più eventi che hanno lo stesso valore in uno specifico insieme di campi, per un numero di volte specificato oppure per un intervallo di tempo specificato. L'evento

aggregato contiene i valori che gli eventi base hanno in comune, più il timestamp dell'evento iniziale e quello dell'evento finale. Il campo *count* contiene il numero di eventi aggregati.

3.3 Registrazione

L'ArcSight ESM utilizza, per la registrazione degli eventi, un database Oracle. In tale database sono memorizzati, oltre agli eventi, anche le configurazioni di sistema e le regole definite dagli utenti.

3.3.1 I componenti

ESM Database Quando lo stream degli eventi arriva all'ESM dagli Smartconnectors, vengono scritti all'interno del Database con uno schema normalizzato. Questo abilita l'ESM ad effettuare analisi a posteriori sugli eventi provenienti dai sistemi sottoposti a monitoraggio.

Un'installazione tipica mantiene i dati on line per un periodo di tempo variabile fra alcune settimane e alcuni mesi.

SmartStorage Partition Management Le SmartStorage Partition sono pozioni di database che possono essere compresse e archiviate (quindi poste off line) per essere utilizzate successivamente in caso di necessità.

ArcSight Logger L'Arcsight Logger è un'appliance ottimizzata per la memorizzazione di grandi quantità di eventi. Il Logger mantiene gli eventi in maniera compressa e inalterabile, allo scopo di poterli estrarre in caso di necessità in caso di analisi forensi.

3.3.2 Lo schema degli eventi

Lo schema degli eventi è il culmine del processo di normalizzazione, e la base della struttura dati che guida la correlazione dell'ESM. I 400 campi dati nello schema sono divisi in 17 gruppi, come mostrato nella tabella 3.2.

Tabella 3.2: Gruppo di eventi

Gruppo eventi	**Descrizione**
Event(root)	Contiene informazioni generali sugli eventi che l'ESM usa per identificare e tracciare
Category	Contiene una descrizione della categoria dell'evento applicata dallo SmartConnector che l'ha ricevuto. Le categorie sono descritte nella tabella 3.1

Gruppo eventi	**Descrizione**
Threat	Descrive la valutazione da parte dell'ESM di quale sia l'importanza dell'evento.
Agent	Descrive lo SmartConnector che ha riportato l'evento nel manager. In un'architettura multi-manager, Agent è lo SmartConnector che ha invito l'evento al manager. In questo caso Agent può essere l'ultimo in una lunga fila di SmartConnector che hanno fatto il forward dell'evento in una geriarchia multi-manager. Gli altri campi convolti in una catena di device sono Device, Final Device, Agent e Original Agent.
Device	Descrive le caratteristiche del sensore che che riporta l'evento allo SmartConnector. Per esempio, se un host ospita un syslog, un HIDS e un web server, i campi in questo gruppo descrivono quale sensore in quell'host ha generato l'evento. Questi campi includono anche i valori ascritti all'evento dal sensore originale, come la severity, che indica la valutazione del livello di minaccia dell'evento da parte del sensore. In un ambiente che usa concentratori questi campi descrivono la prima device della catena che ha processato l'evento. L'ultima device della catena è chiamata Final Device.
Source	Descrive l'asset che è l'origine del traffico di rete rappresentato dall'evento. In un evento che rappresenta un'interazione tra due asset, Source è in coppia con Destination, e insieme, questi campi descrivono il mittente e il ricevente del traffico di rete. Nel caso di un evento che coinvolge solo un asset i campi Source saranno vuoti.
Destination	Descrive l'asse che è il ricevente del traffico di rete rappresentato dall'evento. In un evento che rappresenta un'interazione tra due asset, Destination è in coppia con Source, e insieme questi campi descrivono il mittente e il ricevente del traffico di rete. Nel caso di un evento che coinvolge un solo asset i campi Destination descrivono tale asset.
Attacker	Descrive l'asset che ha iniziato l'azione rappresentata dall'evento. Nel caso di un evento che rappresenta un'interazione tra due asset, Attacker è in coppia con Target, che è il punto focale del traffico di rete. Nella maggior parte dei casi, Attacker è associato con Source, ma in caso di un attacco che causa la divulgazione di informazioni che non dovrebbero andare all'esterno, un sensore, come un IDS, potrebbe intercettare una risposta che indica come il Destination abbia attaccato il Source. Nel caso di un evento che coinvolge solo un asset, i campi Attacker saranno vuoti.
Target	Descrive l'asset che rappresenta il punto focale dell'azione rappresentata dall'evento. Nel caso di un evento che rappresenta un'interazione tra due asset, Target è in coppia con Attacker, che è l'entità che ha iniziato l'attacco. Nel caso di un evento che coinvolge solo un asset, i campi Attacker descrivono il nodo in cui l'azione ha avuto luogo.

Gruppo eventi	Descrizione
File	Si riferisce allo stato corrente di un file in un sistema operativo o di una risorsa ESM che è stata modificata. Questi campi possono essere monitorati nel caso si sia alla ricerca di modifiche su risorse ESM di tipo file e può essere popolato da software di monitoraggio, come Tripwire.
Old File	Si riferisce allo stato precedente di un file in un sistema operativo o di una risorsa ESM che è stata modificata. Questi campi possono essere monitorati nel caso si sia alla ricerca di modifiche su risorse ESM di tipo file e può essere popolato da software di monitoraggio, come Tripwire.
Request	Descrive gli attributi di una richiesta per alcune azioni, come una HTTP GET oppure una query su un database.
Original Agent	In un ambiente multi-Manager, descrive lo SmartConnector che inizialmente ha ricevuto l'evento. È il primo SmartConnector in una catena di SmartConnector che inoltra l'evento in una gerarchia di più Manager.
Final Device	Descrive l'ultimo device che ha processato l'evento prima di essere trasmesso ad uno SmartConnector. Final device entra in gioco solo in un ambiente nel quale un concentratore o un motore di analisi crea una catena di device.
Event Annotation	Contiene ogni assegnazione fatta nell'ambito della gestione di un workflow.
Device Custom	I campi appartenenti a questo gruppo sono riservati per attributi specifici del device che ha generato l'evento, non catturati dal resto dello schema. Questi campi sono definiti dall'autore dello SmartConnector. Ogni campo contiene una coppia etichetta/valore. Se i campi Device Custom vengono utilizzati in filtri, regole o data monitor, occorre includere sempre sia l'etichetta che il valore.
Flex	Nel caso lo schema ESM non catturi tutti i dati da monitorare di un certo device e non ci sia uno SmartConnector personalizzato, è possibile configurare i campi Flex nello schema dello SmartConnector per riportare questi dati. Per esempio, potrebbe essere necessario estendere un FlexConnector per catturare maggiori informazioni, o popolare questi campi in eventi correlati quando viene innescata una regola. Questi campi sono configurabili all'interno del setup di uno SmartConnector. Se i campi del gruppo Flex sono definiti, ogni campo contiene una coppia etichetta/valore. Se i campi Flex vengono utilizzati in filtri, regole o data monitor, occorre includere sempre sia l'etichetta che il valore.

3.4 Analisi

3.4.1 La correlazione

La correlazione implementata dall'ESM permette di evidenziare la relazione tra eventi, inferire il significato di queste relazioni, assegnare una priorità e fornire

infine un framework per implementare una reazione. Il contesto della correlazione è fornito dal modello di rete (vedi sez. 3.4.2.2), la fase di messa in evidenza, l'inferenza e l'azione sono forniti dalle regole. La priorità è determinata dalla categorizzazione e dalla modellazione della rete.

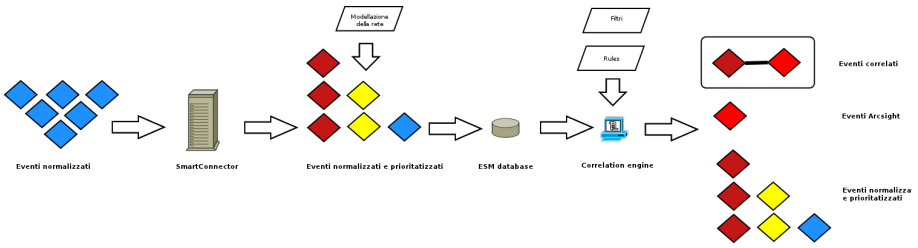

Figura 3.4.1: Il processo di correlazione

3.4.1.1 Rule

Una regola dell'ESM è una procedura programmata che valuta la presenza di condizioni specifiche e pattern all'interno degli eventi. Se viene trovata una corrispondenza, può essere intrapresa un'azione di risposta. Le regole sono la colonna portante del motore di correlazione ESM e sono la componente che rileva significati specifici all'interno del costante flusso di eventi. Vengono costruite usando aggregazioni e espressioni booleane per valutare oggetti come campi di eventi, modelli di rete e active lists.

Le regole esprimono condizioni attraverso le quali il flusso di eventi viene valutato. Queste condizioni possono essere espresse a partire dal modello di rete e degli asset, della priorità dell'evento, delle "Active list" (3.4.1.3) e delle "Session list" (3.4.1.3). Le regole possono essere costruite in maniera modulare per fare uso di blocchi di altre condizioni espresse attraverso filtri o altre regole.

I *filtri* sono il mattone base utilizzato per costruire le regole; essi permettono, utilizzando strumenti della logica booleana, di definire criteri sugli attributi degli eventi: gli eventi che li soddisfano continueranno ad essere valutati all'interno delle regole, altrimenti verranno scartati.

Simple rule Le "*simple rule*" vengono innescate quando gli eventi soddisfano una serie di condizioni, per esempio, eventi che hanno come target un certo asset e sono classificati come ostili.

Se una "simple rule" è configurata per aggregare eventi multipli che soddisfino una condizione su un attributo, la regola è innescata quando più di un evento soddisfa la condizione. Per esempio, se la regola è configurata per aggregare tre eventi, la regola è attivata quando i tre eventi capitano all'interno dell'intervallo di tempo specificato.

Join rule Il "*join*" permette di connettere eventi da differenti nodi allo scopo di verificare gli attributi che possono avere in comune. La "*Join rule*" riconosce

pattern che coinvolgono più di un tipo di evento e viene innescata dagli eventi che soddisfano due o più set di condizioni. Per esempio, una join rule può essere innescata quando ad un evento sul sistema di intrusion detection corrisponde un evento permit sul firewall ed entrambi hanno come target lo stesso asset sulla stessa porta da parte dello stesso ip di provenienza. Se la join rule è configurata per aggregare eventi multipli, la regola è innescata quando il numero di eventi impostato soddisfa la condizione.

Rule aggregation È possibile avere l'innesco di un'azione ogni volta che le condizioni attraverso le quali è definita la regola vengono soddisfatte. È però anche possibile definire aggregazioni per innescare l'azione dopo un certo numero di volte che le condizioni vengono soddisfatte in un certo intervallo di tempo in cui certi campi sono unici o identici. L'aggregazione può essere definita in base a:

- numero di condizioni soddisfatte in un certo intervallo di tempo;
- aggregazione quando campi specifici sono unici;
- aggregazione quando campi specifici sono identici.

3.4.1.2 Azioni

Alle regole è sempre associata un'azione che viene eseguita quando le condizioni che definiscono la regola sono soddisfatte. Oltre a definire l'azione occorre definire quando l'azione viene scatenata. I criteri possibili sono i seguenti:

- al primo evento;
- dopo un certo numero di eventi in un intervallo di tempo;
- ad ogni evento;
- al primo raggiungimento di una soglia;
- dopo un certo numero di volte che la soglia viene raggiunta;
- ogni volta che la soglia viene raggiunta;
- dopo un certo numero di minuti.

Una volta deciso quando l'azione deve essere scatenata, occorre decidere quale è l'azione. Alcune azioni possibili sono le seguenti:

- invio di una notifica;
- esecuzione di un comando;
- creazione di un case all'interno dello strumento di ticketing Arcsight o aggiunta ad un case già creato;
- aggiunta o rimozione da un'active list;
- aggiunta o rimozione da una session list.

3.4.1.3 Liste

Una lista è una modalità di monitoraggio degli asset. Una lista è una locazione temporanea in memoria usata per contenere informazioni che possono essere usate in altre attività di correlazione o monitoraggio. L'informazione è aggiunta ad una lista basate su regole . È possibile avere una lista di indirizzi IP sospetti, attività VPN, o altri tipi di valori specifici. Queste liste possono essere utilizzate per essere lette da altre regole, monitor, report. Possono essere utilizzate due tipi differenti di liste.

Active list. È possibile aggiungere informazioni a questo tipo di lista automaticamente attraverso la definizione di regole oppure manualmente. Ogni lista ha un tempo di vita specifico (TTL) per i suoi asset. Il TTL è l'ammontare di tempo che l'asset rimarrà nella lista. Gli asset nella Active List sono costantemente rivalutati e il TTL viene azzerato ogni qualvolta che viene scatenata l'azione di aggiunta dell'asset nell'active list. Se il TTL è impostato a 0, l'informazione non viene mai rimossa dall'active list.

Session list. Una session list è definita per essere usata per un periodo di tempo specifico, non soltanto come segnaposto per informazioni su un campo, in cui l'informazione può scadere ed essere rimossa dalla lista. Le session list sono anche utilizzate per monitorare l'attività di sessione.

3.4.2 Knowledge base

La componente di knowledge base in ArcSight ESM è denominata ArcSight ESM network model. Questa componente aiuta nella costruzione di criteri di correlazione dettagliati così come nell'assegnare una priorità agli eventi processati dall'ESM.

3.4.2.1 ArcSight Asset Model

L'Asset Model è il punto in cui vengono definiti i vari asset da monitorare all'interno dell'organizzazione. Al fine di ottenere il massimo dei benefici dalla modellazione degli asset, occorre fornire le seguenti informazioni, soprattutto per gli asset più critici.

- **Vulnerabilità**. Come già detto, una vulnerabilità è uno stato particolare o una debolezza di un sistema hardware o software che può essere sfruttata da un exploit. Spesso le vulnerabilità all'interno delle organizzazioni possono essere rilevate attraverso dei tool di vulnerability scan. In questo caso è possibile popolare il network model con i dati del vulnerabily scan utilizzando un apposito SmartConnector che comunica all'ESM Manager una serie di eventi. Quando il Manager riceve eventi da un vulnerability scanner, cerca innanzi tutto di individuare l'asset contenuto nel vulnerability scan all'interno degli asset già modellati nel sistema. Se l'asset non viene trovato ne crea uno. Se l'organizzazione possiede un database degli asset nel quale siano presenti molti attributi, come per esempio l'owner-

ship, è possibile utilizzare l'attributo External ID per fare riferimento a tale database.

- **Location.** È una informazione opzionale che può fornire parecchi dettagli sull'origine e la destinazione di un evento.

- **Categoria di asset**. Descrive le proprietà di un asset utili in fase di valutazione delle minacce o di reazione ad eventi. Sebbene questa opzione debba essere impostata e mantenuta manualmente, fornisce informazioni come la tipologia dell'asset, l'ownership, la criticità, che possono essere utilizzate in fase di costruzione di filtri, regole e report per correlare gli eventi associati a questo asset.

3.4.2.2 ArcSight Network Model

Il Network Model è il punto in cui viene definita la modalità in cui i gruppi di asset da monitorare sono rappresentati all'interno dell'organizzazione. Al fine di ottenere il massimo dei benefici dalla modellazione della rete, occorre fornire le seguenti informazioni.

- **Asset**. Un asset è definito come un endpoint di rete con un indirizzo IP, MAC address, host name o ID esterno. Ogni singola interfaccia di rete visibile è considerata un asset distinto all'interno del Network Model. Mentre l'ESM crea automaticamente gli asset per modellare i nodi di rete che ospitano i componenti ArcSight (Database, Console, Manager, Connettori), è importante creare in anticipo ogni asset importante. Questa informazione, in congiunzione con quelle contenute nell'Asset Model (vulnerabilità, location e categoria), sono importanti in fase di costruzione dei contenuti all'interno dell'ESM. È possibile configurare gli *Asset Group*, gruppi logici di asset e gli *Asset Range*, gruppi di asset con lo stesso range di IP.

- **Zones**. Possono rappresentare ogni parte della rete e sono identificate da un blocco di indirizzi IP contiguo. Le zone rappresentano solitamente un gruppo funzionale all'interno della rete e ogni asset o asset range deve essere associato ad una zona.

- **Networks**. Sono una collezione logica di zone. Nel caso fossero presenti due o più subnet con NAT che usano lo stesso address space privato, si definirà una network. Le network devono essere associate a una zona; gli asset all'interno di tale zona saranno associati automaticamente alla network.

La creazione del Network Model può avvenire con metodi diversi, alcuni dei quali basati sulla console ESM e altri basati sugli SmartConnector.

I metodi basati sulla console ESM sono due. Esiste un primo metodo che permette di configurare individualmente gli asset ed un secondo metodo che permette invece di importare gli asset in modalità batch basato su un file csv.

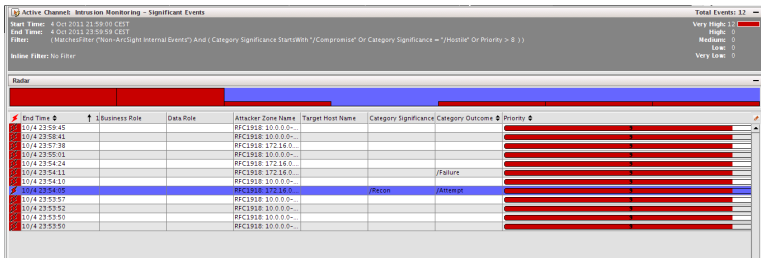

Figura 3.5.1: Esempio di Active Channel

I metodi basati su Smartconnector sono ancora due. Un primo metodo permette di definire un flex connector configurato per importare automaticamente le informazioni contenute all'interno di un file csv. Un secondo metodo permette di importare le informazioni sugli asset da un tool di vulnerability scanner (come FoundStone, ISS Internet Scanner o Nessus).

Tutti i metodi elencati precedentemente permettono di integrare le informazioni contenute nel network model di ESM con quelle importate dalle fonti esterne.

3.5 Monitoraggio

I processi di normalizzazione e di correlazione permettono ai Security Operatione Center di avere consapevolezza in tempo reale degli eventi che occorrono all'interno della rete. I tool di monitoraggio e di investigazione permettono di tracciare una situazione durante la sua evoluzione, vedere l'origine di un evento, vedere i sistemi coinvolti e comprendere gli effetti sugli altri nodi di rete.

I tool di monitoraggio che l'ESM mette a disposizione sono:

- Active Channel
- Dashboard
- Query viewer

3.5.1 Active Channel

Gli Active Channel sono uno strumento molto importante in fase di investigazione sugli incidenti e in fase di monitoraggio real-time. All'interno di un Active Channel è possibile visualizzare i dati che soddisfano un certo filtro in un certo intervallo di tempo definito o in tempo reale.

Esempio di Active Channel è riportato alla figura 3.5.1

In fase di creazione di un nuovo Active Channel sono richieste informazioni specifiche.

- *Nome del channel*. Nome unico per l'Active Channel.

- *Timestamp di inizio e fine del monitoraggio.* Intervallo di tempo da monitorare
- *Timestamp da utilizzare.* È possibile utilizzare il timestamp del dispositivo che ha generato i log oppure quello dell'ESM.
- *Valutare in caso di attacco o continuamente.* Questa opzione permette di definire se l'Active Channel deve mostrare un intervallo di tempo specifico oppure mostrare gli eventi in real time.
- *Filtro da utilizzare.* Il filtro utilizzato può essere un filtro creato precedentemente oppure uno creato specificatamente per l'Active Channel.
- *Campi da utilizzare.* Questa opzione permette di definire i campi da mostrare nell'Active Channel.

3.5.2 Dashboard

Scopo delle *Dashboard* è la visualizzazione di indicatori dello stato di sicurezza dell'organizzazione, così come riportato all'ESM dalle sorgenti dei dati. Le dashboard sono formate da data monitor individuali in una varietà di formati grafici o tabellari che riassumo il flusso degli eventi e comunicano l'effetto del traffico di eventi su specifici sistemi della rete. Le dashboard forniscono diversi tipi di vusualizzazione e analisi del flusso di eventi: sono pertanto il mezzo ideale per visualizzare gli eventi della rete in una varietà di viste statistiche.

Esempio di dashboard è riportato alla fig. 3.5.2

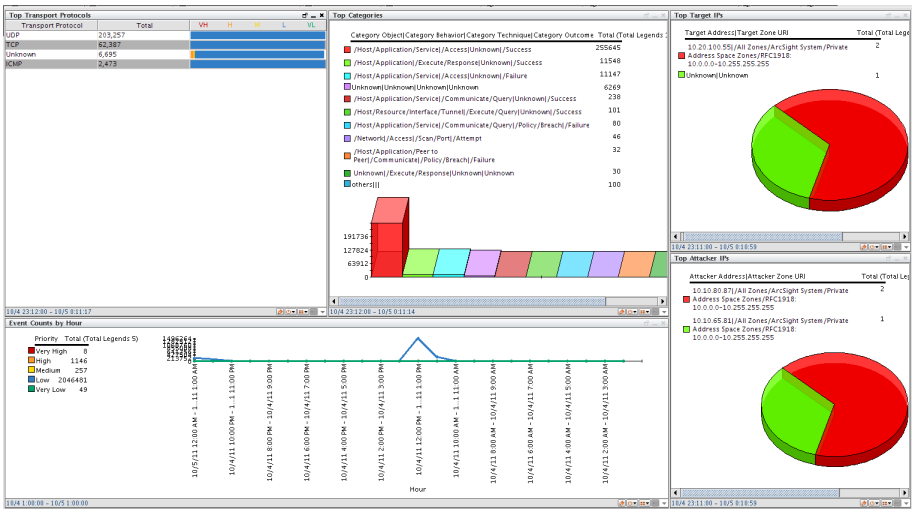

Figura 3.5.2: Esempio di Dashboard

3.5.3 Query Viewer

I *Query Viewer* combinano la capacità di eseguire query SQL da parte dei trend e dei report con la capacità di visualizzazione e drill-down degli active channel per creare grafici e tabelle interattive. I query viewer sono altamente personalizzabili e permettono di avere una vista a largo raggio e nello stesso tempo di accedere a dettagli in drill-down. I dati raccolti da un query viewer possono essere aggiunti ad una dashboard o pubblicati come report. I query viewer utilizzano query basate su eventi e altre risorse, come trend, active list, session list, asset, ecc. Sono lo strumento ideale per investigare situazioni potenzialmente sospette.

3.6 Reportistica e analisi degli incidenti

Una volta che gli eventi sono stati processati dal Manager e memorizzati nel database, è possibile eseguire una serie di operazioni batch che permettono di analizzare incidenti, trovare nuovi pattern e eseguire report sull'attività dei sistemi

3.6.1 Query

Una *Query* è una risorsa che permette di definire i parametri dei dati che si vuole ottenere da una sorgente dati. Il risultato di una query diventa la base per un o più report o trend. Le sorgenti dati che possono essere utilizzate per definire una query sono gli eventi contenuti nel database ESM, i dati contenuti in un'active list, session list o raccolti da un trend. Possono essere utilizzati dati interni all'ESM come per esempio gli asset.

In una query è possibile selezionare i campi dati da riportare e funzioni specifiche su di essi.

3.6.2 Trend

Un *Trend* è una risorsa che definisce come e con che frequenza valutare tendenze. Un trend è costituito da una o più query eseguite con una certa frequenza. Un trend può essere utilizzato come fonte dati primaria per un report oppure può essere utilizzato come fonte dati per un'altra query che raffina i risultati della query iniziale.

3.6.3 Report

Un report è una risorsa che lega una o più fonti dati a un template e imposta gli attributi in output, come il formato del file, dimensioni della carta, limiti di righe e vincoli di time zone.

Una volta che il report è definito, è possibile eseguirlo manualmente, eseguirlo automaticamente ad intervalli regolari, o eseguire un report "*delta*" per confrontare i risultati di un report con un altro.

Parte II

Un caso di studio: la Regione Emilia-Romagna

Capitolo 4

Gestione della sicurezza informatica

La Regione Emilia-Romagna mostra già da tempo una spiccata sensibilità al tema della sicurezza informatica, sensibilità che si è concretizzata sia sul piano organizzativo che su quello di assegnazione delle risorse, tanto da diventare punto di riferimento anche per altre pubbliche amministrazioni.

Negli ultimi anni si è operato principalmente in tre direzioni:

1. definizione di policy di sicurezza dell'ente, che hanno portato all'adozione di appositi Disciplinari Tecnici, ognuno dei quali tratta diversi aspetti ed è rivolto a diverse tipologie di utenti;
2. strutturazione di un sistema di verifiche e controlli per la gestione della sicurezza nel suo complesso;
3. messa in opera di soluzioni tecnologiche al fine di assicurare e migliorare la sicurezza informatica, ottemperando anche agli obblighi previsti dalla normativa vigente.

In questo capitolo descriveremo quanto realizzato dall'Ente in queste tre direzioni e quale sia l'impatto sul sistema di monitoraggio realizzato.

4.1 Le policy di sicurezza

I principali standard internazionali che trattano la sicurezza informatica raccomandano alle organizzazioni la definizione di linee guida e policy di sicurezza per il proprio sistema informativo.

Le policy di sicurezza, che hanno il fine ultimo di proteggere le persone e le informazioni dell'organizzazione, definiscono le regole di comportamento per utenti, amministratori di sistema e management, autorizzando il personale addetto alla sicurezza informatica a monitorare i sistemi e fare indagini in caso di sospetti incidenti di sicurezza.

La Regione Emilia-Romagna nel corso degli ultimi anni ha provveduto alla definizione di policy di sicurezza per il sistema informativo dell'ente attraverso l'adozione di appositi Disciplinari Tecnici, ognuno dei quali tratta diversi aspetti ed è rivolto a diverse tipologie di utenti.

I Disciplinari Tecnici riguardanti la sicurezza informatica adottati finora sono i seguenti.

- Disciplinare Tecnico per gli utenti del sistema informatico;
- Disciplinare Tecnico per amministratori di sistema;
- Disciplinare Tecnico in materia di sicurezza di applicazioni informatiche;
- Disciplinare Tecnico verifiche e controlli;
- Disciplinare Tecnico incidenti di sicurezza;
- Disciplinare Tecnico relativo al controllo degli accessi;
- Disciplinare Tecnico in materia di videosorveglianza.

Uno degli scopi del sistema di monitoraggio oggetto di questa tesi è la verifica delle policy di sicurezza regolamentate attraverso i Disciplinari Tecnici sopra elencati, soprattutto le policy riguardanti gli utenti del sistema informatico e gli amministratori di sistema.

4.2 Il sistema di verifiche

Per garantire la sicurezza del proprio sistema informatico un'organizzazione, oltre a definire le regole di comportamento di utenti, amministratori di sistema e management, deve formalizzare un sistema di verifiche e controlli, autorizzando il personale addetto alla sicurezza ad effettuare il monitoraggio della sicurezza e a verificare il rispetto delle policy di sicurezza dell'organizzazione, delle normative e degli standard internazionali, individuare eventuali attacchi ed essere in grado di proporre eventuali modifiche o nuove implementazioni ai sistemi di sicurezza sulla base delle verifiche effettuate.

La Regione Emilia-Romagna disciplina tale sistema all'interno del Disciplinare Tecnico verifiche e controlli, adottato il 21 luglio 2009. Tale disciplinare prevede quattro tipi di verifiche:

- *puntuali preventive*: attività di verifica effettuate precedentemente all'implementazione o alla modifica sostanziale di un sistema o di un processo per verificarne la rispondenza alle politiche di sicurezza;
- *puntuali a posteriori*: attività di verifica effettuate a seguito del verificarsi di incidenti di sicurezza;
- *periodiche*: attività di verifica, manuali o automatizzate, per contrastare minacce incombenti o potenziali, effettuate con cadenza periodica programmata;

- *a campione*: attività di verifica effettuate su campioni scelti secondo criteri prestabiliti e ad intervalli di tempo non fissi.

Il sistema di monitoraggio della sicurezza dovà fornire strumenti che permettano di effettuare tali verifiche, in particolare per le verifiche puntuali a posteriori e per le verifiche periodiche.

4.3 Le soluzioni tecnologiche

L'analisi dei rischi effettuata annualmente in occasione dell'aggiornamento del Documento Programmatico per la Sicurezza della Giunta Regionale, consente di monitorare e verificare le vulnerabilità del sistema di sicurezza anche alla luce degli aggiornamenti normativi, tecnologici, procedurali e organizzativi, e di pianificare le necessarie contromisure. Le contromisure possono essere organizzative o tecnologiche.

In questo paragrafo descriveremo brevemente alcune soluzioni tecnologiche di sicurezza adottate dalla Regione Emilia-Romagna; poiché dal punto di vista del sistema di monitoraggio della sicurezza tali soluzioni tecnologiche rappresentano la fonte principale delle informazioni, la descrizione riguarderà soprattutto questo aspetto, descrivendo il tipo di informazione che si può ricavare dal sistema e i contenuti dei log.

4.3.1 Sistemi firewall

L'Ente è dotato di un cluster di firewall statefull in tecnologia Checkpoint, situato sulla frontiera esterna della rete regionali a protezione delle reti dei server, delle reti degli uffici e della DMZ. Oltre ai nodi che compongono il cluster è presente un server che funge da management (SmartCenter), fornendo un'interfaccia per l'installazione delle policy, conservando il database delle configurazioni, ricevendo e conservando i log, in formato proprietario, provenienti dai nodi.

4.3.2 Sistemi anti malware

L'Ente è dotato di diverse tipologie di sistemi anti malware, tutti di tecnologia Trend Micro. Su tutte le workstation e i server fisici è installato Trend Micro Office Scan o Server Protect. Sui sistemi di virtualizzazione è presente Trend Micro Deep Security, un sistema anti malware specifico per ambienti virtuali Vmware, il quale, utilizzando apposite API dedicate alla sicurezza fornite da Vmware, agisce come antimalware, come firewall e IPS per il traffico da e verso i server virtuali senza bisogno di installare alcunché sulle macchine virtuali. Per finire l'elenco del sistemi anti malware, citiamo Trend Micro Interscan Messaging Security Suite (IMSS), sistema anti malware dedicato alla posta elettronica e Trend Micro Interscan Web Security Virtual Appliance, sistema dedicato alla sicurezza della navigazione web.

4.3.3 Sistemi di Intrusion Prevention e Intrusion Detection

Il sistema di Intrusion Prevention e Intrusion Detection a disposizione dell'Ente, in tecnologia Tipping Point, è costituito da alcune sonde posizionate sulla frontiera esterna della rete regionale e sulle frontiere fra le reti dei server e le reti degli uffici. Tali sonde ispezionano tutti i pacchetti del traffico di rete che le attraversa e, sulla base di apposite signature rilasciate dal produttore e costantemente aggionate e delle policy impostate dall'amministratore, bloccano o segnalano eventuali pacchetti che possono costituire minacce alla sicurezza. Oltre alle sonde il sistema di Intrusion Prevention e Intrusion Detection contiene un server che funge da managment e che fornisce un'interfaccia per l'installazione delle policy, conservando il database delle configurazioni, ricevendo e conservando i log, in formato proprietario, provenienti dalle sonde.

4.3.4 Virtual Private Network

Il sistema in dotazione per l'accesso remoto è un sistema Checkpoint di VPN SSL, ovvero una VPN che utilizza il protocollo SSL (Secure Socket Layer) e che veicola il traffico di rete attraverso un tunnel utilizzato per garantire la protezione delle comunicazioni. Le policy di accesso sono molto granulari, permettendo, per ogni utente, di definire applicazioni e/o combinazioni di host e protocolli utilizzabili.

4.3.5 Web Proxy

Le postazioni di lavoro della rete regionale sono configurate in modo tale da permettere l'accesso al web solo attraverso un sistema di web proxying. Il sistema di web proxying ha lo scopo di rendere più efficiente la navigazione, mantenendo una cache locale delle pagine web e di rendere più sicura la navigazione, restringendo l'accesso ad alcune risorse web in base a policy definite. Il sistema di web proxying regionale, utilizzabile solo previa autenticazione, è costituito da un servizio di web cache open source (Squid), un sistema di content filtering proprietario (Trend Micro) basato sulla categorizzazione dei siti e un sistema open source di content filtering dinamico basato sull'analisi realtime dei siti visitati.

4.3.6 I sistemi di autenticazione

4.3.6.1 Il dominio Active Directory

Il meccanismo primario per l'autenticazione degli utenti per l'accesso alle risorse utilizzato nell'Ente si basa su Microsoft Active Directory. Tale tipo di autenticazione (c.d. autenticazione di dominio), prevede l'identificazione dell'utente che accede ad una risorsa tramite userid e password. Sono presenti due domini regionali, uno dedicato agli utenti interni alla rete regionale e un altro che comprende utenti esterni all'Ente che accedono ad applicazioni e servizi interni

all'Ente. L'autenticazione di dominio è impiegata per accedere alle postazioni di lavoro, al sistema di posta elettronica, alle cartelle di rete su file server.

Gli eventi del sistema di autenticazione Active Directory sono registrati all'interno dell'Event Viewer dei Domain Controller dei rispettivi domini, dove viene registrato il timestamp dell'evento, il nome utente, la modalità di autenticazione utilizzata, l'host di provenienza, l'host di destinazione, la modalità di autenticazione (Kerberos, NTLMv2, ecc). I domain controller tengono inoltre traccia di tutte le modifiche apportate ad oggetti di Active Directory, come utenti, gruppi e computer.

4.3.6.2 Il sistema di Identity and Access Management

La Regione Emilia-Romagna dispone di un sistema di Identity & Access Management (IAM). Il sistema di IAM è finalizzato alla gestione razionale, scalabile ed omogenea delle utenze del Sistema Informativo della Regione ottemperando al tempo stesso alle normative ed ai requisiti di legge in tema di sicurezza informatica e di protezione dei dati personali.

Il sistema di IAM è composto dalle seguenti componenti:

- un servizio di *Directory* per la gestione centralizzata delle utenze interne ed esterne, sul quale poggiano le funzioni di "profilatura" e "autenticazione" di sistemi e applicazioni integrati nello IAM. Il Directory è popolato tramite il sistema di Identity Management (vedi punto seguente), che si occupa anche di sincronizzare le password delle utenze all'interno del Directory con quelle dei domini Active Directory;

- una soluzione di *Identity Management*, che, interfacciandosi a diversi repository utente, consente la gestione dell'intero ciclo di vita delle identità su specifici sistemi e applicazioni, la sincronizzazione delle password degli utenti e la delega ai referenti alla gestione delle loro utenze; consente inoltre l'automatizzazione del processo di provisioning degli account, integrato con i processi organizzativi mediante l'utilizzo di workflow;

- una soluzione di *Access Management* che permette l'accesso in Single Sign On alle applicazioni web integrate, liberando le applicazioni stesse dalla gestione dell'autenticazione.

Tramite il sistema di Identity e Access Management sono state gestite anche le utenze amministrative dei server Linux e dei server Windows che non fanno parte del dominio Active Directory, permettendo gli accessi degli amministratori con credenziali personali e permettendo l'accesso mediante account amministrativi generici (Administrator o root) solo da console e non via rete.

Il sistema di Access Management è inoltre integrato con il sistema di autenticazione federata della Regione Emilia-Romagna (fedERa), agendo sia come "Identity Provider", permettendo ai proprio utenti di accedere con le proprie credenziali a servizi esposti da altri Enti del territorio regionale, che come "Service Provider", permettendo ad utenti di altri Enti l'uso di applicazioni integrate con l'Access Manager.

4.3.6.3 Il servizio RADIUS

All'interno del Sistema Informatico della Regione Emilia-Romagna è inoltre presente un sistema RADIUS che ha lo scopo di implementare un ulteriore metodo per l'autenticazione, autorizzazione e accounting per gli utenti che hanno necessità di accedere a risorse eterogenee. Nello specifico il sistema RADIUS implementato si basa su Cisco ACS ed è configurato in modo da utilizzare gli utenti presenti all'interno del dominio Active Directory interno. Il servizio RADIUS è utilizzato per l'accesso agli apparati di rete e per l'accesso ad alcune appliance. Tale configurazione permette di accedere con account personali evitando gli account generici con password condivise tra più utenti.

4.3.7 Il Configuration Management Database

La Regione Emilia-Romagna dispone di un Configuration Management Database (CMDB) contenente le informazioni più significative relative alle componenti del sistema informatico. Tale database costituisce di fatto il sistema informativo del sistema informatico dell'ente e contiene i dettagli dei configuration item (CI) della infrastruttura IT, intesi come gli asset costituenti l'intero ambito informatico, sia materiali (hardware) che immateriali (software).

Il CMDB aiuta l'organizzazione nella comprensione delle relazioni tra le componenti censite e la loro configurazione e rappresenta un componente fondamentale nei processi di change management.

I dati contenuti in questo database sono strategici per il buon governo dell'infrastruttura e, al fine di garantire un elevato livello qualitativo del sistema, è fondamentale assicurare un costante aggiornamento delle informazioni in esso contenute. Tale obiettivo è perseguibile attraverso regolari attività di allineamento dei dati. Il CMDB dell'Ente è basato sul prodotto CMDBuild; si tratta di una applicazione web realizzata con Software Open Source, completamente configurabile per modellare ed amministrare il database degli asset informatici e supportarne i workflow di gestione. CMDBuild è un sistema flessibile ed espandibile in modo graduale ed autonomo dall'utilizzatore, orientato all'utilizzo delle best practices di qualità ITIL (IT Information Library) e rilasciato con licenza open source GPL.

Attraverso il CMDB sono censiti la quasi totalità degli asset materiali ed immateriali gestiti dal Servizio Informativo Informatico Regionale, in particolare:

- *asset materiali*: apparati di rete, server, rack;
- *asset immateriali*: database e grant di accesso, applicazioni web e software installati sui server, amministratori di sistema.

Ai fini della realizzazione del sistema di monitoraggio della sicurezza, è importante che le informazioni censite dal CMDB siano messe a disposizione del SIEM, sul quale potranno essere definite regole che tengano conto di tali informazioni. In tale maniera sarà per esempio possibile definire monitoraggi specifici per gli asset critici, altri per i web server, monitorare gli accessi degli amministratori

di sistema, accessi ai database da parte di utenti che non dovrebbero essere autorizzati. Le modalità di sincronizzazione delle informazioni riguardanti reti e asset fra il CMDB e il SIEM sono oggetto delle fasi di modellazione della rete e degli asset; nel paragrafo 5.3 verrà descritto come tali fasi sono state affrontate.

4.4 La gestione degli incidenti di sicurezza

La gestione degli incidenti di sicurezza informatica è un tema che tutte le organizzazioni devono essere pronte ad affrontare in quanto, nonostante tutte le attività di prevenzione e di analisi dei rischi, non tutti gli incidenti possono essere prevenuti ed è meglio affrontarli avendo una procedura definita. La procedura deve avere lo scopo di permettere una rilevazione rapida dell'incidente, di minimizzare i danni e le perdite, mitigare le debolezze e ripristinare i sistemi.

La procedura utilizzata dalla Regione Emilia-Romagna è codificata dal Disciplinare Tecnico per incidenti di sicurezza, adottato in forma sperimentale il 9 marzo 2009. Tale disciplinare prevede la presenza di un'unità di gestione degli incidenti di sicurezza informatica (UGISI), con le seguenti caratteristiche:

- rappresenta il punto di riferimento a cui rivolgersi per segnalare un incidente di sicurezza;
- gestisce tutte le attività inerenti un incidente di sicurezza, ivi comprese quelle relative alla sua documentazione e notifica;
- garantisce la disponibilità e rintracciabilità di liste di contatti (es.: personale dipendente, collaboratori, fornitori, manutentori), necessarie per la gestione di un incidente di sicurezza;
- garantisce che la gestione incidenti risponda alle esigenze dell'Ente, provvedendo che sia sempre mantenuta aggiornata:
  - a valle di cambiamenti tecnologici, infrastrutturali e organizzativi;
  - a valle di incidenti di sicurezza che mettano in evidenza aspetti di miglioramento nella procedura stessa.

La procedura di gestione si articola nelle fasi di seguito elencate e schematizzate nella figura 4.4.1.

Durante la fase di analisi è prevista la categorizzazione dell'incidente, in base agli eventi preventivi e indicativi riscontrati. Il SIEM può essere utile nel rilevare rapidamente gli eventi indicativi di tutte le tipologie di incidente; esempi di eventi indicativi che possono essere rilevati dal SIEM sono:

- attività di port scan, host scan, vulnerability scan, ping, traceroutes, DNS zone transfers, OS fingerprinting, banner grabbing;
- tentativi di accesso a file contenenti informazioni critiche (es.: password-files) presenti nel sistema;

- traffico di rete fortemente sbilanciato (molto traffico in ingresso, poco in uscita alla rete);
- antivirus software alert;
- tentativi di accesso al servizio che presenta una vulnerabilità;
- log dei dispositivi di rete (Firewall, router) relativi alla presenza di comunicazioni client-server legati alla presenza di Trojan Horse;
- traffico anomalo da/verso determinati sistemi.

Un'altra fase in cui il SIEM è fondamentale è la fase di analisi delle evidenze, fatta sia a scopo legale che cautelativo, che di indagine interna volta a rimuovere le cause dell'incidente. La ricerca all'interno dei log può rendere evidenti le modalità in cui l'incidente ha avuto luogo.

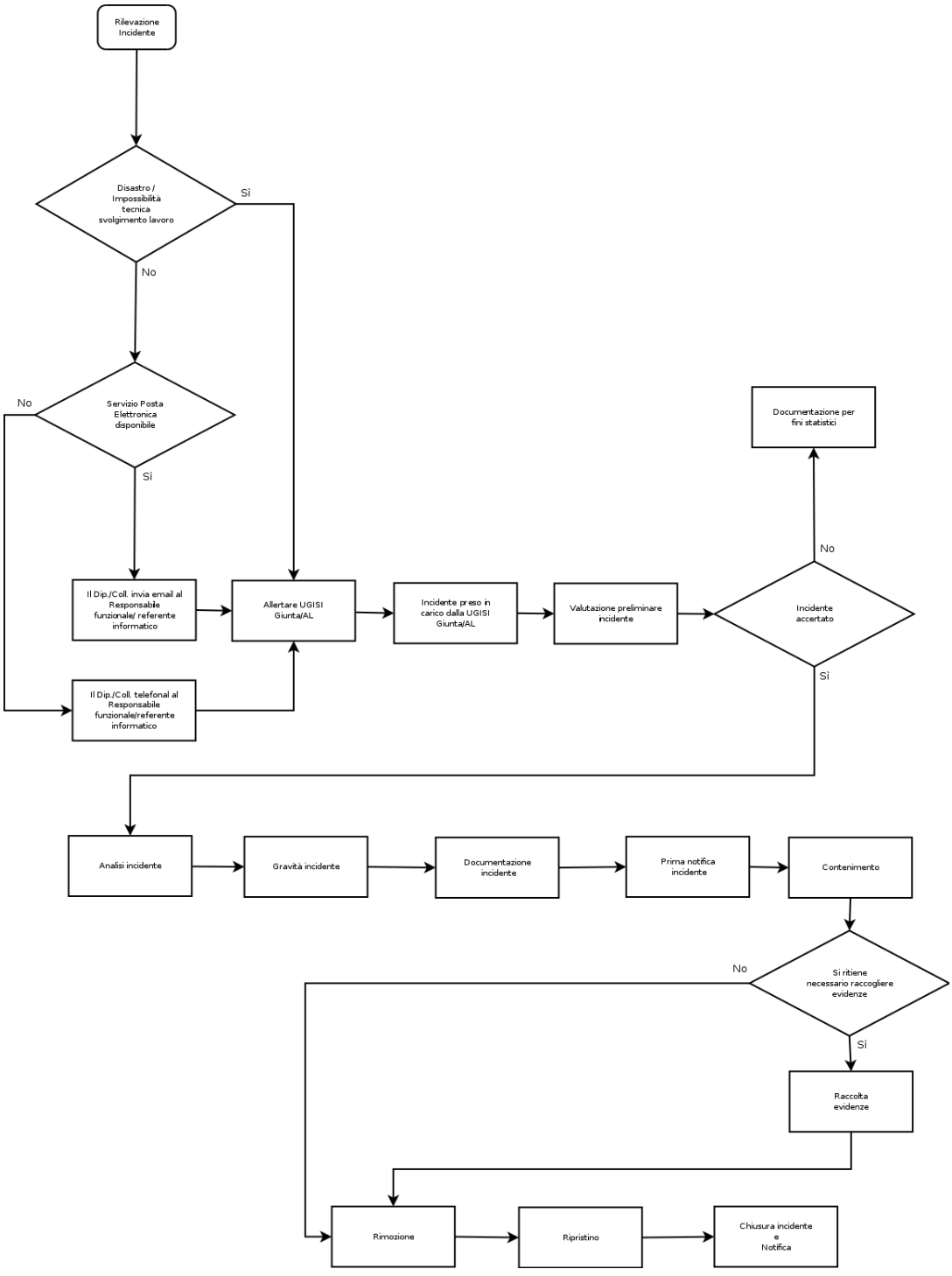

Figura 4.4.1: Gestione degli incidenti di sicurezza

Capitolo 5

Realizzazione del sistema di monitoraggio

Il sistema di monitoraggio della sicurezza informatica in Regione Emilia-Romagna, basato, come già detto, su un modello SIEM, è l'evoluzione di un sistema di log management adottato dalla Regione Emilia-Romagna allo scopo di adeguarsi al provvedimento del Garante per la Protezione dei Dati Personali sugli Amministratori di sistema del 27 novembre 2008, le cui disposizioni sono entrate in vigore il 15 dicembre 2009. Il processo di implementazione del sistema di log management è stato svolto avendo sempre presente come obiettivo secondario l'integrazione di eventi significativi dal punto di vista della sicurezza informatica dell'Ente.

In questo capitolo verrà descritto il processo di realizzazione del sistema di monitoraggio della sicurezza informatica all'interno della Regione Emilia-Romagna, descrivendo il sistema di log management di partenza, la scelta dell'architettura del SIEM, la modellazione della rete e degli asset, la definizione, a partire da alcuni eventi di interesse, di regole, strumenti di monitoraggio e reportistica.

5.1 Il sistema di log management

L'obbligo, previsto dal provvedimento del Garante sopra citato, di adottare strumenti atti alla registrazione degli accessi logici degli amministratori di sistema, registrando in maniera inalterabile login avvenuti con successo, login falliti e logout, insieme al timestamp di tali eventi, non era soddisfabile utilizzando gli strumenti in essere. All'interno dell'Ente i log degli accessi erano infatti presenti unicamente all'interno dei sistemi che li avevano generati e i tempi di conservazione erano incerti. Era presente unicamente un server Syslog che raccoglieva in un punto centrale i log dei sistemi server linux; sebbene tale sistema potesse costituire un punto di partenza per la creazione di un sistema di log management centralizzato, è stato valutato che ciò non fosse conveniente, sia perché non tutti

i sistemi su cui erano stati designati amministratori di sistema erano compatibili con syslog, sia perché i log immagazzinati non avevano caratteristiche di integrità e inalterabilità.

Vista la necessità di acquisire uno strumento di log management si è pensato di approfittarne per scegliere uno strumento che potesse, attraverso la raccolta dei log, aiutare nell'individuazione di eventi significativi dal punto di vista della sicurezza, orientandosi perciò nella realizzazione di un SIEM. Requisiti essenziali nella scelta del prodotto erano anche la più ampia presenza possibile di connettori già configurati per supportare i sistemi su cui erano stati individuati amministratori di sistema, la presenza di metodi per creare connettori "custom" verso i sistemi non supportati nativamente e la possibilità di memorizzare il database degli eventi su un sistema di Storage Area Network (SAN).

La valutazione delle soluzioni disponibili ha portato a scegliere la soluzione ArcSight, nello specifico l'appliance L7200-SAN (*logger appliance*), che supporta fino a 75000 eventi per secondo (EPS), insieme all'appliance C3200 (*connector appliance*), che contiene i connettori verso le sorgenti di log e funge anche da console di management per gli altri connettori installati su altri device. Altri connettori sono installati su un server virtuale Windows o, in alcuni casi, sui sistemi sorgenti dei log. I connettori contenuti nella soluzione ArcSight (SmartConnector) hanno lo scopo di filtrare gli eventi che non sono di interesse, di aggregare eventi simili e soprattutto normalizzare e categorizzare gli eventi adattandoli allo schema ArcSight di categorizzazione degli eventi.

La scelta delle sorgenti di log da integrare all'interno del sistema di log management è stata effettuata con l'obiettivo primario di ottemperare al provvedimento del garante, senza tuttavia trascurare tutti quegli eventi non relativi agli accessi degli amministratori ma che fossero significativi dal punto di vista della sicurezza informatica.

Di seguito viene descritta la tipologia di log presenti sul sistema di log management al momento dell'avvio del progetto di realizzazione del sistema di monitoraggio della sicurezza informatica e le modalità di integrazione.

Sistemi server Windows Alcuni connettori standard contenuti sulla connector appliance sono configurati per prelevare via RPC i log di tipo security contenuti all'interno dei registri degli eventi dei sistemi server Windows fisici e virtuali dell'Ente (circa 250); l'invio avviene quindi con metodo pull.

Sistemi server Linux La connector appliance contiene un server syslog, configurabile per utilizzare il protocollo udp o tcp. Il syslog dei server Linux dell'Ente (circa 100), sono configurati per inviare i log al connector appliance; l'invio avviene quindi in modalità push.

Sistemi di sicurezza Tutte le categorie di sistemi di sicurezza descritti al capitolo 4.3 sono integrati con il sistema di log management.

Per i *firewall* l'integrazione avviene mediante un connettore standard installato su un server Windows. Il connettore preleva in real time i log dal server di

management utilizzando lo standard OPSEC LEA (Log Export API). La versione adottata utilizza il protocollo SSL per assicurare che il traffico che attraversa la rete tra lo SmartCenter e la componente di collezionamento del SIEM sia criptato. I firewall generano un evento per ogni sessione del traffico di rete che li attraversa, indicando il timestamp dell'evento, l'ip di origine e di destinazione, il protocollo layer 4 utilizzato, la porta tcp o udp di origine e di destinazione, il nodo firewall e l'interfaccia di rete attraversata dal pacchetto, la policy applicata. Per il sistema di *VPN SSL*, le modalità di interazione con il sistema di log management sono le stesse dei sistemi firewall. Il sistema VPN SSL genera eventi a seguito dell'autenticazione degli utenti, indicando il timestamp dell'evento, l'ip di origine e di destinazione, il protocollo layer 4 utilizzato, la porta tcp o udp di origine e di destinazione, la policy applicata.

Per quel che riguarda i *sistemi anti malware* elencati nel paragrafo 4.3.2, tutti, ad eccezione di Deep Security, permettono di inviare i log degli eventi significativi ad un concentratore, il Trend Micro Control Manager, che si appoggia ad un database. Un connettore standard contenuto sulla connector appliance, attraverso query sql, preleva i log da tale database, in modalità pull. Poiché per il sistema Deep Security non è possibile utilizzare il Trend Micro Contro Manager, per tale sistema viene fatto un forward degli eventi alla connector appliance mediante il protocollo Syslog. Gli eventi generati dai sistemi anti malware contengono il timestamp dell'evento, il sistema dove è stato rilevato il malware, il malware rilevato, il file, l'url o il messaggio di posta elettronica che lo conteneva, l'operazione effettuata dal sistema anti malware e l'esito dell'operazione. Altri eventi registrati sono l'aggiornamento dei database delle signature del malware ed eventuali scansioni complete.

Le sonde di *Intrusion Detection and Prevention* generano un evento per ogni pacchetto che fa match con una delle signature presenti, per la quale sia stata definita una policy che lo preveda. Viene indicato il timestamp dell'evento, l'ip di origine e di destinazione, il protocollo layer 4 utilizzato, la porta tcp o udp di origine e di destinazione, il nodo firewall e l'interfaccia di rete attraversata dal pacchetto, la policy applicata, una descrizione della minaccia. Il SIEM riceve in real time i log dal server di management utilizzando il protocollo Syslog.

Per quel che riguarda il sistema di *web proxying*, all'interno del file di access log di Squid viene registrato il timestamp, il nome utente, l'ip del client che si connette, l'uri richiesto, l'esito dell'operazione, l'azione richiesta sulla cache, il metodo HTTP. Il SIEM interagisce attraverso un connettore installato sui server dove è presente Squid, il quale processa in real time i file di log, li aggrega, li normalizza e li invia al SIEM.

Sistemi di autenticazione Gli eventi del sistema di autenticazione *Active Directory* sono registrati all'interno dell'Event Viewer dei Domain Controller dei rispettivi domini. Il SIEM preleva i log attraverso uno dei connettori installati sulla connector appliance dedicati ai server Windows.

Per quel che riguarda il sistema di *Identity and Access Management*, ognuno dei componenti del sistema di IAM ha un suo sistema di logging.

Il *Directory Server* registra all'interno di file di testo il timestamp e la query ldap effettuata (tra cui l'operazione di bind, ovvero l'autenticazione). La comunicazione con il SIEM avviene attraverso un connettore installato sui server stessi dove è in esecuzione il Directory Server.

L'*Identity Manager* registra all'interno di un database Oracle gli eventi di autenticazione all'interno del sistema stesso e gli eventi di modifica degli oggetti gestiti dal sistema. Gli attributi presenti sono il timestamp, il tipo di operazione effettuata, il nome utente, il sistema di provenienza. La comunicazione con il SIEM avviene mediante un connettore custom installato centralmente.

L'*Access Manager*, infine, registra all'interno di file di testo gli eventi di autenticazione degli utenti sul portale delle applicazioni e ogni accesso ad ogni singolo url esposto dalle applicazioni integrate con l'Access Manager. Gli attributi presenti sono il timestamp, il nome utente, il sistema di provenienza, l'url a cui si è tentato di accedere. La comunicazione con il SIEM avviene attraverso un connettore installato sui server stessi dove è in esecuzione l'Access Manager.

Infine il servizio *RADIUS* (Cisco ACS) memorizza all'interno di un database proprietario gli eventi di autenticazione, autorizzazione ed accounting, memorizzando timestamp, sistema di provenienza, nome utente e gruppo di appartenenza dell'utente. La comunicazione con il SIEM avviene attraverso il protocollo Syslog.

Sistemi Database Oracle, MSSql e Postgres I sistemi RDBMS sono integrati con lo strumento di log management mediante connettori standard presenti sulla connector appliance. Nel caso di Oracle i log vengono letti dal database stesso, nel caso di MSSQL i log vengono presi da file di testo prodotto sul sistema dove è installato l'RDBMS dalla componente di audit dell'RDBMS stesso, nel caso di Postgres si utilizza il protocollo syslog.

Software SAP All'interno dell'Ente sono presenti diversi landscape SAP, sia di produzione che di test. Tali sistemi sono integrati mediante connettori standard presenti sulla connector appliance. Tali connettori processano appositi file di audit contenuti sui server dove è installato SAP.

Applicazioni web La maggior parte delle applicazioni web presenti nell'Ente ha un'architettura multi-tier, con il frontend realizzato attraverso un sistema di bilanciamento, che ha la possibilità di operare layer 7: il sistema LBL di TCO Group. Tale bilanciatore registra i log degli accessi su una tabella di un database Oracle. L'integrazione di tali eventi avviene mediante un connettore custom residente sulla connector appliance, configurato per prelevare gli eventi all'interno del database. Gli eventi registrati contengono il timestamp, il sistema sorgente e di destinazione, l'url invocato, l'operazione http, i parametri dell'uri, i cookies, l'esito dell'operazione.

Le applicazioni web con autenticazione centralizzata hanno il frontend realizzato da server Apache che, attraverso il modulo di policy agent del sistema

Sun Access Manager, si occupa dell'autenticazione e della verifica delle autorizzazioni dell'utente. L'integrazione di tali eventi avviene mediante un connettore standard installatato sui server di frontend, che processa i file di log di Apache e invia i log aggregati e normalizzati al sistema di log management. Gli eventi registrati, oltre agli attributi elencati per i bilanciatori LBL, contengono lo username dell'utente che ha effettuato l'accesso.

Sistema centralizzato di backup L'Ente dispone di un sistema centralizzato di backup in tecnologia IBM, il Tivoli Storage Manager, che provvede, attraverso agenti installati sui server, al backup e all'eventuale rispristino di dati residenti sui filesystem dei server e contenuti in RDBMS. Gli eventi di accesso al sistema, lancio dei backup e dei rispristini effettuati mediante il sistema sono contenuti all'interno di un database proprietario. L'integrazione di tali eventi avviene mediante un connettore custom presente su un server Windows; sul medesimo server Windows è presente un client Tivoli che ad intervalli regolari esegue un'esportazione degli eventi in un file: tale file viene processato dal connettore custom, che invia gli eventi processati al sistema di log management.

5.2 Architettura del sistema di log correlation

Il sistema di log management descritto al paragrafo 5.1 contiene in un database tutti gli eventi di interesse per il monitoraggio della sicurezza informatica dell'Ente adeguatamente normalizzati, con in più strumenti di ricerca e reportistica. Tale sistema è completamente adeguato per la ricerca a posteriori di evidenze di incidenti di sicurezza, per la verifica del rispetto delle policy di sicurezza e per la conformità alle normative (quale il già citato provvedimento del Garante per la protezione dei dati personali sugli amministratori di sistema, motivo per il quale il sistema è stato realizzato). La possibilità di individuare eventi indicativi di incidenti di sicurezza è limitata a ricerche manuali, fatte dagli analisti di sicurezza, e all'analisi dei report schedulati, quindi non in modalità realtime: quello che mancava era quindi uno strumento di log correlation.

Si è quindi proceduto all'acquisizione di uno strumento di log correlation, che, per essere compatibile con i connettori già installati, doveva essere di tecnologia ArcSight. La scelta è caduta sull'appliance Arcsight Express M7200, un sistema Linux contenente un DBMS Oracle e il sofware Arcsight Enterprise Manager (ESM), descritto al capitolo 3 e dimensionato per il numero di sistemi e di eventi presenti nell'Ente.

Tale sistema è stato configurato per ricevere gli eventi dal logger, il quale effettua il forward degli eventi ricevuti. Una volta individuate correlazioni fra gli eventi, l'ESM crea nuovi eventi, i cosiddetti eventi correlati. L'ESM è stato configurato affinché gli eventi correlati, oltre ad essere conservati sul database dell'ESM, vengano inviati al logger, il quale li conserverà nel proprio database rendendoli non modificabili. L'architettura del SIEM è illustrata in figura 5.2.1.

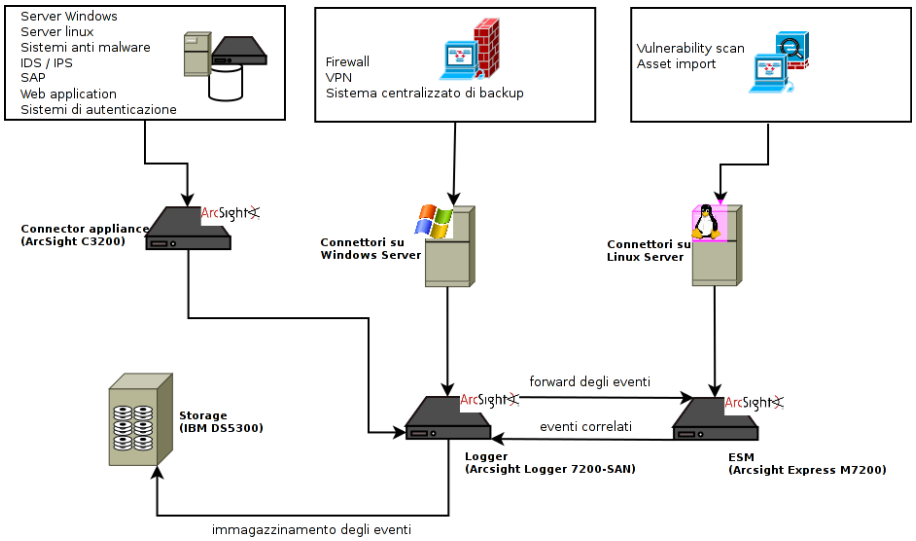

Figura 5.2.1: Architettura del sistema

5.3 Modellazione della rete e degli asset

Al fine della definizione degli eventi di interesse, è opportuno che all'interno del SIEM siano definite le zone di reti dell'organizzazione, in modo che attaccante e vittima degli eventi di interesse siano collocate all'interno della rete dell'organizzazione e che sia possibile definire gli eventi di interesse in base alle reti coinvolte. Allo stesso modo è opportuno che all'interno del SIEM siano definiti gli asset dell'organizzazione, in modo da poter definire eventi di interesse che tengano conto del livello di criticità degli asset, del ruolo da essi ricoperto all'interno dell'organizzazione, delle porte tcp/udp su cui sono in ascolto servizi, delle vulnerabilità presenti, del sistema operativo installato, eccetera.

Presso il sistema informativo della Regione Emilia-Romagna sia le informazioni relative alle reti che quelle relative agli asset sono contenute all'interno del CMDB.

5.3.1 Importazione delle zone

Le zone definite sul CMDB sono relative ai domini di broadcast definiti all'interno della lan dell'organizzazione. Le reti degli uffici fanno parte di zone che rispecchiano la collocazione fisica (es. il piano di un edificio) e hanno indirizzamento ip dinamico (tramite dhcp), mentre le reti dei server fanno parte di zone raggruppate secondo la funzione logica del server e hanno indirizzamento ip statico.

L'importazione delle zone è avvenuta partendo da un file csv prodotto dal CMDB e importato sul SIEM attraverso un apposito tool dell'ESM. Il formato del file CSV dal quale è stata fatta l'importazione è mostrato in tabella 5.1. È da

notare come nella definizione della zona occorra dichiarare se l'indirizzamento è statico o dinamico.

Tabella 5.1: Formato del file CSV delle zone

Nome	Descrizione	Obbligatorio	Ripetibile
Name	Nome descrittivo della zona, come lo scopo o la locazione geografica.	Sì	No
Start Address	Il primo IP dell'intervallo che definisce la zona.	Sì	No
End Address	L'ultimo IP dell'intervallo che definisce la zona.	Sì	No
Dynamic	Determina se i dispositivi definiti nella zona usano indirizzamento dinamico. Può contenere **true** o **false**.	Sì	No
Category URI	URI della categoria di asset da assegnare alla zona. Può essere ripetuta perché una zona può essere assegnata a più categorie di asset. **Esempio**: /All Asset Categories/All Site Asset Categories/Business Impact Analisys/Business Role/Service/Web/	No	Sì

5.3.2 Importazione degli asset e definizione delle categorie di asset

All'interno del CMDB sono definiti gli asset materiali e immateriali dell'Ente. La modellazione degli asset prevede che un asset venga identificato in maniera univoca attraverso il suo indirizzo ip (asset fisici aventi più indirizzi ip risultano essere più asset all'interno del modello). In fase di inserimento di un asset occorre poi definire quali sono le categorie alle quali l'asset appartiene. All'interno del CMDB sono definite le categorie di asset elencate di seguito.

- *Area di amministrazione*; tale informazione all'interno del CMDB è utilizzata per avere traccia di chi siano gli amministratori dell'asset; all'interno del SIEM, oltre che essere utile per rilevare gli accessi degli amministratori, lo è anche come ruolo ricoperto dall'asset.
- *Sistema operativo*; tale informazione all'interno del CMDB è utilizzata per la gestione del catalogo del software e per la gestione degli aggiornamenti; all'interno del SIEM è utilizzata per la creazione di monitoraggi specifici per asset con un certo sistema operativo o per una sua versione specifica.
- *Criticità del sistema*; tale informazione all'interno del CMDB è utilizzata per derivarne le modalità di esecuzione di operazioni di manutenzione o

di fermi programmati; all'interno del SIEM è utilizzata per poter definire regole dedicate ad asset critici; il tipo di criticità dell'asset è inoltre utilizzato dall'ESM per calcolare la formula di priorità di un evento.

- *Locazione*; tale informazione all'interno del CMDB è utilizzata per la gestione dell'hardware e dei cablaggi; all'interno del SIEM è utilizzata per eventuali monitoraggi basati sulla locazione fisica.

La prima importazione degli asset all'interno del SIEM è avvenuta esportando le informazioni contenute all'interno del CMDB in un file csv; tale file è stato opportunamente modificato per far coincidere le categorie degli asset del CMDB con gli URI associati alle categorie definite all'interno del SIEM. Il file csv è stato poi importato utilizzando lo stesso tool dell'ESM utilizzato per l'importazione delle zone. Il formato del file csv utilizzato è mostrato in tabella 5.2.

Se la prima importazione è avvenuta attraverso una procedura manuale, occorreva impostare poi una procedura automatizzata per permettere a regime la sincronizzazione fra le informazioni sugli asset contenute nel CMDB e quelle contenute nel SIEM, in quanto avvengono piuttosto frequentemente variazioni sugli asset e sulle loro configurazioni. A tal fine è stato utilizzato un apposito connettore Arcsight, l'*Asset Import file FlexConnector*. Tale connettore permette di configurare una directory nella quale vengono posizionati i file csv: ogni qualvolta un nuovo file csv viene posizionato nella directory il connettore lo processa, inviando i risultati all'ESM. Gli asset già esistenti all'interno dell'ESM vengono modificati con i nuovi dettagli che via via vengono trovati all'interno del file csv.

Per l'automazione dell'operazione di creazione dei file csv da dare in input al connettore, è stato creato uno script Python che, processando i risultati di una query sql eseguita sul database del CMDB, va a compilare il file csv che verrà poi elaborato dal connettore.

5.3.3 Vulnerabilità degli asset

All'interno del SIEM è importante avere conoscenza delle vulnerabilità a cui sono affetti i singoli asset e delle porte tcp e udp su cui siano in ascolto servizi. Tali informazioni sono cruciali per poter individuare attacchi che cerchino di utilizzare vulnerabilità effettivamente presenti all'interno degli asset e sono inoltre utilizzate dall'ESM per calcolare la priorità degli eventi individuati.

Presso la Regione Emilia-Romagna vengono effettuati regolari vulnerability assessment su tutti gli asset presenti, utilizzando il software di vulnerability scanning Tenable Nessus. Un apposito connettore Arcsight, il *Tenable Nessus .nessus File* permette di configurare una directory nella quale vengono posizionati i report delle scansioni: ogni qualvolta in tale directory appare un file *<nome_report>.nessus_done*, il report *<nome_report>.nessus* viene processato. Attraverso uno shell script appositamente creato, la scansione degli asset con le informazioni su vulnerabilità e porte aperte viene automaticamente importata all'interno del SIEM.

Tabella 5.2: Formato del file CSV degli asset

Nome	Descrizione	Obbligatorio	Ripetibile
Name	Nome descrittivo dell'asset. Se il nome non è specificato, verrà generato un nome unico.	No	No
Host Name	Nome DNS del dispositivo rappresentato dall'asset.	No	No
IP Address	Indirizzo IP del dispositivo di rete rappresentato dall'asset.	Sì	No
MAC Address	MAC address del dispositivo di rete rappresentato dall'asset.	No	No
Static Address	Definisce se l'indirizzo di rete dell'asset è in una zona statica o dinamica. Può contenere **true** o **false**.	No	No
Category URI	URI della categoria di asset. Può essere ripetuta perché lo stesso asset può essere categorizzato in più modi. **Esempi**: /All Asset Categories/RER/Area Riferimento/Amministratori Server Linux - S345 /All Asset Categories/System Asset Categories/Criticality/High	No	Sì

5.4 Individuazione degli eventi di interesse

Sono state individuate categorie di eventi che possono costituire minacce per il sistema informatico dell'Ente. Per ogni categoria individuata, sono state definiti filtri e regole di correlazione, usati poi per popolare console di monitoraggio e generare report per il monitoraggio della sicurezza a più alto livello.

Gli eventi di interesse individuati sono i seguenti:

- autenticazione degli utenti;
- attacchi sulla rete;
- attacchi e malware a livello host;
- attacchi alle applicazioni web.

5.5 Autenticazione degli utenti

La categoria di eventi di interesse legate all'autenticazione degli utenti ha l'obiettivo di individuare attacchi di forza bruta, tentativi di indovinare le password, malware e applicazioni mal configurate.

5.5.1 Regole di correlazione

All'interno dell'ESM è possibile individuare gli eventi di autenticazione, indipendentemente dalla sorgente che li ha prodotti, verificando il valore del campo *categoryBehavior*, che in tali casi contiene il valore *"/Authentication/Verify"*; il campo *categoryOutcome* conterrà l'esito del tentativo di autenticazione: "*/Success*", "*/Failure*" o "*/Attempt*".

5.5.1.1 Tentativi ripetuti di login provenienti da una singola sorgente

Si vuole creare un evento correlato ogni qualvolta si hanno cinque login falliti provenienti da un singolo host nell'arco di un minuto.

E' stato inizialmente predisposto un filtro per l'individuazione di tale evento, che costituirà il mattone sul quale costruire successivamente regole, strumenti di monitoraggio e report. Tale filtro, denominato "*Attack Login Source*", è così costituito:

```
( NotInActiveList("ArcSight Agent Users") AND NotInActiveList("Proxy server")
AND Attacker Address Is NOT NULL AND Category Behavior =
/Authentication/Verify AND Category Outcome = /Failure AND Category Technique
!= /Brute Force/Login AND Device Product != Squid Web Proxy Server )
```

Figura 5.5.1: Filtro: Attack Login Source

Le active list che escludono alcune categorie di asset e utenti, hanno lo scopo di escludere dal monitoraggio alcune categorie di eventi che esulano dagli scopi. Nel nostro caso sono stati esclusi gli eventi di login fallito sui server proxy (avremmo avuto tutti gli eventi di tipo http 407 "Proxy authentication required") e gli eventi di login fallito da parte degli account utilizzati dai connettori del SIEM.

Il filtro "*Attack Login Source*" viene usato poi per la creazione di eventi correlati utilizzando a questo fine una simple rule. Tale rule avrà come condizione la corrispondenza con il filtro precedente, come aggregation cinque condizioni soddisfatte nell'arco di un minuto, aggregando solo gli eventi che hanno l'attributo AttackerAddress identico.

```
Auth_Fail :  MatchesFilter("Attack-Login Source")

Aggregate if at least 5 matching conditions are found within 1 Minutes AND
these event fields are the same (Auth_Fail.Attacker Zone Resource,
Auth_Fail.Attacker Address)
```

Figura 5.5.2: Rule: Attack Login Source

La rule così creata genererà un evento correlato al raggiungimento della soglia impostata. Sull'evento correlato vengono impostati i seguenti valori per i campi:

```
message:  Repeat Attack-Login source
categoryBehavior:  /Authentication/Verify
categoryOutcome:  /Failure
categoryTechnique:  /Brute Force/Login
```

5.5.1.2 Tentativi ripetuti di login rivolti ad un singolo account

Si vuole creare un evento correlato ogni qualvolta si hanno cinque login falliti rivolti ad un singolo account nell'arco di un minuto.

E' stato inizialmente predisposto un filtro per l'individuazione di tale evento, che costituirà il mattone sul quale costruire successivamente regole, strumenti di monitoraggio e report. Tale filtro, denominato "*Attack Login Target*", è così costituito:

```
( NotInActiveList("ArcSight Agent Users") AND NotInActiveList("Proxy server")
AND Target User Name Is NOT NULL AND Category Behavior =
/Authentication/Verify AND Category Outcome = /Failure AND Category Technique
!= /Brute Force/Login AND Device Product != Squid Web Proxy Server )
```

Figura 5.5.3: Filtro: Attack Login Target

Le active list che escludono alcune categorie di asset e utenti, hanno lo scopo di escludere dal monitoraggio alcune categorie di eventi che esulano dagli scopi. Nel nostro caso abbiamo escluso gli eventi di login fallito sui server proxy (avremmo avuto tutti gli eventi di tipo http 407 "Proxy authentication required") e gli eventi di login fallito da parte degli account utilizzati dai connettori del SIEM.

Il filtro "*Attack Login Target*" viene usato poi per la creazione di eventi correlati utilizzando a questo fine una simple rule. Tale rule avrà come condizione la corrispondenza con il filtro precedente, come aggregation cinque condizioni soddisfatte nell'arco di un minuto, aggregando solo gli eventi che hanno l'attributo AttackerAddress identico.

```
Auth_Fail :  MatchesFilter("Attack-Login Target")

Aggregate if at least 5 matching conditions are found within 1 Minutes AND
these event fields are the same (Auth_Fail.Attacker Zone Resource,
Auth_Fail.Attacker Address)
```

Figura 5.5.4: Rule: Attack Login Target

La rule così creata genererà un evento correlato al raggiungimento della soglia impostata. Sull'evento correlato vengono impostati i seguenti valori per i campi:

```
message:  Repeat Attack-Login target
categoryBehavior:  /Authentication/Verify
categoryOutcome:  /Failure
categoryTechnique:  /Brute Force/Login
```

5.5.1.3 Attacchi di forza bruta

Se vengono rilevati diversi successivi tentativi falliti di autenticazione, provenienti da un singolo host oppure aventi come oggetto un certo account, e successivamente dallo stesso host o verso lo stesso account un evento di login che ha successo, potremmo trovarci in presenza di un attacco riuscito di forza bruta.

Per individuare attacchi di questo tipo è possibile utilizzare gli eventi correlati generati dalle rule ai due punti precedenti.

Sono stati inizialmente predisposti due filtri, *"Attack-Login Source Correlated"* e "*Attack-Login Target Correlated*", che sono filtri che individuano gli eventi correlati creati dalle due simple rule precedenti.

```
( NotInActiveList("ArcSight Agent USers") AND NotInActiveList("Proxy server")
AND Type = Correlation AND Attacker Address Is NOT NULL AND Category Behavior
= /Authentication/Verify AND Category Outcome = /Failure AND Category
Technique = /Brute Force/Login AND Device Product != Squid Web Proxy Server )

( NotInActiveList("ArcSight Agent USers") AND Category Behavior =
/Authentication/Verify AND Category Outcome = /Failure AND Category Technique
= /Brute Force/Login AND Device Product != Squid Web Proxy Server AND Target
User Name Is NOT NULL AND Type = Correlation )
```

Figura 5.5.5: Filtri: Attack Login Source Correlated e Attack Login Target Correlated

Tali filtri sono stati poi utilizzati per la definizione della join rule "*Brute Force Logins*", che permette la creazione di eventi correlati al verificarsi di sospetti attacchi riusciti di forza bruta.

```
Matching Event:  ( Brute_Force.End Time <= Login_Success.End Time AND ( (
Brute_Force.Attacker Address = Login_Success.Attacker Address AND
Brute_Force.Attacker Zone Resource = Login_Success.Attacker Zone Resource ) OR
Brute_Force.Target User Name = Login_Success.Target User Name ) )

Brute_Force :  ( ( MatchesFilter("Attack-Login Source Correlated") OR
MatchesFilter("Attack-Login Target Correlated") ) AND NotInActiveList("Trusted
List") AND NotInActiveList("ArcSight Agent USers") )

Login_Success :  ( NotInActiveList("Trusted List") AND Category Behavior =
/Authentication/Verify AND Category Outcome = /Success AND Category Technique
!= /Brute Force/Login )
Aggregate if at least 5 matching conditions are found within 2 Minutes AND
these event fields are the same (Brute_Force.Customer Resource,
Brute_Force.Target User ID, Login_Success.Target User ID, Login_Success.Target
User Name, Brute_Force.Target User Name, Login_Success.Customer Resource)
```

Figura 5.5.6: Rule: Brute Force Logins

La rule così creata genererà un evento correlato al raggiungimento della soglia impostata. Sull'evento correlato vengono impostati i seguenti valori per i campi:

```
message: Repeat Attack-Login target
categoryBehavior: /Authentication/Verify
categoryOutcome: /Success
categoryTechnique: /Brute Force/Login
```

5.5.1.4 Errori di autenticazione sulla VPN

Si vuole creare un evento correlato ad ogni tentativo di autenticazione fallita sulla VPN. L'accesso in VPN, infatti, non avviene attraverso meccanismi di strong authentication, ma tramite username e password ed è utilizzata anche da utenti che dispongono di privilegi elevati sulla rete regionale.

I log degli eventi di autenticazione sono caratterizzati dal campo *categoryBehavior*, che in tali casi contiene il valore *"/Access"*; il campo *categoryDeviceGroup* conterrà il valore "*/Firewall*" e il campo *DeviceEventClassId* conterrà infine il valore "*reject*".

È stata creata la rule "*VPN Authentication Failed*", definita di seguito.

```
( Category Behavior = /Access AND Category Device Group = /Firewall AND Device
Event Class ID = reject AND Attacker Address Is NOT NULL
```

Figura 5.5.7: VPN Authentication Failed

La rule così creata genererà un evento correlato alla prima occorrenza di evento che corrisponde alla definizione; sull'evento correlato vengono impostati i seguenti valori:

```
categoryBehavior: /Authentication/Verify
categoryDeviceGroup: /VPN
categorySignificance: /Informational/Error
categoryTechnique: /Brute Force/Login
```

La rule, ad ogni evento correlato generato, andrà a popolare un'active list con l'ip di provenienza del login fallito e il nome dell'account con cui è stata tentata l'autenticazione.

5.5.1.5 Modifica delle configurazioni di utenti e host

Si vuole creare un evento correlato ogni qualvolta vengano effettuate modifiche su utenti, quali creazione, assegnazione a gruppi, concessione di privilegi, reset password. Si vuole inoltre tenere traccia dell'utente che ha fatto le modifiche. Questa categoria di eventi è molto importante in un contesto esteso come il sistema informatico della Regione Emilia-Romagna, dove molte di queste operazioni non sono fatte direttamente dagli amministratori, ma delegate a referenti. La gestione degli utenti all'interno del sistema informatico della Regione Emilia-Romagna avviene attraverso un programma che interagisce con il dominio Active Directory e attraverso il sistema di Identity & Access Management.

I log di entrambe queste categorie sono caratterizzati dal campo *categoryBehavior*, che conterrà il valore "*/Modify/Configuration*".

E' stato inizialmente predisposto il filtro "*Configuration Modification*", così costituito:

```
( MatchesFilter("Non-ArcSight Events") AND Category Behavior =
/Modify/Configuration )
```

Figura 5.5.8: Filtro: Configuration Modification

Tale definizione utilizza il filtro "*Non-Arcsight Events*", che ha lo scopo di escludere gli eventi generati dall'ESM o dal logger.

A partire dal filtro appena definito viene definita la rule "*Successfull Configuration Change*":

```
( Target Address Is NOT NULL AND Target Zone Is NOT NULL AND Category Outcome
= /Success AND MatchesFilter("Configuration Modifications") AND Category
Object != /Host/Operating System )

Aggregate if at least 1 matching conditions are found within 2 Minutes AND
these event fields are the same (event1.Target User Name, event1.Message,
event1.MyAction, event1.Attacker User Name)
```

Figura 5.5.9: Rule: Successfull Configuration Change

La rule così creata genererà un evento correlato al raggiungimento della soglia impostata. Sull'evento correlato vengono impostati i seguenti valori per i campi:

```
categoryBehavior:  /Modify/Configuration
deviceCustomString1:  $MyAction
deviceCustomString1Label:  Action
priority:  2
```

La variabile *$MyAction* contiene il tipo di operazione svolta sull'utente e contiene valori quali "Reset password", "Add Group", eccetera.

La rule, oltre a generare un evento correlato andrà a popolare un'active list con il nome utente che ha fatto la modifica, l'utente oggetto della modifica, l'azione effettuata, i dettagli dell'azione, il timestamp.

5.5.1.6 Accesso ai sistemi mediante account amministrativi non personali

Le policy della Regione Emilia-Romagna prevedono che il login venga effettuato solamente utilizzando account personali, anche per quel che riguarda le utenze amministrative, e che gli account impersonali utilizzati dalle applicazioni non vengano utilizzati per l'accesso interattivo ai sistemi. L'accesso con account amministrativi non personali deve essere limitato a casi particolari e comunque solo attraverso le console dei sistemi, non via rete. Per tale motivo si rende necessario monitorare il ricorso a tali eccezioni.

E' stata predisposta la query "*Privileged Users Login*", così costituita:

```
( InActiveList("Administrative Accounts List") AND Category Behavior =
/Authentication/Verify [ignore case] AND Category Outcome = /Success [ignore
case] )
```

Figura 5.5.10: Query: Privileged Users Login

La lista "*Administrative Accounts Lists*" contiene l'elenco degli account amministrativi non personali, quali Administrator, root, admin, eccetera.

5.5.2 Strumenti di monitoraggio

Gli strumenti predisposti per il monitoraggio dell'autenticazione degli utenti, consistono in alcuni active channel basati sulle regole create e in alcune dashboard in cui viene visualizzato, attraverso liste e grafici aggiornati in realtime, un compendio significativo degli eventi di interesse.

5.5.2.1 Monitoraggio di ripetuti login falliti e attacchi di forza bruta

Si vuole predisporre una dashboard che permetta di visualizzare in forma grafica e in real time gli eventi relativi a login falliti e ad attacchi di forza bruta.

A questo scopo, a partire dai filtri "*Attack-Login Source Correlated*", "*Attack-Login Target Correlated*" e "*Attack Brute Force*", sono state creati data monitor di tipo "*Last N events*", che permettono di visualizzare una lista degli ultimi N eventi che soddisfano un filtro e data monitor di tipo "*Top Value Counts*", che permettono di visualizzare un grafico con gli N oggetti per il quali il filtro è stato soddisfatto. Tali data monitor sono stati combinati per ottenere una dashboard, che ha un aspetto del tipo mostrato in figura 5.5.11.

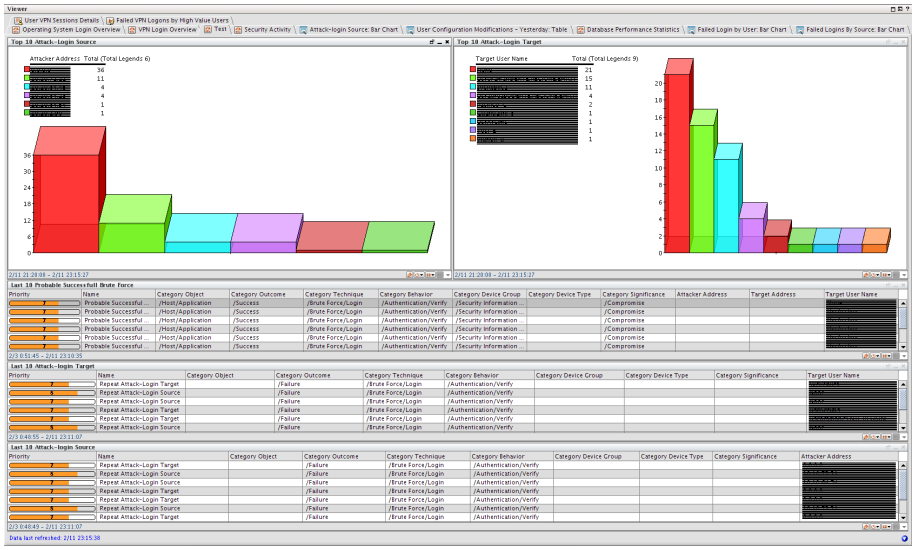

Figura 5.5.11: Dashboard di monitoraggio dei login falliti

5.5.2.2 Monitoraggio degli eventi di autenticazioni sulla VPN

Si vuole creare una dashboard che permetta di visualizzare in forma grafica e in real time gli eventi di autenticazione sulla VPN.

A questo scopo, sono stati creati i filtri "*VPN Successfull Login*" e "*VPN Failed Login*", mostrati in figura.

```
( Name = authcrypt AND Device Custom String3 = smartcenter AND ( Message
Contains " connected" OR Message StartsWith connected ) )
```

Figura 5.5.12: Filter: VPN Successfull Login

```
( Category Behavior = /Access AND Category Device Group = /Firewall AND Device
Event Class ID = reject AND Attacker Address Is NOT NULL
```

Figura 5.5.13: Filter: VPN Failed Login

A partire dai filtri creati, sono stati predisposti data monitor di tipo "*Last N events*", che permettono di visualizzare una lista degli ultimi N eventi che soddisfano un filtro e data monitor di tipo "*Top Value Counts*", che permettono di visualizzare un grafico con gli N oggetti per il quali il filtro è stato soddisfatto. Tali data monitor sono stati combinati per ottenere una dashboard.

5.5.2.3 Autenticazioni fallite sulla VPN da parte di utenti privilegiati

Allo scopo di monitorare gli eventi di autenticazione fallita da parte di utenti privilegiati, ovvero di utenti che attraverso la VPN hanno accesso a diversi sistemi, anche critici, è stato predisposto un active channel. Tale active channel è basato sulla rule "*VPN Authentication Failed*", combinando il nome dell'utente con una active list appositamente predisposta e popolata a mano, contenente gli utenti privilegiati.

5.5.3 Reportistica

5.5.3.1 Utilizzo della VPN

È stato predisposto un report, eseguito giornalmente, che mostra le connessioni degli utenti alla rete regionale attraverso VPN, in modo da poter evidenziare eventuali comportamenti anomali. Per ogni connessione, il report mostra il nome utente, l'ip di provenienza, i timestamp di inizio connessione e di fine connessione.

5.5.3.2 Modifica delle configurazioni degli utenti

È stato predisposto un report, eseguito settimanalmente, che mostra una lista di tutti gli utenti creati, modificati e cancellati, contenente il timestamp dell'operazione, l'amministratore che ha effettuato la modifica e il sistema su cui la modifica è stata effettuata.

5.5.3.3 Monitoraggio delle sessioni amministrative

È stato predisposto un report, eseguito settimanalmente, che mostra, per ogni amministratore e per ogni sistema amministrato, il numero di connessioni effettuate ogni giorno del periodo di riferimento del report.

Tale report ha anche lo scopo di essere utilizzato nell'ambito delle verifiche dell'operato degli amministratori di sistema, richieste dal provvedimento del garante per la protezione dei dati personali relativo agli amministratori di sistema.

5.6 Attacchi sulla rete

La categoria di eventi di interesse legate ad attacchi sulla rete ha l'obiettivo di individuare scansioni di rete e presenza di malware.

5.6.1 Regole di correlazione

All'interno dell'ESM è possibile individuare eventi di attacchi sulla rete monitorando gli eventi provenienti soprattutto da firewall e IPS.

Gli eventi provenienti da firewall sono caratterizzati dal valore */Firewall* contenuto all'interno del campo *categoryDeviceGroup* e dal valore */Access* contenuto all'interno del campo *categoryBehavior*. Il campo *categoryOutcome* conterrà */Success* o */Failure* a seconda che il firewall abbia accettato o bloccato la connessione.

Gli eventi provenienti da IPS sono caratterizzati dal valore */IDS/Network* contenuto all'interno del campo *categoryDeviceGroup* e dai valori Permit o Block contenuti all'interno del campo *deviceAction*, a seconda che il pacchetto sia stato solo segnalato o anche bloccato. I campi *categoryBehavior* e *categoryOutcome* possono contenere diversi valori a seconda dal tipo di minaccia o attacco rilevato.

5.6.1.1 Alto numero di connessioni negate

Si vuole generare un evento correlato ogni qualvolta si hanno più di 900 tentativi di connessione negate in 1 minuto da parte di host esterni verso un singolo host interno su porte udp differenti maggiori della 1024.

Per generare tali eventi è stata definita la rule "*High Number of Denied Connections*":

(Type = Base AND Category Behavior = /Access AND Category Device Group = /Firewall AND Category Object = /Host/Application/Service AND Category Outcome = /Failure AND NotInActiveList("Event-based Rule Exclusions"))

Aggregate if at least `900` matching conditions are found within `1 Minutes` AND these event fields are the same (`event1.Category Object, event1.Device Product, event1.Category Device Group, event1.Attacker Zone Resource, event1.Device Address, event1.Attacker Address, event1.Category Behavior, event1.Category Outcome, event1.Device Vendor, event1.Device Host Name, event1.Device Zone Resource, event1.Attacker Host Name`)

Figura 5.6.1: Rule: High Number of Denied Connections

La rule così creata genererà un evento correlato al raggiungimento della soglia impostata.

5.6.1.2 Connessioni in outbound su porte differenti

Si vuole generare un evento correlato ogni qualvolta si hanno più di 100 tentativi di connessione in un minuto da parte di host interni verso un singolo host esterno su porte udp differenti maggiori della 1024.

Per generare tali eventi è stata definita la rule "*Firewall Network Port Scan*":

((Category Behavior = /Access OR Category Behavior = /Access/Start) AND Category Device Group = /Firewall AND Category Outcome = /Success AND NotInActiveList("_Test Trusted") AND (NotInActiveList("_RER Suspicious List") OR NotInActiveList("_Test Scanned List")) AND Attacker Zone URI StartsWith /All Zones/Site Zones/ AND NotTarget Zone URI StartsWith /All Zones/Site Zones/ AND NotAttacker Port <= 1024)

Aggregate if at least **100** matching conditions are found within **2 Minutes** AND these event fields are unique (**Allow_TCP_UDP.Target Port**) AND these event fields are the same (**Allow_TCP_UDP.Target Address, Allow_TCP_UDP.Attacker Zone Resource, Allow_TCP_UDP.Username, Allow_TCP_UDP.Target Zone Resource, Allow_TCP_UDP.Attacker Address**)

Figura 5.6.2: Rule: Firewall Network Port Scan

La rule così creata genererà un evento correlato al raggiungimento della soglia impostata. Sull'evento correlato vengono impostati i seguenti valori per i campi:

```
categoryBehavior: /Access
categoryDeviceGroup: /Security Information Manager
categoryObject: /Network
categoryOutcome: /Attempt
categoryTechnique: /Scan/Port
categoryDeviceCustomString1: $Username
categoryDeviceCustomString1Label: Username
```

La variabile *$Username*, assegnata al campo *categoryDeviceCustomString1*, è valorizzata andando a prelevare il valore del nome utente associato all'indirizzo IP da cui è partito l'attacco da una lista che tiene associato in tempo reale, basandosi sui dati della navigazione degli utenti, un certo ip con nome utente.

5.6.2 Strumenti di monitoraggio

Gli strumenti predisposti per il monitoraggio di attacchi sulla rete, consistono in alcuni active channel basati sulle regole create e in alcune dashboard in cui viene visualizzato, attraverso liste e grafici aggiornati in realtime, un compendio significativo degli eventi di interesse provenienti da firewall e IPS.

5.6.2.1 Overview degli eventi provenienti dal firewall

Si vuole predisporre una dashboard che permetta di visualizzare in forma grafica e in real time un'overview degli eventi provenienti dal firewall.

Sono stati innanzi tutto definiti i due filtri "*Denied Inbound Connections*", per ottenere le connessioni dalla rete esterna alla rete regionale bloccate dal firewall e "*Denied Outbound Connections*", per ottenere le connessioni dalla rete regionale alla rete esterna. I due filtri sono mostrati in figura:

(Category Behavior = /Access AND Category Device Group = /Firewall AND Category Object = /Host/Application/Service AND Category Outcome = /Failure AND (Device Direction = Inbound OR MatchesFilter("Inbound Events")))

(Category Behavior = /Access AND Category Device Group = /Firewall AND Category Object = /Host/Application/Service AND Category Outcome = /Failure AND (Device Direction = Outbound OR MatchesFilter("Outbound Events")))

Figura 5.6.3: Filtri: Denied Inbound Connections e Denied Outbound Connections

I filtri "*Inbound Events*" e "*Outbounds Events*", utilizzati per la creazione dei filtri precedenti, permettono di ottenere eventi il cui ip di provenienza sia interno o esterno alla rete dell'organizzazione.

Partendo dai due filtri sono state creati data monitor di tipo "*Last N events*", che permettono di visualizzare una lista degli ultimi N eventi che soddisfano un filtro, e data monitor di tipo "*Top Value Counts*", che permettono di visualizzare un grafico con gli N oggetti per il quali il filtro è stato soddisfatto. Tali data monitor sono stati combinati per ottenere una dashboard, che ha un aspetto del tipo mostrato in figura.

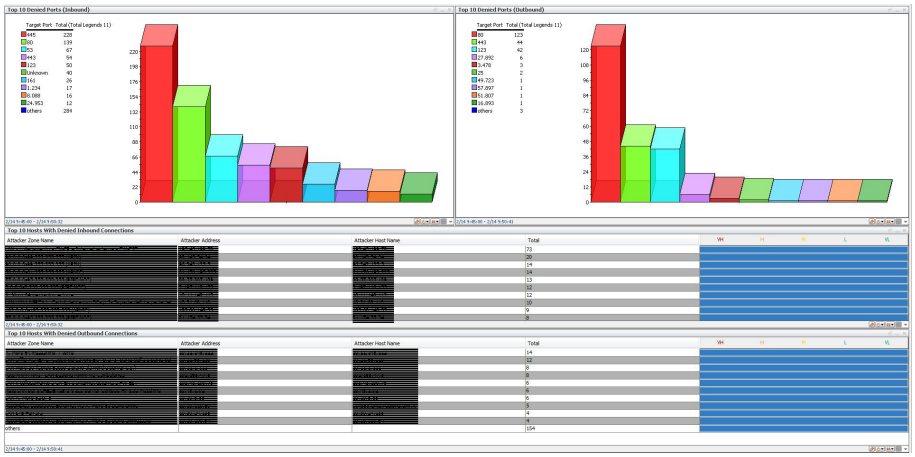

Figura 5.6.4: Dashboard: Firewall Overview

5.6.2.2 Overview degli eventi provenienti dall'IPS

Si vuole predisporre una dashboard che permetta di visualizzare in forma grafica e in realtime un'overview degli eventi provenienti dall'IPS.

È stato innanzi tutto definito il filtro "*IDS - IPS Events*", per ottenere gli eventi provenienti dal sistema IPS. Il filtro è mostrato in figura:

(Category Device Group StartsWith /IDS AND Category Device Group != /IDS/Host/Antivirus)

Figura 5.6.5: Filtro: IDS - IPS Events

Partendo da tale filtro sono state creati data monitor di tipo "*Top Value Counts*", che permettono di visualizzare un grafico o una tabella con gli N oggetti per il quali il filtro è stato soddisfatto. Tali data monitor sono stati combinati per ottenere una dashboard, che ha un aspetto del tipo mostrato in figura.

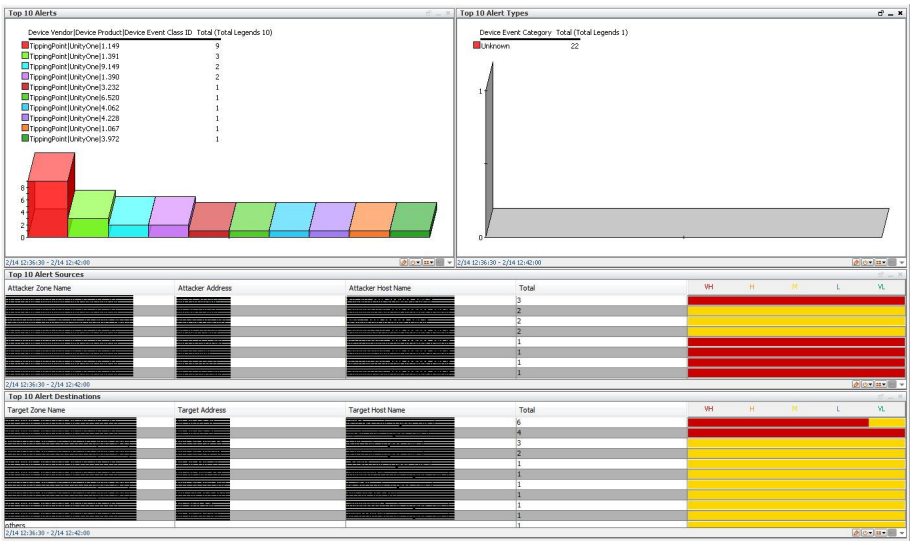

Figura 5.6.6: Dashboard: IPS Overview

5.6.3 Reportistica

5.6.3.1 Uso di protocolli in chiaro in outbound

È stato predisposto un report, eseguito giornalmente, che mostra l'utilizzo in outbound di protocolli in chiaro, quali ad esempio l'ftp. Il report contiene indirizzo e nome host sorgente, indirizzo e nome host destinatario, la porta di destinazione e il numero di eventi.

5.6.3.2 IP interni bloccati

È stato predisposto un report, eseguito settimanalmente, che mostra i principali IP interni bloccati. Il report contiene indirizzo sorgente, indirizzo di destinazione e il numero di pacchetti bloccati.

5.6.3.3 IP esterni bloccati

È stato predisposto un report, eseguito settimanalmente, che mostra i principali IP esterni bloccati. Il report contiene indirizzo sorgente, indirizzo di destinazione e numero di pacchetti bloccati.

5.6.3.4 Principali alert da IDS / IPS

È stato predisposto un report, eseguito giornalmente, che mostra i principali alert provenienti da IPS. Il report contiene la signature rilevata, la sua descrizione e il numero di occorrenze.

5.7 Attacchi e malware a livello host

La categoria di eventi di interesse legate ad attacchi e malware a livello host ha l'obiettivo di individuare host che possono essere infetti o compromessi.

5.7.1 Regole di correlazione

All'interno dell'ESM è possibile individuare host compromessi monitorando gli eventi provenienti dal sistema antimalware o dal sistema IPS.

Gli eventi provenienti da firewall sono caratterizzati dal valore */IDS/Host/Antivirus* contenuto all'interno del campo *categoryDeviceGroup*.

Gli eventi provenienti da IPS sono caratterizzati dal valore */IDS/Network* contenuto all'interno del ramo *categoryDeviceGroup* e dai valori *Permit* o *Block* contenuti all'interno del campo *deviceAction*, a seconda che il pacchetto sia stato solo segnalato o anche bloccato. I campi *categoryBehavior* e *categoryOutcome* possono contenere diversi valori a seconda dal tipo di minaccia o attacco rilevato.

5.7.1.1 Malware rilevato ma non rimosso

Si vuole generare un evento correlato ogni qualvolta un malware su un host viene rilevato dal sistema anti malware, ma quest'ultimo non riesce a rimuoverlo.

Per generare tali eventi è stata definita la rule "*Antivirus Unsuccessfull Clean*":

(Category Device Group = /IDS/Host/Antivirus AND Device Custom String5 Contains unsuccessful AND Device Custom String6 Contains unsuccessful)

Aggregate if at least **1** matching conditions are found within **2 Minutes** AND these event fields are the same (**event1.Device Custom String5, event1.Device Custom String6, event1.File Name, event1.File Path, event1.Name, event1.Target Address, event1.Target Zone Resource, event1.Target Host Name**)

Figura 5.7.1: Rule: Antivirus Unsuccessfull Clean

La rule così creata genererà un evento correlato al primo evento che soddisfa la regola. Oltre a impostare l'evento correlato si andrà a popolare un'active list con i seguenti campi:

`Target Address`

`Target Zone`

`Name`

`File Name`

`File Path`

`Timestamp`

5.7.1.2 Worm Rilevato

Si vuole definire una regola di correlazione che abbia lo scopo di rilevare malware per il quale non sia stata ancora rilasciata la relativa signature all'interno dei sistemi IPS.

È stato innanzi tutto definito il filtro:

```
( Target Port != 8443 AND Attacker Address Is NOT NULL AND Target Port Is
NOT NULL AND Not( Attacker Asset ID InGroup("/All Asset Categories/Site Asset
Categories/Application/Type/Domain Name Server/") Or Attacker Asset ID
InGroup("/All Asset Categories/Site Asset Categories/Application/Type/Email/")
Or Attacker Asset ID InGroup("/All Asset Categories/Site Asset
Categories/Application/Type/Proxy/") ) )
```

Figura 5.7.2: Filter: Target Port Activity By Attacker

Il filtro è stato poi utilizzato all'interno di un data monitor di tipo moving average, denominato anch'esso "*Target Port Activity By Attacker*". Un data monitor di tipo "moving average" calcola l'ammontare medio di eventi in un intervallo di tempo specificato. Il data monitor "*Target Port Activity by Attacker*" utilizza il filtro in fig. 5.7.2, raggruppando i campi "*Target Port*" e "*Attacker Address*" per calcolare l'utilizzo medio di una porta target per un attaccante e generare un evento correlato avente lo stesso nome del data monitor se l'utilizzo medio cambia del 100% nell'intervallo di tempo configurato per uno di questi gruppi.

Sono state poi definite due rule, "*Possible Outbound Network Sweep*" e "*Possible Inbound Network Sweep*" che generano eventi correlati nel caso di sospetti network sweep.

```
( Type != Correlation AND Attacker Address Is NOT NULL AND Device Product !=
ArcSight AND Device Vendor != ArcSight AND Target Address Is NOT NULL AND
Target Port Is NOT NULL AND Not( Attacker Asset ID InGroup("/All Asset
Categories/Site Asset Categories/Application/Type/Domain Name Server/") Or
Attacker Asset ID InGroup("/All Asset Categories/Site Asset
Categories/Application/Type/Email/") Or Attacker Asset ID InGroup("/All Asset
Categories/Site Asset Categories/Application/Type/Proxy/") ) AND Category
Behavior != /Access/Stop AND MatchesFilter("Internal to Internal Events") )

( Type != Correlation AND Attacker Address Is NOT NULL AND Device Product !=
ArcSight AND Device Vendor != ArcSight AND Target Address Is NOT NULL AND
Target Port Is NOT NULL AND Not( Attacker Asset ID InGroup("/All Asset
Categories/Site Asset Categories/Application/Type/Domain Name Server/") Or
Attacker Asset ID InGroup("/All Asset Categories/Site Asset
Categories/Application/Type/Email/") Or Attacker Asset ID InGroup("/All Asset
Categories/Site Asset Categories/Application/Type/Proxy/") ) AND Category
Behavior != /Access/Stop AND MatchesFilter("Outbound Events") )
```

Figura 5.7.3: Rules: Possible Outbound Network Sweep e Possible Inbound Network Sweep

Gli eventi correlati generati dal data monitor e dalle rule vengono infine utilizzati per la definizione della join rule "*Worm Outbreak*":

Matching Event: (event1.Attacker Zone = event2.Attacker Zone AND event1.Attacker Address = event2.Attacker Address AND event1.Target Port = event2.Target Port)

event1 : (NotInActiveList("Worm Infected Systems") AND (Name = Possible Internal Network Sweep OR Name = Possible Outbound Network Sweep) AND Type = Correlation AND Device Product = ArcSight AND Device Vendor = ArcSight)

event2 : (Name = Target Port Activity by Attacker [ignore case] AND Type = Correlation AND Device Event Category StartsWith /datamonitor/movingaverage/threshold/rising [ignore case] AND Device Custom Number1 > 100 AND Device Custom Number2 > 1 AND NotInActiveList("Worm Infected Systems"))

Aggregate if at least **1** matching conditions are found within **10 Minutes** AND these event fields are the same (**event1.Attacker Asset Resource, event1.Target Port, event1.Attacker Zone Resource, event1.Attacker Address, event1.Customer Resource, event1.Attacker Zone**)

Figura 5.7.4: Rule: Worm Outbreack

La join rule così creata ha lo scopo di individuare casi in cui da un attaccante aumenti il traffico verso un certo target (ip e porta) e contemporaneamente venga effettuato un network sweep verso il medesimo target. La rule genererà un evento correlato al primo evento che soddisfa la regola. Oltre a impostare l'evento correlato si andrà a popolare un'active list con i seguenti campi:

`Attacker Zone`

```
Attacker Address
Target Port
```

L'evento correlato generato dalla rule avrà i seguenti campi impostati:

```
categoryBehavior:  /Communicate
categoryDeviceGroup:  /Security Information Manager
categoryObject:  /Host/Infection/Worm
categoryOutcome:  /Success
categorySignificance:  /Compromise
priority:  10
```

5.7.2 Strumenti di monitoraggio

5.7.2.1 Overview dei sistemi antivirus

Si vuole predisporre una dashboard che permetta di visualizzare in forma grafica e in realtime un'overview degli eventi provenienti dal sistema antimalware.

È stato innanzi tutto definito il filtro "*Virus Activity*", per ottenere gli eventi provenienti dal sistema IPS. Il filtro è mostrato in figura:

((Category Object StartsWith /Vector/Virus OR Category Object StartsWith /Host/Infection/Virus) OR ((Category Behavior StartsWith /Modify/Content OR Category Behavior = /Found/Vulnerable OR Category Behavior StartsWith /Modify/Attribute OR Category Behavior = /Delete) AND Category Device Group = /IDS/Host/Antivirus AND Device Custom String1 Is NOT NULL))

Figura 5.7.5: Filtro: Virus Activity

Partendo da tale filtro sono stati creati data monitor di tipo "*Event Graph*", che permettono di visualizzare un grafico dell'attività dei virus e data monitor di tipo "*Moving Average*", che permettono di visualizzare gli incrementi, rispetto al valore medio, del numero di host sui quali è stato rilevato un malware.

5.7.3 Reportistica

5.7.3.1 Sorgenti di malware

È stato predisposto un report che mostra una lista di host soggetta ad un certo malware, raggruppato per il malware rilevato.

5.7.3.2 Malware rilevato

È stato predisposto un report che mostra la lista dei malware rilevati e, per ognuno di essi, il numero di occorrenze riscontrate.

5.8 Attacchi alle applicazioni web

La categoria di eventi di interesse legate ad attacchi alle applicazioni web ha l'obiettivo di individuare attacchi rivolti alle applicazioni web. Va in ogni caso

considerato che per rilevare questo genere di attacchi sono più efficaci altri strumenti quali application firewall o IDS.

5.8.1 Regole di correlazione

All'interno dell'ESM è possibile individuare gli attacchi alle applicazioni web monitorando gli eventi provenienti dai web server che costituiscono il frontend delle applicazioni web.

Gli eventi provenienti da firewall sono caratterizzati dal valore del campo *Request URL* non nullo.

5.8.1.1 Directory traversal

Si vuole generare un evento correlato ogni qualvolta venga individuato un attacco di tipo "directory traversal", ovvero il caso in cui un attaccante cerchi di "uscire" dal contesto dell'applicazione per arrivare sul filesystem del server che funge da server web.

All'interno dell'ESM è possibile rilevare attacchi di questo tipo monitorando gli eventi provenienti dai web server che fanno da frontend per le applicazioni web (bilanciatori, reverse proxy, ecc.).

Per generare questi eventi è stato innanzi tutto definito il filtro "*Web Application*":

```
( Request Method Is NOT NULL AND Device Vendor NOT Contains Squid )
```

Figura 5.8.1: Filtro: Web Application

La definizione del filtro esclude gli eventi provenienti dai web proxy, in quanto anche essi hanno il campo Request Method non nullo.

A partire dal filtro appena definito viene definita la rule "*Web Attack*":

```
( MatchesFilter("_RER Web Application") AND Request Url Contains ../../..  )

Aggregate if at least 1 matching conditions are found within 1 Minutes AND
these event fields are the same (event1.Target Address, event1.Attacker Zone
Resource, event1.Attacker Address, event1.Target Zone Resource)
```

Figura 5.8.2: Rule: Web Attack

La rule così creata genererà un evento correlato al primo evento che la soddisfa e inoltre andrà a popolare un'active list con l'ip dell'attaccante, il target e l'url richiesto.

Capitolo 6

Conclusioni

Il lavoro svolto ha riguardato la realizzazione di un sistema di monitoraggio della sicurezza informatica mediante il modello SIEM all'interno della Regione Emilia-Romagna. I risultati ottenuti hanno permesso di constatare come un SIEM, adeguatamente configurato per tenere conto delle caratteristiche del sistema informatico dell'organizzazione, dei dati disponibili e dei rischi individuati, possa rappresentare un valido strumento a disposizione di un Security Operation Center di un'organizzazione complessa, utile per il monitoraggio real-time della sicurezza dell'infrastruttura informatica e per la generazione di reportistica dei sistemi e delle applicazioni.

Tale risultato avviene mediante l'acquisizione, la conservazione e l'elaborazione delle informazioni contenute all'interno dei log. Ogni dispositivo o applicazione, infatti, genera log con informazioni utili a identificare e gestire situazioni rilevanti per la sicurezza e il funzionamento dei sistemi. L'importanza dei log ha portato allo sviluppo di pratiche per la gestione e l'utilizzo degli stessi log che in molti casi sono anche state tradotte in norme alle quali le aziende dotate di sistemi IT si devono attenere (es. SOX, PCI, normativa italiana sul controllo degli amministratori di sistema). I log di dispositivi e applicazioni, pur contenendo potenzialmente un notevole patrimonio informativo, vengono normalmente analizzati solo successivamente al verificarsi di incidenti o malfunzionamenti, allo scopo di capire le cause di quanto successo. L'esigenza da cui parte un corretto processo di log management è quella di estrarre da questa grande mole di dati presente all'interno dell'organizzazione le informazioni necessarie a garantire la sicurezza dei sistemi informatici in maniera proattiva.

Affinché questo processo sia portato a termine correttamente occorre implementare un'infrastruttura complessa con strumenti che si occupino della corretta acquisizione, conservazione, analisi e correlazione dei log, della reportistica e della ricerca. La complessità del processo fa sì che non sia sufficiente l'installazione e la configurazione di uno dei prodotto SIEM commerciali o open source presenti sul mercato.

La corretta configurazione del sistema è basata sull'individuazione di eventi di interesse, ovvero di eventi che possono costituire una minaccia o requisiti di

business; affinché tali eventi di interesse siano individuati correttamente è necessario che l'organizzazione abbia operato una seria analisi dei rischi e definito politiche di sicurezza. Nel caso della Regione Emilia-Romagna, come descritto all'interno della tesi, entrambi i requisiti erano soddisfatti.

Altro prerequisito essenziale per la fase di messa in opera del SIEM è la presenza di un modello per la corretta categorizzazione degli asset. Nel caso della Regione Emilia-Romagna tali informazioni sono presenti all'interno del CMDB.

Per la realizzazione del sistema di monitoraggio della sicurezza informatica all'interno della Regione Emilia-Romagna sono state necessarie diverse fasi.

Individuazione dell'architettura. L'architettura scelta è quella di un sistema agentless con connettori concentrati su alcuni sistemi. I connettori inviano gli eventi filtrati, aggregati e normalizzati al sistema di log management, il quale firma gli eventi ricevuti e li immagazzina in un database; a sua volta il log manager invia gli eventi al sistema di log correlation, che li analizza e attiva gli strumenti di monitoraggio e reportistica configurati.

Individuazione delle sorgenti di eventi. Per ogni sorgente di eventi è stato individuata la forma migliore di integrazione, configurando di conseguenza i connettori con il sistema di log management ed il SIEM.

Modellazione della rete e degli asset. Le informazioni su zone di rete, sugli asset e la loro categorizzazione, contenute all'interno del CMDB, sono state riportate sul SIEM, impostando anche meccanismi di sincronizzazione automatica. Sul SIEM sono state inoltre riportate le informazioni sulle vulnerabilità che colpiscono i vari asset, impostando meccanismi di importazione automatica dei risultati dei report dei vulnerability assessment svolti periodicamente.

Individuazione di eventi di interesse e definizione di strumenti specifici. Sono stati definiti eventi di interesse appartenenti alle categorie: autenticazione degli utenti, attacchi sulla rete, attacchi e malware a livello host, attacchi alle applicazioni web. Per ogni evento di interesse sono state costruite regole di correlazione, strumenti di monitoraggio e reportistica, sia operativi, a disposizione degli operatori del SOC e analisti della sicurezza, sia di più alto livello, a disposizione del management.

Possibili sviluppi futuri del lavoro svolto, oltre all'individuazione di ulteriori eventi di interesse e la conseguente definizione di strumenti di monitoraggio specifici, sono la realizzazione di workflow per la gestione degli alert aperti dal sistema di monitoraggio della sicurezza, l'integrazione con il workflow di gestione degli incidenti di sicurezza, l'integrazione del SIEM con il sistema di trouble ticketing della Regione Emilia-Romagna.

Bibliografia

1. ***Guide to Computer Security Log Management*** - NIST Special Publication 800-92 - September 2006 (cap. 1,2)
   http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

2. ***Sicurezza aziendale e continuità del business*** - Giuseppe Saccardi, Gaetano Di Blasio, Riccardo Florio - Reportec - 2010 (cap. 1)

3. **Sicurezza in informatica** - Charles P. Pfleeger, Shari Lawrence Pfleeger - Pearson Prentice Hall - 2008 - ISBN 978-88-7192-363-5 (cap. 1)

4. ***Successful SIEM and Log Management Strategies for Audit and Compliance*** - David Swift - SANS Institute InfoSec Reading Room - November 2010 - (cap. 1,2,5)
   http://www.sans.org/reading_room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance_33528

5. ***A Practical Application of SIM/SEM/SIEM Automating Thread Identification*** - David Swift - SANS Institute InfoSec Reading Room - December 2006 - (cap. 1,5)
   http://www.sans.org/reading_room/whitepapers/logging/practical-application-sim-sem-siem-automating-threat-identification_1781

6. ***Keys to Implementing a Successfull Security Information Management Solution (or Centralized Security Monitoring)*** - Michael Martin - SANS Institute InfoSec Reading Room - December 2003 - (cap. 1)
   http://www.sans.org/reading_room/whitepapers/bestprac/keys-implementing-successful-security-information-management-solution-or-centralized-security_1303

7. ***Security Information and Event Management (SIEM) Implementation*** - David R. Miller, Shon Harris, Allen A. Harper, Stephen Vandyke, Chris Blask - Mc Graw Hill - 2011 - ISBN 978-0-07-170109-9 (cap. 1,2,3)

8. ***Security Operation Center concepts & Implementation*** - Renaud Bidou - (cap. 2)
http://www.iv2-technologies.com/SOCConceptAndImplementation.pdf

9. ***Disciplinare Tecnico per gli utenti del sistema informatico della Regione Emilia-Romagna*** - Dicembre 2011 (cap. 4)

10. ***Disciplinare Tecnico per amministratori di sistema della Regione Emilia-Romagna*** - Gennaio 2012 (cap.4)

11. ***Disciplinare Tecnico per la gestione degli incidenti di sicurezza informatica della Regione Emilia-Romagna*** - Marzo 2009 (cap. 4)

12. ***ESM 101: Concepts for Arcsight ESM*** - ArcSight - May 2010 (cap. 3,5)

13. ***ArcSight ESM User Guide*** - Arcsight - September 2011 (cap. 3,5)

14. ***ArcSight ESM Standard Content Guide*** - ArcSight - May 2009 (cap. 5)