# FONDIARIA - SAI

# SISTEMA DI LOG MANAGEMENT

## *Controllo degli accessi, monitoring delle situazioni anomale, alerting e reporting*

Milano


| | |
|---|---|
| **Hacking Team S.r.l.** | http://www.hackingteam.it |
| *Via della Moscova, 13*<br>*20121 MILANO (MI) - Italy* | info@hackingteam.it |
| *Tel. +39.02.29060603* | *Fax +39.02.63118946* |

| STORIA DEL DOCUMENTO | | |
|---|---|---|
| Versione | Data | Modifiche Effettuate |
| 1.0 | 13 Luglio 2004 | Emissione |
| // | // | // |
| // | // | // |

| INFORMAZIONI | | |
|---|---|---|
| Data di Emissione | 13 Luglio 2004 | |
| Versione | 1.0 | |
| Tipologia Documento | Documento di Progetto | |
| Numero di Protocollo | // | |
| Numero Pagine | 20 | |
| Numero Allegati | 2 | |
| Descrizione Allegati | 1 | Whitepaper-LM.pdf |
| | 2 | Outsourcing-LM.pdf |
| Redatto da | Aldo Scaccabarozzi | |
| Approvato da | Gianluca Vadruccio | |

# INDICE

# INDICE DELLE FIGURE



# INDICE DELLE TABELLE

# 1 Introduzione

## *1.1 Obiettivi*

Il presente documento ha lo scopo di descrivere la proposta di realizzazione di una soluzione di Log Management da parte di Hacking Team SRL. Il progetto nasce in risposta alle esigenze di gestione, analisi e correlazione dei log prodotti dai sistemi e dalle applicazioni presenti nell'infrastruttura informativa. Il sistema di Log Management consentirà di avere il pieno controllo dello stato dell'infrastruttura informatica in tempo reale, di ottenere le informazioni relative ad eventi specifici, identificare le attività che li hanno generati e intraprendere specifiche azioni in risposta agli stessi.

## *1.2 Ambiente di riferimento*

L'infrastruttura informatica di SAI, oggetto del progetto di Log Management, è così costituita:

- Sistemi di difesa perimetrale dell'accesso a Internet (si veda Figura 1 - Accesso Internet)
  - 2 Firewall di front-end in HA Checkpoint v4.1 (di possima migrazione a NG)
  - 2 Firewall di back-end in HA Cisco PIX
  - 1 sonda SNORT attestata su internet
  - 1 sonda SNORT attestata sulla DMZ
- Sistemi di difesa perimetrale del nodo di accesso (Figura 2 - Rete Trust e di Accesso)
  - 2 Firewall in HA Checkpoint v4.1 (di possima migrazione a NG)
  - 1 sonda SNORT attestata all'esterno dei 2 FW
- Sistemi di difesa perimetrale del nodo Trust (Figura 2 - Rete Trust e di Accesso)
  - 2 Firewall in HA Checkpoint v4.1 (di possima migrazione a NG)
  - 1 sonda SNORT attestata all'esterno dei 2 FW
- Sistemi applicativi
  - Modulo WebSeal di Tivoli access manager (livello di autenticazione)
  - Web server Apache (Front End)
  - Websphere Application Server
  - IBM MainFrame

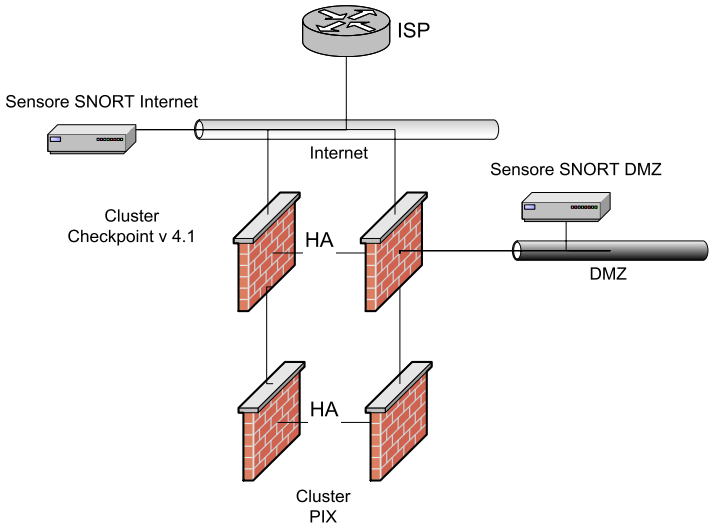


**Figura 1 - Accesso Internet (Torino)**

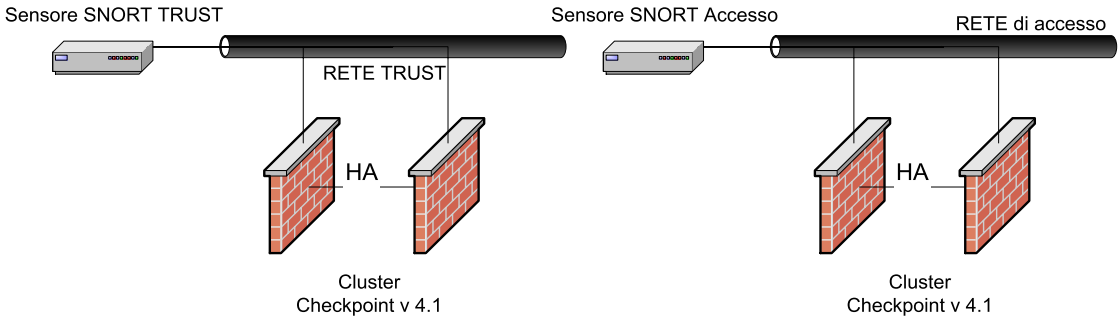


**Figura 2 - Rete Trust e di Accesso (Torino)**

Obiettivo del progetto di Log Management è raccogliere i log provenienti dai sistemi e dalle applicazioni sopra citate, al fine di consentire:

- La centralizzazione dei log dell'infrastruttura di difesa perimetrale (Firewall e IDS)
- La centralizzazione dei log degli applicativi al fine di monitorare gli accessi alle risorse critiche
- Correlare i diversi log allo scopo d'individuare situazioni anomale e/o potenzialmente "pericolose"
- L'identificazione e l'eventuale allarmistica legata ad eventi ritenuti critici e/o potenzialmente "pericolosi"

## 1.3 Soluzione

La soluzione di Log Management proposta è basata sul software Network Security Manager (NSM[1]), prodotto da Intellitatics®. Caratteristica fondamentale della soluzione di Log Management adottata è la non intrusività rispetto al sistema informativo del cliente. Tutte le informazioni d'interesse saranno inviate alla componente centrale, il central server, come mostrato in Figura 3. Per ogni dispositivo, applicazione o sistema esiste uno specifico ricettore in grado di normalizzare i dati contenuti nei log ricevuti.

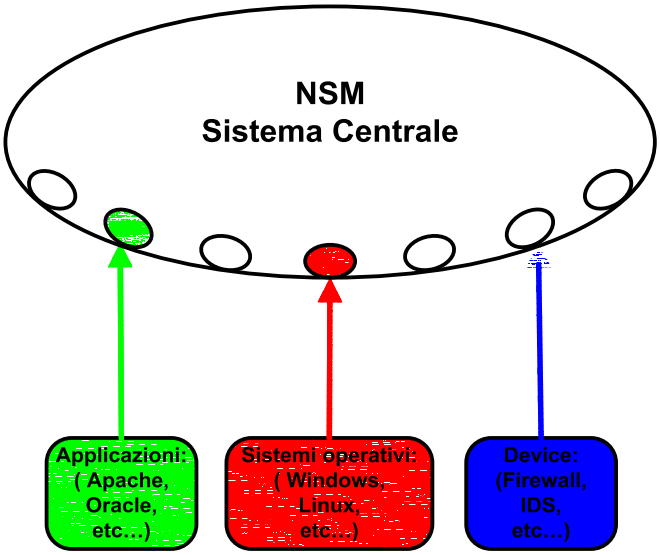


**Figura 3 - Central Server**

Le operazioni svolte dal sistema centrale sono:

- Raccolta dei i log prodotti dai vari dispositivi e applicazioni
- Elaborazione e memorizzazione delle informazioni ricevute in un unico formato, decisamente più comprensibile rispetto ai log originali
- Analisi e correlazione dei dati, fornendo opportuni strumenti di supporto a tali attività
- Esecuzione di specifiche azioni in risposta a particolari eventi
- Gestione della documentazione relativa a un Incident Handling, necessaria per fornire le informazioni utili ad intraprendere le opportune contromisure

[1] Per una descrizione precisa della soluzione tecnica si rimanda al whitepaper relativo al Log Management: Whitepaper-LM.pdf

La soluzione prevede un'architettura scalabile che, per mezzo di uno o più livelli intermedi di consolidamento, di controllo delle politiche di sicurezza e di correlazione degli eventi, consente di distribuire il carico di lavoro del Central Server su più unità (Event Collector), come mostrato in Figura 4.

L'ambiente oggetto del progetto di Log Management, descritto nel paragrafo precedente, ad oggi non richiede l'utilizzo di un'architettura distribuita, che potrebbe però diventare necessaria nel caso in cui venga scelta una soluzione gestita in outsourcing[2]. La scalabilità della soluzione garantisce anche in un secondo momento l'introduzione di uno o più livelli di consolidamento dei log, caratteristica importante in un'ottica di gestione complessiva dell'infrastruttura informatica (server e client).

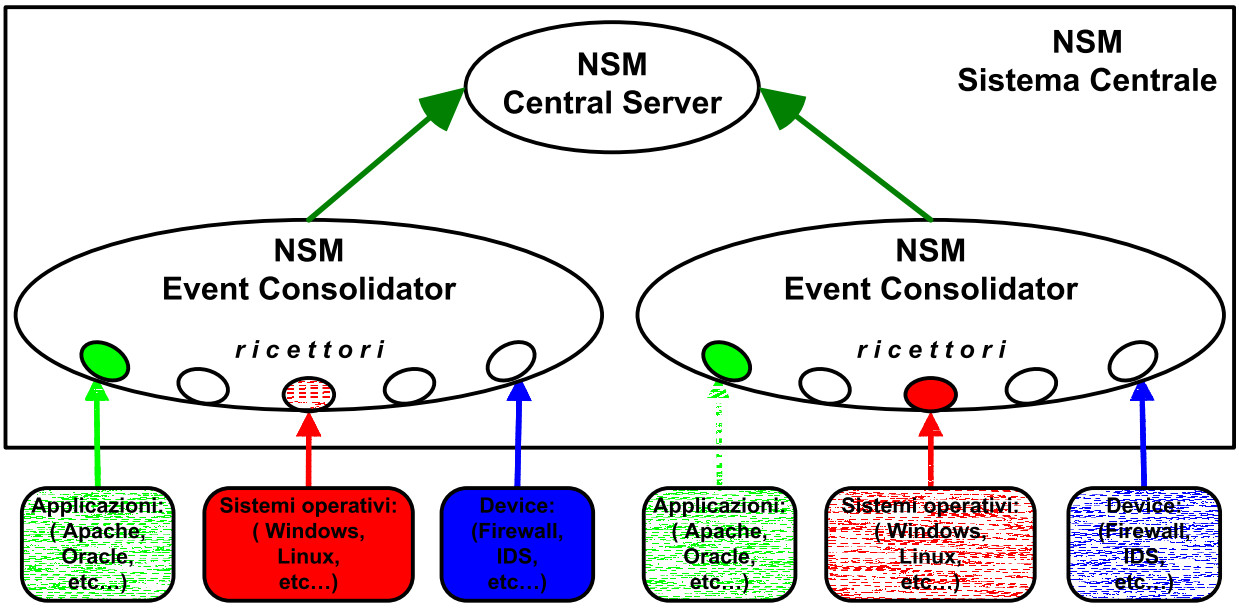


**Figura 4 - Architettura distirbuita**

[2] Si rimanda all'allegato Outsourcing.pdf per una descrizione dettagliata dell'offerta di Log Management gestito in outsourcing

# 2 Descrizione del progetto

## *2.1 Architettura*

L'architettura proposta per il sistema di Log Management è costituita da un Central Server, mostrato in Figura 5, che svolge le funzioni di:

- Centralizzazione dei log relativa
- Normalizzazione dei log
- Memorizzazione dei log (in formato raw e su database proprietario)
- Reportistica tramite interfaccia Web
- Allarmistica e correlazione degli eventi
- Gestione dell'Incident handling

Il Central Server non necessita di alcun software di terze parti, in quanto essendo una soluzione embedded, prevede un sistema operativo hardenizzato, un database proprietario per la memorizzare dei log e un interfaccia web per la generazione dei report.

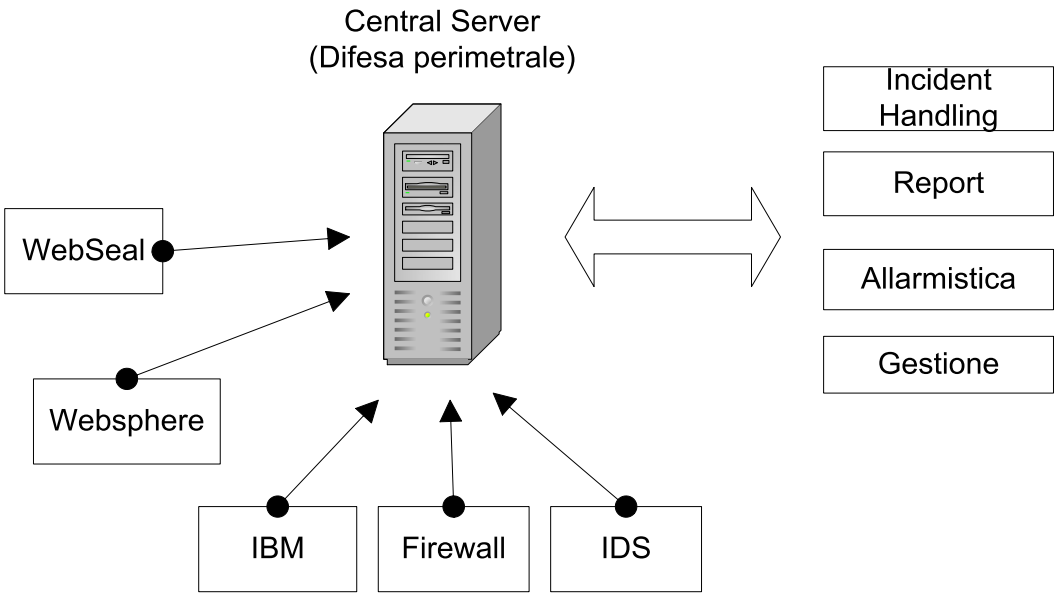


**Figura 5 - Architettura soluzione Log Management**

L'architettura proposta è stata studiata sulla base dei log prodotti giornalmente e sintetizzati in Tabella 1. Nel effettuare il calcolo si è stimato che un evento occupi mediamente 100 Byte.

| Sistemi / Applicativi | Log giornalieri | Eventi |
|---|---|---|
| Difesa Perimetrale (Polo di Torino FW+IDS) | 665 MB/giorno | 78 E/secondo |
| Difesa Perimetrale (Polo di Milano + Firenze) | 500 MB/giorno | 60 E/secondo |
| WebSeal | 990 MB/giorno | 117 E/secondo |
| Websphere | 240 MB/giorno | 29 E/secondo |
| IBM Mainframe | 3.827.000 record/giorno | 44 E/secondo |

**Tabella 1 - Stima dei log prodotti**

Il fattore critico di un progetto di log management risiede nell'integrazione delle varie componenti all'interno della soluzione adottata. Il problema può essere suddiviso nei seguenti due scenari differenti:

1. La componente *è nativamente* supportata dal sistema di log management
2. La componente *non è nativamente* supportata dal sistema di log management

Per questa ragione nei prossimi paragrafi sarà studiata, caso per caso, l'integrazione dell'ambiente di riferimento descritto al punto 1.3.

### 2.1.1 Componente nativamente supportato

In questo caso, essendo già disponibile un normalizzatore in grado d'interpretare i log dell'applicazione/sistema, l'integrazione dovrà tenere in considerazione se l'evento[3] d'interesse è costituito da uno o più log dell'applicazione stessa. Possiamo quindi identificare due casi:

- L'evento d'interesse corrisponde a un *singolo log* dell'applicazione
- L'evento d'interesse corrisponde a *due o più log* dell'applicazione

Nel primo caso l'integrazione non richiede un particolare sforzo, mentre nel secondo caso è necessario identificare la sequenza di log che caratterizzano l'evento d'interesse e quindi la definizione di una opportuna regola di correlazione.

### 2.1.2 Componente non nativamente supportata

In caso di applicazioni e/o sistemi non supportati nativamente è necessario distinguere tra:

1. applicazioni in grado di memorizzare i propri log nel sistema di logging del S.O. (Windows, Linux, SUN, etc…)
2. applicazioni dotate di un proprio sistema di logging

[3] I singoli log di un dispositivo supportato sono normalizzati e registrati dal prodotto, ma in generale potremmo essere interessati a identificare, nonché registrare, uno specifico evento composta da più log.

Il primo caso può essere ricondotto alle "applicazioni nativamente supportate", poiché la soluzione di log management prevede normalizzatori per i principali sistemi operativi. Il tempo d'integrazione è quindi funzione del numero di eventi che si intendono monitorare.
Il secondo caso richiede invece uno studio approfondito dell'applicazione e la costruzione di un normalizzatore ad hoc. Nel caso il sistema di logging proprietario dell'applicazione non supporti l'invio dei log tramite protocolli come SNMP, SYSLOG, SMTP, FTP o Database[4] si renderà necessaria anche la realizzazione di un agente in grado di trasferire i log dall'applicazione al sistema centrale.

### *2.2 Integrazione dei sistemi Firewall*

Sia i firewall Checkpoint, sia i firewall Cisco PIX risultano essere tra i dispositivi ufficialmente supportati, quindi non esiste la necessità di sviluppare agenti specifici.

### *2.3 Integrazione dei sistemi IDS*

Il sistema di Intrusion Detection Snort è ufficialmente supportato dal prodotto, quindi non esiste la necessità di sviluppare un agente specifico.

### *2.4 Integrazione dei log del modulo WebSeal*

L'applicazione non risulta essere ufficialmente supportata quindi sarà necessario sviluppare un ricettore per tale applicativo. Nel dettaglio i file di log:

1. AZN.LOG: file relativo ai login di sistema
2. REQUEST.LOG: file relativo alle risorse richieste all'access manager
3. REFER.LOG: file relativo alla manipolazione delle richieste
4. AGENT.LOG: file relativo ai client chiamanti

dovranno essere trasferiti al central server per poi essere elaborati dal ricettore. Per garantire la riservatezza della comunicazione sarà opportuno adottare un file transfer sicuro (SCP) che preveda l'utilizzo della crittografia.

### *2.5 Integrazione dei log di Websphere*

L'applicazione non risulta essere ufficialmente supportata quindi sarà necessario sviluppare un ricettore per tale applicativo. Nel dettaglio i file di log:

1. L1: log in formato testo relativi all'interfaccia di front-end (informazioni di sessione)
2. L2: log in formato testo relativi all'interfaccia di back-end (informazioni sulle transazioni)

[4] Il sistema è in grado di esportare i log qualora questi siano memorizzati in un DB oracle, sql, mysql.

dovranno essere trasferiti al central server per poi essere elaborati dal ricettore. Per garantire la riservatezza della comunicazione sarà opportuno adottare un file transfer sicuro (SCP) che preveda l'utilizzo della crittografia.

### *2.6 Integrazione dei log MainFrame*

L'applicazione non risulta essere ufficialmente supportata quindi sarà necessario sviluppare un ricettore per tale applicativo. Nel dettaglio i log SMF:

1. SMF tipo 30 (Process Accounting and Availability data)
2. SMF tipo 80 (RACF processing information)
3. SMF tipo 110 (CICS/ESA statistics)
4. SMF tipo 120 (Component Broker performance statistics)

dovranno essere trasferiti al central server per poi essere elaborati dal ricettore. Per garantire la riservatezza della comunicazione sarà opportuno adottare un file transfer sicuro (SCP) che preveda l'utilizzo della crittografia. I log specifici ai tipi sopraelencati dovranno quindi essere esportati in un uno o più file tramite uno script specifico, per mezzo ad esempio dell'utiliy REGEXX.

# 3 Pianificazione attività

## *3.1 Struttura delle attività (WBS)*

La soluzione di Log Management sarà inserita nell'ambiente di Fondiaria SAI in tre fasi successive:

- **Valutazione:** in questa fase sarà valutata la soluzione proposta
- **Fase Pilota:** in questa fase sarà collegata al sistema l'infrastruttura di difesa perimetrale (Firewall + IDS) e alcune tipologie di log di applicativi
- **Fase Operativa:** in questa fase sarà completata l'integrazione della componenti applicative

Alla fine di consentire a Fondiaria SAI di valutare l'efficacia della soluzione di Log Management descritta nel paragrafo 1.3, verrà effettuata una installazione di prova del sistema (**Valutazione**). La macchina messa a disposizione da Fondiaria SAI, verrà predisposta da HackingTeam per integrare i log provenienti dai seguenti sistemi:

- 1 Firewall Checkpoint
- 1 Sistema IDS Snort
- Una tipologia di log relativa al file AZN.LOG prodotto da Web Seal (Esempio: login fallite)

Attraverso un'opportuna configurazione, sarà configurato il database degli asset critici per Fondiaria SAI, allo scopo di consentire l'identificazione degli eventi di particolare interesse per il business aziendale.

In Figura 3Figura 6 sono mostrate le attività che costituiscono la fase pilota del progetto di Log Management, durante la quale saranno integrati i sistemi di difesa perimetrale mostrati in Figura 1 e Figura 2:

- Firewall Checkpoint
- Cisco PIX
- IDS Snort
- Log relativi al file AZN.LOG (WebSeal)
- Log di tipo L2 relativi all'applicazione WebSphere
- Log di tipo 30 relativi al IBM ManiFrame

La criticità di questa fase è assicurarsi che il sistema di Log Management riceva e interpreti correttamente le informazioni provenienti dai dispositivi sopra citati, distinguendo opportunamente gli eventi relativi agli asset critici, rispetto a quelli non critici.

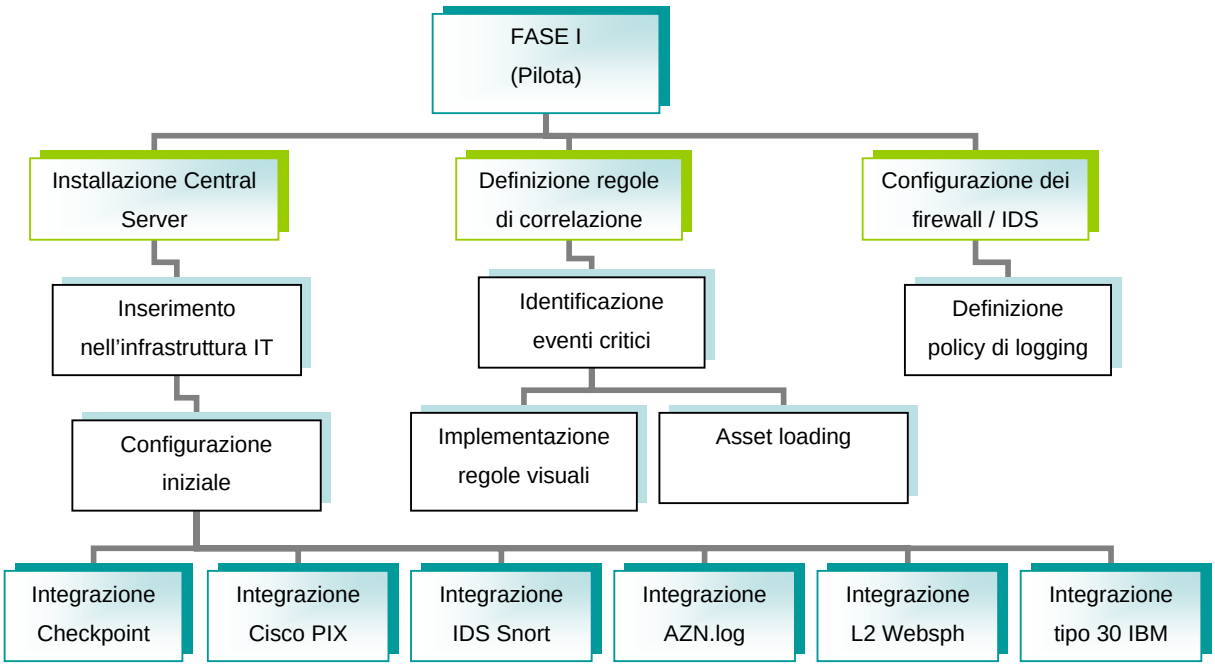


**Figura 6 - Attività Fase 1 (Pilota)**

La fase 2, schematizzata in Figura 7, integrerà i restanti sistemi d'interesse presenti nell'infrastruttura di Fondiaria SAI:

- Modulo WebSeal di Tivoli access manager (livello di autenticazione)
- Websphere Application Server
- IBM MainFrame

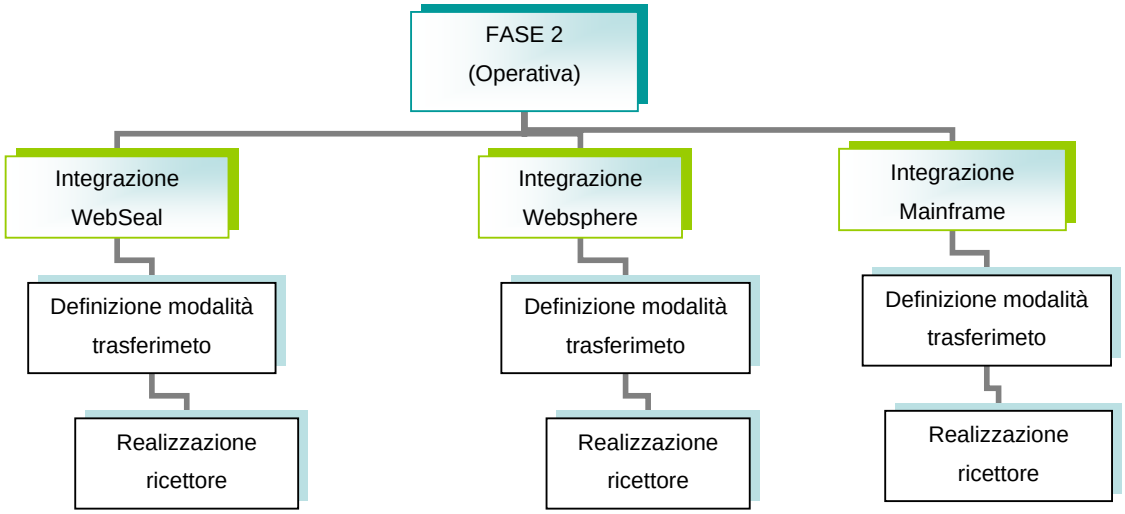


**Figura 7 - Attivita Fase 2 (Operativa)**

## *3.2 Fase Pilota*

In Tabella 2 sono riportate le attività legate alla fase pilota insieme a una breve descrizione.

| Attività | Descrizione |
|---|---|
| Installazione Server | Installazione software e configurazione di sistema |
| Definizione degli asset | Inserimento dei dati relativi agli asset aziendali: nome dei sistemi, locazione fisica, criticità, etc… |
| Definizione policy di logging | Attivazione delle policy di auditing sui firewall e sul sistema IDS. Configurazione e invio dei log al central server |
| Integrazione dei sistemi FW CheckPoint | Predisposizione del sistema per ricevere i log dai firewall checkpoint |
| Integrazione dei sistemi FW Cisco PIX | Predisposizione del sistema per ricevere i log dai firewall PIX |
| Integrazione dei sistemi IDS Snort | Predisposizione del sistema per ricevere i log dai sistemi di intrusion detection Snort |
| Integrazione dei log AZN.log | Creazione del ricettore per interpretare i log degli accessi relativi al modulo WebSeal |
| Integrazione dei log L2 | Creazione del ricettore per interpretare i log delle transazioni relative al software Websphere |
| Integrazione degli SMF 30 | Creazione del ricettore per interpretare i log relativi ai record di tipo 30 dei MainFrame IBM |
| Definizione regole di correlazione | Configurazione delle regole di correlazione legate all'identificazioni degli eventi d'interesse |
| Definizione regole di storing | Definizione degli eventi da memorizzare nel database rispetto a log in formato raw |
| Definizione report | Costruzione di eventuali report in base ad esigenze specifiche |

| | |
|---|---|
| Testing e rilascio infrastruttura | Verifica del corretto funzionamento del sistema |

**Tabella 2 - Attività Fase Pilota**

## *3.3 Fase Operativa*

In Tabella 3 sono riportate le attività legate alla fase operativa insieme a una breve descrizione.

| Attività | Descrizione |
|---|---|
| Definizione metodologia di trasferimento dei log | Realizzazione del sistema di trasferimento dei log vesro il central server |
| Integrazione dei sistemi WebSeal | Integrazione dei restatni log generati da WebSeal (costruzione ricettore) |
| Integrazione di WebSphere | Integrazione dei restanti log generati da WebSphere (costruzione ricettore) |
| Integrazione dei MainFrame | Integrazione dei restanti log generati dal MainFrame (costruzione ricettore) |
| Integrazione degli asset | Inserimento dei dati relativi agli asset aziendali coinvolti nella seconda fase. |
| Definizione regole di correlazione | Configurazione delle regole di correlazione legate all'identificazioni degli eventi d'interesse |
| Definizione regole di storing | Definizione degli eventi da memorizzare nel database rispetto a log in formato raw |
| Definizione report | Costruzione di eventuali report in base ad esigenze specifiche |
| Testing e rilascio infrastruttura | Verifica del corretto funzionamento del sistema e rilascio dell'infrastruttura |

**Tabella 3 - Attività Fase operativa**

## *3.4 Gestione dei rischi*

Le criticità di un progetto di Log Management sono dovute alla corretta integrazione delle componenti nel sistema stesso. Possiamo perciò identificare come fattori di rischio tutti gli imprevisti che potrebbero compromettere, inficiare o influire in termini temporali sul raggiungimento degli obiettivi:

- **Non corretto funzionamento dei ricettori:** questo rischio comporta la registrazione non corretta del log interessato, imputabile a un aggiornamento o cambiamento delle versioni del S.O. o dell'applicativo d'interesse. Tipicamente questo rischio non compromette la riuscita del progetto, poiché la soluzione di Log Management consente la costruzione o la modifica di un ricettore. E' pero plausibile un allungamento dei tempi a causa della necessità di apportare le opportune modifiche al sistema di Log Management.

- **Incapacità di logging:** questo rischio è legato all'incapacità da parte della componente di registrare le informazioni necessarie per individuare gl'eventi d'interesse. Questo problema deve essere evitato durante lo studio di fattibilità del progetto, verificando che tutte le informazioni che caratterizzano un dato evento siano presenti nei log del sistema e/o dell'applicazione.

# 4 Varianti di progetto

Eventuali variazioni al progetto dovranno essere discusse e approvate dal personale autorizzato. Questo richiede l'identificazione di un responsabile interno di Fondiaria SAI, che risulterà essere il referente per eventuali variazioni di progetto. Ogni variante al progetto dovrà quindi essere approvata sia dal referente della parte committente, sia dal responsabile del progetto che HackingTeam identificherà durante la creazione del gruppo di lavoro.

# 5 Accettazione e rilascio infrastruttura

Al termine delle due fasi verranno effettuati dei collaudi allo scopo di certificare il corretto funzionamento dell'infrastruttura di Log Management. I piani relativi ai test di validazione del sistema saranno proposti da Hacking Team a Fondiaria SAI, la quale individuerà all'interno della propria organizzazione le persone che presidieranno la fase di testing, ossia incaricate dell'autorità necessaria a garantire l'accettazione del progetto.

Alla conclusione dei test seguirà il rilascio dell'infrastruttura, che potrà avvenire secondo due modalità:

- **Affiancamento:** in questa modalità il servizio di Log Management diventerà a tutti gli effetti un servizio interno di Fondiaria SAI. In questo caso, Hacking Team provvederà a fornire un opportuno periodo di affiancamento (training interno) del personale che avrà in gestione l'infrastruttura di Log Management.
- **Outsourcing:** in questa modalità il servizio di Log Management diventerà a tutti gli effetti un servizio esterno fornito da Hacking Team a Fondiari SAI[5]. Nel caso di outsourcing saranno definiti opportuni livelli di servizio (SLA) sulla base delle necessità del cliente.

In caso si scelga la soluzione in outsourcing l'architettura relativa al progetto assumerà una struttura distribuita, simile a quella mostrata in Figura 4. Il Central Server installato presso il cliente diventerà di fatto un Event Collector, in grado di svolgere le medesime funzioni, ma al tempo stesso sarà gestito a livello di policy da un Central Server presente nell'infrastruttura di Hacking Team.

[5] Si rimanda all'allegato Outsourcing-LM.pdf per i dettagli relativi all'offerta di outsourcing

# 6 Condizioni economiche

Il listino prezzi di NSM, a differenza di molti suoi concorrenti, è indipendente dal numero di device dai quali raccoglie i log e dipende esclusivamente dal numero di server AF o DA che per necessità di scalabilità si vogliono installare. Nella versione 5.x non è più necessario acquistare la licenza del database in quanto già presente nel modulo centrale. Il costo dei vari moduli è il seguente:

- NSM – AF: Advanced Function è il cuore dell'architettura di NSM. E' in grado di acquisire dati dai device fino a oltre 20.000 eventi al secondo. In architetture complesse è il modulo che raccoglie le informazioni dai Data Acquisition Server e che può generare le regole da distribuire agli altri componenti. Il costo a listino è di € 55.000.
- NSM – DA: Data Acquisition è il componente che, in presenza di architetture complesse e scalabili viene specializzato nella raccolta di log specifici per area geografica o per funzione. Ogni DA può gestire oltre 20.000 eventi al secondo. Il costo a listino è di € 25.000.
- NSM – AA: Advanced Analytics supporta una più rapida investigazione e un'analisi più approfondita degli eventi con l'utilizzo di un ambiente OLAP che consente anche di prendere decisioni tattiche e strategiche per migliorare il grado di sicurezza dell'organizzazione. Il costo a listino è di € 36.000.
- Remote Console: E' l'interfaccia per l'amministratore e per chi inserisce le regole nel sistema. Il costo a listino è di € 2.800.
- Fail–Over Licence: Il costo della licenza di Fail-Over ha un costo del 50% della primaria.

La manutenzione può essere erogata in due modalità:

- Standard Maintenance (software upgrades and Support 8x5 North American Time Zone): 15% all'anno dal primo anno
- Enhanced Maintenance: (software upgrades and Support 24x7 per level 1 severity): 22% all'anno dal primo anno