

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
<i>Via della Moscova, 13 20121 MILANO (MI) - Italy</i>	info@hackingteam.it
<i>Tel. +39.02.29060603</i>	<i>Fax +39.02.63118946</i>

STORIA DEL DOCUMENTO		
Versione	Data	Modifiche Effettuate
1.0	15 Dicembre 2004	Emissione
//	//	//
//	//	//

INFORMAZIONI		
Data di Emissione	15 Dicembre 2004	
Versione	1.0	
Tipologia Documento	Allegato Tecnico	
Numero di Protocollo	//	
Numero Pagine	18	
Numero Allegati	0	
Descrizione Allegati	1	//
	2	//
Redatto da	Aldo Scaccabarozzi	
Approvato da	Gianluca Vadruccio	

INDICE

1	Introduzione	5
1.1	Obiettivi	5
1.2	Ambiente di riferimento.....	5
1.3	Soluzione	7
2	Descrizione del progetto	9
2.1	Architettura	9
2.1.1	Componente nativamente supportato	10
2.1.2	Componente non nativamente supportata	11
2.2	Integrazione dei sistemi Firewall.....	11
2.3	Integrazione dei sistemi IDS	11
2.4	Integrazione dei log del modulo WebSeal.....	11
3	Pianificazione attività	13
3.1	Struttura delle attività (WBS)	13
3.2	Fase Pilota	15
3.3	Fase di Produzione.....	16
3.4	Gestione dei rischi.....	16
3.5	Varianti di progetto	17
4	Accettazione e rilascio infrastruttura	18

INDICE DELLE FIGURE

Figura 1 - Accesso Internet (Torino).....	6
Figura 2 - Rete Trust e di Accesso (Torino).....	6
Figura 3 – Sistema centrale (NSM AF).....	7
Figura 4 - Architettura distribuita	8
Figura 5 - Architettura soluzione Log Management	9
Figura 6 – Attività Fase Pilota	14
Figura 7 – Attività Fase di Produzione.....	15

INDICE DELLE TABELLE

Tabella 1 - Stima dei log prodotti.....	10
Tabella 2 - Attività Fase Pilota.....	15
Tabella 3 – Attività Fase di Produzione	16

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 informatica. 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'obiettivo del cliente è focalizzato all'integrazione di:

- N. 1 (uno) firewall Checkpoint
- N. 1 (uno) firewall PIX (che consolida i log nella stessa management Checkpoint del firewall precedentemente citato)
- N. 2 (due) sensori SNORT attivi sulla stessa sonda
- N. 1 (uno) Modulo WebSeal di Tivoli access manager, attraverso l'analisi di tre tipologie di log: azn.log, request.log e refer.log.

Considerando che, una volta integrata la management di Checkpoint per i firewall sopra elencati qualunque altro modulo firewall afferente ad essa sarebbe automaticamente normalizzato, la soluzione potrà essere adottata per i seguenti device di firewalling presenti dal cliente (a patto che ovviamente siano tutti agganciati alla stessa Management Checkpoint):

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 prossima 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 prossima 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 prossima migrazione a NG)
 - 1 sonda SNORT attestata all'esterno dei 2 FW

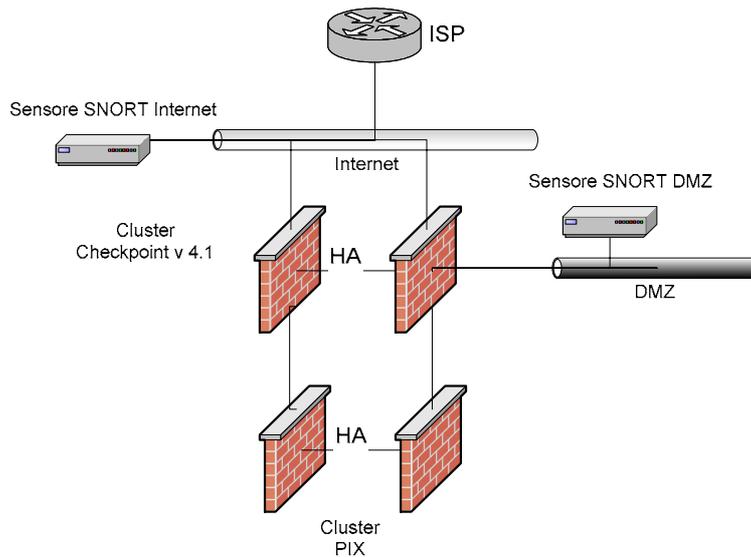


Figura 1 - Accesso Internet (Torino)

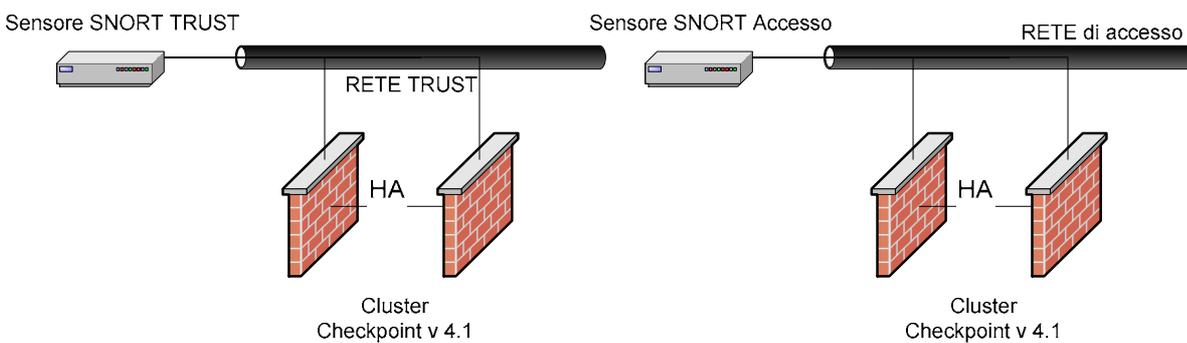


Figura 2 - Rete Trust e di Accesso (Torino)

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 (NSM¹), 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, AF (Advanced Function), 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.

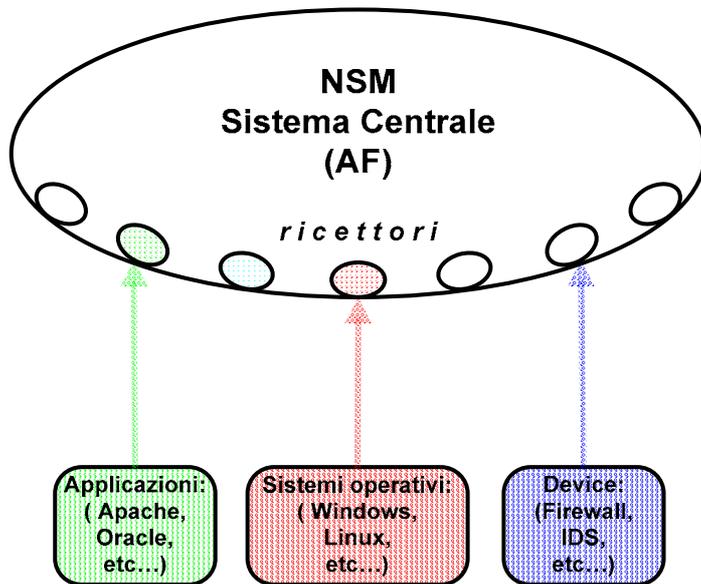


Figura 3 – Sistema centrale (NSM AF)

¹ Per una descrizione precisa della soluzione tecnica si rimanda al whitepaper relativo al Log Management: Whitepaper-LM.pdf, consegnato al cliente precedentemente.

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

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, potrebbe consentire di distribuire il carico di lavoro della componente centrale AF su più unità (DA – Data Acquisition), 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. 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).

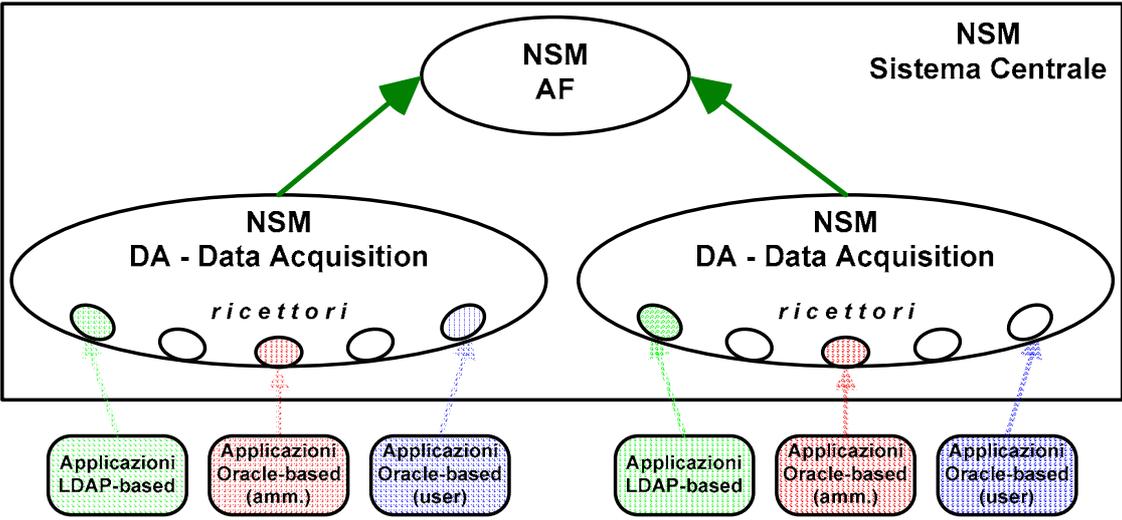


Figura 4 - Architettura distribuita

2 Descrizione del progetto

2.1 Architettura

L'architettura proposta per il sistema di Log Management è costituita da un server centrale NSM AF, 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 modulo AF 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.

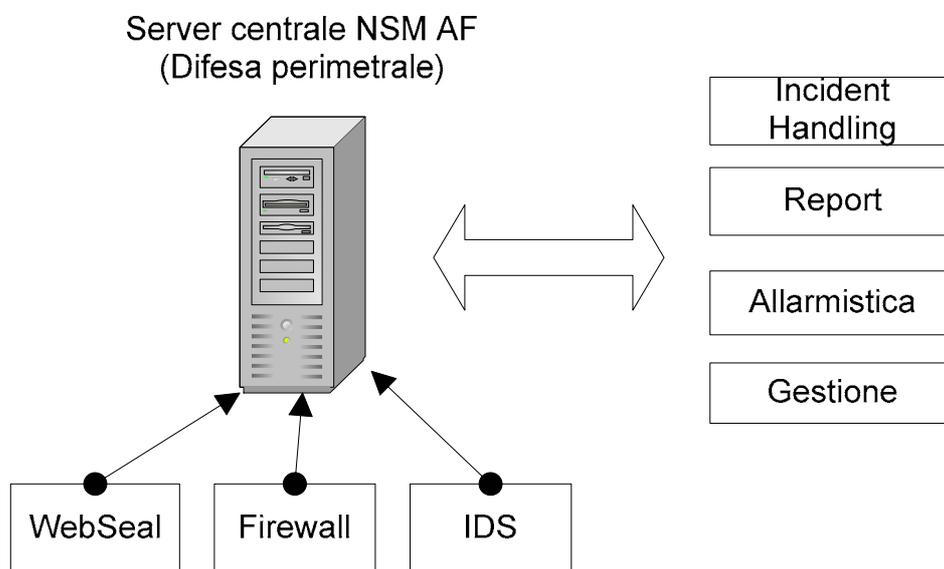


Figura 5 - Architettura soluzione Log Management

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
TOTALE	2.155 MB/giorno	255 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'evento² 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

² I singoli log di un dispositivo supportato sono normalizzati e registrati dal prodotto, ma in generale si potrebbe essere interessati ad identificare, nonché registrare, uno specifico evento composto da più log.

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

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 Database³ 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 Il sistema è in grado di esportare i log qualora questi siano memorizzati in un DB oracle, sql, mysql.

3. REFER.LOG: file relativo alla manipolazione delle richieste

dovranno essere trasferiti alla componente AF centrale 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.

3 Pianificazione attività

3.1 Struttura delle attività (WBS)

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

- **Fase Pilota:** in questa fase sarà collegata al sistema l'infrastruttura di difesa perimetrale (Firewall + IDS) e alcune tipologie di log di applicativi (fase già eseguita)
- **Fase di Produzione:** in questa fase sarà completato e messo in produzione l'intero sistema di log management, corredato di tutte le regole di correlazione e le personalizzazioni necessarie.

Alla fine di consentire a Fondiaria SAI di valutare l'efficacia della soluzione di Log Management descritta nel paragrafo 1.3, è stata effettuata una installazione di prova del sistema (**Fase Pilota**).

La macchina messa a disposizione da Fondiaria SAI, è stata predisposta da Hacking Team per integrare i log provenienti dai seguenti sistemi:

- Firewall Checkpoint
- Cisco PIX
- IDS Snort
- Log relativi al file AZN.LOG (WebSeal)

Attraverso una opportuna operazione, è stato configurato il database degli asset critici per Fondiaria SAI, allo scopo di consentire l'identificazione degli eventi di particolare interesse per il business aziendale.

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

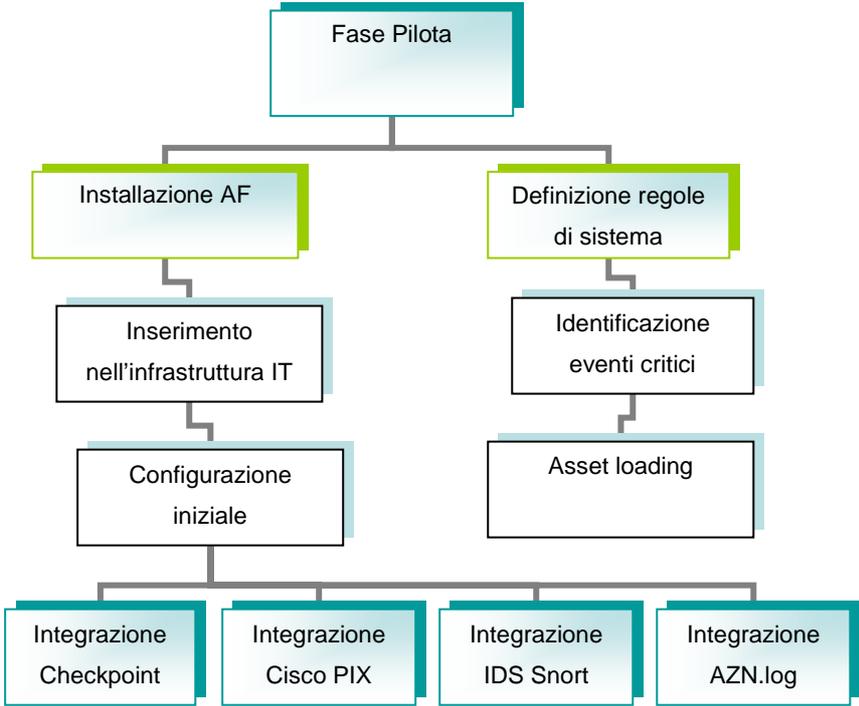


Figura 6 – Attività Fase Pilota

La fase 2 (**Fase di Produzione**), schematizzata in Figura 7, permetterà di:

- installare la componente AF di produzione
- integrare le componenti firewall, snort e webseal
- personalizzare l'intero sistema

coprendo quindi tutti i sistemi d'interesse presenti nell'infrastruttura di Fondiaria SAI

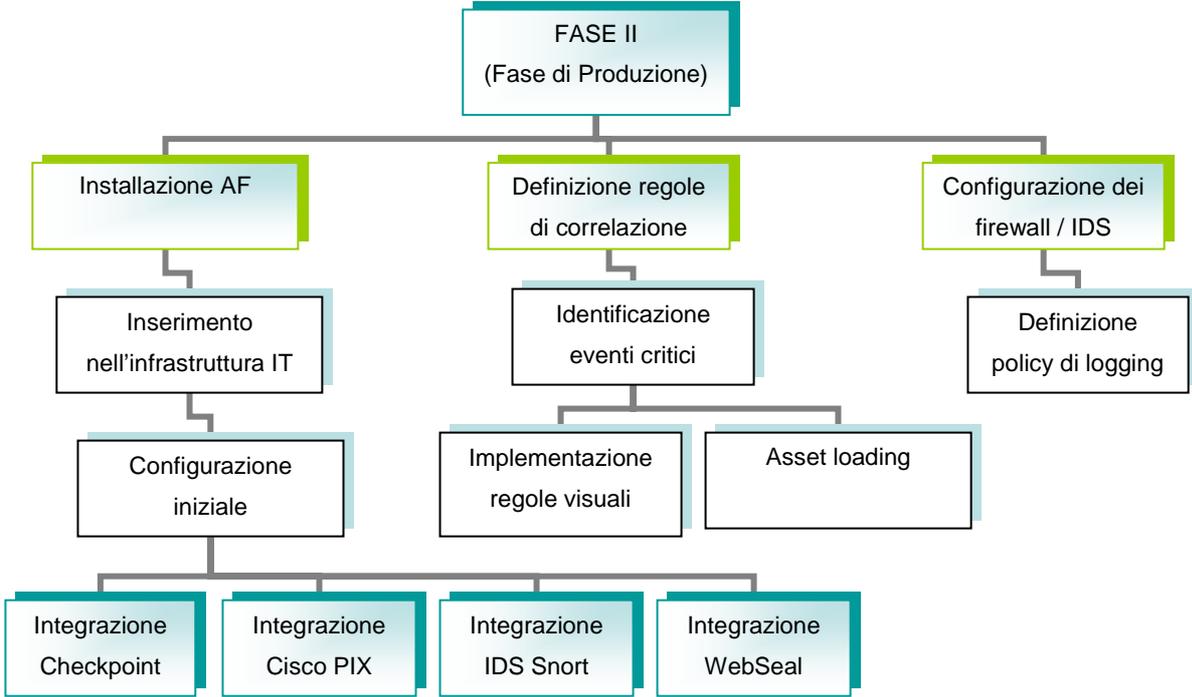


Figura 7 – Attività Fase di Produzione

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...
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

Tabella 2 - Attività Fase Pilota

3.3 Fase di Produzione

In Tabella 3 sono riportate le attività legate alla fase operativa 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
Definizione metodologia di trasferimento dei log	Realizzazione del sistema di trasferimento dei log verso il sistema NSM AF
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 Cisco PIX
Integrazione dei sistemi IDS Snort	Predisposizione del sistema per ricevere i log dai sistemi di intrusion detection Snort
Integrazione dei log WebSeal	Creazione del ricettore per interpretare i log degli accessi relativi al modulo WebSeal
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 di Produzione

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' però 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 gli 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.

3.5 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 Hacking Team identificherà durante la creazione del gruppo di lavoro.

4 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 presiederanno la fase di testing, ossia incaricate dell'autorità necessaria a garantire l'accettazione del progetto.

Alla conclusione dei test seguirà il rilascio dell'infrastruttura e, se richiesto, un periodo di affiancamento durante il quale l'infrastruttura 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.