]HackingTeam[

SIA

# SIA

# 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 | 29 Giugno 2005 | Emissione |
| // | // | // |
| // | // | // |

| INFORMAZIONI | | |
|---|---|---|
| Data di Emissione | 29 Giugno 2005 | |
| Versione | 1.0 | |
| Tipologia Documento | Allegato Tecnico | |
| Numero di Protocollo | // | |
| Numero Pagine | 19 | |
| Numero Allegati | 0 | |
| Descrizione Allegati | 1 | // |
| | 2 | // |
| 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'obiettivo del cliente è focalizzato all'integrazione di:

- AAA active directory (3) e RAS (Juniper) (3)
- Console AntiVirus TrendMicro (11)
- Firewall StoneGate e CheckPoint Firewall-1 (5)
- Sonda IDS NFR o Snort (1)
- HoneyPot (2)
- Gestione presenze (accesso fisico) (1)

Obiettivo del progetto di Log Management è raccogliere i log provenienti dai sistemi sopra citati, al fine di consentire:

- La centralizzazione dei log dell'infrastruttura di difesa perimetrale (Firewall e IDS)
- 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, AF (Advanced Function o Security Manager), come mostrato in Figura 1. Per ogni dispositivo, applicazione o sistema esiste uno specifico ricettore in grado di normalizzare i dati contenuti nei log ricevuti.

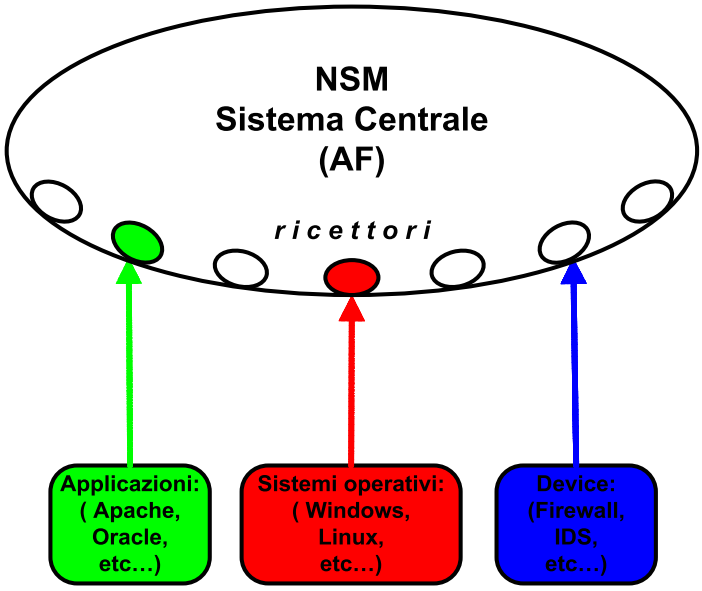


**Figura 1 – Sistema centrale (NSM AF)**

Le operazioni svolte dal sistema centrale sono:

- Raccolta dei 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

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

- 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 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).

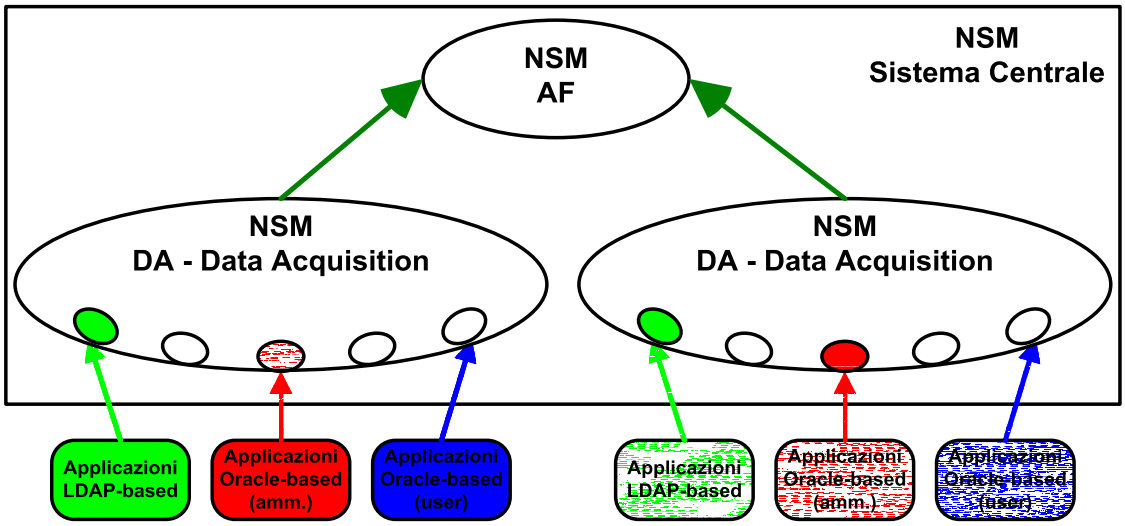


**Figura 2 - Architettura distribuita**

# 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 3, che svolge le funzioni di:

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

e di 2 (due) moduli DA che svolgono le funzioni di:

- Raccolta dei log
- Normalizzazione dei log

I moduli AF e DA necessitano esclusivamente della licenza Linux Red Hat Enterprise; dispongono nativamente di un database proprietario per la memorizzare dei log e di un'interfaccia web per la generazione dei report.

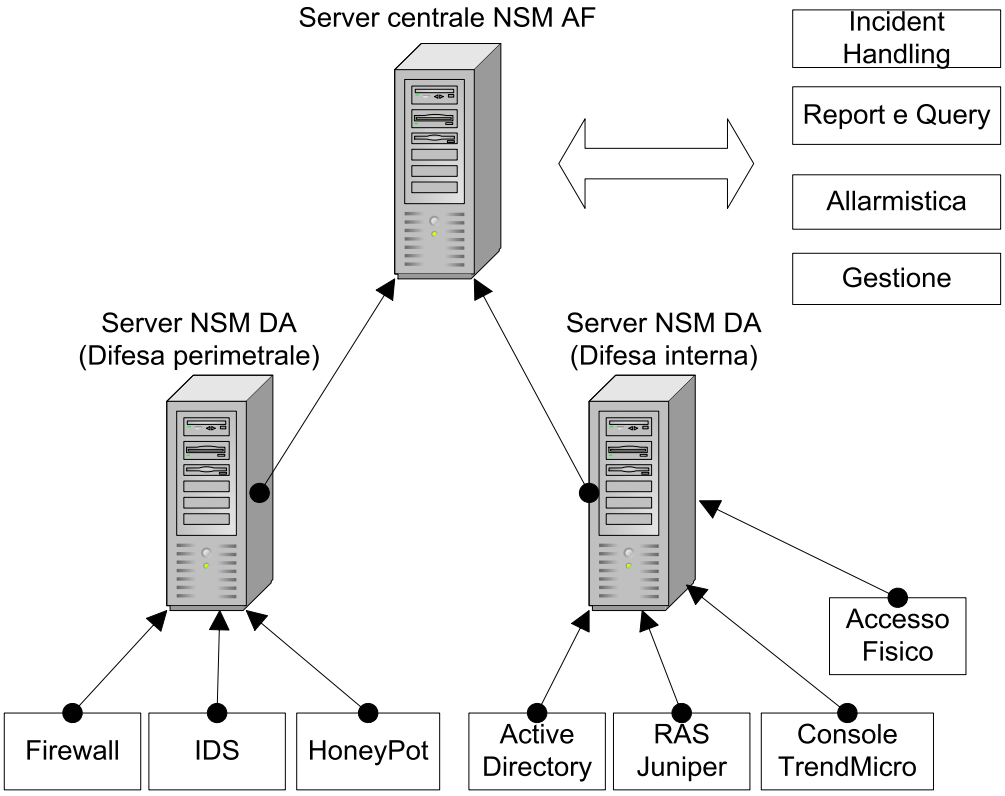


**Figura 3 - Architettura soluzione Log Management**

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[2] 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 supportato

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 Database[3] 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*

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

[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.

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

Il firewall StoneGate non risulta essere ufficialmente supportato e quindi sarà necessario sviluppare un ricettore per tale applicativo. Si suppone che tale sorgente di log sia comunque in grado di spedire i propri log in un formato standard come syslog o snmp.

### *2.3 Integrazione dei sistemi IDS*

I sistemi di Intrusion Detection sia di Snort che di NFR risultano ufficialmente supportati dal prodotto, quindi non esiste per entrambi la necessità di sviluppare un agente specifico.

### *2.4 Integrazione del sistema HoneyPot*

Nessun sistema HoneyPot risulta essere ufficialmente supportato e quindi sarà necessario sviluppare un ricettore per tale applicativo. Si suppone che tale sorgente di log sia comunque in grado di spedire i propri log in un formato standard come syslog o snmp.

### *2.5 Integrazione dei log del modulo AAA*

La directory Microsoft Active Directory è ufficialmente supportata dal prodotto, quindi non esiste la necessità di sviluppare un agente specifico.

Il sistema RAS di Juniper non risulta essere ufficialmente supportato e quindi sarà necessario sviluppare un ricettore per tale applicativo. Si suppone che tale sorgente di log sia comunque in grado di spedire i propri log in un formato standard come syslog o snmp.

## *2.6 Integrazione dei log del sistema antivirus*

La console del sistama Antivirus di TrendMicro è ufficialmente supportata dal prodotto, quindi non esiste la necessità di sviluppare un agente specifico.

## *2.7 Integrazione dei log del sistema di rilevamento e gestione presenze*

Nessun sistema di gestione e rilevamento delle presenze (accesso fisico) risulta essere ufficialmente supportato e quindi sarà necessario sviluppare un ricettore per tale applicativo. Si suppone che tale sorgente di log sia comunque in grado di spedire i propri log in un formato standard come syslog o snmp.

# 3 Pianificazione attività

## *3.1 Struttura delle attività (WBS)*

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

- **Fase Pilota:** in questa fase sarà collegata al sistema l'infrastruttura di difesa perimetrale (Firewall + IDS + HoneyPot) con i relativi normalizzatori
- **Fase di completamento:** in questa fase saranno collegate le sorgenti di log rimanenti e sviluppati gli opportuni normalizzatori
- **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.

Attraverso un'opportuna operazione, si potrà configurare il database degli asset critici per SIA, allo scopo di consentire l'identificazione degli eventi di particolare interesse per il business aziendale.
La criticità di questa fase consiste nell'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.

La fase 1 (**Fase Pilota**), schematizzata in Figura 4, permetterà di:

- installare la componente AF
- installare la componente DA riguardante la difesa perimetrale
- centralizzare e normalizzare le sorgenti di log perimetrali: firewall, ids e honeypot (almeno una sorgente per tipologia)
- configurare la parte di base del sistema

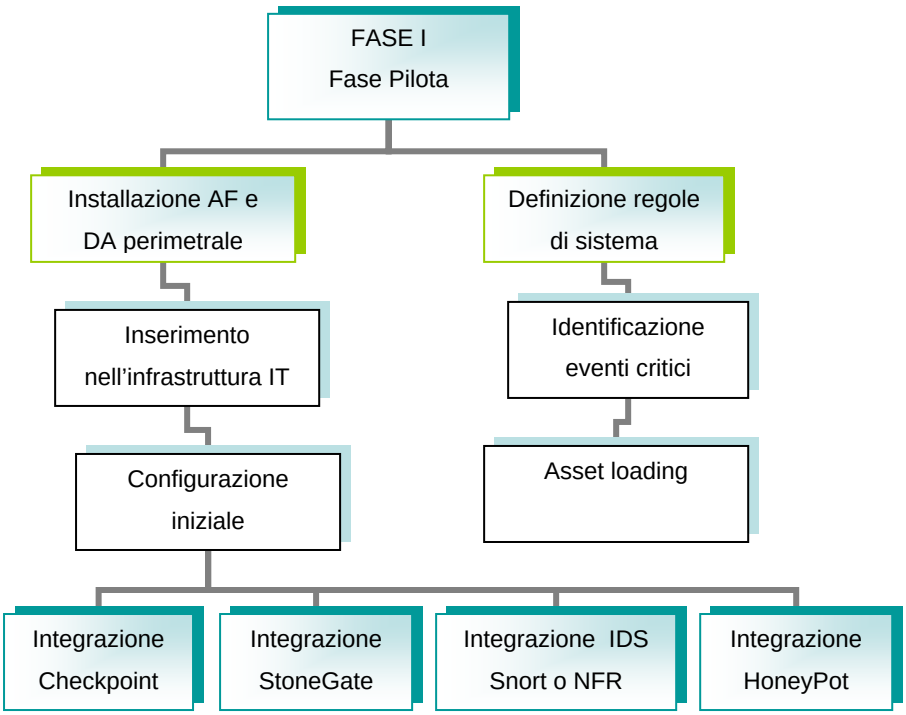


**Figura 4 – Attività Fase Pilota**

La fase 2 (**Fase di Completamento**), schematizzata in Figura 5, permetterà di:

- installare la componente DA riguardante la difesa interna
- centralizzare e normalizzare le sorgenti di log interni: Active Directory, RAS Juniper, Console TrendMicro ed il sistema di gestione presenze dell'accesso fisico (almeno una sorgente per tipologia)
- configurare la parte di base del sistema

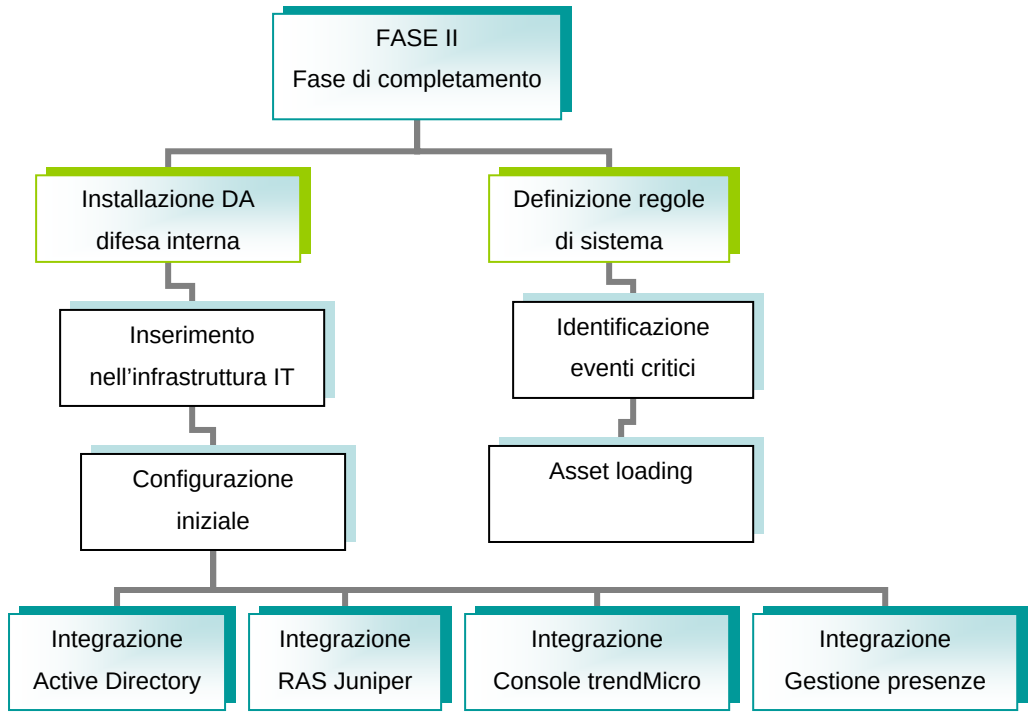


**Figura 5 – Attività Fase di Completamento**

La fase 3 (**Fase di Produzione**), schematizzata in Figura 6, permetterà di:

- configurare l'AF e i due DA opportunamente
- integrare e completare le sorgenti di log rimaste, relativamente alle tipologie elencate nelle due fasi precedenti
- personalizzare l'intero sistema secondo i requisiti richiesti e stabiliti nella fase di progettazione iniziale
- esecuzione dei test e fase di collaudo (consegna del progetto)

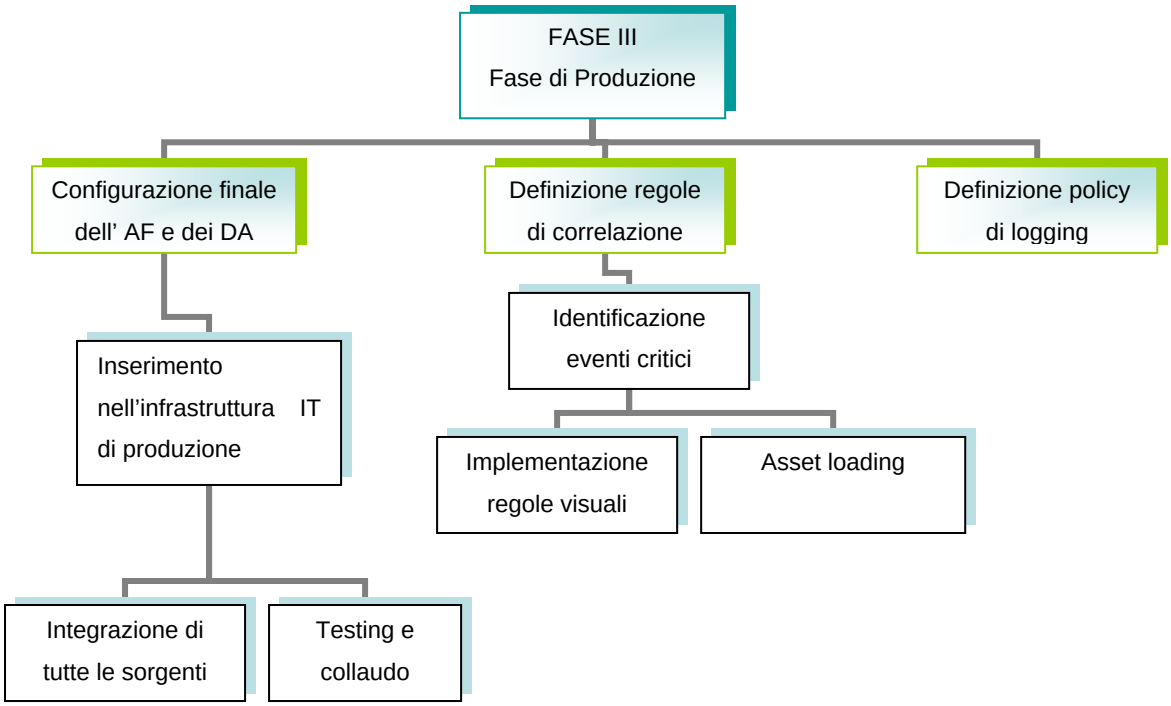


**Figura 6 – Attività Fase di Produzione**

## *3.2 Fase Pilota*

In Tabella 1 sono riportate le attività legate alla fase pilota insieme a una breve descrizione.

| ATTIVITA' FASE I – Fase Pilota | |
|---|---|
| **Attività** | **Descrizione** |
| Installazione Server AF e del DA perimetrale | Installazione software e configurazione di sistema |
| Definizione degli asset | Inserimento dei dati relativi agli asset aziendali: nome dei sistemi, locazione fisica, criticità, etc… |
| Integrazione del sistema FW CheckPoint | Predisposizione del sistema per ricevere i log dai firewall Checkpoint |
| Integrazione del sistema FW StoneGate | Predisposizione del sistema per ricevere i log dai firewall StoneGate mediante la creazione del ricettore atto all'interpretazione |
| Integrazione dei sistemi IDS | Predisposizione del sistema per ricevere i log dai sistemi di intrusion detection Snort oppure da quelli di NFR |

| | |
|---|---|
| Integrazione dei log del sistema HoneyPot | Creazione del ricettore per interpretare i log di sicurezza relativi al sistema HoneyPot |

**Tabella 1 - Attività Fase Pilota**

## *3.3 Fase di Completamento*

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

| ATTIVITA' FASE II – Fase di Completamento | |
|---|---|
| **Attività** | **Descrizione** |
| Configurazione Server AF e installazione del DA interno | Installazione software e configurazione di sistema |
| Definizione degli asset | Inserimento dei dati relativi agli asset aziendali: nome dei sistemi, locazione fisica, criticità, etc… |
| Integrazione della directory di Microsoft | Predisposizione del sistema per ricevere i log da Active Directory |
| Integrazione del sistema RAS di Juniper | Predisposizione del sistema per ricevere i log dal RAS di Juniper mediante la creazione del ricettore atto all'interpretazione |
| Integrazione del sistema Antivirus | Predisposizione del sistema per ricevere i log dalla console TrendMicro |
| Integrazione dei log del sistema di gestione presenze | Creazione del ricettore per interpretare i log di sicurezza relativi al sistema di rilevamento presenze (accesso fisico) |

**Tabella 2 - Attività Fase di Completamento**

## *3.4 Fase di Produzione*

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

| ATTIVITA' FASE II – Fase di Produzione | |
|---|---|
| **Attività** | **Descrizione** |
| Configurazione AF e DA | Configurazione e tuning di sistema per la produzione |
| 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 |
| Definizione metodologia di trasferimento dei log | Realizzazione del sistema di trasferimento dei log verso il sistema NSM AF |
| Integrazione delle sorgenti | Completamento della centralizzazione di tutte le sorgenti rimaste (relative alle tipologie di log elencate ed integrate nelle fasi I e II) |
| Integrazione degli asset | Inserimento dei dati relativi agli asset aziendali coinvolti. |

| | |
|---|---|
| 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 (COLLAUDO) | Verifica del corretto funzionamento del sistema e rilascio dell'infrastruttura |

**Tabella 3 – Attività Fase di Produzione**

## *3.5 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.

## *3.6 Varianti di progetto*

Eventuali variazioni al progetto dovranno essere discusse e approvate dal personale autorizzato. Questo richiede l'identificazione di un responsabile interno di SIA, 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 tre 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 SIA (durante la fase di progettazione iniziale), 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 e, se richiesto e commercialmente approvato, un periodo di affiancamento durante il quale l'infrastruttura di Log Management diventerà a tutti gli effetti un servizio interno di SIA.

In questo caso, Hacking Team provvederà a fornire

1. un corso avanzato sul sistema e la tecnologia implementati
2. un periodo di affiancamento (training interno) del personale che avrà in gestione l'infrastruttura di Log Management