ADVANCTION

SECURITY RISK MANAGEMENT

# Security Log management

## Guida alla gestione dei log di sicurezza

SECURITY LOG MANAGEMENT

# Guida alla gestione dei log di sicurezza

**Versione 1.0**

ADVANCTION

**Giugno 2008**



**Svizzera - Italia**

# Indice dei contenuti

**1 Introduzione**
Tipologie di log ....4
Software di sicurezza ....5
Sistemi operativi ....5
Applicazioni ....5
La necessità di un Log Management ....6
Le sfide del Log Management ....6
Generazione e memorizzazione dei log ....6
Protezione dei log ....7
Analisi dei log ....7
Una gestione dei log efficace ....8

**2 L'infrastruttura di Log Management**
Architettura ....9
Le funzioni ....10
Funzioni generali ....11
Storage ....11
Analisi ....12
Eliminazione ....12

**3 Pianificazione del Log Management**
Definire ruoli e responsabilità ....13
Stabilire policy adeguate ....14
Generazione dei log ....14
Trasmissione dei log ....14
Archiviazione dei log e cancellazione ....14
Analisi dei log ....15
Problematiche legali relative al Log Management ....16
Stabilire policy attuabili ....17
Progettare un'infrastruttura di Log Management ....18

**4 I Processi operativi del Log Management**
Configurazione delle sorgenti di log ....19
Generazione dei log ....19
Archiviazione e smaltimento dei log ....20
Sicurezza dei log ....21
Analizzare i dati di log ....22
Comprendere i log ....22
Assegnare la priorità corretta alle entry ....23
Confrontare analisi a livello di sistema e di infrastruttura ....23
Rispondere agli eventi identificati ....24
Gestire lo storage a lungo termine ....25
Altri supporti operativi ....26
Test e convalida ....26

# 1 Introduzione

Un log è una registrazione di eventi avvenuti all'interno di sistemi e reti di un'organizzazione. I log sono composti da righe o *entry*: ogni entry contiene informazioni relative a uno specifico evento accaduto all'interno di un sistema.
Originariamente, i log venivano usati principalmente nella risoluzione dei problemi, ma negli ultimi anni sono sempre più utilizzati per svariate funzioni, come ad esempio l'ottimizzazione dei sistemi e delle performance di rete, la registrazione delle attività utente e per avere informazioni preziose per investigare attività malversatorie.
I log si sono evoluti per contenere informazioni reative a diversi tipi di eventi e, in molte organizzazioni, molti log contengono record relativi alla sicurezza: alcuni esempi di questo sono gli audit log, che tracciano l'autenticazione degli utenti, e i log dei device di sicurezza, che registrano possibii attacchi.
A causa della sempre più diffusa presenza di server e stazioni di lavoro interconnessi, e della sempre crescente quantità di minacce contro le reti e i sistemi, il numero, il volume e la varietà dei log di sicurezza è aumentato notevolmente. Questo ha creato la necessità della gestione dei log (*Log Management*), ovvero il processo di generare, trasmettere, archiviare, analizzare e, infine, eliminare i log dei sistemi.

## Tipologie di log

I log generati dai sistemi possono essere ascrivibili alle seguenti categorie:
- Log di sicurezza, contenenti informazioni relative ala sicurezza dei sistemi
- Log dei sistemi operativi
- Log applicativi
- Le due ultime tipologie di log contengono diverse informazioni tra cui anche informazioni relative alla sicurezza.
- Molti dei log creati all'interno di un'organizzazione possono avere rilevanza anche per la sicurezza: ad esempio, i log di device di rete, come router e switch, e di programmi di Network Monitoring possono contenere informazioni rilevanti per operazioni di audit e di incident management.

Questi log sono generalmente utilizzati dalla sicurezza al momento del bisogno come fonte supplementare di informazioni.

Ogni organizzazione deve considerare il valore di ogni potenziale fonte di log nella fase di progettazione di un'infrastruttura di Log Management.

Alcune delle sorgenti di log generano eventi in modo continuativo, altre invece girano periodicamente e possono generare log in modalità batch, spesso a intervalli regolari.

## Software di sicurezza

Molte aziende utilizzano diversi tipi di software di sicurezza per le reti e i sistemi allo scopo di individuare attività malversatorie, proteggere sistemi e dati e supportare le analisi a seguito di incidenti.
I seguenti tipi di software di sicurezza sono tra le sorgenti principali di log:

- Software Antimalware
- Software di accesso remoto
- Web Proxy
- Software di vulnerability management
- Authentication Servers
- Router
- Firewall
- Sistemi di Network Access Control

## Sistemi operativi

I sistemi operativi di host, server, stazioni di lavoro e device di rete normalmente registrano varie informazioni relative alla sicurezza. I dati più comuni sono:

- Eventi di sistema. Gli eventi di sistema sono azioni operative svolte dalle componenti del SO, come ad esempio la chiusura di un sistema o il lancio di un servizio. Normalmente vengono registrati gli eventi non andati a buon fine e molti di quelli che hanno avuto successo; molti sistemi operativi consentono di scegliere quali tipologie di log registrare.
- Record di audit. Questi record contengono informazioni sugli eventi di sicurezza, come ad esempio i tentativi di autenticazione andati a buon fine o falliti, l'accesso ai file, il cambio di policy di sicurezza, i cambi di account, ecc. Anche in questo caso molti SO permettono di scegliere e parametrizzare i dati da registrare

## Applicazioni

Alcune applicazioni generano i propri file di log, altre utilizzano le caratteristiche di log del sistema operativo che le ospita.
Le applicazioni variano sensibilmente nel tipo di informazioni registrate. In questa lista sono elencati i tipi di informazioni più comunemente presenti nei log:

- **Richieste del client e risposte dal server**, molto utili nella ricostruzione di sequenze di eventi.
- **Informazioni sull'account**, come ad esempio tentativi di autenticazione falliti o di successo, modifiche agli account (creazione, cancellazione, assegnazione dei privilegi, ecc), e utilizzo dei privilegi. Ma anche identificazione di eventi di sicurezza come i tentativi di indovinare una password con un attacco a forza bruta e l'escalation dei privilegi.
- **Informazioni sull'utilizzo**: ad esempio il numero di transazioni in un determinato periodo e la dimensione delle transazioni. Queste informazioni possono essere utili per alcune forme di monitoraggio di sicurezza.
- **Azioni operative significative**, come il lancio di un'applicazione, i problemi, le modifiche alle applicazioni. Questi elementi possono essere utilizzati per identificare problemi operativi e compromissioni alla sicurezza.

Molte di queste informazioni possono essere registrate da applicazioni, fattore che rende il loro log particolarmente prezioso per attività di auditing, di analisi di incidenti, di compliance relative alle applicazioni.
Questi log sono spesso in formati proprietari che li rendono più difficili da utilizzare e i dati ivi contenuti sono spesso dipendenti dal contesto, fattore che rende necessarie più risorse per la loro interpretazione.

## La necessità di un Log Management

Sono molti i benefici che un'azienda può ottenere da un'accurata attività di gestione dei log:

- maggiore garanzia che informazioni di sicurezza siano archiviate con sufficiente dettaglio per un priodo di tempo adeguato;
- revisioni e analisi di routine dei log permettono di identificare incidenti di sicurezza, violazioni di policy, attività fraudolente e problemi operativi dopo pochi istanti dall'accadimento, e offrono inoltre informazioni preziose per risolvere i problemi;
- i log possono essere inoltre utili per svolgere analisi di audit e forensi, supportando le investigazioni interne e identificando tendenze operative e problemi di lungo termine.

## Le sfide del Log Management

Molte aziende affrontano problematiche di gestione dei log simili tra loro eche hanno soprattutto lo stesso problema di fondo: bilanciare la quantità limitata di risorse dione dei log con un sempre crescente numero di dati di log.

### Generazione e memorizzazione dei log

In ogni azienda, la maggior parte dei sistemi operativi, dei software di sicurezza e delle varie applicazioni genera log. Questo rende complessa la loro gestione per i seguenti motivi:

- **molteplici sorgenti di log:** i log sono localizzati su vari sistemi e pertanto necessitano una gestione dispersa per tutta l'azienda. Inoltre, una singole fonte di log può generare molti log;
- **contenuto dei log inconsistente**: ogni fonte di log registra le informazioni che ritiene più importanti, rendendo difficoltoso collegare eventi registrati da diverse sorgenti di log perché potrebbero non avere nessun valore in comune (ad esempio, la fonte di log 1 registra lo username ma non l'IP, mentre a fonte di log 2 effettua l'operazione inversa).
  Inoltre, ogni fonte di log può presentare valori in modo diverso, come ad esempio la data, oppure la definizione di un protocolo.
- **Orari non consistenti**. Ogni sistema che genera log utilizza il suo clock per assegnare un orario all'evento; se quindi l'orologio del sistema non è accurato anche il timestamp dell'evento non lo sarà, rendendo l'analisi dei log più difficoltosa , particolarmente quando si dovranno analizzare log provenienti da più sistemi.

- **Formati di log non consistenti**. Molte sorgenti di log utilizzano i formati più disparati per i loro log, come ad esempio file di testo con campi separati da virgole o tab, database, syslog, SNMP, XML e file binari. Alcuni log sono scritti per essere leggibili dall'uomo, altri no. Alcuni sono scritti in un formato standard, atri in un formato proprietario.

Per facilitare l'analisi dei log, le aziende devono implementare metodi automatici per convertire log con diversi contenuto e formato in un formato standardizzato con una rappresentazione dei campi dati consistente.
Poiché molti sistemi registrano alcune informazioni di log per la sicurezza, spesso con molti log per host, il numero di log in ogni azienda può essere piuttosto alto: molti log registrano grandi voumi di dati su base giornaliera, cosicché il volume quotidiano totale dei dati di log di un'azienda può essere notevole.

## Protezione dei log

Dal momento che i log contengono registrazioni per la sicurezza di sistemi e reti, la loro protezione da violazioni di confidenzialità o integrità è un punto fondamentale.
Questi elementi richiedono di affrontare problematiche di sicurezza e privacy che vedono coinvolti sia i dipendenti che visionano i log sia coloro che possono essere in grado di accedere ai log con modi autorizzati o meno.
I log non adeguatamente protetti nello storage o durante la trasmissione possono essere suscettibili di alterazioni o distruzioni più o meno intenzionali: questo fattore può permettere di nascondere l'identità di un attaccante mediante la manipolazione di evidenze o che attività malversatorie possano passare inosservate.

Le aziende hanno anche la necessità di proteggere la disponibilità dei propri log: molti log hanno una dimensione massima (che riguarda ad esempio il numero di eventi o la dimensione del file): quando la dimensione viene raggiunta può accadere che i vecchi dati vengano sovrascritti o che il processo di log non scriva più nulla.
Per rispondere alle necessità di retention dei dati, le aziende devono mantenere copie dei log per un periodo più lungo di quello supportato dalla fonte di log, e quindi stabilire un processo di archiviazione.
A causa del volume dei log, potrebbe essere appropriato ridurre i log filtrando gli eventi che non è necessario archiviare.
È infine necessario proteggere la confidenzialità e l'integrità dei log archiviati.

## Analisi dei log

In molte aziende, sono stati gli amministratori di rete o di sistema ad avere la responsabilità dell'analisi dei log, processo che è stato sempre considerato di bassa priorità se paragonato con altri compiti che richiedono tempi di risposta immediati, come la gestione di problemi operatiivi o la risoluzione di vulnerabilità di sicurezza.
L'analisi dei log spesso è svolta poco efficientemente e senza particolari training, e senza neppure adeguati strumenti che automatizzino il processo di analisi. Molti di questi strumenti sono particolarmente importanti per l'individuazione di pattern che a un operatore umano potrebbero sfuggire, come la correlazione di entry da log multipli relative al medesimo evento.
L'analisi dei log è spesso considerata come un compito da svolgere successivamente all'individuazione di un problema, e non in modo proattivo, per individuare attività in

corso e identificare segnali di problemi imminenti. Molti log non vengono quindi analizzati in tempo reale.

## Una gestione dei log efficace

Un'organizzazione può adottare alcune procedure per implementare una gestione dei log efficace:

- **Assegnare la giusta priorità al Log Management**. È opportuno definire le specifiche e gli obiettivi per il monitoraggio dei log, tenendo in considerazione anche normative, necessità di auditing e policy organizzative. È opportuno assegnare una priorità agli obiettivi prendendo in considerazione anche il beneficio della riduzione del rischio.
- **Stabilire policy e procedure per il Log Management**. Policy e procedure consentono di avere un approccio consistente per tutta l'organizzazione e assicurano che le richieste normative siano soddisfatte. Gli audit periodici, i test e la validazione sono modi per confermare che standard e linee guida del monitoraggio dei log siano seguite.
- **Creare e mantenere un'infrastruttura di Log Management sicura**. È necessario implementare le componenti di un'infrastruttura di Log Management e determinare come queste componenti interagiscono tra loro. Questo contribuisce a preservare l'integrità dei dati di log da modifiche o cancellazioni accidentali o intenzionali, nonchè a mantenere la confidenzialità dei dati di log. È altresì critico creare un'infrastruttura abbastanza robusta per gestire non solo i volumi di dati attesi, ma anche per far fronte ai picchi in situazioni estreme.
- **Offrire un supporto adeguato allo staff con responsabilità definite per il Log Management.** Una volta definito lo schema di gestione dei log, è necessario fornire un training adeguato allo staff circa le sue competenze di Log Management. Il supporto comprende anche gli strumenti per il Log Management, direttive tecniche sull'attività e la disseminazione delle informazioni all'interno.

# 2

# L'infrastruttura di Log Management

L'infrastruttura di Log Management è composta dall'hardware, dal software e dalle reti utilizzate per generare, trasmettere, archiviare, analizzare ed eliminare i dati di log.

## Architettura

Un'infrastruttura di Log Management è composta normalmente dai seguenti tre livelli:

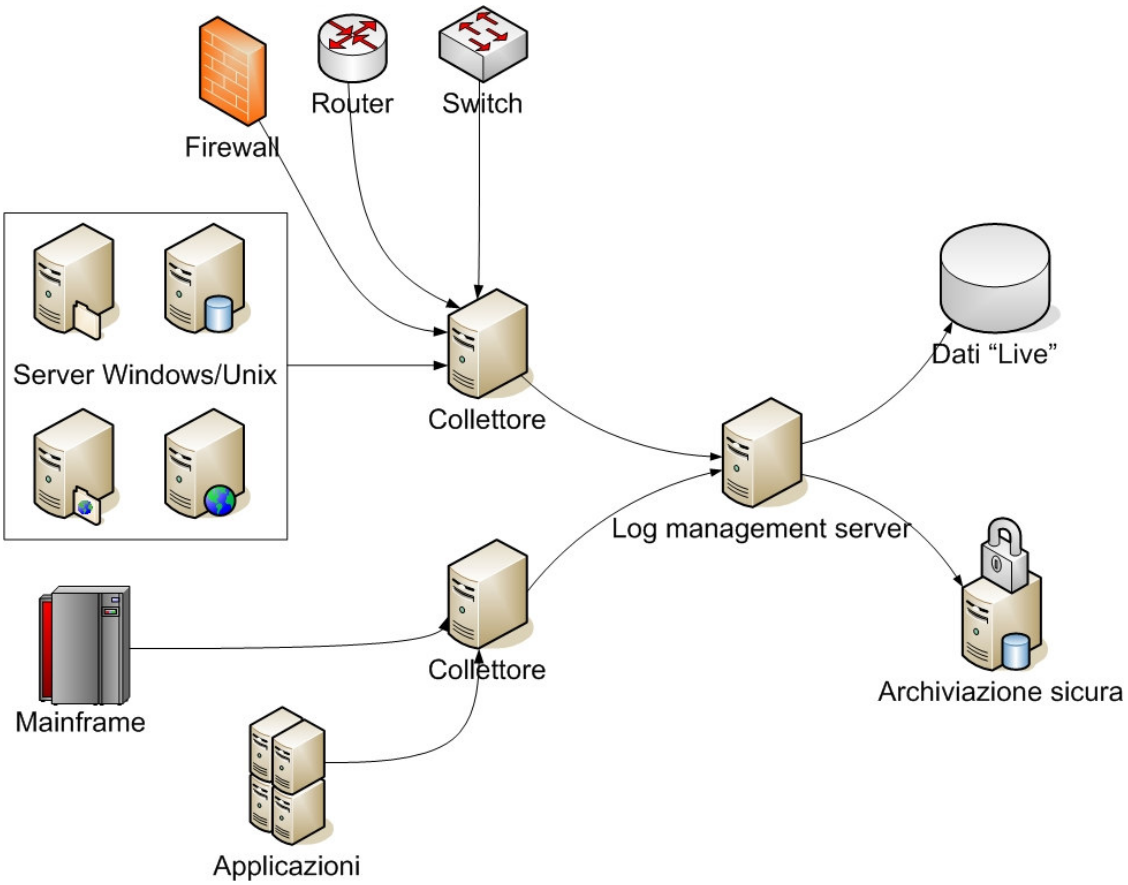
- **Generazione dei log**. Il primo livello contiene l'host che genera i dati di log. Alcune tipologie di sistemi rendono disponibili, attraverso la rete, i propri log ai log server nel secondo livello. Altri li rendono disponibli attraverso delle copie dei log stessi.
- **Analisi dei Log e Storage**. Il secondo livello si compone di uno o più server di log che ricevono i dati di log dai sistemi del primo ivello. I dati vengono trasferiti ai server sia in tempo reale che periodicamente. I server che ricevono i dati di log dalle sorgenti sono chiamati collettori o aggregatori. I dati di log possono essere archiviati sui log server o su database separati.
- **Monitoraggio dei Log**. Il terzo livello compnrende le console che possono essere utilizzate per monitorare, visionare i dati di log, nonché i risultati delle analisi automatiche. Le console di monitoraggio possono essere anche utilizzate per generare reports e per gestire i log server e gli agenti. Infine, i privilegi di accesso alle console possono essere limitati solo alle funzioni necessarie e alle necessarie sorgenti di log.

Il secondo livello (Analisi dei log e storage) può variare sensibilmente in complessità e struttura: l'installazione più semplice è composta da un singolo server di log che gestisce le funzioni di analisi e storage. Dipendentemente dalla complessità della struttura da monitorare, il secondo livello può essere configurato come segue:

- Log server multipli, dove ognuno svolge una funzione specializzata. Ad esempio, un log server si occupa del collezionamento, dell'analisi e dello storage a breve termine, e un altro server svolge funzioni di storage a lungo termine
- Log server multipli dove ognuno svolge analisi e/o storage per generatori di log di un certo tipo, depositando i dati in una locazione condivisa.
  In entrambi i primi due casi casi può essere opportuno provvedere alla ridondanza dei log server.
- Due livelli di log server, in cui il primo è costituito da server distribuiti in grado di ricevere log dalle sorgenti e inoltrare alcuni o tutti i dati di log a un secondo livello di server centralizzati. (si possono aggiungere livelli uteriori per rendere questo tipo di architettura più flessibile, scalabile e ridondata). In alcuni casi, i server di primo ivello possono agire da cache server, in grado di ricevere log dai generatori e inoltrarli ad altri log server. Un'architettura di questo tipo può essere implementata anche per proteggere il secondo livello di log server da attacchi diretti oppure quando sussistono delle criticità di rete tra le sorgenti di log e il secondo livello di log server.

La comunicazione tra i componenti di un'infrastruttura di Log Management avviene attraverso la rete aziendale. Questo tipo di comunicazione può essere protetto utilizzando la criptografia.

All'interno di un'azienda potrebbe essere necessaria una sola infrastruttura di Log Management per tutta l'azienda, ma nelle grandi imprese tale infrastruttura potrebbe raggiungere una dimensione tale da rendere il progetto non affrontabile. Per questo motivo, le grandi aziende si dotano di più infrastrutture di Log Management, ognuna delle quali caratterizzata da un ambito ben definito, che può essere relativo alla struttura interna, alle tipologie di sistemi o di log, o ancora alla locazione degli uffici.




**Schema di architettura standard di un'infrastruttura di Log Management**

## Le funzioni

Un'infrastruttura di Log management svolge normalmente diverse funzioni che assistono nell'archiviazione, nell'analisi e nell'eliminazione dei dati. Queste funzioni sono svolte in modo che i log originali non vengano alterati.

Le funzioni di un'infrastruttura di Log Management sono:

## Funzioni generali

- **Il Log Parsing** è l'estrazione di dati da un log in modo che i valori estratti possano essere utilizzati da un altro processo di logging. Il parsing può essere una componente di altre funzioni di log, come la conversione o la visualizzazione di log
- **Il filtraggio di eventi** consiste nell'eliminazione dall'analisi, dal reporting e dallo storage di lungo termine di entry del log che non contengono informazioni di interesse. Ad esempio, entry duplicate o contenenti informazioni standard potrebbero essere filtrate poiché non forniscono informazioni utili all'analisi.
- **L'aggregazione degli eventi** permette di consolidare entry simili tra loro in una sola entry contenente il numero delle occorrenze dell'eventi. L'aggregazione può essere svolta sia dal generatore dei log oppure può essere una componente dei processi di riduzione o di correlazione.

## Storage

- Per **rotazione dei log** si intende la chiusura di un file di log e l'apertura di un nuovo file quando il primo file viene considerato completo. Normalmente la rotazione viene effettuata periodicamente o quando il log raggiunge una determinata dimensione. Tra i benefici più importanti della rotazione vi sono la preservazione delle log entry e il mantenimento dei file di log in una dimensione gestibile. Quando un file di log viene ruotato, il file precedente può essere compresso per risparmiare spazio.
- **L'archiviazione dei log** è il mantenimento dei log per un periodo di tempo esteso, per scopi normativi o di compliance alle policy interne. Esistono due tipi di archiviazione: retention e preservazione. Il primo è un'archiviazione regolare come parte delle attività operative standard. Il secondo è invece il mantenimento di log che normalmente verrebbero scartati, perché contengono informazioni su attività di particolare interesse. La *Log preservation* viene effettuata come supporto per investigazioni o gestione degli incidenti.
- **La compressione dei log** è l'archiviazione di un file in modo da ridurne lo spazio, ma senza alterarne il contenuto.
- **La Log Reduction** è un'attività di rimozione di entry non necessarie da un log per creare un log più piccolo. È simile alla event reduction, che rimuove campi dati non necessari dalle log entry. Il processo di riduzione viene spesso svolto insieme all'archiviazione, in modo che solo le entry e i campi dati di interesse siano inseriti nello storage di lungo termine.
- **La Log Conversion** è l'estrazione di informazioni da un log e l'inserimento delle sue entry in un log in un secondo formato. Ad esempio, la conversione può estrarre i dati da un database e salvarli in formato XML in un file di testo.
- Nella **normalizzazione dei log**, ogni campo dati del log viene convertito, secondo una particolare rappresentazione dei dati, e categorizzato. Uno degli usi più comuni della normalizzazione è la memorizzazione della data in un formato singolo: ad esempio, una fonte di log può scrivere la data dell'evento in notazione anglosassone (2:34:56 P.M. EDT) e chiamarla Timestamp, mentre un'altra fonte potrebbe scriverla nel formato europeo (con le 24 ore) e denominarla Event Time. La normalizzazione dei dati rende l'analisi e la reportistica più semplice quando vengono utilizzati più formati di log.

- **Il controllo di integrità** dei file di log avviene calcolando un *message digest* per ogni file e archiviando il digest in modo sicuro per assicurare che venga individuata qualsiasi modifica ai file di log archiviati. Gli algoritmi di calcolo di message digest più utilizzati sono MD5 e SHA-1. Nel caso il log file sia stato alterato, non ci sarà corrispondenza con il message digest originale.

### Analisi

- **La correlazione di eventi** permette di individuare relazioni tra due o più log entry. La forma più comune di correlazione (o *event correlation*) è basata su regole che permettono di collegare più log entry da una fonte singola o da più sorgenti, basandosi su valori presenti nei log, come il timestamp, l'indirizzo IP, il tipo di evento, ecc. La correlazione può anche essere effettuata in altri modi, utilizzando quindi metodi statistici o strumenti di visualizzazione.
- **La visualizzazione** permette di visionare le entry dei log in un formato leggibile.
- **La reportistica** permette di visualizzare il risultato delle analisi, ma anche di riassumere attività significative in un determinato periodo di tempo o anche per estrarre informazioni dettagliate su un particolare evento o serie di eventi.

### Eliminazione

- **La cancellazione dei log** consiste nella rimozione di entry da un log prima di una certa data. È un'attività svolta per rimuovere vecchi log non più necessari perché di nessuna importanza o perché sono stati archiviati.

# 3 Pianificazione del Log Management

Per implementare e mantenere con successo un'infrastruttura di Log Management, è necessario pianificare attentamente e svolgere varie attività preparatorie, in modo da creare procedure consistenti, affidabili ed efficienti di Log Management che vadano incontro alle necessità aziendali e offrano un valore aggiunto all'organizzazione.

## Definire ruoli e responsabilità

All'interno della fase di pianificazione, un'organizzazione deve definire ruoli e responsabilità delle persone e dei gruppi che saranno coinvolti nella gestione dei log. Tra i ruoli individuali e di gruppo troviamo:

- **Amministratori di reti e sistemi**, che sono spesso responsabili della configurazione dei log sui sistemi e i device di rete, dell'analisi periodica dei log, della reportistica sulle attività di gestione dei log e delle attività di manutenzione ordinaria sui log.
- **Amministratori della sicurezza**, responsabili della gestione e del monitoraggio dell'infrastruttura di Log Management, responsabili della configurazione dei log sui device di sicurezza, della reportistica sul risultato delle attività di Log Management e del supporto per la configurazione dei log sui sistemi.
- **Computer security incident response team**, che utilizza i dati dei log nella gestione degli incidenti
- **Sviluppatori di applicazioni,** che possono progettare o adattare applicazioni già esistenti in modo da svolgere le operazioni di logging secondo i requirement e le raccomandazioni
- **Chief information officer (CIO)**, che supervisionano le risorse IT che generano, trasmettono e archiviano i log.
- **Auditor**, che possono usare i dati dei log nelle attività di audit

Dipendentemente dalla dimensione e dalla complessità dell'organizzazione, l'attività di Log Management può essere svolta in modo centralizzato, o decentrato e quindi dagli stessi amministratori di sistemi, rete e sicurezza, responsabili della gestione dei log sui loro sistemi, dello svolgimento di analisi regolari e dell'invio dei dati di log all'infrastruttura di Log Management.
Per fare in modo che il Log Management a livello di sistema venga svolto in modo efficace, è necessario fornire un adeguato supporto agli amministratori dei sistemi, attraverso le seguenti azioni:

- Disseminare informazioni e fornire training sul ruolo che i sistemi e i loro amministratori giocano all'interno dell'infrastruttura di Log Management
- Fornire dei punti di contatto che possano rispondere alle domande degli amministratori sul log
- Incoraggiare gli amministratori a condividere le proprie esperienze e offrire un meccanismo per disseminare le idee (ad es. mailing list, forum, workshop)

- Offrire una guida specifica per integrare i log di sistema con l'infrastruttura di Log Management (ad es. l'installazione di agenti o la configurazione di syslog)
- Fornire strumenti come script di rotazione dei log e software di analisi

## Stabilire policy adeguate

Un'azienda deve definire le necessità e obiettivi per il monitoraggio dei log: i requirement devono includere tutte le normative applicabili e le policy interne. Gli obiettivi devono essere basati su un adeguato bilanciamento tra la riduzione del rischio aziendale e il dispendio di tempo e di risorse da dedicare all'attività di Log Management. I requirement e gli obiettivi devono poi essere utilizzati come base per stabilire la consistenza del progetto di Log Management e assegnare adeguate priorità all'attività.

Le policy che un'azienda deve approntare includeranno:

### Generazione dei log

- Quali tipi di host devono avere un log
- Quali componenti di un host devono generare log (ad es. il sistema operativo, i servizi, le applicazioni)
- Di quali tipi di eventi si deve tener traccia (eventi di sicurezza, connessioni di rete, tentativi di autenticazione)
- Quali dati devono essere tracciati per ciascun tipo di evento (ad es. username, indirizzo IP sorgente, ecc)
- La frequenza di log di ogni tipo di evento (cioè, se tener traccia di ogni occorrenza, se tracciare n istanze in x minuti, tracciare n istanze, ecc)

### Trasmissione dei log

- Quali tipi di host devono trasferire log all'infrastruttura di Log Management
- Quali tipi di entry e dati devono essere trasferiti dagli host individuali all'infrastruttura di Log Management
- Come devono essere trasferiti i dati di log (cioè quali protocolli sono ammissibili), comprendendo anche sistemi non connessi in rete
- Quanto frequentemente i log devono essere trasferiti dagli host all'infrastruttura di Log Management (ad es. in tempo reale, ogni 5 minuti, ogni giorno)
- Come assicurare che confidenzialità, integrità e disponibilità dei dati sia protetta durante i trasferimenti

### Archiviazione dei log e cancellazione

- Con che frequenza i log devono essere ruotati
- Come assicurare che confidenzialità, integrità e disponibilità dei dati sia protetta una volta archiviata (a livello di sistema e di infrastruttura)
- Per quanto tempo devono essere preservati i log (sia a livello di sistema, sia a livello di infrastruttura)
- Come eliminare dati non necessari (sia a livello di sistema, sia a livello di infrastruttura)
- Quanto spazio di storage deve essere reso disponibile
- Come gestire le richieste di preservazione dei log ad esempio per prevenire l'alterazione e la distruzione dei log

## Analisi dei log

- Con che frequenza analizzare i vari tipi di log (sia a livello di sistema, sia a livello di infrastruttura)
- Chi dovrebbe essere in grado di accedere ai dati di log (sia a livello di sistema, sia a livello di infrastruttura) e come tener traccia di tali accessi
- Cosa fare nel caso che vengano individuate anomalie o attività sospette
- Come proteggere la confidenzialità, l'integrità e la disponibilità dei risultati delle analisi (alert, report) sia nello storage che in transito
- Come gestire la divulgazione di informazioni sensibili contenute nei log (ad esempio: password o contenuto di email)
- Le policy aziendali devono inoltre precisare chi, all'interno dell'organizzazione, avrà la responsabilità di stabilire e gestire l'infrastruttura di Log Management.
- L'azienda deve inoltre assicurarsi che gli altri processi, che hanno una qualche relazione con il Log Management, incorporino e supportino le necessità del nuovo processo e possano corrispondere alle richieste funzionali e operative.
- È naturalmente necessario condurre un'analisi dettagliata di tutte le attività che potrebbero influenzare la definizione dei requirement del processo di logging.

La tabella seguente mostra un esempio del tipo di configurazione del logging da specificare nelle policy.

| **Categoria** | **Sistemi poco critici** | **Sistemi mediamente critici** | **Sistemi molto critici** |
|---|---|---|---|
| Per quanto mantenere i dati di log | Da 1 a 2 settimane | Da 1 a 3 mesi | Da 3 a 12 mesi |
| Frequenza di rotazione dei log | Opzionale (se effettuata, almeno ogni settimana o ogni 25 MB) | Ogni 6-24 ore o ogni 2-5 MB | Ogni 15-60 minuti o ogni 0.5-1 MB |
| Con che frequenza trasferire i log alla infrastruttura di Log Management | Ogni 3-24 ore | Ogni 15-60 minuti | Almeno ogni 5 minuti |
| Con che frequenza analizzare i dati di log localmente (manualmente o con automatismi) | Ogni 1-7 giorni | Ogni 12-24 ore | Almeno 6 volte al giorno |
| Controllo di integrità dei log ruotati | Opzionale | Sì | Sì |
| Criptografia per i log ruotati | Opzionale | Opzionale | Sì |
| Criptografia del trasferimento via rete dei log | Opzionale | Sì | Sì |

Le policy organizzative devono anche occuparsi della preservazione dei log in formato originale: spesso le copie del log di traffico vengono inviate a device centralizzati, come anche a strumenti che analizzano e interpretano il traffico di rete. Nel caso che i log possano essere utilizzati come evidenze, le aziende devono acquisire le copie dei file di log originali, dei file centralizzati e interpretare i dati di log, nel caso sussistano questioni relative la fedeltà della copia o del processo interpretativo.

La ritenzione dei log come evidenza può richiedere l'utilizzo di diverse forme di storage e coinvolgere diversi processi.
L'integrità dei log deve anche essere preservata, conservando i log su supporti non-riscrivibili e generando un *message digest* per ogni file di log.
L'azienda devono revisionare periodicamente le raccomandazioni dagli amministratori dei sistemi sui cambiamenti di policy relativi alla riconfigurazione dei controlli di sicurezza: ad esempio, modifiche nelle regole di un firewall potrebbero far aumentare o diminuire considerevolmente il numero di righe di log provenienti da esso o da un sistema di individuazione delle intrusioni.

## Problematiche legali relative al Log Management

Nella stesura delle policy organizzative è necessario cosiderare anche problematiche legali: i log possono catturare (intenzionalmente o accidentalmente) informazioni con implicazioni di privacy o sicurezza, come password, contenuto di email o anagrafiche dei clienti, esponendo tali dati a chi analizza o amministra i sistemi generatori di log. Le aziende quindi devono avere policy riguardanti la gestione o la divulgazione non intenzionale di informazioni sensibili.
Nel quadro normativo italiano, due sono le norme che il Garante per la protezione dei dati personali ha emanato nel corso degli ultimi anni e che richiedono particolare attenzione nel trattamento dei log.
La prima che prenderemo in esame riguarda il trattamento dei dati dei lavoratori dipendenti relativi a posta elettronica e utilizzo di Internet in genere.

**Le linee guida del Garante per posta elettronica e internet**
*Gazzetta Ufficiale n. 58 del 10 marzo 2007*
*http://www.garanteprivacy.it/garante/doc.jsp?ID=1387978*

Nel documento, il Garante per la protezione dei dati personali, prescrive ai datori di lavoro alcune misure, necessarie o opportune, per conformare alle disposizioni vigenti il trattamento di dati personali effettuato per verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet.
Questo allo scopo di preservare la sfera personale e la vita privata di lavoratori e di terzi.

Nel punto 3.2 si afferma:
"3.2. *Linee guida*
In questo quadro, può risultare opportuno adottare un disciplinare interno redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente (verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori, ecc.) e da sottoporre ad aggiornamento periodico.
A seconda dei casi andrebbe ad esempio specificato:
...
- quali informazioni sono memorizzate temporaneamente (ad es., le componenti di *file* di *log* eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente;
- se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di *back up*, della gestione tecnica della rete o di *file* di *log* );

"

La direttiva del 17 gennaio 2008 è dedicata ai fornitori di servizi telefonici e telematici e mira a definire un approccio metodologico sulla conservazione dei dati di traffico.

**Sicurezza dei dati di traffico telefonico e telematico - 17 gennaio 2008**
*Gazzetta Ufficiale n. 30 del 5 febbraio 2008*
*http://www.garanteprivacy.it/garante/doc.jsp?ID=1485429*

Il 17 gennaio 2008 il Garante per la protezione dei dati personali ha pubblicato la disposizione "Conservazione dei dati di traffico: misure e accorgimenti a tutela dell'interessato in attuazione dell'articolo 132 del decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali."
In esso si regolamenta l'attività di conservazione dei dati relativi al traffico telefonico e telematico ed è rivolto a tutti quei fornitori che mettono a disposizione del pubblico servizi di comunicazione elettronica su reti pubbliche di comunicazione.
Il Garante chiede che entro il 31 ottobre del 2008 siano adottate soluzioni informatiche idonee ad assicurare il controllo delle attivita' svolte, che consentano la registrazione, in un apposito audit log, delle operazioni compiute sui dati di traffico e sugli altri dati personali a essi connessi, sia quando consistono o derivano dall'uso interattivo dei sistemi, sia quando sono svolte tramite l'azione automatica di programmi informatici.
I sistemi di audit log devono garantire la completezza,la non modificabilità e l'autenticita' delle registrazioni in essi contenute, con riferimento a tutte le operazioni di trattamento e a tutti gli eventi relativi alla sicurezza informatica sottoposti ad auditing.

## Stabilire policy attuabili

La definizione di requirements e raccomandazioni per la gestione dei log deve essere svolta congiuntamente a un'analisi della tecnologia e delle risorse necessarie per implementarle e mantenerle, delle implicazioni di sicurezza, delle normative alla quale l'azienda è soggetta. Quando possibile, l'azienda deve esaminare i log esistenti e le configurazioni per sviluppare requirements e raccomandazioni. Ad esempio, configurare un sistema operativo per tracciare tutti gli eventi potrebbe generare una quantità tremenda di log, andando a impattare sulle performance della macchina, causando la sovrascrittura delle log entry e rendendo l'analisi dei log un compito improbo.
Inoltre, il volume dei log tende a essere molto dinamico e a cambiare sia nel breve sia nel lungo termine: alcune configurazioni potrebbero diventare non adeguate in determinate circostanze avverse.
Registrare più dati possibili non è necessariamente la cosa migliore da fare: le aziende devono registrare e analizzare i fatti considerati di grande importanza. Alcune aziende scelgono di avere tutti o quasi i dati di log generati e archiviati per almeno un breve periodo di tempo, nel caso fossero necesssri: questo approccio privilegia la sicurezza sull'usabilità e sulle risorse da impiegare.

Nel processo di definizione di richieste e raccomandazioni, le aziende devono usare una certa flessibilità perché ogni macchina è diversa e genererà quantità di dati diversi dalle altre.
La flessibilità è importante perché il comportamento di logging di una macchina potrebbe cambiare sensibilmente a causa di aggiornamenti, patch o modifiche di configurazione. Gli amministratori di sistema devono poi informare gli amministratori dell'infrastrutture di

Log Management per comunicare i cambiamenti di configurazione e assicurarsi che i processi di monitoraggio e analisi, se necessario, siano modificati.

## Progettare un'infrastruttura di Log Management

Dopo aver stabilito una policy iniziale e identificato ruoli e responsabilità, è necessario progettare una o più infrastrutture di Log Management che supportino efficacemente policy e ruoli.

Nella fase progettuale dell'infrastruttura di Log Management, le aziende devono considerare diversi fattori relativi alle necessità attuali e future sia dell'infrastruttura sia delle sorgenti di log individuali.
Tra i maggiori fattori da considerare troviamo:

- **Il volume medio e di picco di dati di log elaborati ogni ora e ogni giorno.** Il volume medio dei dati di log tende ad aumentare nel tempo per molte sorgenti di log. Il volume di picco deve includere la gestione di situazioni estreme, come la diffusione di malware, vulnerability scan e penetration test che potrebbero causare grandi numeri di entry in un periodo molto breve di tempo
- L'utilizzo medio e di picco della banda di rete.
- **L'utilizzo medio e di picco di storage (disco e archiviazione).** Questo aspetto dovrebbe includere un'analisi del tempo e delle risorse necessario per effettuare i backup e archiviare i dati di log, nonché cancellare i dati una volta che non sono più necessari.
- **Le necessità di sicurezza dei dati di log.** Ad esempio, se i dati di log devono essere cryptati nella fase di trasmissione tra sistemi.
- **Il tempo e le risorse necessarie per analizzare i log**.

# 4 I Processi operativi del Log Management

Gli amministratori di sistema devono seguire processi standard per gestire i log di cui sono responsabili. I processi operativi principali coinvolti in questa attività sono:

- la configurazione delle sorgenti di log, ivi compresi la generazione dei log, lo storage e la sicurezza;
- l'analisi dei dati di log;
- l'identificazione di responsi appropriati agli eventi identificati;
- la gestione dell'archiviazione a lungo termine dei dati.

## Configurazione delle sorgenti di log

Gli amministratori di sistema, attraverso un'appropriata configurazione delle sorgenti di log, potranno catturare le informazioni necessarie nel formato desiderato e mantenere i dati per un periodo di tempo adeguato.
Configurare le sorgenti di log è un'attività complessa: basandosi sulle policy aziendali, gli amministratori devono determinare quali sistemi e quali componenti dei sistemi devono partecipare all'infrastruttura di gestione dei log.
Un singolo file di log può contenere informazioni provenienti da diverse sorgenti, dal sistema operativo stesso e dalle applicazioni ospitate: gli amministratori devono aver ben chiaro dei file di log utilizzati dalle varie sorgenti
Successivamente, per ogni sorgente di log identificata, gli amministratori devono determinare quale tipi di eventi devono essere registrati e quali sono le caratteristiche dei dati da registrare per ogni tipo di evento.
La capacità dell'amministratore di configurare ogni sorgente di log dipende dalle funzionalità di log della stessa: alcune sorgenti offrono opzioni di configurazione molto granulari, mentre altre permettono solo di attivare o disabilitare il log.

### Generazione dei log

Assumendo che una sorgente di log offra opzioni di configurazione, è generalmente prudente essere conservativi nella scelta iniziale delle opzioni: un singolo parametro può causare un enorme numero di log entry da registrare, oppure troppe informazioni per ogni evento.
Un log eccessivo può causare la perdita di dati, come anche dei problemi operativi: gli amministratori di sistema devono considerare questa tipologia di problemi non solo sul sistema stesso, ma anche sulle componenti dell'infrastruttura di Log Management (ad esempio, un logging eccessivo può causare un utilizzo superiore di banda e di storage).
È opportuno testare le configurazioni dei log in ambienti dedicati, prima di renderle operative in un ambiente di produzione.

## Archiviazione e smaltimento dei log

Gli amministratori di sistema devono stabilire il modo in cui ogni sorgente di log conserva i suoi dati. Questo dovrebbe essere guidato principalmente da politiche organizzative riguardanti la memorizzazione con particolare riguardo all'inoltro di entry all'infrastruttura di Log Management. Una volta che i requisiti sono stati soddisfatti, gli amministratori hanno normalmente abbastanza flessibilità sulle altre opzioni di configurazione.
Tipicamente, le opzioni di storage per le log entry sono:

- **Not stored.** Le entry di scarso valore, come ad esempio i messaggi di debug comprensibili solo al produttore del software, o i messaggi di errore che non registrano nessun dettaglio dell'attività, possono non essere memorizzate.
- **Solo a livello di sistema.** Le entry che potrebbero avere qualche valore per gli amministratori di sistema, ma che non sono sufficientemente importanti da essere inviate all'infrastruttura di Log Management, dovrebbero essere conservate sul sistema. Ad esempio, in caso di incidente, delle entry aggiuntive a livello di sistema offrono più informazioni sulla serie di eventi relativi. Gli amministratori potrebbero trovare utili queste entry per sviluppare tendenze di lungo termine basandosi sull'attività tipica dei sistemi.
- **Sia a livello di sistema, sia di infrastruttura.** Le entry di particolare interesse dovrebbero essere conservate sul sistema e anche trasmesse all'infrastruttura di Log Management. Le ragioni per avere i log in entrambe le locazioni sono:
    - Nel caso che il sistema o l'infrastruttura abbia un problema, l'altro conserva comunque i dati di log. Ad esempio, se un log server va in crash o un problema di rete impedisce ai sistemi di contattarlo, il log sul sistema aiuta a garantire che i dati di log non vadano persi
    - Durante un incidente su un sistema, il suo log potrebbe venire alterato o distrutto da degli attaccanti. Lo staff di Incident Response può utilizzare i dati dall'infrastruttura di log e compararli con quelli di sistema per stabilire quali dati sono stati modificati o rimossi.
- **Solo a livello di infrastruttura.** Se i log sono conservati sui server dell'infrastruttura, è preferibile che siano conservati anche a livello di sistema. Questo può non essere sempre possibile, ad esempio nei sistemi con scarsa capacità di storage

Tra le possibilità di customizzazione delle sorgenti di log, possiamo trovare diverse varianti:

- i log possono essere scritti in un singolo file. Le infrastrutture di Log Management supportano i formati di log comuni, come ad esempio i valori separati da virgola o TAB, il formato syslog e i database. Alcune infrastrutture supportano anche i formati di log proprietari più diffusi. Se un formato non è supportato dall'infrastruttura, gli amministratori possono implementare programmi di conversione appropriati. Le sorgenti di log che memorizzano i dati in formati proprietari, tipicamente forniscono strumenti di visualizzazione o analisi per assistere gli amministratori nello svolgimento dell'analisi.

- Possono essere utilizzati vari tipi di log di sistema, log proprietari o log standard (ad esempio, syslog). In molti casi, i log non contengono tutti gli stessi dati. I log con formato proprietario spesso contengono più campi dati dei log standard. Un'opzione possibile è l'invio di dati a log multipli. Un'opzione per alcune sorgenti di log è di inviare i dati a diversi log di sistema simultaneamente. Questo permette agli amministratori di sistema di svolgere analisi utilizzando i formati di log proprietari, e rendendo al contempo i dati disponibili all'infrastruttura di Log Management.
- È possibile scrivere i log simultaneamente a livello di sistema e a livello di infrastruttura di Log Management. È possibile, per alcune tipologie di sorgenti di log, specificare quali tipi di entry debbano essere inviate a ogni destinatario.

La rotazione dei log locali è un'altra parte importante della configurazione delle sorgenti di log.
Gli amministratori di sistema e di infrastruttura devono configurare le sorgenti di log per effettuare la rotazione, preferibilmente a intervalli regolari (ogni ora, giornalmente o nel weekend) e quando viene raggiunta una dimensione massima. Se una sorgente di log non offre la possibilità di ruotare i log, dovrà essere l'amministratore a implementare un'utility esterna all'uopo predisposta.

## Sicurezza dei log

Gli amminsitratori di sistema e di infrastruttura devono proteggere l'integrità, la disponibilità e la confidenzialità dei log attraverso i seguenti approcci:

- **Limitare l'accesso ai file di log**. Gli utenti non devono avere alcun accesso alla maggior parte dei file di log fino a meno che sia necessario un determinato livello di accesso per creare log entry. In questo caso, gli utenti devono avere privilegi che permettano loro di effettuare soltanto operazioni di append, ma nessun privilegio in lettura. Gli utenti non devono essere in grado di rinominare, cancellare o altre attività a livello di file sui file di log.
- **Evitare di registrare dati sensibili non necessari.** Alcuni log possono registrare dati sensibili non necessari, come le password. Quando possibile, il logging deve essere configurato per non registrare informazioni non richieste, perché presenterebbe un rischio sostanziale se acceduto da chi non ne ha l'autorizzazione
- **Proteggere i file di log archiviati.** Creare e mettere in sicurezza i message digest per i file di log, criptografare i file di log e fornire protezioni fisiche adeguate per l'archivio.
- **Rendere sicuro il processo di generazione dei log**. Persone non autorizzate non devono essere in grado di manipolare i processi delle sorgenti di log, file eseguibili e di configurazione o altre componenti del log che potrebbero influenzare il logging.
- **Configurare per ogni sorgente di log un adeguato comportamento nel caso di errori del logging.** Ad esempio, la sorgente di log potrebbe sospendere le sue funzionalità nel caso che il logging abbia problemi.
- **Implementare meccaniscmi sicuri di trasporto dei log dal sistema al server centralizzato di Log Management**.

# Analizzare i dati di log

Un analisi efficace dei dati di log è uno degli aspetti più impegnativi del Log Management, ma è anche il più importante. Sebbene l'analisi dei dati sia a volte percepita dagli amministratori come poco interessante e inefficiente, avere a disposizione una robusta infrastruttura di Log Management e dei processi di analisi automatici può migliorare sensibilmente l'intero processo di analisi e produrre preziosi risultati in tempi brevi.

## Comprendere i log

La chiave per condurre l'analisi dei log è la comprensione dell'attività tipica associata ad ogni sistema: sebbene alcune entry siano facili da capire, molte altre non lo sono. Le ragioni primarie di questo sono:

- Necessità di un contesto. Il significato di ogni entry spesso dipende dal contesto che la circonda. Gli amministratori hanno necessità di capire come viene definito questo contesto, anche mediante altre log entry in uno o più log, oppure attraverso sorgenti non di log (ad es. configuration management record). Il contesto è necessario per convalidare log entry non affidabili, come i software di sicurezza che spesso generano falsi positivi nella ricerca di attività maligne.
- Messaggi non chiari. Una riga di un log può contenere un messaggio criptico o un codice significativo solo al produttore del software, ma non all'amministratore, per cui è richiesto il coinvolgimento del produttore. Utilizzare una tecnologia SIEM per analizzare i log riduce il numero di messaggi non chiari poiché i software SIEM spesso conoscono nel dettaglio le pratiche di logging dei produttori di software. Neanche i software SIEM, purtroppo, possono conoscere ogni messaggio, come ad esempio, un nuovo tipo di messaggio associato alla nuova release di un prodotto.

In alcuni casi può non essere possibile avere una piena comprensione di una entry di un log. Una sorgente di log, ad esempio, potrebbe non essere in grado di registrare i dati necessari per dare un adeguato contesto a una entry. Oppure un produttore di software potrebbe non essere in grado di fornire informazioni dettagliate sul significato di un particolare messaggio.
Sebbene sia certamente preferibile per un amministratore comprendere tutte le righe di un log, in molto casi ciò non è possibile, poiché esistono molti diversi tipi di righe di log che non è possibile comprendere con le risorse limitate disponibili.
Il modo più efficace per avere una chiara comprensione dei dati di log è di revisionare e analizzare porzioni di essi con regolarità con lo scopo di avere una chiara immagine delle normali log entry, comprendendo la grande maggioranza delle entry di un sistema (poiché pochi tipi di entry costituiscono una percentuale significativa dei dati di un log, non è così difficile come potrebbe sembrare). Le analisi giornaliere dovrebbero includere anche le righe considerate più importanti, come anche quelle di cui non si ha ancora una completa comprensione.
Nel corso del tempo, una volta che lo stato del log in situazione di normalità è stato approfondito, l'analisi giornaliera dei log occuperà meno tempo e potrà focalizzarsi sulle entry più importanti.

Un altro motivo per capire le entry dei log è quello di automatizzare il processo il più possibile. Comprendendo quali tipi di righe di log sono interessanti e quali no, gli amministratori possono configurare filtri automatici delle entry: questo permetterà di riconoscere gli eventi sospetti e di rispondervi in modo automatico (ad es. inviando avvisi agli amministratori o configurando altri controlli di sicurezza).

## Assegnare la priorità corretta alle entry

Sebbene alcune sorgenti di log assegnano le proprie priorità a ogni entry, tali priorità spesso utilizzano scale o rating tra i più disparati (ad esempio: alto/medio/basso, da 1 a 5, da 1 a 10 ecc), fattore che rende il confronto tra i valori di priorità un compito impegnativo.
Inoltre, i criteri utilizzati dai diversi sistemi per assegnare una priorità alle entry sono basati su set differenti di requisiti, che possono essere non consistenti con i requisiti aziendali.
Per tale motivo, l'organizzazione deve assegnare le sue priorità alle entry dei log basandosi su una combinazione di fattori, tra cui:

- Il tipo di entry (e.g., message code 103, message class CRITICAL)
- La novità del tipo di entry (ad es, questa entry è già apparsa prima d'ora?)
- La sorgente dei log
- Indirizzo Ip sorgente o destinatario (ad es, indirizzo del sorgente su una black list, indirizzo destinatario di un sistema critico, eventi precedenti relativi un indirizzo IP particolare)
- Momento del giorno o giorno della settimana (ad es. una entry può essere accettabile durante certe ore, mentre in altri momenti della giornata non dovrebbe presentarsi)
- Frequenza dell'entry (ad es. n volte negli ultimi x secondi)

Assegnare una priorità può anche prevedere l'uso di correlazioni per fornire un contesto alle entry così che possano essere validate. Ad esempio, se un host-based intrusion detection software individua un attacco di modifica a un file su un sistema e se il log del sistema operativo contiene un'entry di audit che afferma che il file è stato modificato con successo, e i dati delle due sorgenti di log sono correlati, si avrà una prova più certa che si è verificato un attacco. Inoltre si avranno a disposizione più dati sull'attacco.
Un altro esempio di utilizzo della correlazione come fattore di priorità è l'utilizzo di informazioni sulle vulnerabilità conosciute nei sistemi operativi e nelle applicazioni installate per assegnare una priorità più alta alle entry relative a queste vulnerabilità.

## Confrontare analisi a livello di sistema e di infrastruttura

Le analisi sui due livelli sono molto simili. La differenza principale è che per gli amministratori di infrastruttura, l'analisi dei log è spesso una responsabilità primaria. In questo contesto, le analisi sull'infrastruttura sono normalmente svolte in modo continuativo, mentre gli amministratori di sistema devono effettuare analisi periodiche commisurate all'effettiva criticità dei sistemi e delle informazioni da essi ospitate.
Inoltre, gli amministratori di infrastruttura hanno solitamente accesso a strumenti più sofisticati.
Indipendentemente da quanta analisi viene svolta a livello di infrastruttura, gli amministratori di sistema devono svolgere analisi per i seguenti tipi di entry:

- entry che rivestono una certa importanza a livello di sistema ma che non sono inoltrate all'infrastruttura a causa della loro priorità relativa
- entry di sorgenti di log che non possono partecipare automaticamente all'infrastruttura (ad es. formati proprietari non usuali, sistemi standalone, sistemi legacy, ecc)
- entry che non possono essere comprese senza un contesto appropriato disponibile solo a livello di sistema

Su alcuni sistemi, che generano log con formati proprietari, gli amministratori possono svolgere analisi di ogni sorgente utilizzando viewer specifici, strumenti di riduzione e altre utility. Un'altra possibilità è l'esportazione di dati di log verso un database per effettuare query per filtrare i dati dei log a scopo di analisi.
Se molta parte del processo di analisi può essere automatizzato, si potrebbe creare un report di analisi quotidiano e presentarlo all'amministratore. L'amministratore potrà svolgere successive investigazioni sulla base di eventi significativi identificati dal report.

Per svolgere analisi in modo efficace, gli amministratori, sia a livello di sistema che di infrastruttura, devono avere una conoscenza approfondita di ognuno dei seguenti punti:

- Le policy organizzative riguardanti l'uso accettabile, in modo che gli amministratori possano riconoscere le violazioni di policy
- I software di sicurezza utilizzati dai sistemi, comprese le tipologie di eventi relativi alla sicurezza che ogni programma può individuare e il profilo di individuazione generale di ogni programma (ad es. i falsi positivi conosciuti)
- I sistemi operativi e le applicazioni principali utilizzate, ivi incluse le caratteristiche di sicurezza di tali applicazioni e le caratteristiche dei log
- Le caratteristiche delle tecniche comuni di attacco, specialmente come l'uso di queste tecniche può essere registrato da ogni sistema
- I software necessari per svolgere le analisi, come ad esempio i viewer per log, gli script per la riduzione dei log e gli strumenti di query per database

Le organizzazioni spesso richiedono agli amministratori di sistema di riportare i risultati delle loro analisi agli amministratori di infrastruttura.
Questi ultimi devono creare report che riassumano il risultato delle loro attività di analisi e possibilmente anche riassumere i report degli amministratori di sistema.
Condividere regolarmente questi report è una buona prassi per il miglioramente continuo del processo di Log Management.
Inoltre, mostrare la reportistica al management, particolarmente dopo che un problema è stato identificato e corretto sulla base di un'attività di analisi, dimostra i benefici del Log Management anche a livello direttivo.

## Rispondere agli eventi identificati

Nell'attività di analisi, gli amministratori si sistema e di infrastruttura potrebbero identificare eventi significativi, relativi a incidenti o problemi operativi, che necessitano una risposta.
Quando un amministratore identifica un incidente di sicurezza, come definito nelle policy di responso agli incidenti, deve seguire una procedure ben definita per assicurare che l'incidente sia gestito in modo adeguato.
Gli amministratori devono seguire le procedure di risposta agli eventi non di sicurezza, come ad esempio i problemi operativi minori.

È buona norma che gli amministratori di sistema condividano con gli amministratori di infrastruttura gli incidenti e i problemi operativi legati ai log in modo che questi ultimi possano meglio identificare altri esempi della stessa attività e pattern che potrebbero non essere individuati a livello di sistema.

Gli amministratori di sistema e di infrastruttura devono anche essere pronti per assistere i team di incident response, ed eventualmente fornire l'accesso ai log registrati.
Gli amministratori devono anche essere preparati a modificare le configurazioni di logging come parte di un'attività di incident response: eventi avversi, come i worm, possono causare la produzione di un gran quantità di entry, risvolto che può avere impatti negativi sulle performance dei sistemi e sovrascrittura di entry recenti.
Gli amministratori potrebbero aver inoltre la necessità di riconfigurare i log per catturare più dati.

## Gestire lo storage a lungo termine

Gli amministratori sono normalmente responsabili della gestione dell'archiviazione dei loro log: l'organizzazione deve quindi emanare precise linee guida per tale scopo, in modo che i log possano essere conservati per il periodo di tempo richiesto.
Se i dati di log sono già stati trasferiti all'infrastruttura di Log Management, gli amministratori di sistema potrebbero non aver bisogno di dati storici di lungo termine.
Qualora il periodo di conservazione sia piuttosto lungo (mesi o anni) gli amministratori devono:

- **Scegliere un formato di log per i dati archiviati.** Qualora i log siano in formati proprietari, gli amministratori devono determinare se i log devono essere mantenuti in tale formato, in un formato standard o in entrambi. Potrebbe essere difficile leggere un formato proprietario dopo anni, perché il software che lo ha generato non è più disponibile o non supporta più il vecchio formato di log. I log con formato proprietario potrebbero contenere informazioni addizionali e più dettagliate non presenti nei log di formato standard, e quindi potrebbe essere più indicato archiviare tali log in entrambi i formati.
- **Archiviare i dati dei log.** I dati possono essere archiviati su CD, DVD, storage area network (SAN) e appliance o server specializzati. Nella selezione di un media si deve considerare il periodo di conservazione dei dati. Gli amministratori devono anche considerare se l'hardware e il software necessario per accedere al media sarà ancora disponibile al termine del periodo di conservazione. Gli amministratori dovrebbero revisionare periodicamente i formati dei media archiviati per determinare se alcuni di essi sono a rischio di deventare non accessibili, ed eventualmente trasferire tali dati su un nuovo media.
- **Verificare l'integrità dei log trasferiti.** Come descritto nella sezione 2 (pg. 10), questa operazione si effettua mediante la creazione di un message digest per ogni file di log. Se un file di log è stato modificato e il suo message digest ricalcolato, il nuovo message digest non sarà uguale al precedente. Gli amministratori devono comparare i digest per ogni log originale con quello di ogni copia per assicurarsi che il file non sia stato modificato successivamente.
- **Archiviare il media in modo sicuro**. Gli amministratori devono assicurarsi che i media siano protetti fisicamente in modo adeguato, prevenendo accessi fisici non autorizzati, e assicurandosi che adeguati controlli ambientali siano stati posti in essere.

- **Cancellazione dei log archiviati**. Gli amministratori sono anche responsabili del processo di distruzione dei log archiviati che hanno superato il periodo di conservazione stabilito. Questa attività riguarda i log archiviati sui sistemi, negli archivi logici e fisici.

## Altri supporti operativi

Oltre ai processi operativi descritti in questa sezione, gli amministratori di sistema e infrastruttura devono fornire altri tipi di supporto per le operazioni di logging, ovvero:

- Monitorare lo status del logging per ogni sorgente di log per assicurarsi che ogni sorgente sia abilitata, configurata adeguatamente e fuzionante
- Monitorare la rotazione dei log e i processi di archiviazione per accertarsi che i log vengano archiviati e cancellati correttamente e che i vecchi log siano distrutti una volta che non sono più necessari. Il monitoraggio della rotazione dei log deve anche prevedere controlli regolari automatici o manuali per verificare lo spazio ancora disponibile.
- Controllare l'aggiornamento e le patch del software di logging; acquisire, testare e implementare gli aggiornamenti
- Assicurarsi che i clock dei sistemi siano allineati a una fonte comune, così che i timestamp siano allineati sui vari sistemi
- Riconfigurare il logging basandosi su fattori come i cambiamenti di policy, i risultati degli audit, i cambiamenti di tecnologia e le nuove esigenze di sicurezza
- Documentare le anomalie individuate nelle configurazioni e nei processi di logging. Tali anomalie potrebbero indicare attività malversatorie, deviazioni da policy e procedure e debolezze nel meccanismo di logging. Gli amministratori di sistema devono riportare le anomalie agli amministratori di infrastruttura

## Test e convalida

È opportuno svolgere attività periodiche di test e convalida per confermare che le policy, i processi e le procedure di logging siano seguite adeguatamente, sia a livello di infrastruttura che a livello di sistema.
Gli audit di Log Management possono identificare deficienze in policy, procedure, tecnologie e training e possono anche essere d'aiuto nell'identificazione di prassi efficienti.
Le tecniche più comuni per testare e convalidare il processo di log sono:

- **Passiva.** Gli auditor che svolgono test e convalida possono revisionare le configurazioni del logging, dei log di sistema e di infrastruttura, dei log archiviati, per un insieme significativo di sistemi e server di infrastruttura allo scopo di valutare che siano adeguati a policy e procedure interne.
- **Attiva.** Gli Auditors o gli amministratori di sicurezza che svolgono test e convalida possono creare eventi di sicurezza su un insieme significativo di sistemi attraverso azioni di vulnerability scanning, penetration test o azioni di routine e poi assicurarsi che i log di queste attività vengano generati e gestiti secondo le policy e le procedure interne

In alcuni casi, i metodi attivi sono utilizzati non solo per testare e convalidare, ma anche per effettuare audit di altre funzioni. Ad esempio, un auditor può valutare l'efficienza di un'organizzazione interna coinvolta in operazioni di routine nel rispondere ad attività sospette registrate nei log.

Ogni organizzazione dovrebbe condurre audit periodici dei log di sicurezza dell'infrastruttura di Log Management e un sondaggio dei generatori di log. Questa attività può essere svolta come una valutazione del rischio, prendendo in considerazione le minacce a cui sono sottoposti i sistemi coinvolti nei vari livelli di un'infrastruttura di Log Management e i controlli di sicurezza posti in essere per bloccare queste minacce. Gli obiettivi di sicurezza specifici sono:

- I Log Server di infrastruttura devono essere resi sicuri e svolgere unicamente operazioni a supporto del Log Management
- I sistemi generatori di log devono essere messi in sicurezza (ad esempio, allineati alle ultime patch, con servizi non necessari disabilitati, ecc.)
- L'accesso ai log e al software di log, sia dei sistemi sia dell'infrastruttura, deve essere limitato e l'integrità dei log e del software deve essere protetta e verificata
- Le comunicazioni di rete riferite ai log devono essere protette adeguatamente

Ogni organizzazione deve rivedere periodicamente il progetto dell'infrastruttura di Log Management e implementare i cambiamenti sulla base delle nuove necessità.
Allo stesso modo, è opportuno rivedere periodicamente i processi e le procedure di Log Management per garantirne l'efficacia nell'individuazione delle ultime minacce.

# Bibliografia


- Babbin, Jacob et al, Security Log Management: Identifying Patterns in the Chaos, Syngress, 2006.
- Karen Kent e Murugiah Souppaya, Guide to Computer Security Log Management, NIST, 2006
- Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition , Academic Press, 2004
- Tim Grance,Suzanne Chevalier,Karen Kent, Hung Dang , NIST 800-86 Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response , NIST, 2005
- Chris Brenton Tina Bird, Marcus J Ranum Top 5 Essential Log Reports , SANS Institute - http://www.sans.org/resources/top5_logreports.pdf
- Anton Chuvakin, Advanced Log Processing - http://www.securityfocus.com/infocus/1613
- Anton Chuvakin Blog - http://chuvakin.blogspot.com/

SECURITY LOG MANAGEMENT

# Guida alla gestione dei log di sicurezza

Versione 1.0

ADVANCTION

Giugno 2008



Svizzera - Italia