LOG

EVENT LOG MANAGEMENT

Gestione centralizzata, correlazione e "analytics" degli eventi di sicurezza d sistemi e applicazioni aziendali

CLOUDWALL
SECURITY AS A SERVICE

A cosa serve avere i log se non puoi usarli?

Le architetture tradizionali per la sicurezza delle reti e dei sistemi non sono oggi più in grado di garantire una protezione efficace rispetto all'evoluzione delle minacce al sistema informativo sempre più complesse e mirate alle frodi. Sempre piu' spesso le attivita' criminali online sono sostenute da organizzazioni internazionali in grado di mettere a disposizione del miglior offerente strumenti di infezione finalizzati al crimine informatico o botnet pronte "a noleggio" per poche manciate di dollari. Eludere sistemi di sicurezza deboli per rubare informazioni è fonte di profitto per molte organizzazioni cyber-criminali che si differenziano da altre forme più blande di hacktivismo proprio perché mirano a frodi finanziarie. Per queste ragioni gli strumenti di indagine tradizionali, basati su signature, sono da considerarsi non più efficaci.

Difendersi, quindi, dai malware e dai cyber-criminali mediante un'architettura tradizionale di sicurezza non è oggi efficace e risolutivo. Un approccio corretto per identificare e contrastare i nuovi malware richiede da una parte interventi volti a rafforzare le proprie difese con strumenti di analisi statica e dinamica (sandbox) del codice scaricato dalla rete (contrasto al vettore di attacco "drive-by-download") e dall'altra l'adozione di soluzioni che consentano di avere visibilità completa della propria rete, di tenere traccia dell'attività dei malware e di identificare e conoscere gli attacchi e gli hacker che hanno invaso il vostro perimetro. Conoscere gli spostamenti di un hacker da un nodo all'altro della rete permette di agire in un tempo ragionevole, chiudere le vulnerabilità ed isolare e/o aggiornare i sistemi compromessi. Tutto ciò trova realizzazione nelle moderne piattaforme SIEM (Security Information and Event Management), con capacità di analisi per grandi quantità di informazioni (Big Data) generate da diverse tipologie di sorgenti, siano esse end-point che dispositivi di rete/sicurezza, ed in grado di correlare, identificare, indagare e gestire gli incidenti di sicurezza. Tuttavia, la complessita' ed il costo di tali soluzioni, di acquisto, di integrazione e di conduzione operativa, ne hanno fortemente limitato l'adozione da parte delle aziende di medie dimensioni, se non nel perimetro previsto dalla normativa del Garante in materia di Privacy.

Una soluzione di Security Analytics fornita "as a service"
Supporta l'integrazione di qualsiasi dispositivo e formato di log
Offre un servizio di raccolta dei log basato su standard syslog
Supporta politiche personalizzate di analisi e allarmistica
Consente di semplificare l'analisi degli eventi dei sistemi
Supporta la rilevazione di incidenti ed anonalie di sicurezza
Garantisce allarmistica degli incidenti in tempo reale
Trasmette report periodici automatizzati all'amministratore
Fornito "as a service" direttamente dal nostro Private Cloud
Nessun investimento richiesto in hardware e software

100%

#SECURITY
#CLOUD
#SAAS

LOG **EVENT LOG MANAGEMENT**

Una soluzione di Security Analytics "as a service"

CloudWALL LOG | Event Log Management e' la soluzione "as a service" proposta da CloudWALL Italia per la centralizzazione dei log generati da qualsiasi sistema, applicazione o apparato di rete presente all'interno del sistema informativo aziendale, la normalizzazione, correlazione ed analisi intelligente degli eventi allo scopo di rilevare incidenti informatici non rilevabili dalle tradizionali tecnologie basate su "signature" o piu' in generale anomalie di funzionamento del sistema informativo aziendale.

A partire da una console di gestione messa a disposizione direttamente dal nostro Private Cloud, gli amministratori di sistema hanno la possibilita' di accedere ad un ampio set di strumenti che semplificano l'analisi dei log generati dai sistemi aziendali, fornendo al contempo grafici di semplice interpretazione per l'analisi degli andamenti nel tempo e la possibilita' di visualizzare il dettaglio di tutti gli eventi correlati ad uno specifico incidente o tutti i log che hanno prodotto ogni singolo evento.

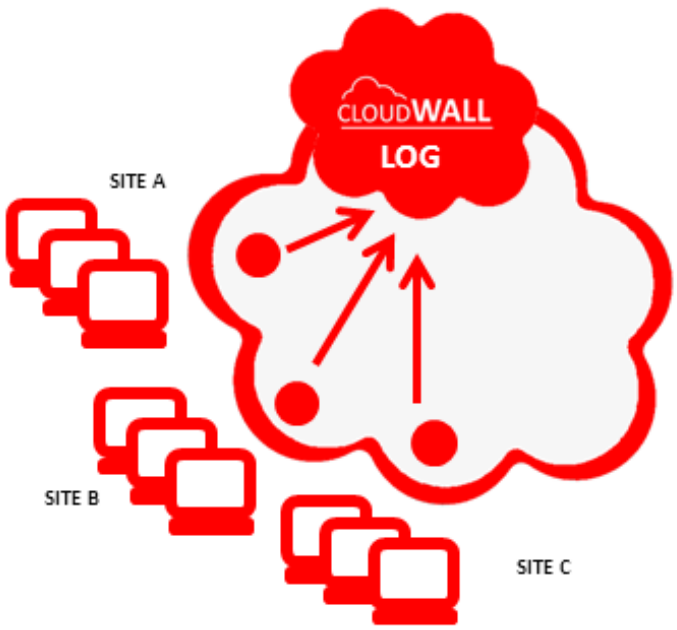
CloudWALL LOG | Event Log Management e' fornito direttamente dal nostro Private Cloud e consente pertanto di ridurre drasticamente i tempi di messa in opera rispetto a qualsiasi soluzione che preveda l'installazione di hardware e software all'interno del sistema informativo aziendale: una volta attivato il servizio e' gia' possibile iniziare a collezionare ed analizzare i propri log!

Grazie alla sua architettura "agent-less" che non richiede l'installazione di hardware o software dedicato all'interno del sistema informativo aziendale, al pieno supporto offerto per i protocolli standard tra cui Syslog, HTTP e HTTPS, alla disponibilita' di un ampio set di "parser" gia' pronti per l'uso, alla possibilita' di arricchire i "parser" esistenti con nuovi campi personalizzati o di creare nuovi "parser" per i propri sistemi e le proprie applicazioni, alle funzionalita' di allarmistica in funzione di politiche e criteri personalizzati definiti da ogni singolo amministratore,

CloudWALL LOG | Event Log Management e' la soluzione in grado di mettere a disposizione le piu' evolute funzionalita' di Security Analytics tradizionalmente offerte dalle soluzioni SIEM (Security Information Event Management) di livello Enterprise nell'ambito di un'offerta "as a service" che non richiede nessun investimento iniziale in hardware e software e che consente al contempo la massima flessibilita' e scalabilita' nel tempo.

Fornito direttamente dal nostro Private Cloud

CloudWALL LOG | Event Log Management e' fornito in modalita' SaaS (Software as a Service) direttamente dal Private Cloud di CloudWALL Italia. Grazie all'architettura centralizzata presso il nostro Private Cloud, CloudWALL LOG | Event Log Management non richiede l'acquisto, l'installazione, la personalizzazione e la gestione di piattaforme hardware e software, costose da acquisire e complesse da gestire, ma soltanto l'attivazione di un servizio che consente di poter iniziare immediatamente a collezionare e correlare i log generati da qualsiasi dispositivo - siano essi sistemi, applicazioni o apparati di rete - presente all'interno del sistema informativo ed in grado di generare un file di log.



Diversamente da altre piattaforme che richiedono l'installazione di agenti proprietari per la gestione dei log, CloudWALL LOG | Event Log Management ha una architettura totalmente agent-less e, grazie al supporto offerto per i protocolli standard tra cui Syslog, HTTP e HTTPS supporta qualsiasi tipo di formato di log senza la necessita' di modifiche al sistema o all'applicazione che li ha generati. Grazie alla possibilita' di sfruttare un lungo elenco di parser pronti per l'uso e alla possibilita' di creare parser personalizzati, CloudWALL LOG | Event Log Management e' in grado di correlare e analizzare formati di log eterogenei a supporto di una maggiore granularita' di analisi degli eventi e di rilevazione delle anomalie.

www.cloudwall.tk
info@cloudwall.tk

NO HARDWARE
SOFTWARE
MAINTENANCE

CLOUDWALL
SECURITY AS A SERVICE

Un potente motore di Security Analytics per i vostri log

CloudWALL LOG | Event Log Management e' stato progettato per fornire il piu' ampio set di funzionalita' di Security Analytics abbinato alla capacita' di supportare la gestione degli eventi generati da qualsiasi dispositivo hardware o software presente all'interno del sistema informativo aziendale.

Qui di seguito un riepilogo delle funzionalita' fornite dalla soluzione.

Raccolta dei log

Architettura "agent-less" basata su protocolli standard come Syslog, HTTP e HTTPS; in grado di interpretare qualsiasi formato di log di tipo testuale indipendentemente dal dispositivo che l'ha generato; capacita' virtualmente illimitata del sistema in grado di supportare picchi di traffico correlati ad incidenti o altre anomalie del sistema informativo;

Correlazione degli eventi

Riconosce automaticamente i formati di log nativamente supportati; consente la creazione di "parser" personalizzati o l'aggiunta di campi "custom" ai "parser" standard; consente di organizzare i dispositivi sulla base della loro tipologia, della funzione o dell'ambito applicativo di riferimento attraverso la gestione per gruppi;

Analisi degli eventi

Funzionalita' avanzate di ricerca in tempo reale a testo libero (o "full text") o limitata a specifici campi dei tracciati log; funzione di filtro degli eventi sulla base di vari parametri tra cui intervallo temporale, campo nel tracciato log, dispositivo sorgente; un potente motore di visualizzazione grafica degli eventi che consente di semplificare l'analisi degli eventi e l'individuazione di anomalie;

Monitoraggio e allarmistica

Fornisce una console di monitoraggio personalizzabili da ogni amministratore che consentono di avere sott'occhio le sole informazioni di interesse, in formato grafico o testuale; mette a disposizione funzionalita' di allarmistica tramite email a fronte del verificarsi di specifiche condizioni precedentemente definite dall'amministratore, che in questo modo puo' ricevere non solo un allarme dell'anomalia rilevata ma anche il dettaglio di tutti gli eventi che hanno generato tale anomalia, a supporto di un pronto intervento di analisi e rimedio;

Conformita' a standard e politiche di sicurezza

Gestione di privilegi autorizzativi personalizzati per gli amministratori sulla base della tipologia di sistemi, componenti applicative o apparati di rete di cui hanno la necessita' di accedere ai dati di log; supporto per attivita' di analisi congiunta tra differenti amministratori tramite funzionalita' di condivisione dei "workspaces"; funzionalita' di archiviazione di lungo termine dei file di log all'interno di risorse di storage in cloud tra cui Amazon S3.

Sicurezza “as a service” fornita dal nostro Private Cloud

Una soluzione di Security Analytics fornita "as a service"
Supporta l'integrazione di qualsiasi dispositivo e formato di log
Offre un servizio di raccolta dei log basato su standard syslog
Supporta politiche personalizzate di analisi e allarmistica
Consente di semplificare l'analisi degli eventi dei sistemi
Supporta la rilevazione di incidenti ed anonalie di sicurezza
Garantisce allarmistica degli incidenti in tempo reale
Trasmette report periodici automatizzati all'amministratore
Fornito "as a service" direttamente dal nostro Private Cloud
Nessun investimento richiesto in hardware e software

Un ecosistema di soluzioni integrate

CloudWALL LOG | Event Log Management si integra con altre soluzioni "as a service" fornite dal Private Cloud di CloudWALL Italia :

- Con CloudWALL MON | Availability Monitoring, per garantire il monitoraggio della disponibilita' e dei livelli di servizio offerti dai siti web e dalle applicazioni online per gli utenti che vi accedono da qualsiasi parte nel mondo;
- Con CloudWALL VAM | Vulnerability Management per rilevare la presenza di vulnerabilita' nell'ambito dei sistemi interni ed esterni all'azienda ed indirizzare un processo periodico di gestione delle vulnerabilita' che tenga conto della severita' delle vulnerabilita' e del valore degli asset impattati;
- Con CloudWALL DIR | Directory Services per garantire la gestione centralizzata degli utenti e dei gruppo, del loro ciclo di vita e del loro profilo autorizzativo rispetto all'accesso ai sistemi e alle applicazioni aziendali;

www.cloudwall.tk
info@cloudwall.tk

CLOUDWALL
SECURITY AS A SERVICE

A proposito di noi

www.cloudwall.tk
info@cloudwall.tk

CloudWALL Italia nasce su iniziativa di un team di professionisti con esperienze decennali nel mondo della Cyber Security che nel 2013 decidono di unire le proprie forze con lo scopo di supportare aziende e partner di canale nel cogliere le opportunita' offerte dalle moderne tecnologie in Cloud per realizzare nuove soluzioni e nuovi servizi ad alto valore aggiunto per la sicurezza del sistema informativo aziendale.

Grazie all'esperienza maturata in anni di "scouting" di nuove tecnologie e ad una profonda conoscenza del mercato delle tecnologie e delle soluzioni disponibili sul mercato mondiale, siamo stati tra gli "early adopter" di molte delle tecnologie di IT Security basate su Cloud oggi disponibili sul mercato e partecipiamo tuttora ai programmi di "beta testing" in collaborazione con i provider internazionali di servizi "cloud-based".

La nostra offerta e' costituita da un ampio portafoglio di soluzioni per garantire la sicurezza del sistema informativo aziendale, l'integrita' e la confidenzialita' dei dati e dei contenuti, la protezione dell'identita' degli utenti. Tutte le nostre soluzioni sono caratterizzate da una architettura centralizzata nel nostro Private Cloud e da un approccio "as a service" che non richiede investimenti iniziali e che garantisce tempi di messa in opera estremamente ridotti.

Grazie a queste caratteristiche, la nostra offerta e' caratterizzata da :

- Architettura centralizzata presso il nostro Private Cloud
- Modalita' di approccio totalmente "as a service"
- Tempi di rilascio e messa in opera estremamente ridotti
- Nessun investimento in hardware e software
- Nessun onere sistemistico e di conduzione operativa
- Costi limitati rispetto a soluzioni "on premise"
- Supporto da parte dei Security Engineer di CloudWALL Italia

Attraverso un'offerta ampia e modulare di soluzioni per la sicurezza del sistema informativo, dei dati e dell'identita' degli utenti, ad una architettura centralizzata nel nostro Private Cloud e ad un approccio totalmente "as a service", CloudWALL Italia e' l'interlocutore ideale per partner di canale, system integrator e fornitori di servizi IT interessati a sfruttare le potenzialita' offerte dalle nostre tecnologie per proporre ai propri clienti nuove soluzioni valore aggiunto e nuovi servizi gestiti in modalita' di Managed Service Provider (MSP) senza la necessita' di prevedere quegli investimenti iniziali in hardware, software, connettivita' e competenze specialistiche tipicamente richiesti per la realizzazione di soluzioni con un approccio "on premise".

Distribuito da

CLOUDWALL
SECURITY AS A SERVICE

CloudWALL Italia
I-20871 Vimercate (MB) | Via Stoppani 10
Phone +39.039.6852630 | Fax +39.039.6852630
www.cloudwall.tk | info@cloudwall.tk
Copyright 2014 Tutti i diritti riservati