

Soluzioni per la gestione dei LOG degli AdS

PREMESSA

La Sicurezza Informatica può essere definita come l'insieme delle misure (di carattere organizzativo e tecnologico) atte a garantire l'autenticazione dell'utente, la disponibilità, l'integrità e la riservatezza delle informazioni e dei servizi, gestiti o erogati in modo digitale.



Nella logica delle misure di prevenzione, il sistematico monitoraggio e controllo dei sistemi informatici nel loro complesso e degli utenti, costituisce una misura determinante.

L'imprevisto aumento di carico o un utilizzo inusuale di risorse da parte di un utente può essere il segnale di un possibile attacco. Due sono le tipologie di strumenti e le relative attività necessarie per tale tipo di prevenzione: il tracciamento e l'analisi dei log ed il monitoraggio sistematico di tutte le risorse hardware, software e di rete che compongono il sistema informatico.

Il provvedimento del Garante Privacy del 27 novembre 2008, ha introdotto l'obbligo per gli amministratori di sistema di conservare gli "access log" ai sistemi per almeno 6 mesi.

Gli "amministratori di sistema" sono figure essenziali per la sicurezza delle banche dati e la corretta gestione delle reti telematiche. Sono esperti chiamati a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali. Ad essi viene affidato spesso anche il compito di vigilare sul corretto utilizzo dei sistemi informatici di un'azienda o di una pubblica amministrazione.

Per questo il Garante ha deciso di richiamare l'attenzione di enti, amministrazioni, società private sulla figura professionale dell'amministratore di sistema e ha prescritto l'adozione di specifiche misure tecniche ed organizzative che agevolino la verifica sulla sua attività da parte di chi ha la titolarità delle banche dati e dei sistemi informatici. Sotto il profilo tecnologico, "devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema". Server e anche i client, intesi come "postazioni di lavoro informatizzate",

sono compresi tra i sistemi per cui devono essere registrati gli accessi degli AdS.

LE CARATTERISTICHE DELLA SOLUZIONE

EventLog Analyzer

Soluzione web based per l'analisi e l'archiviazione dei log

EventLog Analyzer, è una soluzione web-based ed agentless per la gestione dei syslog e degli event log.



Il sistema raccoglie, analizza, archivia e genera report sugli Event Log generati da host Windows e Syslog da hosts UNIX, Router & Switches ed altri dispositivi.

Grazie a EventLog Analyzer, è possibile controllare, gestire e archiviare le migliaia di eventi che vengono generati dai dispositivi di vari tipi di reti.

Dalla console web gli amministratori di sistema possono generare dettagliati report sugli accessi ai sistemi - per ottemperare agli obblighi delle normative - e identificare modifiche di configurazioni, errori di sistema e violazioni di sicurezza.

Funzioni principali

Supporto per sistemi Windows, UNIX e dispositivi di rete.

Reports predefiniti in base agli host o agli eventi.

Reports specifici richiesti dalle normative GLBA, HIPAA, PCI, SOX e legge sulla privacy

Notifiche ed Alert basati su regole

Analisi dei log per la sicurezza

Possibilità di schedulare la generazione e l'invio dei report

Esportazione report in diversi formati.

Soluzioni per la Sicurezza Informatica

EventLog Analyzer Editions

Features	Professional Edition	Premium Edition
Multiple OS Support	✓	✓
Monitored Device Support (Windows, Linux, Unix, AIX, Routers, Switches, Any Syslog device)	✓	✓
Import and Analyze Evt files	✓	✓
Auto Discovery of Hosts	✓	✓
Filter Events before Storing in Database	✓	✓
Compressed Archives	✓	✓
Real-time Display of Events	✓	✓
Automated Alerts	✓	✓
Authorized Access	✓	✓
Host Grouping for Policy Implementation	✓	✓
Schedule Data Collection	✓	✓
Custom Reports	✓	✓
Scheduling Reports	✓	✓
Instant Reports	✓	✓
Multiple Report Formats	✓	✓
Multi-level Drilldown	✓	✓
Trend Analysis	✓	✓
Security Analysis	✓	✓
Compliance Reports (Predefined and	✓	✓

Customization)		
Command Execution on Alerts	✓	✓
SMS and SNMP Trap Notification for Alerts	✓	✓
Internationalization Support to handle Native Logs	✓	✓
Export/Import of Alert, Report, and Filter Profiles	✓	✓
Advanced Search in Raw Logs, Save Result as Report Profile	✓	✓
Analyze Application specific Logs		✓
Support for SQL Server as Backend Database		✓
Custom View & User based Views		✓
Active Directory based Authentication		✓
IBM AS/400 History Logs Analysis		✓

Professional Edition	<ul style="list-style-type: none"> • Regular edition with standard features required for SIM. • Manages event logs & syslogs from licensed number of hosts. • Hosts include Windows, Unix, Routers, Switches, and any syslog device.
-----------------------------	---

Soluzioni per la Sicurezza Informatica

Premium Edition	<ul style="list-style-type: none">• Premium edition is packed with value added features.• Plus the regular features of Professional edition.• Refer Know the difference document for details
------------------------	--

CONDIZIONI TECNICHE

Installazione e configurazione di base di un server ManageEngine EventLog Analyzer, su piattaforma windows.

DETTAGLIO ATTIVITA'

1. Installazione ManageEngine EventLog Analyzer premium o professional edition, su piattaforma windows
2. Configurazione di base del Server
3. Test di accesso console web
4. Configurazione per la raccolta dei log di un campione di host (max 10.) Gli host devono essere presenti nella lista di quelli supportati, devono essere raggiungibili e devono essere rispettati i prerequisiti di rete, e sono necessari le credenziali di amministrazione locale.
5. L'attività verrà concordata con il cliente e verrà erogata durante il normale orario di lavoro (lun/gio 9-13,14-18 e ven 9-13,14-17 - sono escluse le chiusure aziendali)
6. Sono escluse da questo servizio personalizzazioni del software, definizione allarmi, personalizzazioni di report etc.

PREREQUISITI

- Sarà cura del cliente preparare gli ambienti prima dell'inizio del servizio, in base alle specifiche fornite preventivamente dal supporto tecnico Scp (requisiti HW /SW, patch e aggiornamenti, specifiche sulla configurazione della rete, firewall, proxy etc.) I prerequisiti HW/SW richiesti sono quelli dichiarati dal produttore.
- sono richiesti permessi di amministrazione sulle macchine dove verrà eseguita l'installazione.
- Prima di erogare il servizio il supporto tecnico Scp potrebbe richiedere al cliente alcune verifiche/informazioni tramite una checklist. Sarà cura del cliente eseguire le verifiche e fornire le informazioni richieste.

- Il cliente dovrà aver eseguito il back-up di tutti i sistemi coinvolti (server, client, apparati di rete etc.), e se necessario dovrà operare il restore.

Responsabile soluzioni Privacy, è la Dott.ssa Cinzia Cassiadoro (Tel. 0437 938444 - Fax 0437930045 - privacy@scponline.it), mentre il Responsabile delle soluzioni Sicurezza Informatica, è l'ing. **Carlo Bettio** (Tel. 0437 938444 - Fax 0437930045 - sicurezza@scponline.it).

Se siete interessati contattate il commerciale di riferimento ai seguenti recapiti:



Pierpaolo De Paris *servizi commerciali*

p.deparis@scponline.it

Mobile: 39 338 5950163

Scp srl

Sede centrale: via Vittorio Veneto 274 - 32100 Belluno tel. 0437 938.444 fax 0437 930.045 e-mail: info@scponline.it

Ufficio di Treviso: viale della Repubblica 19/B - 31020 Villorba (TV) tel. 0422 308.803 fax 0422 301.006 e-mail: infotv@scponline.it

PEC: scpsrl@legalmail.it

www.scponline.it

Reg. Imprese BL - C.F. e P.I. 00524890258
REA 0056750 - Cap. Soc. € 50.000,00 i.v.
Azienda certificata UNI EN ISO 9001