SIELCO
PERSONALIZZIAMO L'INFORMATICA

SERVICE DESCRIPTION
LOG MANAGEMENT
Ver. 2.0 del 27/06/2022

SOMMARIO

1.Descrizione generale e condizioni di servizio
2.Avviamento del servizio
3.Gestione e mantenimento del servizio
4. Dismissione del Servizio - Recesso
5. SLA
6. Note & Informazioni Aggiuntive

1. DESCRIZIONE GENERALE

Il servizio di Log Management prevede la raccolta dei log dagli endpoint del cliente (p.e. server, switch, firewall, router, NAS, ecc...). tramite agenti e/o collettori locali (JumpBox), e l'invio in modo sicuro alla console multi-tenant in cloud. Quest'ultima si occupa di conservare i log in modo sicuro e conforme alle normative vigenti, inoltre permette la consultazione ed esportazione degli stessi da parte del cliente o di personale terzo autorizzato (p.e. DPO, Auditors, ecc...).

Sono previste due tipologie di servizio:

ADS => Focalizzato nella raccolta dei log di accesso degli amministratori di sistema e prevede la definizione di una lista di utenze in accordo con il cliente.

SIEM => Si estende alla raccolta di qualunque tipo di log, secondo i livelli di servizio previsti, e senza alcun filtro sulle utenze.

N.B. La retention minima dei log è di 183 giorni, mentre la retention massima è di 365 giorni.

Le finalità del servizio SIEM (Security Information and Event Management) possono andare dalla sicurezza informatica all'identificazione di anomalie dei sistemi di produzione, all'indagine in caso di incidenti, fino all'implementazione di sistemi automatizzati di risposta o avviso al verificarsi di particolari eventi riconosciuti attraverso l'analisi e la correlazione dei log.

Tipologia di servizio	Livello di servizio	Tipo di log	Quantità media per Endpoint
ADS	Basic	Log di accesso	2 GB/anno
SIEM	Standard	Log di accesso, log di sistema	5 GB/anno
SIEM	Advanced	Log di accesso, log di sistema, log applicativi	10 GB/anno
SIEM	Premium	Log di accesso, log di sistema, log applicativi e di altro tipo	20 GB/anno

N.B. Tutti i servizi private cloud di Sielco di tipo IaaS, Hosting e Housing includono il servizio di Log Management ADS. Il cliente ha sempre la possibilità di richiedere una quotazione per attivare il servizio SIEM.

STRATEGIE E REQUISITI PER LA RACCOLTA DEI LOG

La raccolta dei log può seguire uno dei tre approcci elencati di seguito, anche sulla base degli accordi contrattuali:

- Inoltro degli eventi nativo (agentless), nel quale un sistema inoltra direttamente i propri log e/o eventi verso la console (per esempio, il syslog Linux).
- Inoltro degli eventi tramite agent, che implica l'installazione di un agent sul sistema per raccogliere e inoltrare i log e/o gli eventi verso la console.
- Raccolta esplicita degli eventi, che inverte la direzione del sistema: un sistema di raccolta eventi esterno che ha accesso diretto a un sistema monitorato effettua accesso esplicito ed estrapola direttamente i log e/o eventi rilevanti in autonomia, periodicamente.

N.B. Un sistema che non ricada in nessuna di queste tre categorie non potrà essere collegato al SIEM, né essere oggetto di monitoraggio diretto.

Inoltre, una delle seguenti tre condizioni deve sussistere:

- Un sistema deve avere accesso diretto alla console cloud, per poter inoltrare i propri eventi e/o log.
- Un sistema deve avere accesso diretto alla console cloud tramite un network di servizio (per esempio, un canale VPN), per poter inoltrare i propri eventi e/o log.
- Un sistema deve avere accesso a una jumpbox configurata localmente, per poter inoltrare i propri eventi e/o log alla console cloud.

CERTIFICAZIONE E CIFRATURA

Tutti gli eventi e log ritenuti dal servizio evolvono attraverso una serie di fasi:

1. Certificazione, la prima fase, durante la quale il log grezzo (o "raw") viene crittograficamente certificato. I meccanismi di certificazione, che utilizzano algoritmi crittograficamente sicuri, possono variare a seconda della tipologia di dati e del contesto operativo.

2. Indicizzazione, step durante il quale il log viene scomposto nelle sue particelle, per convertirlo in un documento consultabile in formato simil-JSON.
3. Cifratura, fase in cui il documento finale, costituito di raw e simil-JSON, viene compresso e protetto tramite algoritmi crittografici asimmetrici.

2. AVVIAMENTO DEL SERVIZIO

Le fasi di avviamento del servizio sono tipicamente:
- Definizione degli asset da monitorare (endpoint e utenze), tipologia di servizio (ADS/SIEM), e relativi livelli di servizio (Basic/Standard/Advanced/Premium).
- Nomina di SIELCO come responsabile esterno al trattamento dati.
- Configurazione tenant dedicato al cliente.
- Deploy dei collettori (tipicamente uno per sede geografica).
-Deploy degli agenti per sistemi Windows/Linux/MacOSX.
- Configurazione syslog per sistemi Linux/Unix o dispositivi di rete.
- Collaudo raccolta log.
- Configurazione regole di correlazione predefinite (solo per SIEM).
- Configurazione dashboard, alert e report predefiniti (solo per SIEM).
- Configurazione utenza di accesso alla console via web e istruzione del personale preposto alla verifica dei log (solo per SIEM e se richiesto dal cliente).

3. GESTIONE E MANTENIMENTO DEL SERVIZIO

Il team di SIELCO, sulla base di consolidate best practices, verifica continuamente lo stato di aggiornamento dei sistemi e dei software utilizzati e mantiene le proprie infrastrutture aggiornate alle ultime versioni supportate dal Servizio.
Questo processo di aggiornamento continuo avviene, in condizioni normali, senza causare disservizi, tuttavia, in concomitanza di eventi rilevanti, potrebbero essere necessari:
1. Interventi di manutenzione straordinaria, che potranno comportare disservizi, e verranno concordati non meno di quarantotto ore prima della loro esecuzione.
2. Interventi di manutenzione di emergenza, che potranno comportare disservizi, e verranno annunciati non meno di trenta minuti prima della loro esecuzione.
A titolo puramente esemplificativo, la pubblicazione di una vulnerabilità zero day critica per le infrastrutture del Servizio va a configurarsi come evento rilevante, e potrebbe richiedere manutenzione straordinaria o di emergenza.
N.B. Gli agenti/collettori locali, quando non riescono a contattare la console in cloud, mantengono i log in una cache locale per poi inviarli quando la comunicazione ritorna disponibile. La cache ha comunque una capacità limitata.

IMPORTANTE

Il cliente è tenuto a comunicare tempestivamente la variazione delle utenze da loggare.

CHANGE MANAGEMENT

Nel corso della vita del servizio, le necessità operative possono evolversi e variare. A titolo puramente esemplificativo, un aggiornamento di sicurezza su un apparato di rete potrebbe portare lo stesso a produrre log di formato differente rispetto a quanto precedentemente raccolto, richiedendo una modifica alla configurazione del sistema di Log Management.
Casistiche come questa rientrano nelle logiche evolutive del change management, componente del servizio che ha a che fare con l'evoluzione dei meccanismi di ingestione e analisi dei log.
Rientrano nell'area di competenza del change management le seguenti attività:
- Creazione di una regola di correlazione.
- Modifica di una regola di correlazione.
- Eliminazione di una regola di correlazione.
- Aggiunta di una sorgente di log.
- Modifica di una sorgente di log.
- Eliminazione di una sorgente di log.
- Aggiunta di un meccanismo di log parsing.
- Modifica di un meccanismo di log parsing.
- Rimozione di un meccanismo di log parsing.
N.B. Tutti i livelli di servizio includono un pacchetto di tre change all'anno per endpoint, calcolate sul numero complessivo degli endpoint.

4. DISMISSIONE DEL SERVIZIO – RECESSO

Il Cliente dovrà comunicare tramite PEC la propria volontà di recesso dal Servizio entro il giorno 15 del mese corrente, impegnandosi a pagare la mensilità in corso. Il recesso decorre dall'inizio del mese successivo.
La dismissione del Servizio prevede:
- Disattivazione del sistema di raccolta log (agenti e collettori).
- Eliminazione del tenant del cliente e relative configurazioni.
- Cancellazione immediata dei dati e/o esportazione su supporto cifrato fornito dal cliente.

Tutto il materiale di proprietà di SIELCO, fornito in ambito di Servizio, deve essere restituito integro e perfettamente funzionante entro 10 giorni lavorativi dall'efficacia del recesso tramite corriere a spese del Cliente.

5. SLA

Il sistema di Log Management è attivo 24x7 ed è in gradodi generare ticket di incident nel caso dimalfunzionamento di uno dei suoi componenti(console/collettori/agenti). Il personale di SIELCOgestisce tali segnalazioni tramite presidio da lunedì avenerdì, nelle fasce orarie 8:00-12:30 e 14:00-17:30, conpresa in carico entro 4 ore e definizione entro 8 ore.
Anche le service request (p.e. consultazione o esportazione log), vengono gestite tramite portale di ticketing con le stesse modalità, mentre le change request vengono analizzate ed evase in modalità best effort.

6. NOTE & INFORMAZIONI AGGIUNTIVE

Per informazioni aggiuntive dettagliate si rimanda alla sessione "Documenti a corredo" presente sul sito SIELCO alla pagina
https://sielco.it/condizioni_contrattuali/
SIELCO si impegna a restituire eventuali asset (materiali o immateriali) del cliente, detenuti al fine di erogare il servizio, entro 30 giorni dalla cessazione dello stesso. Il costo di spedizione è a carico del cliente.

Data _____

Firma per accettazione _____