SERVICE DESCRIPTION
LOGGING
Ver. 1.1 - Aggiornamento del 20/11/2021

Sommario

1.	Descrizione generale e condizioni di servizio	4.	Dismissione del servizio/Recesso
2.	Avviamento del servizio	5.	SLA
3.	Gestione e mantenimento del servizio	6.	Informazioni aggiuntive & Restituzione degli asset

1. Descrizione generale

Il servizio di logging prevede la raccolta log dagli asset del cliente (p.e. server, switch, firewall, router, NAS, ecc...). tramite un collettore locale che ha il compito di normalizzare i dati in ingresso, comprimerli e cifrarli prima dell'invio alla console. Quest'ultima può essere installata sia in locale che in cloud e 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...).

Definizione elenco utenze da loggare (solo per servizio standard).
Il servizio standard è focalizzato nella raccolta dei log di accesso degli amministratori di sistema (ex DL196), mentre il servizio SIEM (Security Information and Event Management), può essere esteso alla raccolta di ogni tipologia di log, anche quelli applicativi, e senza alcun filtro sugli utenti, previa autorizzazione esplicita da parte del cliente.
Le finalità del servizio SIEM 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 in caso di particolari eventi.

Tutti i servizi private cloud di Sielco di tipo IaaS, Hosting o anche Housing includono il logging standard. Il cliente ha sempre la possibilità di richiedere una quotazione per attivare il servizio SIEM e configurare delle regole di correlazione con le relative azioni (p.e. notifica via mail, esecuzione di script, ecc...).
Requisiti:
1)Il cliente deve essere in possesso delle credenziali amministrative di tutti gli apparati coinvolti nel servizio e deve poterli configurare secondo le specifiche che verranno fornite (ES: attivare il protocollo SNMP sugli apparati di rete.)
2)Nel caso di logging ad apparati on-prem, deve essere presente una linea internet adeguata al traffico dei log (dipendente dal numero degli apparati e dei log)
3)Nel caso di logging di apparati on-prem deve essere permesso l'accesso verso i server SIELCO che collezionano i log

2. Avviamento del servizio

Le fasi di avviamento del servizio sono tipicamente:
- Definizione dei sistemi da monitorare e tipologia del servizio (Standard/SIEM)
- Nomina come responsabile esterno al trattamento dati
- Configurazione tenant dedicato al cliente
- Deploy dei collettori (tipicamente uno per sede geografica)
- Deploy degli agenti (solo per sistemi windows)
- Configurazione syslog per sistemi linux/unix o dispositivi di rete
- Test ricezione log
- Definizione e test regole di correlazione (solo per SIEM e se richiesto dal cliente)
- Creazione di un utenza per l'accesso alla console via web
- Istruzione del personale del cliente preposto alla verifica dei log
- Le utenze create per accedere al portale di gestione dei log non avranno privilegi amministrativi.

3. Gestione e mantenimento del servizio

Il personale SIELCO eseguirà le seguenti attività periodiche:

- Aggiornamento del sistema di logging secondo le best practice del vendor
- Monitoraggio del sistema di logging
- Revisione delle regole di correlazione (se previsto dall'offerta commerciale)

N.B. Le attività di manutenzione verranno eseguite principalmente senza dare disservizi, tuttavia, potrebbe essere necessario concordare delle fasce di manutenzione straordinaria, per gestire le attività che rendano necessario un disservizio programmato.
Gli agenti, quando non riescono a contattare la console in cloud, salvano i log in una cache locale e poi li inviano quando torna disponibile il sistema.
La cache ha comunque una capacità limitata.
Il cliente è tenuto a comunicare la variazione delle utenze da loggare.

(segue)

SERVICE DESCRIPTION
LOGGING
Ver. 1.0 del 02/07/2020

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 - cancellazione delle configurazioni - disinstallazione degli agenti (se presenti) - cancellazione dei dati e/o esportazione su supporto cifrato Tutto il materiale di proprietà di SIELCO fornito in ambito del Servizio deve essere restituito integro e perfettamente funzionante entro 10 giorni lavorativi dall'efficacia del recesso, a mezzo corriere, a spese del Cliente. Qualora il Cliente non provvedesse alla restituzione del materiale di proprietà SIELCO, la stessa si riserva ogni	***5. SLA*** Il sistema di monitoraggio è attivo 24x7 ed è in grado di generare ticket di incident nel caso di malfunzionamento della console in cloud. SIELCO gestisce le segnalazioni generate, tramite presidio da lunedì a venerdì, nelle seguenti fasce orarie 8:00-12:30 e 14:00-17:30. Il personale SIELCO monitora la console, ma è onere del cliente segnalare se l'agente non sta inviando i log segnalando al personale se è una situazione eccezionale e sulla quale si deve intervenire o se è una situazione normale dovuta alla manutenzione dei sistemi.Il cliente ha la possibilità di sottoscrivere il servizio ISRC per monitorare lo stato degli agenti. ***6. Informazioni aggiuntive & Restituzione degli asset*** 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.