CASE STUDY SI COLLECTION

PIATTAFORMA SGBOX
NEXT GENERATION SIEM & SOAR

PROFILO AZIENDALE

Si Collection S.p.A. è una delle realtà più consolidate nel mercato italiano per i servizi di "Credit Management" conto terzi, con oltre 30 anni di esperienza nel settore.

L'azienda rappresenta un punto di riferimento per Istituzioni Finanziarie, Investitori, Banche, Compagnie Assicurative, Pubbliche Amministrazioni e Utility.

L'ESIGENZA

Si Collection opera su un **ecosistema applicativo articolato**, composto da un **gestionale storico (legacy)** e dal nuovo **ERP Laweb4**, entrambi utilizzati per la gestione dei processi core di servicing e valorizzazione del credito.

A supporto delle attività di analisi e controllo di gestione, l'azienda utilizza inoltre diversi applicativi dedicati a specifiche esigenze, come **piattaforme di business intelligence e portali applicativi**.

La criticità di tali sistemi, sia in termini operativi sia in relazione al trattamento dei dati personali, ha reso necessario adottare un **approccio strutturato alla raccolta e alla conservazione dei log**, in linea con i requisiti del **GDPR** e con le indicazioni del **Garante della Privacy**.

Oltre agli aspetti di compliance normativa, l'azienda avvertiva la necessità di dotarsi di una soluzione in grado di assicurare un **monitoraggio continuo delle attività sospette e dei potenziali disservizi applicativi**.

> **Si Collection è pienamente soddisfatta della piattaforma SGBox e del servizio di Managed Services offerto da SecureGate.**
>
> **La qualità della soluzione, unita a un supporto continuo e competente, ci ha permesso di innalzare il livello di controllo sulla sicurezza e sulla continuità operativa, rendendo il SIEM un asset strategico a supporto della compliance e della gestione del rischio.**
>
> **I risultati ottenuti hanno confermato la validità dell'investimento, portandoci ad ampliare ulteriormente le risorse dedicate a questa iniziativa.**

info@sgbox.eu
www.sgbox.eu
Via Melchiorre Gioia 168, Milano

Considerata la dimensione del team IT interno e il profilo di rischio, Si Collection ha individuato nella piattaforma SIEM SGBox una valida alternativa funzionale a un Security Operation Center (SOC) tradizionale, capace di offrire visibilità centralizzata, alerting proattivo e supporto nell'individuazione tempestiva di anomalie o incidenti di sicurezza.

SOLUZIONE IMPLEMENTATA

Oltre alla raccolta centralizzata dei log, è stato attivato un sistema di **monitoraggio su specifiche pagine web applicative**, in modo da ricevere notifiche automatiche in caso di anomalie o problemi di funzionamento.

Nel corso del progetto, **Si Collection ha esteso la licenza della piattaforma SGBox da 10 a 25 data source**, integrando nuovi sistemi individuati come ad alto rischio in relazione alla tipologia dei dati trattati e alla loro criticità operativa.

Questa scelta si inserisce in un percorso di rafforzamento del profilo di sicurezza aziendale, ulteriormente consolidato con l'ottenimento della **certificazione ISO 27001 nel 2025**.

L'obiettivo dell'estensione non è stato esclusivamente l'aumento del numero di sorgenti monitorate, ma l'**ampliamento strategico del perimetro di controllo**, includendo anche sistemi esterni all'infrastruttura IT tradizionale.

In questo contesto rientra il progetto di integrazione di asset esterni, come il pannello di gestione dell'antivirus AVG e la console di sicurezza di Google.

FUNZIONALITA' SGBOX

- **Log Management**: raccolta centralizzata e conservazione dei Log in linea con i requisiti del **GDPR** e del **Garante della Privacy**.
- **Correlazione e alerting**: l'analisi approfondita degli eventi provenienti da diverse fonti permette di individuare proattivamente comportamenti anomali o potenziali incidenti di sicurezza.
- **Active Directory Auditor:** monitoraggio centralizzato degli eventi legati alla gestione delle utenze nella rete Windows.
- **Managed Service:** configurazione evolutiva della piattaforma, grazie ad una collaborazione continua con incontri mensili dedicati al fine-tuning dell'applicativo. Analisi degli aggiornamenti di versione, valutazione delle nuove funzionalità disponibili e definizione delle modalità più efficaci per la loro applicazione nel contesto specifico di Si Collection.

VANTAGGI E RISULTATI OTTENUTI

Grazie all'implementazione delle componenti di Log Management e Active Directory Auditor, Si Collection ha potuto **raccogliere e centralizzare i dati di sicurezza dei dispositivi aziendali in piena conformità con le normative sulla privacy**.

La raccolta dei log ha inoltre permesso di ottenere una **visione in tempo reale sullo stato di sicurezza della rete**, con un monitoraggio avanzato degli accessi degli utenti.

Un ulteriore vantaggio concreto riguarda il **monitoraggio della disponibilità delle applicazioni web**.

SGBox consente infatti di rilevare situazioni di disservizio non solo sulla base della raggiungibilità dell'infrastruttura, ma anche **analizzando il contenuto delle pagine di risposta degli applicativi**.

Questo approccio permette di intercettare malfunzionamenti applicativi **anche quando l'"application server" risulta operativo**, integrando e completando le funzionalità degli strumenti di monitoraggio già presenti in azienda.

L'approccio evolutivo garantito dal servizio di Managed Services, basato su incontri periodici di ottimizzazione e sull'adozione di best practice di sicurezza, ha contribuito ad **aumentare l'efficacia del sistema di alerting e a migliorare i tempi di reazione agli eventi rilevanti**.

> **I benefici ottenuti hanno portato Si Collection ad ampliare le risorse economiche dedicate alla piattaforma e al servizio, riconoscendone il valore strategico all'interno del proprio modello di governance IT e di sicurezza.**

SVILUPPI E SCENARI FUTURI

Si Collection intende proseguire nel percorso di evoluzione della piattaforma SGBox, ampliando e affinando progressivamente il perimetro delle sorgenti monitorate, con un focus sempre maggiore sulle **funzionalità di correlazione e alerting.**

Tra i prossimi sviluppi è prevista **l'integrazione dei log provenienti dalla piattaforma di protezione endpoint AVG** e dalla **console di sicurezza di Google**, con l'obiettivo di **arricchire il contesto informativo** e migliorare la capacità di **individuare tempestivamente comportamenti anomali o potenziali incidenti di sicurezza**.

A seguito dell'estensione della licenza, è inoltre prevista l'integrazione dei log relativi alle connessioni VPN del personale interno, dei consulenti e dei fornitori IT, gestite dal firewall del Cloud provider di SI Collection.

Questa integrazione consentirà di **arricchire le regole di correlazione già esistenti** e di **affinare ulteriormente i meccanismi di alerting**, con particolare attenzione all'individuazione di pattern di accesso anomali o non coerenti con i profili abituali degli utenti, come connessioni da località inattese o in orari non lavorativi.

Tali sviluppi si inseriscono in una strategia di miglioramento continuo della sicurezza informatica, in cui **la piattaforma SIEM assume un ruolo sempre più centrale** non solo per la compliance normativa, ma anche come **strumento di supporto proattivo** alla prevenzione dei rischi e alla continuità operativa.