SGBOX

CASE STUDY AIL AZIENDE INDUSTRIALI LUGANO

PIATTAFORMA SGBOX
NEXT GENERATION SIEM & SOAR

PROFILO AZIENDALE

Aziende Industriali Lugano (AIL) è il più importante distributore al dettaglio e all'ingrosso di acqua, gas naturale ed energia elettrica del Canton Ticino. I loro prodotti e servizi sono acquistati quotidianamente da oltre 110000 clienti privati e aziendali, distribuiti in circa 54 Comuni.

AIL costruisce e gestisce le reti necessarie al trasporto dei prodotti dal punto di produzione o di acquisto fino al cliente.

L'ESIGENZA

L'infrastruttura di sicurezza di AIL è composta da molteplici dispositivi che generano un gran numero di log, informazioni importanti che devono essere conservate e gestite centralmente.

AIL era alla ricerca di una soluzione da utilizzare internamente per raccogliere e analizzare tutti i log generati dagli apparati di rete, dalle applicazioni web, dai data source e dai dispositivi OT (Operational Technology).

In passato il cliente aveva eseguito dei test con prodotti concorrenti ad SGBox, ma non aveva trovato la soluzione più idonea per via della difficoltà di adattamento all'infrastruttura IT e OT esistente.

La scelta è ricaduta su SGBox per la flessibilità della piattaforma e per la capacità di ottenere una visione centralizzata e immediata sullo stato di sicurezza aziendale.

> **Dopo attente analisi abbiamo scelto SGBox quale partner ideale che avrebbe potuto facilmente integrarsi con i nostri sistemi. Si è rivelata essere una piattaforma di log aperta in grado di raccogliere le informazioni provenienti da qualsiasi tipologia di sistema. È di facile utilizzo e rapida implementazione ed è compatibile con tutte le infrastrutture di sicurezza IT.**
>
> **Michele Rusconi - Responsabile dell'Unità Servizi IT/OT e Cybersicurezza**

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

> **Il team di SGBox ha realizzato un assessment approfondito e ci ha affiancato in tutta la fase di start-up e implementazione della soluzione, tenendo conto delle nostre specifiche esigenze.**
>
> **Michele Rusconi - Responsabile dell'Unità Servizi IT/OT e Cybersicurezza**

APPROCCIO

Il team di SGBox, dopo aver eseguito diverse analisi preliminari per la configurazione di circa 250 data source, ha dato il via alla fase di sviluppo di un sistema ad hoc affiancando il reparto IT di AIL.

Il punto di partenza è stata la creazione di regole di correlazione, che hanno permesso al cliente di identificare diversi comportamenti sospetti/malevoli tramite tecniche del MITRE ATT&CK.

Terminata la fase di on-boarding, AIL ha potuto proseguire l'implementazione in autonomia grazie alla facilità di configurazione e alla flessibilità di SGBox nel riconoscimento delle sorgenti.

FUNZIONALITA' IMPLEMENTATE

- **Gestione avanzata dei Log**: raccolta, normalizzazione e gestione avanzata di tutti i log provenienti dai data source.
- **Playbook SOAR di SGBox**: a fronte di un IP malevolo, è possibile bloccarlo sul firewall utilizzando le funzionalità SOAR di SGBox adattandosi alle esigenze specifiche, una su tutte la notifica attraverso l'app di messaggistica svizzera "Threema".
- **Funzione Template**: funzione utile per estrarre informazioni in seguito ad una potenziale minaccia, che permette di produrre report e audit di sicurezza facili da interpretare.

VANTAGGI

La soluzione implementata da SGBox ha permesso ad AIL di poter usufruire di una soluzione pronta all'uso per la gestione delle informazione di sicurezza di un gran numero di dispositivi.

Questo ha permesso di ottenere una visione in tempo reale sullo stato di sicurezza aziendale e di poter individuare proattivamente le minacce prima che si verifichino, un fattore determinante per mantenere la continuità operativa.

SCENARI FUTURI

Il cliente sta continuando ad utilizzare la soluzione SGBox e ha espresso la volontà di implementare anche la funzione di Incident Management, per trasformare gli alert generati dalle regole di correlazione non solo in avvisi tramite e-mail, ma in allarmi veri e propri da gestire tramite l'IM (Incident Management).

Il team SGBox si è messo a disposizione per svolgere un corso di formazione specifico, attraverso il quale AIL ha potuto acquisire le competenze tecniche fondamentali per sfruttare autonomamente il potenziale della piattaforma.

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