**CYBEROO**

**Si prega di compilare la scheda rispettando il limite massimo di 5000 caratteri, spazi inclusi**

Descrizione della problematica o del bisogno nell'azienda o pubblica amministrazione utente.

## Cliente

Il cliente è una multinazionale con 13 sedi in tutto il mondo, con un fatturato superiore ai 24M€ ed EBITDA di circa 8M€.

Il cliente ha complessivamente circa 1200 postazioni di lavoro informatizzate, ha HQ italiano e magazzini e sedi produttive nella maggior parte dei sedi nel mondo.

Il cliente progetta e produce prodotti rivolti ai clienti finali. Questo fa sì che il brand sia particolarmente conosciuto e ad esso sia posta molta attenzione in diversi paesi del mondo.

Nella sede Italiana il cliente ha adottato una sonda di rete per gestire la Cyber Security. Tale sonda ha la visibilità di una sola porta del firewall il cui traffico viene inviato mediante una SPAN port.

## Esigenza

Nel tempo il cliente ha subito diversi attacchi: phishing, domini clone, infezione da malware. Nei casi più gravi sono avvenuti pagamenti errati dovuti ad attacchi di phishing.

Le principali esigenze del cliente raccolte in fase di analisi erano:

- Necessità di una visione completa del dominio cyber delle sedi nel mondo, compresa la sede HQ per la quale la visibilità del solo perimetro, mediante la sonda preesistente, non era più considerata adeguata.

- Trovare una soluzione che distribuita nel mondo mantenesse sotto controllo i costi. L'installazione della singola sonda in ogni sede era, per esempio, stata considerata troppo onerosa
- Trovare una soluzione che permettesse un controllo più granulare di ciò che succede ai client, migliorativo rispetto alla soluzione di Threat Hunting in uso.
- Necessità di comprendere quando vengono generati domini clone in preparazione ad attacchi di phising.
- Avere un servizio in grado di chiudere autonomamente i domini clone nel caso vengano creati.

Descrizione della soluzione tecnologica (tecnologie usate, architettura, ecc.).

La soluzione proposta per rispondere alle esigenze del cliente è stata la Cyber Security Suite di Cyberoo nel range 1000-2000 (calcolato come numero di postazioni di lavoro sommato al numero dei server presenti nelle sedi).
La Cyber Security Suite si compone di due soluzioni definite XDR e Threat Intelligence a cui si aggiunge l'analisi dell' iSOC (il nostro team di specialisti ed Hacker Etici) con livello di servizio h24.

Descrizione del progetto di implementazione - complessità, tempi, aspetti organizzativi, costi, ecc.

L'approccio adottato è stato quello di procedere con lo studio di integrazione che permette di raccogliere le informazioni di tutte le sedi nel mondo mediante opportune checklist predeterminate.
Il cliente ha deciso di sostituire in tutte le sedi la soluzione d Threat Hunting con l'agente nativo della Cyber Security Suite poiché ne migliorava la visibilità e ne garantiva ugualmente il livello di protezione e di auto-remediation.
In meno di 2 mesi il cliente ha ottenuto la Cyber Security Suite completamente installata in tutte le sedi, così come definito in fase di studio di Integrazione.
L'attivazione, sui client e sui server, del Cyber Security Suite Client è stato svolto mediante GPO ed è stato dato mediante un invio massivo una sede alla volta ottenendo una installazione globale in pochi giorni.

Descrizione dei principali benefici raggiunti dall'azienda o pubblica amministrazione utente.

Il cliente convenuto che la Cyber Security Suite era la soluzione completa che aspettava da tempo per poter implementare la cyber security della propria infrastruttura.

In particolare i risultati ottenuti durante l'attivazione della soluzione sono stati:

- La soluzione ha permesso di vedere raccolte in una unica dashboard tutte le informazioni delle sedi. In particolare è stata attivata la modalità multitenant che ha permesso al personale IT dell'HQ di vedere separatamente ogni singola sede e al personale IT delle single sedi di vedere solo i propri dati.
- L'attivazione della soluzione ha permesso di rilevare un dominio malevolo che in poche ore è stato fatto chiudere evitando così il protrarsi di un attacco di phishing.

Nel corso dei primi sei mesi di utilizzo, fra le varie attività svolte dall'iSOC di Cyberoo, le attività più rilevanti risultano essere l'aver permesso di:

- Sventare un attacco tentato mediante un Cryptolocker che non è stato attivato.
- Sventare un attacco di tipo Man in the Middle che è stato bloccato nel tentativo di attivare una rule di automatic forwarding nella posta di un utente dell'amministrazione
- Rilevare credenziali di alcuni utenti all'interno di un recente databreach

Descrizione degli elementi distintivi e di reale innovatività/originalità della soluzione, anche con riferimento a soluzioni «concorrenti».

· Visione d'insieme delle minacce "Interne" ed "Esterne".

· Piattaforma in grado di "ingerire" e normalizzare i dati provenienti da fonti eterogenee.

· Integrazione agnostica di servizi terzi tramite API (è sufficiente che producano log in serie storica)

· Threat Intelligence automatizzata, tramite crawler che scandagliano fonti nel deep e dark web.

· Eliminato il 1° livello del SOC tramite Intelligenza Artificiale che filtra gli alert ed evita falsi positivi.