Wiit S.p.A. – Cyber Threat Intelligence

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

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

Azienda Cliente: Primario studio legale internazionale

Il cliente è uno studio legale internazionale con sedi in Italia, EU, UK Medio Oriente ed Africa: costituisce con più di 700 collaboratori uno dei "top legal" europei. Gli ambiti di attività coprono le principali aree di settore (M&A, finance e bancario, regulation,fiscale, contenzioso, IT e privacy, ecc.) con una particolare attenzione al settore dell'innovazione attraverso una società creata appositamente per lo sviluppo e l'applicazione delle soluzioni più innovative nel settore legal.
L'esigenza primaria del cliente è stata quella di individuare una soluzione facile, immediata ed efficace che permettesse di raccogliere informazioni di intelligence relative a minacce di tipo cyber o di reputazione correlabili al cliente, utilizzando come sorgente anche il "dark web" ed il "deep web". La soluzione ha come obiettivo quello di contestualizzare le cyber-minacce rilevate, assegnando un grado di priorità, criticità e di mettere a disposizione le opportune e più adeguate contromisure (automatiche o attivabili su richiesta) atte a contrastare o eliminare la minaccia stessa in tempi molto rapidi.
Il cliente da tempo ha definito una strategia di medio termine in ambito cybersecurity, mirata a coprire in maniera sempre più ampia e completa i propri ambiti operativi ed organizzativi:
in particolare il progetto implementato va inquadrato nell'ambito del perimetro di Cyber Threat Intelligence (CTI), sintetizzabile attraverso i seguenti concetti chiave:

- Andare a monitorare e controllare i contenuti non presenti in "clear web" per verificare eventuali informazioni aziendali collegabili ad una potenziale (o reale) minaccia informatica;
- Anticipare e prevenire eventuali attacchi e danni di immagine e sottrazione di dati sensibili;
- Attuare tempestivamente le azioni di difesa e monitoraggio degli asset principali aziendali appartenenti a key people, domini internet aziendali, account riconducibili a persone dell'organizzazione, dati finanziari (finalizzati ad attivtà fraudolente).

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

La soluzione è stata implementata sfruttando una innovativa piattaforma SaaS di mercato che fornisce un prodotto verticale in grado di scandagliare contenuti di differenti tipologie (detti *asset*), inerenti svariati contesti aziendali (es. parole chiave, domini internet, account email aziendali, account social, tecnologie in uso ecc.) presenti nel cosidetto "deep & dark web" non raggiungibili attraverso strumenti tradizionali di analisi e ricerca ("clear web").

Il "dark web" è la terminologia che si usa per definire i contenuti del World Wide Web nelle darknet (reti oscure) che si raggiungono via Internet attraverso specifici software (es. TOR), configurazioni e accessi autorizzativi. Il dark web è una piccola parte del "deep web", la parte di web che non è indicizzata da motori di ricerca.

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

Il progetto presenta una modalità di implementazione non invasiva e con tempi di implementazione contenuti (startup in meno di 24h e successiva fase di "fine tuning" nelle settimane successive).
Il perimetro del servizio prevede la copertura di 300 asset con un supporto specialistico per le remediation con SLA di 8 h.
Un aspetto importante del progetto è stato quello di avere un impatto molto limitato in fase di startup sui processi operativi e le tecnologie del Cliente grazie alla bassissima invasività della piattaforma SaaS utilizzata.
Grazie a questo aspetto il progetto possiede intrinsecamente la possibilità di essere scalato sul cliente o ripetuto su un numero e tipologie di clienti.

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

Tra i principali benefici raggiunti si possono annoverare:
- Aumento dell'efficacia della strategia di cybersecurity del cliente e abbattimento del rischio associato con l'allargamento del perimetro di monitoraggio degli asset aziendali (dark e deep web);
- Maggiore proattività nella gestione delle minacce, e possibilità di utilizzare le integrazioni con altre soluzioni tecnologiche di prevenzione già presenti in azienda;
- Miglioramento della reputazione e solidità del brand aziendale e fidelizzazione dei clienti
- Possibilità di estendere ai propri clienti i benefici e la conoscenza in un settore ad elevata competenza verticale, come la CTI e la protezione cyber degli asset informativi critici; integrando e migliorando il risultato globale rispetto alle tematiche legali più tradizionali (visione olistica)
- velocità di implementazione
- bassissimo impatto su utenti e infrastrutture esistenti

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

La soluzione adottata ha permesso di utlizzare alcuni elementi innovativi quali:
- La CTI (Cyber Threat Intelligence) è "su misura" (tailored intelligence) per i clienti
- La rappresentazione fornita costituisce una vista semplice ed immediata delle minacce rilevate nel deep e dark web in modo chiaro e sintetico, senza necessità di utilizzo di strumenti inefficaci, complessi e molto spesso non esenti da rischi
- Integrazione nativa tra minacce e contromisure attraverso la cosiddetta "actionable intelligence" in grado di rimuovere le minacce attraverso operazioni di takedown (ad esempio: rimozione di domini fake registrati, inserimento di blocchi automatici sui sistemi di protezione perimetrale, correlazione tra utenze interne ed evidenze di compromissioni account rilevate nel deep web)
- Continuo aggiornamento, automatico e tempestivo, del perimetro di informazioni rilevanti per il cliente, senza bisogno di intervento manuale con l'utilizzo integrato ed automatico di

diverse sorgenti (feeds) e elementi di rilevazione attacchi e minacce (IOCs).

- Possibilità di utilizzare il motore di ricerca integrato per analisi e ricerche immediate di minacce o informazioni relative a entità attive nel campo della cybercriminalità, trend di settore, notizie o informazioni rilevanti.