axitea
SECURITY EVOLUTION

CASE STUDY

Axitea rivoluziona il mercato italiano dei SOC grazie a Cortex XSOAR

Quando Axitea comunica ai propri clienti che il suo Security Operations Centre (SOC) si avvale del XSOAR di Palo Alto Networks, l'attenzione è massima. Questa moderna piattaforma di orchestrazione, automazione e risposta alla sicurezza sta aiutando il provider italiano di soluzioni di sicurezza fisica e logica a conquistare nuovi spazi di mercato, scalare le attività del SOC e garantire un'esperienza fluida e coerente agli analisti.

paloalto NETWORKS

IN BREVE

Cliente
Axitea

Dimensioni dell'impresa
20,000+ clienti

Luogo
Italia

Prodotti e servizi
Servizi di sicurezza fisica e cyber

Settore
Tecnologico

La sfida

Gli analisti SOC impiegavano troppo tempo per passare da un sistema all'altro, individuare falsi positivi ed eseguire attività manuali ripetitive lungo tutto il ciclo di vita di un incidente.

Requisiti

- Monitoraggio e risposta SOC agili e resilienti.
- Processi SOC automatizzati, con meno interventi manuali.
- Monitoraggio scalabile per sostenere la crescita aziendale.
- Integrazione universale con tecnologie di sicurezza di terze parti.

Soluzione

Cortex XSOAR di Palo Alto Networks

Stare al passo con la crescente domanda di servizi SOC

L'incremento della richiesta di servizi SOC ha indotto Axitea a scegliere processi più scalabili e un sistema più efficiente in grado di far fronte al crescente volume di alert e attività. La presenza di processi di monitoraggio frammentati rendeva difficile scalare l'operatività del SOC e, in ultima istanza, limitava la crescita del business dato che gli analisti impiegavano troppo tempo per passare da una console all'altra.

LE SFIDE

Proteggere il futuro dell'Italia

Dal 1914 Axitea si dedica alla ricerca e allo sviluppo di nuove tecnologie e servizi di sicurezza volti a rispondere ai cambiamenti del settore, conservando quello spirito pionieristico che da sempre contraddistingue il suo approccio. Infatti, al fine di soddisfare un mercato in rapida evoluzione, oggi Axitea integra i servizi di sorveglianza con tecnologie innovative e sistemi avanzati di protezione fisica e informatica.

Il passaggio alla cybersecurity è stata una delle mosse più lungimiranti nella storia di Axitea. Secondo la Banca Europea per gli Investimenti, in Italia ci sono circa 4,3 milioni di piccole e medie imprese (PMI) che generano il 67% del PIL del Paese: una delle percentuali di PMI più alte in Europa. La stragrande maggioranza di queste è alla ricerca di servizi di cybersecurity agili ed efficienti, e Axitea sta diventando il provider di riferimento per molte di loro.

In questo contesto, il SOC di Axitea è stato pensato per unificare e coordinare le capacità di rilevamento e risposta alle minacce dei suoi clienti. Tuttavia, i sistemi di monitoraggio tradizionali installati in precedenza richiedevano sei analisti per la sola gestione degli incidenti. La prima sfida per Axitea, quindi, era legata alla scalabilità.

> Con la precedente piattaforma di monitoraggio, gli eventi venivano inseriti in un sistema di ticketing e gestiti direttamente all'interno della tecnologia in uso con una procedura che non era scalabile.

Cesare Di Lucchio, SOC Manager, Axitea

La seconda sfida di Axitea era trovare una piattaforma di orchestrazione, automazione e risposta agli eventi di sicurezza che si integrasse con diverse fonti di dati dei clienti, tra cui gateway Web, EDR (Endpoint Detection and Response), firewall e data loss prevention, nonché con svariati provider di tecnologie di sicurezza.

La terza sfida riguardava l'esperienza dell'utente finale.

> Gli analisti dovevano eseguire molte operazioni manualmente, passando da uno strumento di monitoraggio all'altro. Nel caso di incidente, non potevamo garantire una risposta entro un'ora o due, per cui abbiamo dovuto pensare a una strategia SOAR diversa.

Cesare Di Lucchio, SOC Manager, Axitea

REQUISITI

Automazione, scalabilità e visibilità

Tra i requisiti per la piattaforma SOAR di nuova generazione:

- Assicurare ai clienti monitoraggio e risposta agili e resilienti.
- Automatizzare i processi SOC, eliminando il più possibile gli interventi manuali.
- Scalare il monitoraggio per supportare le ambizioni di crescita aziendale di Axitea.
- Implementare sistemi agnostici per l'integrazione universale con diverse soluzioni di sicurezza di terze parti.

SOLUZIONE

La risposta definitiva a quasi tutte le domande sulla cybersecurity

Axitea ha scelto di trasformare il processo di risposta agli incidenti del suo SOC con Cortex XSOAR di Palo Alto Networks.

> Palo Alto Networks è la risposta migliore a quasi tutte le domande sulla cybersecurity. L'affidabilità e l'efficacia del loro portfolio di prodotti connessi sono attestate da aziende di tutto il mondo, e il loro staff è estremamente competente. Di XSOAR ci è piaciuta in particolare la rapidità con cui abbiamo potuto creare i playbook.

Cesare Di Lucchio, SOC Manager, Axitea

Cortex XSOAR aggrega gli avvisi provenienti da diverse fonti di rilevamento (sicurezza cloud e SaaS, firewall, EDR, reti private virtuali (VPN), sicurezza delle email e altro) prima di eseguire playbook automatizzati per l'arricchimento e la risposta a questi incidenti. I playbook si coordinano tra tecnologie, team di sicurezza e utenti esterni offrendo visibilità e interventi centralizzati sui dati.

> Raccogliamo dati da diversi sistemi dei clienti, da Darktrace e Sophos a Trend Micro e Microsoft Defender. Una singola dashboard unificata ci fornisce la visione completa su tutte le informazioni che ci interessano. Ad esempio, possiamo visualizzare il volume degli incidenti in base al loro livello di gravità – critica, media o bassa – e il tempo medio di assegnazione. La dashboard mostra anche gli incidenti per tipo di tecnologia e il motivo per cui l'incidente è stato risolto.

Cesare Di Lucchio, SOC Manager, Axitea

Il modello SOC-as-a-service porta questa soluzione a un livello superiore. In precedenza, Axitea gestiva solo le soluzioni EDR che aveva installato. Oggi, invece, gestisce qualunque soluzione EDR. Gli SLA contrattualizzati con i clienti definiscono tempi di risposta precisi, ad esempio di 30 minuti per gli incidenti critici e di un'ora per quelli di alto livello. "Pochissime organizzazioni possono offrire livelli così elevati di visibilità e flessibilità", afferma Di Lucchio.

Inoltre, la community di Cortex XSOAR è una delle più estese nel mondo SOAR, con oltre 900 integrazioni nel Marketplace Cortex e playbook predefiniti per i casi d'uso più comuni.

> Le integrazioni del Marketplace rappresentano per Axitea un reale vantaggio: siamo in grado di integrare rapidamente nuovi clienti SOC e di scalare i nostri servizi.

Cesare Di Lucchio, SOC Manager, Axitea

VANTAGGI

XSOAR è un vero fattore di differenziazione

Con Cortex XSOAR, Axitea sta ridefinendo orchestrazione, automazione e risposta della sicurezza di oltre 500 clienti. I vantaggi includono:

- **Sostegno alla crescita di business:** l'uso di Cortex XSOAR sta contribuendo in modo significativo alla crescita dei ricavi di Axitea. "Quando dichiariamo di utilizzare Cortex XSOAR ai nostri clienti, questi prestano grande attenzione. È un vero e proprio fattore di differenziazione, soprattutto tra le PMI che hanno ben chiaro il valore di un servizio SOC automatizzato e gestito", afferma Di Lucchio.
- **Scalabilità integrata:** la piattaforma è scalabile e standardizza i processi di risposta agli incidenti. "Man mano che siamo cresciuti, ci siamo trovati a dover intervenire su un numero sempre maggiore di eventi di sicurezza. Tuttavia, i flussi di lavoro automatizzati per la risposta agli incidenti consentono ai nostri analisti di concentrarsi sugli incidenti più critici".
- **Aumento della produttività:** prima di implementare XSOAR, il SOC aveva sei analisti dedicati, mentre ora ne impiega solamente due, nonostante un deciso incremento del numero di clienti.
- **Minore necessità di analisti aggiuntivi:** nonostante un incremento delle attività SOC del 50% negli ultimi 12 mesi, il numero di analisti richiesti dal SOC di Axitea non è aumentato.
- **Risposta più rapida agli incidenti:** gli analisti utilizzano ricerche, query e indagini istantanee per velocizzare indagini complesse in tempo reale e la risposta agli incidenti. "Con Cortex XSOAR possiamo correlare avvisi, incidenti e indicatori provenienti da diverse origini su un'unica piattaforma", afferma Di Lucchio.

Il contributo dei Professional Services di Palo Alto Networks è stato essenziale per questo successo.

> Il team di esperti ha automatizzato i nostri casi d'uso per ciascun cliente e ci ha supportato nell'implementare i playbook e nello strutturare l'offerta SOC-as-a-service."

Cesare Di Lucchio, SOC Manager, Axitea

Per ulteriori informazioni su Palo Alto Networks, visita il sito web dove troverai molte altre storie di clienti.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com