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.

L'azienda Cliente aveva la necessità di raggiungere un livello di sicurezza superiore al convenzionale, tipicamente basato su sistemi perimetrali, fine di proteggersi da attacchi informatici sotto forma di Malware, tentativi di intrusione e sottrazione di informazioni strategiche. Inoltre, data la tipologia dell'Azienda, il cliente aveva la necessità di sviluppare un sistema difensivo specifico per linee di produzione di tipologia SCADA. Un ulteriore necessità era relativa alla proattività della soluzione/servizio che doveva essere in grado di agire come parte integrante dell'Azienda e dello schema di difesa informatica.

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

Le tecnologie utilizzate sono state interamente scritte dal team di sviluppo di Yoroi e costituiscono la soluzione denominata Cyber Security Defense Center che si basa, essenzialmente su tre componenti: 1) Piattaforma di ThreatINTEL che unisce le capacità di Cyber Intelligence a quelle di Defense Center e Incident Response formando un connubio davvero innovativo. 2) Sensore Polifunzionale proprietario in grado di effettuare 12 diversi step di analisi. 3) Sandbox Multipla proprietaria.

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

Il progetto prevede l'iniziale inserimento del Sensore Polifunzionale (Genku) all'interno della rete del Cliente al fine di verificare l'eventuale presenza di Malware o minacce informatiche. Una volta effettuate le analisi locali, il Sensore potrà chiedere una "Second Opinion" al motore centrale posizionato in un Private Cloud rigorosamente basato in Italia e attingere, eventualmente, alle capacità di analisi e reverse engineering offerte dalla Sandbox Multipla sempre posizionata in un'area specifica del private cloud. Il tutto accessibile mediante un portale dedicato con accessi specifici e multi-tenant.

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

Il principale beneficio raggiunto è un sensibile aumento della sicurezza in generale dovuto, principalmente, alla possibilità di avere una visione d'insieme della postura aziendale e dell'efficacia delle difese informatiche.
Il secondo e altrettanto importante beneficio è stato quello di avere un vero e proprio Partner sempre disponibile e proattivo nella forma di un Analista dedicato alla difesa e alla mitigazione delle minacce riscontrate.
Il terzo beneficio è stato quello di sviluppare, in team con gli Analisti Yoroi, una soluzione di SCADA Security costruita nel rispetto delle Policy di Sicurezza stabilite dall'Azienda senza doversi adattare a quanto offerto in modalità standard dal mercato

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

I principali elementi distintivi dei Servizi di Sicurezza Gestiti offerti da Yoroi sono (principalmente):

a) L'unione di Threat Intelligence e Defense / Incident Response sotto forma di Servizio Gestito.
b) La costruzione di un intero set di Servizi allo scopo di potenziare le capacità dell'Analista umano che viene collocato al centro del progetto. "Defence Belongs to Humans" è il nostro credo.
c) Le tecnologie sviluppate dal Yoroi sono frutto della ricerca costante e dell'ascolto delle esigenze dei Clienti che cerchiamo di soddisfare creando nuovi servizi e funzionalità
d) La visione d'insieme dello stato della sicurezza aziendale rappresenta un enorme conquista per tutti i Clienti in difficoltà per via della frammentazione delle soluzioni di sicurezza offerta da troppi vendor diversi
d) L'Italianità di tutta la Soluzione, i rapporti con CERT Nazionali ed Internazionali, Enti Governativi Nazionali e Internazionali contribuiscono alla creazione di una ThreatINTEL davvero efficace