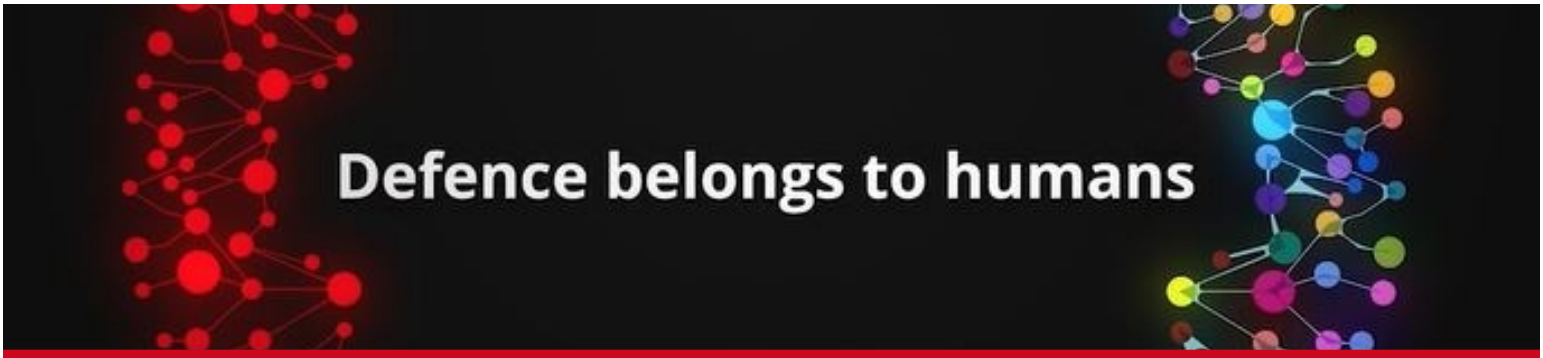


YOROI

CASE STUDY

CLIENTE
Aeroporto Internazionale di Milano-Bergamo

PARTNER
Delo Group

Informazioni generali

Mercato

- ✓ Trasporto

Lo scenario

- ✓ Infrastruttura strategica
- ✓ Costante rischio di Cyber Attacchi
- ✓ Visibilità delle minacce limitata
- ✓ Mancanza di Analisti di Cyber Sicurezza

Gli obiettivi

- ✓ Creazione di un sistema che consenta la visione d'insieme della postura di Sicurezza della Rete
- ✓ Costruzione di un efficace ERT
- ✓ Aumento del grado di sicurezza unificando e mettendo a fattor comune tutte le risorse già in campo

Il Cliente

L'aeroporto internazionale "Il Caravaggio" di Milano Bergamo è il terzo aeroporto Italiano per numero di passeggeri.
Situato a 5 Km dal centro di Bergamo e 50 Km dal centro di Milano assieme agli aeroporti di Milano Malpensa e Milano Linate forma il sistema aeroportuale milanese con oltre 40 milioni di passeggeri annui (2016).
Lo scalo è principalmente utilizzato da compagnie aeree a basso costo per le quali risulta essere il primo per numero di passeggeri e, per la società di ricerca specializzata britannica Skytrax, rientra tra i 10 migliori aeroporti low-cost del mondo.

"Da subito sono rimasto colpito dalla filosofia di Yoroi che mette l'Analista umano al centro del progetto di Cyber Sicurezza e utilizza tecnologie innovative al servizio dello stesso per potenziarne le capacità"
Ettore Pizzaballa, ICT Manager, SACBO SpA

Il Challenge

La frammentazione delle Soluzioni di Sicurezza di Vendor differenti causa evidenti problemi in termini di:

- Mancanza di visione d'insieme
- Difformità di giudizio riguardo alla pericolosità della stessa minaccia vista da sistemi diversi
- Visibilità limitata a ciò che viene visto dalle difese in essere

A questo va aggiunta la grande difficoltà di reperire Analisti specializzati dei quali è nota la mancanza a livello mondiale.

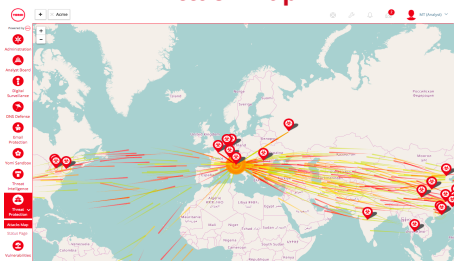
A questi fatti è poi doveroso ricordare che l'infrastruttura aeroportuale Internazionale di Milano Bergamo ha un profilo di alto interesse per cyber-criminali ed è un bersaglio e una risorsa nazionale da difendere utilizzando tutte le risorse possibili.

La Soluzione

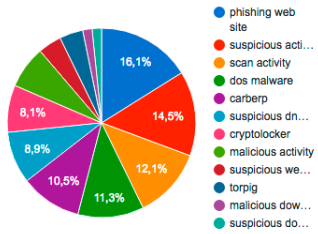
Yoroi Cyber Security Defense Center (C-SDC)

- ✓ Sistema di Threat Intelligence Managed Advanced Threat Protection "MATP"
- ✓ Sensore Polifunzionale "Genku"
- ✓ Sandbox multipla (Bare-Metal) "Yomi"
- ✓ Sistema DNS Defense integrato

Attack Map



Status Page - Threats Pie Chart



Gli Analisti Yoroi

I Benefici

- ✓ Gruppo di Analisti Yoroi che lavorano fianco a fianco con il cliente
- ✓ Punto di visibilità dello stato di sicurezza univoco
- ✓ Proattività del sistema

L'erogazione dei Servizi gestiti di Cyber Sicurezza effettuata da Yoroi prevede l'utilizzo di tutte le tecnologie già schierate a difesa dell'Azienda al fine di integrare la "vista" di ognuna in una "visione d'insieme" completata dal Sensore Polifunzionale Genku.
Grazie a ciò, l'Analista Yoroi e il team di Sicurezza del Cliente, hanno ottenuto una visibilità univoca concentrata nella console C-SDC.

- Mediante l'Analist Board è possibile monitorare in tempo reale tutte le segnalazioni provenienti dal campo, verificarne l'eventuale grado di pericolosità e procedere all'identificazione della minaccia.
- Qualora venga individuata una minaccia, l'Analista ha la possibilità di inviarla alla Sandbox al fine di provocarne la "detonazione" in un ambiente protetto, comprenderne la reale pericolosità e creare il protocollo di mitigazione più appropriato da trasmettere al Cliente.
- L'Attack Map consente l'analisi in diretta dello stato della rete e delle minacce consentendo il "drill-down" fino a raggiungere il payload delle stesse.
- La Status Page permette di visualizzare in un unico pannello lo "Zoo del Malware" che attraversa la rete, la sua "Geolocalizzazione", i "Top targeted" e "Top Infected" host fornendo un colpo d'occhio univoco sullo stato di sicurezza e gli Indici di Compromissione (IoC).
- Infine il Sistema di Protezione DNS offe un vero e proprio "scudo protettivo" che impedisce il completamento della comunicazione necessaria al Malware per potersi attivare e/o effettuare esfiltrazioni di dati (call-back, leaks)

Grazie all'erogazione del Servizio Gestito di Cyber Sicurezza C-SDC di Yoroi, il Cliente ha messo in campo un *team di Analisti specializzati che si integra perfettamente con il Team interno*, utilizza tutte le tecnologie già implementate (aumentandone il ROI), aumenta la visibilità sulle eventuali minacce e, infine, dispone di *un punto di conoscenza univoco con modalità di intervento proattivo*. Sarà sempre l'Analista Yoroi ad avvertire il Cliente dell'eventuale presenza di una minaccia, fornendo tutte le informazioni necessarie alla mitigazione della stessa.

Il cliente, ha sempre a sua disposizione l'Analista Yoroi al fine di ottenere informazioni o, se necessario, pareri sulle minacce in corso o la prevenzione di possibili future minacce.

Ogni fine settimana, il portale C-SDC viene aggiornato con un report indicante tutti gli "incidenti" di sicurezza riscontrati e il dettaglio del loro stato registrato mediante il sistema di ticketing che conserva il tracciato della gestione, gli SLA e tutte le informazioni correlate.

A proposito di Yoroi

Il continuo ed inesorabile aumento di minacce informatiche induce ogni organizzazione ad un cambiamento epocale coinvolgendo un nuovo ambiente denominato "Cyber Space". Fino a che a trarre profitto da un attacco sarà un essere umano, solamente un essere umano potrà contrastarlo

Defence Belongs to Humans

Contatti

Yoroi S.r.l.
Via Santo Stefano, 11
40125 – Bologna (BO)
Tel. 051 0301005
www.yoroi.company