
TINEXTA CYBER

CYBSEC.CLUB

DEFENCE BELONGS TO HUMANS

# Descrizione del prodotto

**CYBSEC.CLUB** è il circolo esclusivo fondato da YOROI e rivolto a Imprenditori, CISO, CTO e CIO, con l'obiettivo di poterli supportare con contenuti e strumenti che li aiutino a migliorare la difesa informatica delle organizzazioni di cui hanno la responsabilità.

**CYBSEC.CLUB** è animato da una comunità di esperti di cybersecurity con una significativa esperienza sul campo; persone che hanno la volontà e il desiderio di condividere conoscenze, competenze, strategie, intuizioni, analisi e informazioni tempestive con le figure chiave a cui le aziende affidano il fondamentale compito di realizzare e implementare la difesa dai crimini informatici.

**Perché un CLUB ?**

E' sempre più evidente che la battaglia contro il crimine informatico deve essere condotta da un'azienda alzando in misura sostanziale il livello di attenzione, di consapevolezza e di conoscenza al proprio interno.
Ma una corretta strategia di difesa non può prescindere dall'adeguata comprensione del contesto nel quale l'azienda opera.
Inoltre è di fondamentale rilevanza che la conoscenza sia aggiornata. Il crimine informatico, infatti, ha un enorme vantaggio su chi deve difendersi - che in termini di strategie militari è considerato di massimo valore strategico - ed è quello di decidere quando e dove attaccare.

Questo implica per un'organizzazione la necessità di dover difendere SEMPRE ed INTERAMENTE il proprio perimetro informatico.
Un ritardo nell'aggiornamento continuo sulle minacce più recenti e sulle ultime vulnerabilità rilevate potrebbe, ad esempio, significare per un'organizzazione l'impossibilità di difendersi efficacemente.

Ma lo sforzo della singola organizzazione da solo non basta; occorre che il sistema nella sua interezza aumenti in modo costante il livello di sicurezza complessivo, altrimenti l'impegno e gli investimenti della singola azienda rischia di essere vanificato.

In CYBSEC.CLUB pensiamo che lo scambio di informazioni tempestive, di conoscenza e di esperienze maturate sul campo sia l'elemento essenziale per il raggiungimento di un livello superiore di sicurezza della singola organizzazione e quindi, a cascata, dell'intero sistema imprenditoriale italiano.

**Qual è lo scopo del CYBSEC CLUB**

Lo spirito della membership è quello di creare una comunity di Security Manager che hanno l'obiettivo primario di aumentare la capacità di performance dei loro team e di ottenere il massimo dai loro partner esterni, grazie ad una piattaforma attraverso la quale i membri del circolo possono ricevere, da un gruppo significativo di esperti che operano quotidianamente sul campo, informazioni aggiornate in tempo reale sulle ultime minacce e sugli attacchi in corso, suggerimenti di azioni urgenti da intraprendere per fronteggiarli, analisi approfondite su temi specifici di particolare rilevanza, consulenza strategica sull'approccio più efficace con il quale strutturare sistemi di difesa cyber performanti e valutazioni su nuove tecnologie o nuovi approcci operativi che si vanno affermando. Il tutto declinato con un taglio verticale sulla cyber security che sia certamente di rigore scientifico ma anche fortemente operativo.

**Come nasce l'idea del CLUB**

Come spesso succede siamo partiti da quella che è stata la soluzione che abbiamo messo a punto per risolvere un problema che riteniamo essere di fondamentale importanza, che riguarda non soltanto noi direttamente ma chiunque si occupi in posizioni di responsabilità di difesa cibernetica: la necessità di sapere sempre e tempestivamente cosa è successo nel Cybermondo.

In particolare:

- quali sono state le ultime vulnerabilità rilevate in reti, servizi e sistemi informatici?
- quali sono stati gli attacchi cibernetici avvenuti a livello globale?
- quali sono gli argomenti legati alla sicurezza che stanno scalando l'attenzione internazionale?

Come è facile immaginare, i vertici di Yoroi, per non rischiare di esporre la società che guidano e soprattutto i clienti che le si affidano a rischi che potrebbero avere sottostimato, da sempre hanno ritenuto indispensabile cercare risposte tempestive a quelle domande, analizzando siti, forum, data base, blog e fonti specializzate; tutte fonti che hanno verificato nel tempo essere affidabili, aggiornate e credibili e a cui se ne aggiungono continuamente di nuove per avere un panorama di informazioni sempre più esaustivo.

Questa attività è - come è facilmente intuibile - particolarmente "time consuming", e il tempo è oggi la risorsa più preziosa di tutte.

Per poter dunque ottimizzare il tempo dedicato a questo approfondimento - che rischiava di non bastare mai - imprescindibile per chiunque abbia una responsabilità significativa nella difesa di aziende ed organizzazioni, Marco Ramilli ha progettato un software che svolge un importante lavoro di scouting tra quelle fonti che abbiamo citato e che consente una visione "alta e di insieme" e un efficace aggiornamento sui temi più caldi delle ultime ore, in un arco di tempo rapido e sufficiente per organizzare un'azione di prevenzione.

Questa attività è parte fondamentale di quella che noi consideriamo una delle tre fasi fondamentali nella costruzione di un'efficace difesa cibernetica, la ***fase predittiva***; a cui si aggiungono poi la ***fase di prevenzione e quella reattiva/proattiva.***

Provare infatti ad anticipare un attacco informatico, piuttosto che dover reagire ad esso, è uno dei fondamenti strategici della difesa; come dimostra, in campo militare, l'importanza che tutti gli stati assegnano alle attività di intelligence, che hanno per definizione l'obiettivo di anticipare le mosse dei nemici.

Siamo dunque pienamente consapevoli di quanto impegnativo sia, sotto il profilo della profondità delle competenze necessarie, dell'attenzione continua richiesta e della tenuta nervosa, il ruolo di un CISO; e quanti rischi corra - in caso di un attacco che produca danni all'azienda di cui fa parte - di apparire come chi:

- abbia sbagliato strumenti e strategia;
- abbia sottostimato gli investimenti necessari per la dotazione di strumenti e tecnologie, per l'allargamento del team di difesa e per la formazione del personale;
- non abbia fatto crescere a sufficienza la consapevolezza aziendale sui temi della sicurezza digitale;
- non si sia sufficientemente aggiornato sui nuovi attacchi, sui nuovi approcci, sulle nuove tecnologie.

Ci è sembrato dunque che fosse importante - e in coerenza con la mission di questo Club - , poter mettere a disposizione dei responsabili della security delle aziende italiane anche il nostro software, oltre al patrimonio delle nostre conoscenze, che si arricchisce giornalmente per le nostre esperienze sul campo e per i processi di osmosi e di knowledge sharing implementati all'interno di Yoroi tra i team di difesa, di offesa, di compliance e di sviluppo software.

La Piattaforma contiene tre sezioni che si aggiornano quotidianamente:

1. **Ultime vulnerabilità rilevate**
   Le ultime vulnerabilità rilevate vengono catturate direttamente dal NVD stream (National Vulnerability Database, NIST) e visualizzate in modo conveniente per una semplice consultazione. Le aggregazioni per organizzazione, per tipologia e per "score" presenti in Cybsec.Club vengono proposte per facilitare una visione ad alto livello sul cambiamento nel tempo di quest'ultime.

2. **Minacce recenti**
   Le minacce recenti vengono individuate calcolando la frequenza delle analisi effettuate nelle ultime 24 ore sulle seguenti aree: clienti diretti, reti internazionali di appartenenza, detonazioni di artefatti - che hanno raggiunto il numero ragguardevole di oltre 2 milioni al giorno - nelle sandbox in essere (Infocert, VirusTotal, Abuse, Yomi Pubblica) e feed da terze parti. Le analisi in sandbox permettono al sistema di visualizzare meta-tags di analisi tra cui la famiglia di malware individuata, la tipologia di portatore malware ed altri numerosi Indici di Compromissione che vengono utilizzati per offrire al cliente una esperienza specifica sulle ultime minacce riscontrate.

3. **Trend sulla sicurezza**
   La base dati dalla quale vengono estratti i trend sulla sicurezza (con cadenza giornaliera) racchiude un vasto bacino di sorgenti informative. Vengono raccolte informazioni dai principali magazine e testate giornalistiche del settore, da numerosi Tweeters, da sorgenti RSS, da canali istituzionali e chat telegram. Per ognuno di tali sorgenti viene estratto il topic e calcolata la sua frequenza. Topic con maggiore frequenza diventano automaticamente "trend". Per ogni trend vengono visualizzate le sorgenti che hanno portato quel topic a diventare trend e vengono rese navigabili all'utente affinché abbia la possibilità di leggere l'articolo completo e non semplicemente il topic.

Oltre alla componente software il Club presenta poi diverse sezioni:

- Podcast/Webinar
- Blog
- Report
- Interviste
- Eventi di networking


**Yoroi S.r.l.**
www.yoroi.company - info@yoroi.company

**Piazza Sallustio, 9**
00187 – Roma (RM)
+39 (051) 0301005



Yoroi S.r.l. società soggetta ad attività di direzione e coordinamento esercitata dalla Tinexta S.p.A.

Yoroi ® è un marchio registrato

Registrazione N°: 016792947

**Authorized to Use CERT™**
CERT is a mark owned by
Carnegie Mellon University

TF-CSIRT
Trusted Introducer