CYBER Pro Threat Intelligence

DATA SHEET

Cyber Pro Threat Intelligence

Per anticipare le nuove minacce informatiche e difendere la tua organizzazione dagli attacchi

Cyber Pro Threat Intelligence è la soluzione sviluppata per la difesa preventiva, analitica e proattiva da minacce informatiche di molteplici tipologie. Nasce con l'obiettivo di difendere e rendere più resiliente il core business di un'organizzazione.

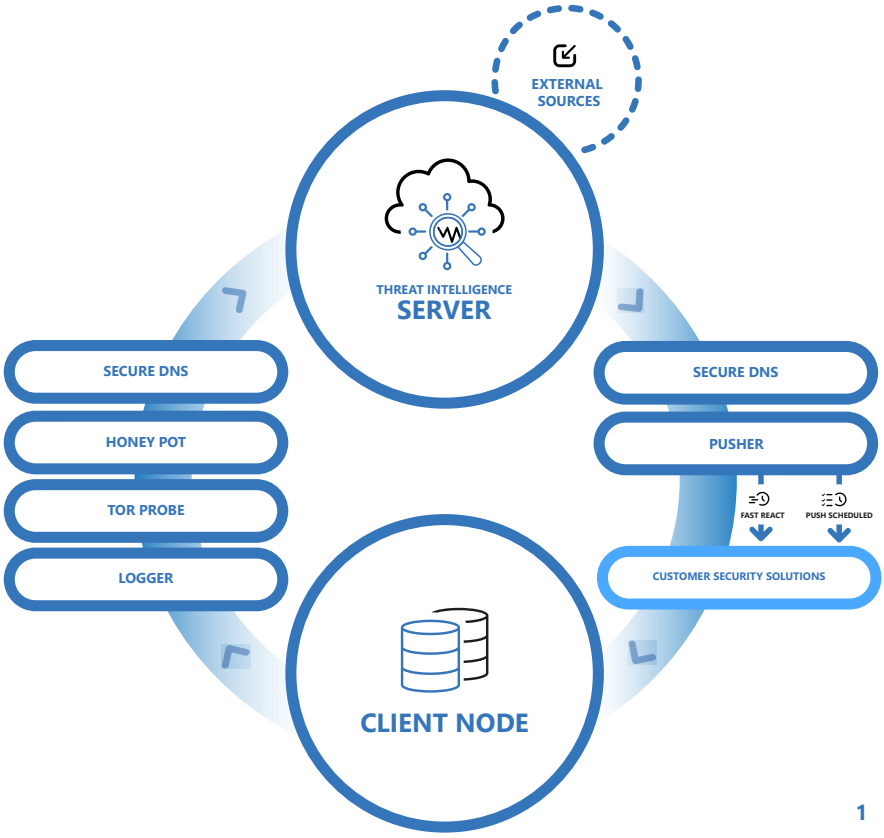
È NECESSARIO UN NUOVO APPROCCIO

Le minacce informatiche sono tra le problematiche più importanti che le organizzazioni si trovano ad affrontare ma vi è **un evidente lacuna nelle capacità di difesa delle azende**.

Per prevenire gli attacchi è necessario avere una profonda conoscenza del nemico, in particolare delle tecniche maggiormente utilizzate e degli **Indicatori di Compromissione**, anche noti come **IOC**, che possono identificarlo.

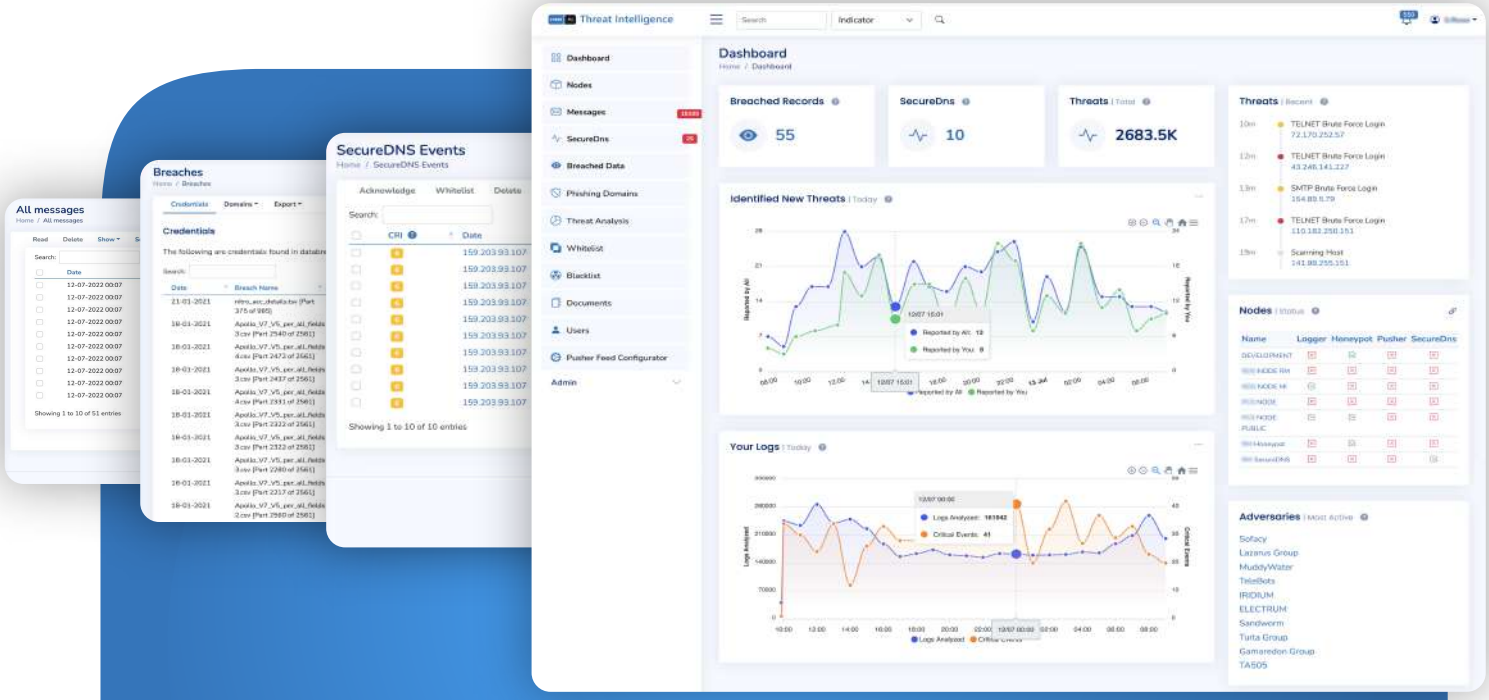
Ciò che differenzia **Cyber Pro Threat Intelligence** dalle altre soluzioni presenti sul mercato, è la capacità di essere estremamente **modulare ed integrato** con gli strumenti di difesa già presenti all'interno dell'infrastruttura aziendale quali **antivirus, firewall e servizi di endpoint protection** (EDR, XDR, IPS, etc.).

Inoltre, ogni installazione di Cyber Pro Threat Intelligence **invia al database centrale le detection, incrementando costantemente la lista degli IOCs** noti.
In questo modo, oltre a **reperire informazioni dalle maggiori banche dati mondiali**, è possibile attingere **anche a fonti locali**, ovvero provenienti da aziende del territorio.



FEATURES

Il prodotto è pensato per essere utilizzato da un ampio panorama di utenti, compresi i non tecnici, grazie ad un'interfaccia grafica semplice ed intuitiva che, allo stesso tempo, consente di gestire in maniera granulare ed efficace una vasta gamma di servizi.
L'implementazione è rapida ed efficace e non implica cambiamenti architetturali della propria infrastruttura.



DASHBOARD
Nella piattaforma è presente una Dashboard che raggruppa le informazioni in maniera chiara e sintetica dando una visione globale sulle funzionalità di sicurezza implementate.

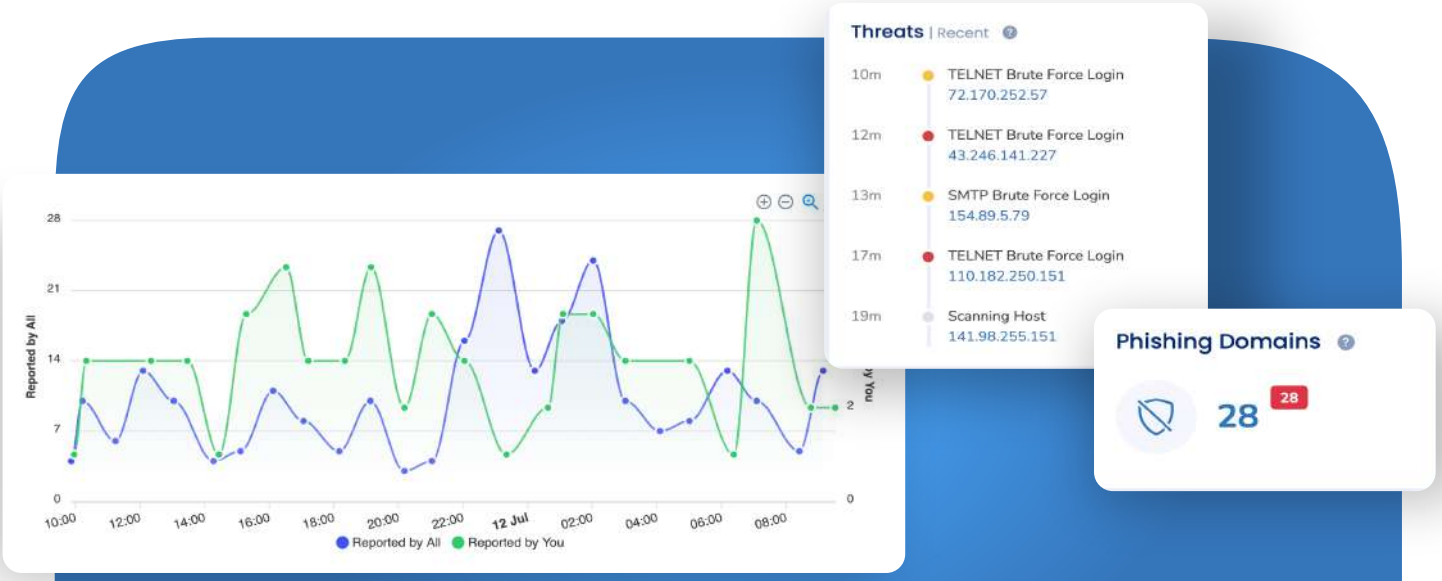
IOCs
Gli indicatori di compromissione (IOC) sono costantemente aggiornati, provengono sia da fonti OSINT che CLOSINT. Gli IOCs (Malware, C2, Hash, Documenti malevoli, Ipv4, Domini, Url, Tor Exit Nodes, Vpn, Proxy) confluiscono in un Database in Cloud centralizzato e condiviso che contribuisce alla protezione in tempo reale dei dispositivi.

HONEYPOT
Permette di sapere in tempo reale chi ci sta attaccando e come lo sta facendo. Honeypot utilizza delle esche che simulano dei servizi comuni, come per esempio un server web. Una volta rilevato un attacco si innesca automaticamente il servizio Fast React che blocca l'indirizzo IP negli apparati di sicurezza preposti.

BLACK LIST/WHITE LIST
Consente di inserire in maniera semplice indirizzi IP / URL in Black List o in White List direttamente nei propri apparati di sicurezza.

SECURE DOCUMENT
Permette di caricare i documenti prodotti nell'ambito dei servizi di cybersecurity. I dati sensibili sono criptati per garantirne la massima riservatezza e condivisi con il cliente che è in possesso di una chiave univoca che gli permette di decifrare il documento.

PUSHER
Inserisce l'indicatore di compromissione all'interno dei device del cliente consentendo



di mantenere aggiornati gli indicatori di compromissione. Il Push viene schedulato in giorni e orari specifici. Con il modulo di Fast React il servizio agisce in real time.

✓ LOGGER

Legge i Log degli apparati di sicurezza attraverso il Nodo, facendo confluire nel cloud centrale i log e andando ad alimentare il database di Threat Intelligence.

✓ THREAT ANALYSIS

Esegue l'analisi statica dei file attraverso la funzionalità di Analyze File e di Analyze Logs alla ricerca di indicatori dannosi nel database di Threat Intelligence. Il report fornisce un'analisi dettagliata, permettendo di determinare la pericolosità dei file analizzati.

✓ CLOUD SANDBOX

Analizza in modo dinamico qualsiasi File o URL sospetto in una Sand Box dedicata. Durante il controllo, viene effettuata una verifica dei file in un ambiente di esecuzione personalizzabile, per estrapolare informazioni utili a comprenderne il comportamento ed i possibili rischi.

✓ NODE

È un appliance che può essere fisico o virtuale, risiede presso l'infrastruttura del cliente così da consentire una scalabilità maggiore e tempistiche di latenza minori. Eroga diversi servizi quali Logger, Torprobe, Pusher, Honeypot e Secure DNS.

✓ PHISHING DOMAINS

A partire dal dominio del cliente, attraverso algoritmi evoluti vengono calcolati e verificati tutti i domini potenzialmente malevoli utilizzabili per azioni offensive. I report forniti consentono agli amministratori di sistema di intraprendere azioni preventive come ad esempio il blocco antispam.

✓ FAST REACT

A fronte del rilevamento di attacchi consente di aggiornare istantaneamente le configurazioni all'interno dei dispositivi di sicurezza del cliente.

✓ DARK WEB & BOTNET MONITORING

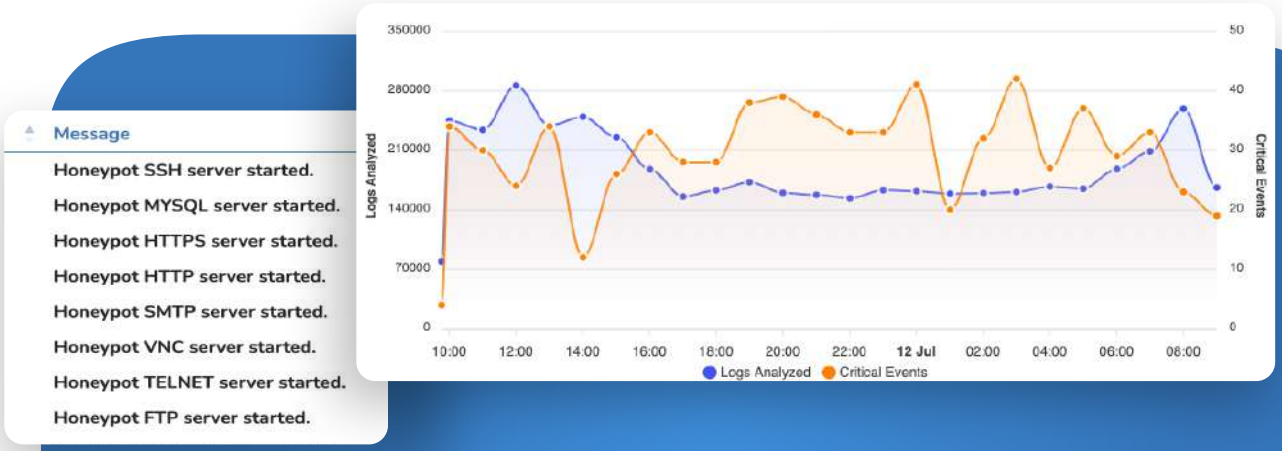
Viene costantemente ispezionato il Dark Web e le Botnet (forum underground utilizzati dai criminali informatici) al fine di individuare Data Breach ed eventuali credenziali trafugate. Le informazioni ricevute permettono di intraprendere le azioni più opportune a seguito di violazioni di dati aziendali e prevenire che vengano utilizzate da attori malevoli.

✓ ADVANCED SUPPORT

È possibile interagire con un esperto al fine di chiedere informazioni o delucidazioni di base sulla piattaforma in termini di comprensione del dato o delle funzioni in essa presenti.

Threat Intelligence

DATA SHEET



✓ SECURE DNS

Consente di proteggere le organizzazioni dalle nuove minacce identificando e bloccando le connessioni dannose.

Ogni singola richiesta generata dagli utenti viene prima controllata dal DNS, che ne verifica la bontà. Qualora venisse individuata una connessione verso una destinazione identificata come malevola, essa verrà automaticamente bloccata.

È importante ricordare che più del 91% di tutti i malware utilizza il DNS per comunicare verso internet e trafugare dati o reindirizzare il traffico verso siti malevoli, e quasi tutti i domini di Phishing hanno una data di creazione molto recente.

✓ EXTERNAL PERIMETER ASSESSMENT

Analizza le vulnerabilità dei servizi esposti in internet al fine di individuare immediatamente eventuali falle di sicurezza.

THREAT INTELLIGENCE PLAN

	BASIC	ADVANCED	PREMIUM
DASHBOARD	✓	✓	✓
IOCS	✓	✓	✓
HONEYPOT	✓	✓	✓
BLACK LIST/WHITE LIST	✓	✓	✓
SECURE DOCUMENT	✓	✓	✓
PUSHER	✓	✓	✓
LOGGER	✓	✓	✓
THREAT ANALYSIS	✓	✓	✓
NODE	✓ 10	✓ 20	✓ 30
PHISHING DOMAINS	✗	✓	✓
FAST REACT	✗	✓	✓
DARK WEB & BOTNET MONITORING	✗	✓	✓
CLOUD SANDBOX	✗	✓ 10 SUBMISSIONS / MONTH	✓ 30 SUBMISSIONS / MONTH
ADVANCED SUPPORT	✗	✓ 2 REQUESTS / MONTH	✓ 10 REQUESTS / MONTH
SECURE DNS	✗	✗	✓
EXTERNAL PERIMETER ASSESSMENT	ADD-ON	ADD-ON	ADD-ON