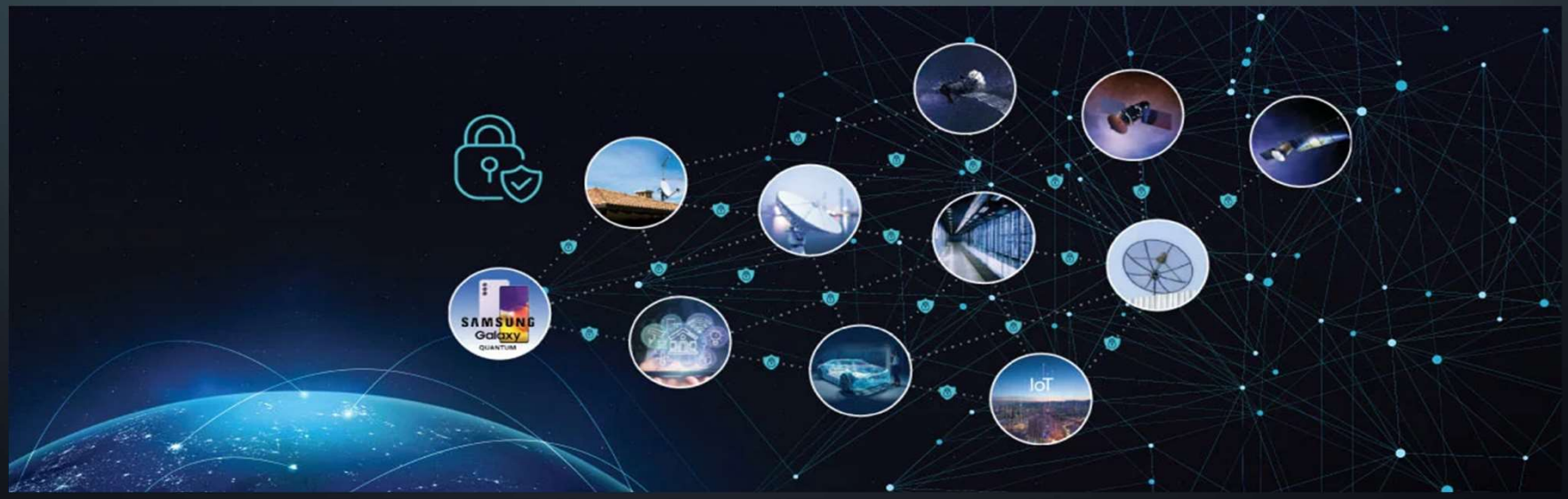
PIZZONI
MODERN OFFICE

- **"Proteggi il tuo business, difendi il tuo successo: scegli con noi, la TUA Cybersecurity**!

Sperare di non essere la prossima vittima di un attacco informatico **non e' una strategia !!**

Con l'aumento degli attacchi, investire nella cybersecurity diventa fondamentale per proteggere il tuo business e dormire sonni tranquilli.



ALWAYS ONE STEP AHEAD

Why?

Tutto ciò che facciamo è mettere in discussione lo status quo.
Crediamo nel approcciare diversamente, pensare “fuori dalla scatola”

How?

Grazie ad una continua ricerca ed analisi di attacchi aumentiamo la nostra conoscenza sulle più recenti e sofisticate tecniche usate dai criminali ed Adattiamo le nostre metodologie di difesa ricercando le più innovative soluzioni sul mercato.

What?

Siamo forti di una notevole esperienza tecnica grazie alla quale abbiamo fatto crescere la consapevolezza parlando di CyberSecurity.
Potiamo delle innovative soluzioni che hanno un filo logico nella applicazione della strategia aziendale di cyber security.

PIZZONI
MODERN OFFICE

ALWAYS ONE STEP AHEAD

- profonda conoscenza della Cyber Security ed intelligence
- continuo studio ed aggiornamento delle tecniche di attacco

Defending with an Hacker point of view

Soluzioni di CYBER SECURITY basate su **metodologie innovative** in grado di essere realmente in linea con gli elevati standard che oggi le aziende necessitano per difendersi

PIZZONI
MODERN OFFICE

Deceptive Bytes
Prevention by Deception

DECEPTIVE BYTES

PREVENZIONE CON L'INGANNO

DIFESA INFORMATICA ATTIVA DEGLI ENDPOINT

IN UN PANORAMA DI MINACCE AVANZATE IN CONTINUA CRESCITA, UNA SOLUZIONE STA FACENDO LA DIFFERENZA.

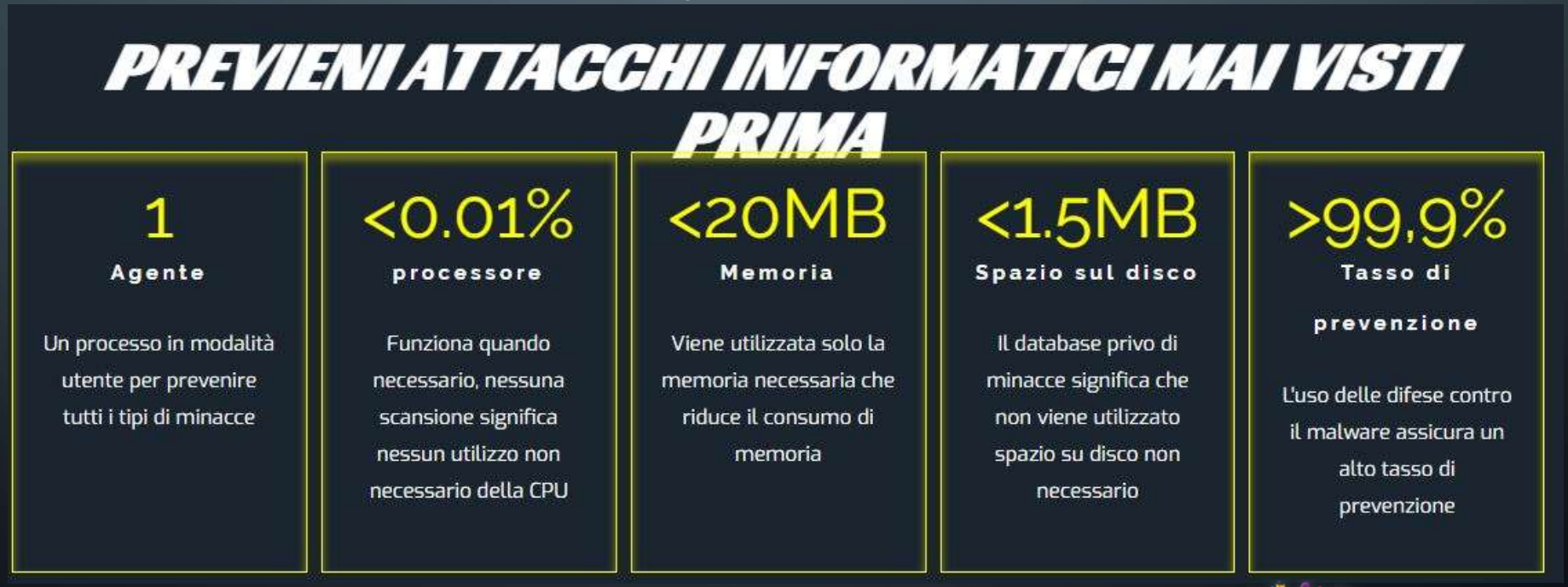
FORNISCE UNA PROTEZIONE A PIÙ FASI CHE RISPONDE DINAMICAMENTE ALLE MINACCE MAN MANO CHE SI EVOLVONO E UTILIZZA LO STESSO GIOCO DEGLI ATTACCANTI.

TASSO DI PREVENZIONE SUPERIORE AL 99,9% CONTRO RANSOMWARE E MALWARE.

PIZZONI
MODERN OFFICE

UTILIZZA LE DIFESE DEL MALWARE CONTRO DI ESSO

La soluzione è una piattaforma di prevenzione/inganno completamente incentrata sugli endpoint che crea informazioni dinamiche e ingannevoli, risponde alla natura in evoluzione del panorama delle minacce avanzate e interferisce con i tentativi degli aggressori di riconquistare l'ambiente che li scoraggia dall'eseguire i loro intenti dannosi, attraverso tutte le fasi di compromissione nella Kill Chain di attacco, coprendo tecniche malware avanzate e sofisticate, assicurandosi costantemente che tutti gli endpoint e i dati dell'azienda siano protetti.



PIZZONI
MODERN OFFICE

FORNISCE UNA SOLUZIONE INNOVATIVA CONTRO LE MINACCE NELLE RISORSE PIÙ CRITICHE ED ESPOSTE DELLE AZIENDE, I LORO ENDPOINT!
LA SOLUZIONE CREA INFORMAZIONI DINAMICHE E INGANNEVOLI CHE INTERFERISCONO CON QUALSIASI TENTATIVO DI RICOGNIZIONE DELL'AMBIENTE E SCORAGGIANO QUALSIASI RANSOMWARE O MALWARE DALL'ESEGUIRE I SUOI INTENTI DANNOSI...

PREVENTIVO E PROATTIVO

✓ Previene minacce sconosciute e sofisticate
✓ Tassi di prevenzione e rilevamento molto elevati
✓ Rilevamento e risposta in tempo reale

LEGGERO

✓ Protezione a livello di sistema con gestione precisa
✓ Distribuzione in pochi secondi e facile da usare
✓ Basso utilizzo delle risorse (CPU, memoria e disco)

SENZA FIRMA

✓ NESSUN aggiornamento costante
✓ Funziona in ambienti autonomi/disconnessi e VDI
✓ Blocca milioni di minacce utilizzando una sola tecnica di evasione

AFFIDABILE

✓ Elevata stabilità - funziona in modalità utente
✓ Attivazione di avvisi ad alta fedeltà
✓ Tasso di falsi positivi da basso a inesistente

PIZZONI
MODERN OFFICE

EFFICACE CONTRO

- APTs
- Ransomware
- CryptoMiners
- Zero-Day attacks
- Fileless attacks
- Trojans
- Evasive malware
- Worms
- Spyware
- Viruses
- Malicious documents (Office, PDFs, etc..)
- Malicious links (Browsers, email clients, etc..)
- Bots/Botnets
- PUPs/PUAs
- And more...

PIZZONI
MODERN OFFICE

SERAPHIC

Seraphic Security offre alle aziende protezione e controllo proprio dove ne hanno bisogno: direttamente nel browser, indipendentemente dal browser, dal fatto che sia installato su un dispositivo aziendale o personale, o che l'utente sia un dipendente o una terza parte.
Trattando la sicurezza del browser web come un cittadino di prima classe, e non come un ripensamento, è possibile consolidare le molteplici funzionalità di sicurezza e governance di diverse soluzioni in un'unica piattaforma di sicurezza del browser aziendale.

Browser – grande problema irrisolto

Il browser è diventato il principale strumento di produttività per i dipendenti a causa di tendenze trainanti come il lavoro in remoto, il BYOD e le applicazioni SaaS basate sul Web.
Le violazioni delle policy da parte dei dipendenti e gli attacchi degli hacker hanno trasformato il browser nella minaccia più seria per le aziende, tuttavia le soluzioni esistenti non riescono a proteggere il browser, sono difficili da utilizzare e da utilizzare e compromettono in modo significativo l'esperienza dell'utente.

PIZZONI
MODERN OFFICE

LE VULNERABILITÀ DEL BROWSER SONO IN AUMENTO

Chrome
^ **2,481**

Firefox
^ **1.993**

Explorer
^ **1,168**

Safari
^ **1.142**

PIZZONI
MODERN OFFICE

PREVENZIONE DEGLI EXPLOIT

Seraphic crea uno strato di astrazione tra il codice JavaScript e il motore JavaScript, interrompendo la prevedibilità del motore di esecuzione e rendendo un browser non sfruttabile da vulnerabilità note o sconosciute

PREVENZIONE DELL'INGEGNERIA SOCIALE

Seraphic blocca il phishing e altri attacchi di sociale engineering e previene la perdita di credenziali dell'utente utilizzando la telemetria dell'esecuzione del browser in tempo reale e il contesto di navigazione.

PREVENZIONE DEGLI ATTACCHI ALLE APP WEB

Seraphic protegge la vostra organizzazione da attacchi basati sulla vulnerabilità delle applicazioni Web come XSS, CSRF, clickjacking, cryptojacking, session hijacking e molti altri.

PREVENZIONE DELLA PERDITA DEI DATI

Seraphic garantisce che le risorse aziendali non vadano perse, non siano utilizzate in modo improprio o non siano accessibili a utenti non autorizzati. Seraphic ha visibilità su tutte le azioni degli utenti e l'analisi viene eseguita localmente, in modo che i dati sensibili non lascino il browser.

PIZZONI
MODERN OFFICE

CYFOX

CyFox è una soluzione XDR basata sull'intelligenza artificiale che riduce la complessità della gestione di più sistemi di cybersecurity consolidando diverse soluzioni e strumenti di sicurezza in un'unica piattaforma.
L'esclusivo motore di "Attack Hunting" del prodotto agisce come un analista informatico digitale che riduce i falsi positivi e il tempo di permanenza, accelera la risposta agli incidenti di cybersecurity e implementa autonomamente una strategia per identificare gli attacchi.

PIZZONI
MODERN OFFICE

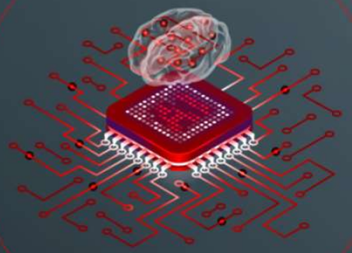
SEMPLIFICARE LE OPERAZIONI DI SICUREZZA

Proteggere la vostra organizzazione in crescita dalle minacce informatiche è fondamentale, ma sottrae tempo e risorse alle attività di crescita. Sia che la vostra azienda sia dotata di un'infrastruttura IT composta da una sola persona o di un team di sicurezza che sta ampliando le proprie competenze e risorse, CyFox vi permette di monitorare, raccogliere e analizzare i dati in tutta la vostra rete, dai dispositivi IoT ai file dei server.

Dotata di un motore di apprendimento automatico per la caccia agli attacchi in più fasi, di avvisi in tempo reale e di un monitoraggio continuo di ogni byte di dati, la nostra soluzione XDR di rilevamento e risposta autonomi è l'unica tecnologia di cui avrete bisogno per mantenere al sicuro le vostre risorse e la vostra azienda.

PIZZONI
MODERN OFFICE

MOTORE DI CACCIA AGLI ATTACCHI AI DI NUOVA GENERAZIONE



La nostra soluzione mappa le vulnerabilità esistenti dell'organizzazione e utilizza il marchio CyFox "Attack Hunter", dotato di intelligenza artificiale, per identificare le minacce. Quindi correla autonomamente tali vulnerabilità con i vettori di attacco noti, in modo che gli analisti possano facilmente rilevare gli attacchi ed eseguire immediatamente la mitigazione e la risposta.

PIZZONI
MODERN OFFICE

MONITORAGGIO ROBUSTO DELLE RISORSE

- Ottenere una panoramica di tutte le risorse aziendali
- Esaminare gli utenti e i gruppi del dominio
- Rilevare installazioni di software/hardware non autorizzate
- Visualizzazione di una rappresentazione visiva della mappa della rete
- Esportazione di report per soddisfare i requisiti di conformità: inventario delle risorse, vulnerabilità e riepiloghi esecutivi

PROTEGGERE LE VULNERABILITÀ

- Esaminare e gestire le vulnerabilità nei sistemi operativi e nel software degli elementi di rete da un unico cruscotto.
- Rilevamento di endpoint con credenziali predefinite e porte aperte
- Visualizzazione delle applicazioni non aggiornate
- Generare report per migliorare la vostra posizione di conformità
- Integrazione con NVD del NIST per essere sempre aggiornati sulle nuove CVE

ANALISI FORENSE AVANZATA

- Rilevare le anomalie analizzando il comportamento di utenti ed entità (UEBA)
- Monitorare la rete alla ricerca di attività dannose utilizzando un motore IDS.
- Impostazione di regole di policy personalizzate per mitigare le potenziali minacce
- Rilevare il software dannoso utilizzando il nostro cacciatore di malware
- Monitorare e rilevare l'accesso degli utenti ai dati sensibili con un motore FIM
- Visualizzazione dell'analisi del traffico per rilevare fughe di notizie, acquisizione di privilegi, attacchi e altro ancora.
- Utilizzo di honeypot per identificare movimenti laterali e vettori di attacco

PIZZONI
MODERN OFFICE

VOTIRO

VOTIRO

Votiro ZT Cloud fornisce contenuti sicuri agli utenti e alle applicazioni

La nostra soluzione API aperta elimina le minacce trasmesse dai file che colpiscono i lavoratori remoti, le applicazioni ricche di contenuti, i data lake, la supply chain e le interazioni digitali. Ottenete dati sicuri e informazioni sulle minacce su scala.

PIZZONI
MODERN OFFICE

RILEVARE E DISATTIVARE MALWARE E RANSOMWARE

Votiro ZT Cloud rileva le minacce note e sconosciute nei contenuti che arrivano nella vostra organizzazione e disarma proattivamente il file prima che raggiunga l'endpoint.

ANALISI DEI DATI PER MINACCE, PRIVACY E CONFORMITÀ

Conoscete meglio i vostri dati in entrata, sapendo che sono sicuri.

Mantenete la conformità e prendete le decisioni migliori per la vostra azienda.

RIDUZIONE DEL LAVORO PER I TEAM SOC, DATA SECURITY E IT

Dedicate meno tempo al blocco e alla messa in quarantena dei file e riducete i falsi positivi.

In questo modo si libera il tempo del team per concentrarsi su ciò che conta di più.

DOWNLOAD SICURO DEI FILE

Gli utenti lavorano da qualsiasi luogo e accedono ai contenuti utilizzando e-mail, browser web o piattaforme di collaborazione.

Votiro rileva e disarma le minacce senza compromettere la sicurezza e la produttività.

SCAMBI DI DATI SICURI

Le minacce dannose si nascondono negli FTP vulnerabili e nelle interazioni digitali automatizzate basate su API.

Votiro rileva e disarma le minacce note e sconosciute nei contenuti senza interrompere la continuità aziendale.

CARICAMENTO SICURO DEI CONTENUTI

Siete preoccupati per il caricamento di file dannosi su portali web, data lake e piattaforme di gestione dei dati rivolti ai consumatori?

Votiro applica i principi di Zero Trust per ridurre al minimo l'accesso ai dati, eliminare le minacce e garantire contenuti sicuri utilizzabili da applicazioni e servizi aziendali.

PIZZONI
MODERN OFFICE

L7DEFENSE

Gli abusi delle API sono il vettore di attacco più frequente che provoca violazioni dei dati per le applicazioni aziendali. Le aziende di tutte le dimensioni si affidano ad Ammune™ by ammune.ai per mantenere sicure le loro API.

PIZZONI
MODERN OFFICE

Ammune™ Copertura del flusso di sicurezza API

Ricerca & Classificazione

Visibilità completa della vostra "penetrazione API". Propria e di terze parti, esterna e interna

Data Validation

Tutti i flussi di dati devono essere conformi ai contratti API, alle politiche, ecc.

Protezione contro le minacce

Resilienza contro malware, exploit, abusi, credenziali rubate

Sicurezza nel trasporto

Crittografia del traffico, isolamento della rete, prevenzione DDoS, protezione anti-bot, ecc.

Analisi & automazione

Monitoraggio delle attività, rilevamento delle anomalie, mitigazione automatica delle minacce

PIZZONI
MODERN OFFICE

CARATTERISTICHE PRINCIPALI DI AMMUNE

- Soluzione completa, protegge le API, su scalaSoluzione completamente autonoma basata su ML/AI senza alcun intervento umano
- Genera automaticamente politiche di protezione ("regole")
- Protezione fin dalla prima richiesta
- Rari casi di errori falsi positivi (meno dello 0,1%)
- Piattaforma agnostica, on premises o on cloud
- Nessun impatto evidente sulla rete
- Costo totale di proprietà (TCO) molto basso

SENHA SEGURA

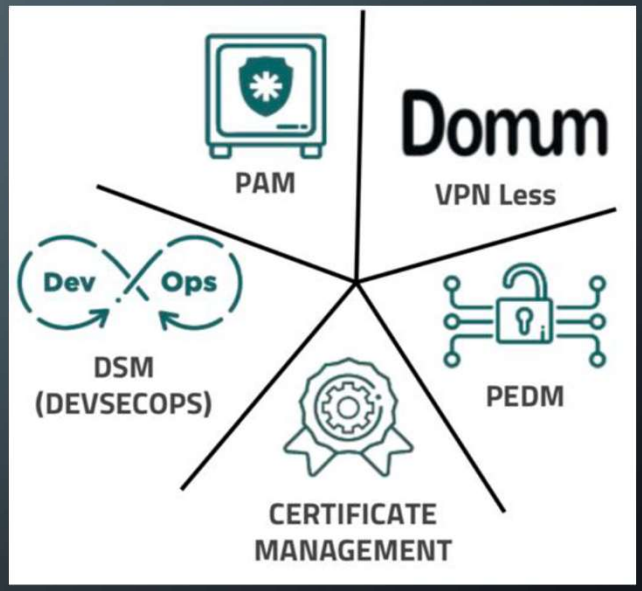
senhasegura

TECNOLOGIA

La piattaforma brasiliana Full Privilege Lifecycle PAM Automation and Security fondata 20 anni fa. Fornisce una soluzione completa di PAM (Priviledge Access Management)

VANTAGGI

- Soluzione integrata e completa di PAM, PEDM, Certificate Management, DSM
- Scopre e centralizza tu/e le credenziali privilegiate e crea autenticazione forti, autorizzazioni e responsabilità per i suoi usi.



PIZZONI
MODERN OFFICE

BRANDSHIELD

TECNOLOGIA

Basata sull'AI Brandshield è una soluzione tecnologica **anti-contraffazione e anti-phishing.** Esegue la rilevazione nel clear web, analizza le potenziali minacce e rileva tentativi di phishing, l'abuso e le violazioni dei marchi online, e le vendite contraffatte. I loro professionisti esperti e competenti rimuovono queste minacce senza sosta.

VANTAGGI

- Controllo completo degli avvisi di minaccia e delle azioni di contrasto
- Rilevatore di copie di siti web
- Avvisi push delle minacce
- Interruzione del database di siti di phishing
- Trappole Honeypot nei social media
- Bot Telegram anti truffe

PIZZONI
MODERN OFFICE

ASSAC NETWORK

Assac Networks

ASPIS

TECNOLOGIA

L’unica soluzione **ANTI-HACKING/GESTIONE MINACCE/ANTI-TAPPING** all-in-one per una protezione completa degli smartphone BYOD (bring your own device). La soluzione di Assac Networks fornisce protezione di livello militare per smartphone Android e iOS come offerta SAAS B2B.

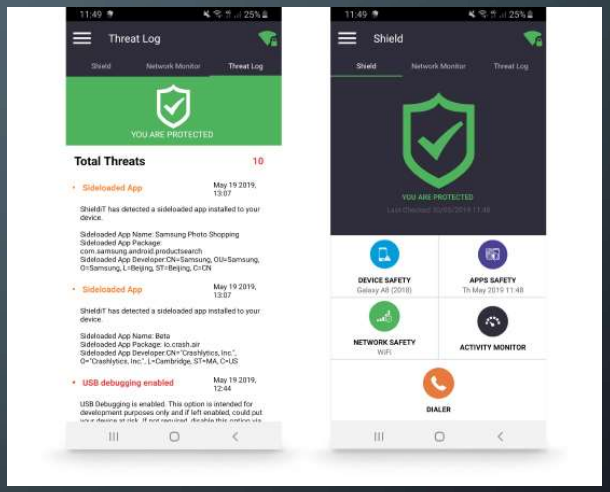
VANTAGGI

- Soluzione unica
- Comunicazioni point-to-any-point breve/ate
- Autonomous Intrusion Prevention
- System (IPS): ShieldiT difende dagli attacchi informatici sia sulla rete che sull'host
- Facile da implementare e integrare
- Crittografia di livello militare

PIZZONI
MODERN OFFICE

GESTIONE

Un cruscotto di gestione intuitivo e facile da usare che controlla centralmente tutte le funzionalità di ShieldiT:



- Sale voce e sale conferenze
- Connettività gateway PSTN
- Chat e allegati
- Configurazione VPN
- Azioni di mitigazione
- Gestione delle chiavi di crittografia
- Protezione cruciale per le aziende, le organizzazioni governative e i fornitori di servizi

La tecnologia di ShieldIT sfrutta l'esperienza ventennale di Assac Networks nella protezione delle reti delle organizzazioni di sicurezza interna e di difesa di tutto il mondo. Ora Assac Networks offre lo stesso livello di protezione agli smartphone aziendali, alle agenzie governative e agli operatori di telefonia mobile.

PIZZONI
MODERN OFFICE

TERAFENCE

Terafence
IoT Cyber Security

TECNOLOGIA

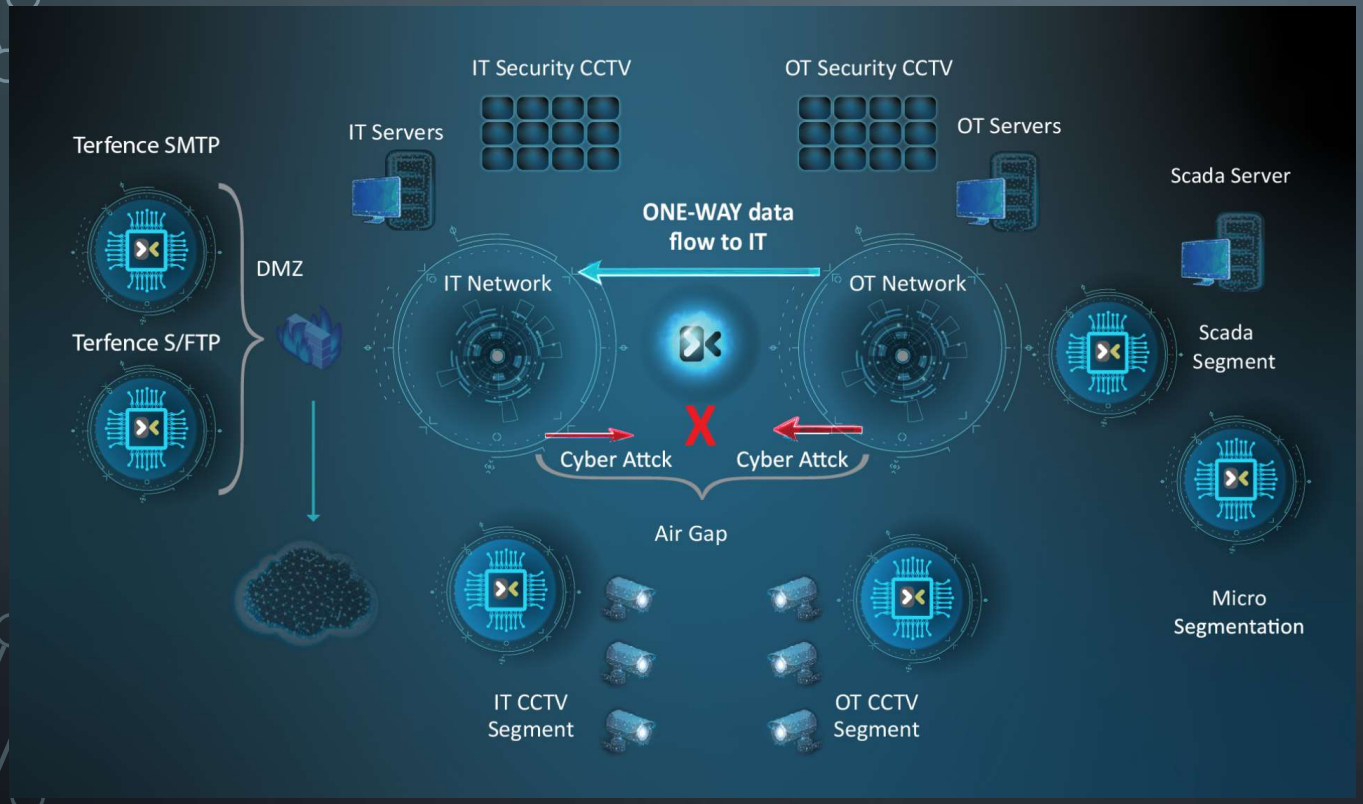
La comunicazione one-way che protegge la connettività dei dispositivi IoT e protegge le reti delle infrastrutture critiche. Una soluzione di protezione delle reti IoT basata su separazione fisica delle reti a livello hardware.

VANTAGGI

- Blocca completamente l'ingresso e l'uscita di dati da reti IoT e degli attacchi dannosi per i sistemi
- Comunicazione one-way tramite hardware ridotto ed economico.
- Conversione di più protocolli dalla rete protetta a più protocolli per la rete non protetta.
- Proliferazione IoT / sensori per proteggere dalle attività di botnet.

PIZZONI
MODERN OFFICE

COME FUNZIONA



Il dispositivo fisico Terafence è posizionato tra segmenti di rete di diversa classificazione e consente il flusso dei dati in base ai requisiti dell'applicazione. Una volta impostata una direzione, il percorso di ritorno, semplicemente, non esiste.

PIZZONI
MODERN OFFICE

CYBEREADY

TECNOLOGIA

CybeReady è l'unica piattaforma di Security Awarness basata su intelligenza artificiale che implementa una metodologia di apprendimento adattivo di grado superiore che garantisce un cambiamento nel comportamento dei dipendenti nei confronti degli attacchi di phishing. L'automazione dell'apprendimento umano di CybeReady consente ai dipendenti di formarsi tu/o l'anno, avanzando continuamente e adattando le proprie competenze per prepararsi agli attacchi di phishing del mondo reale.

VANTAGGI

La soluzione è completamente gestita, rendendo CybeReady la soluzione di formazione sulla consapevolezza della sicurezza con il costo totale di proprietà (TCO) più basso disponibile oggi.

PIZZONI
MODERN OFFICE

CYREBRO

CYREBRO

TECNOLOGIA

CYREBRO è il tuo SOC gestito di sicurezza informatica online che integra tutti i tuoi eventi di sicurezza con il monitoraggio strategico di intelligence proattiva sulle minacce e di risposta rapida agli incidenti.

VANTAGGI

•Gli algoritmi di rilevamento proprietari monitorano, analizzano e interpretano strategicamente le conseguenze degli eventi in tu/e le soluzioni di sicurezza e gli ambienti aziendali •Integrazione automatica con tutti i sistemi e le sorgenti •Analisi contestuale istantanea •Consiglia attività di remediation in tempo reale

PIZZONI
MODERN OFFICE

PIZZONI MODERN OFFICE S.R.L.