www.brain-it.it

www.andip.it

Associazione Europea Protezione Dati

www.tagdistribuzione.com

# La Cybersecurity
## al servizio della Privacy

**BrainIT** è nata come risposta ad una necessità: aiutare la produzione ed il business, sia dei privati sia delle PA, a creare sicurezza e proteggersi dai sempre più pericolosi rischi informatici. Effettuiamo nei nostri laboratori e con i nostri partner un continuo scouting innovativo per selezionare i migliori prodotti software e le migliori metodologie per ogni tipo di business, perché è importante ricordare che ogni azienda è diversa e unica, necessita quindi di cure e attenzioni dedicate e non omologate. Oggi, per avere successo, ogni azienda deve avere alla base una solida architettura di cyber security, riuscendo ad unire protezione e usabilità; solo cosi possiamo garantire ai nostri clienti operatività in piena sicurezza, mantenendo sempre l'efficienza.
Grazie ai rapporti con i nostri partner, oltre ad offrire soluzioni innovative ed efficaci, copriamo tutto il territorio nazionale e possiamo seguire, con successo e velocità, le aziende per il supporto post-vendita.
Ogni problematica relativa alla gestione e all'aggiornamento dei software è gestita da un team tecnico certificato e, attraverso l'assistenza on site o da remoto, i nostri clienti non temono interruzioni nei processi lavorativi né invasioni esterne.
Il nostro pensiero ci ha permesso di essere tra i primi ad implementare sicurezza e affidabilità nel nuovo mondo tecnologico che si sta aprendo davanti a noi conosciuto come futuro digitale.

DECEPTIVE BYTES
CYBER SECURITY

### INNOVATIVA TECNOLOGIA CYBER "DECEPTIVE" - AD INGANNO

Le caratteristiche principali:
Utilizza una nuova tecnologia per scovare attacchi anche sconosciuti e sofisticati con la metodologia dell'inganno (Deceptive). Fornisce una soluzione innovativa contro le minacce nelle risorse più critiche ed esposte delle imprese, i loro end-point! La soluzione risponde dinamicamente alle minacce mano a mano che si evolvono andando a creare informazioni dinamiche e ingannevoli che interferiscono con qualsiasi tentativo di ricognizione dell'ambiente e dissuadono l'attaccante dall'eseguire i suoi intenti malevoli, attraverso tutte le fasi di compromissione nella catena di attacco – coprendo tecniche di malware avanzate e sofisticate, assicurandosi costantemente che tutti gli end-point e i dati nell'azienda siano protetti.

In grado di intercettare il 98% degli attacchi noti o completamente sconosciuti, indipendentemente dal grado di complessità, richiede pochissime risorse e non deve essere costantemente aggiornato.
Premiato da GARTNER come COOL VENDOR.

Terafence
IoT Cyber Security

### PROTEGGI LA CONNETTIVITÀ DEGLI IoT E DELLE RETI DI INFRASTRUTTURE CRITICHE

La soluzione di TERAFENCE è hardware-based di avanguardia che attraverso una comunicazione one-way (flusso di dati unidirezionale) protegge da intercettazioni ed attacchi la connettività dei dispositivi IoT e protegge le reti delle infrastrutture critiche. La tecnologia mantiene il flusso di dati dei dispositivi IoT isolandoli fisicamente da tutti i tipi di minacce informatiche.

Questa tecnologia innovativa funge da barriera fisica che separa completamente i dispositivi IP dal loro centro di controllo, mantenendo intatto il flusso di dati unidirezionale e il controllo. In altre parole, nessun codice può aprire la porta della tua rete perché non c'è alcuna porta da aprire. Terafence non ha alcun indirizzo IP, nessun sistema operativo e nessuna CPU per negoziare il passaggio. L'unità Terafence è completamente trasparente alla rete.

LIGHT-SPEED
Artificial Intelligence for Life

### INTELLIGENZA ARTIFICIALE APPLICATA ALLA VIDEO SORVEGLIANZA

Monitorare le immagini di telecamere con l'intelligenza artificiale in ausilio o in sostituzione di operatori umani per aumentare la sicurezza delle aree pubbliche e dello sport.

ALARM:
videosorveglianza con RILEVAMENTO AUTOMATICO IN TEMPO REALE di situazioni di pericolo che coinvolgono persone, veicoli, animali, ambiente e infrastrutture: incidenti, sovraffollamento, uso scorretto di infrastrutture di trasporto, accesso in aree pericolose, ammaloramento e ostacoli su strade, fumo e incendi.

MONITOR:
videosorveglianza con MISURAZIONE AUTOMATICA IN TEMPO REALE di quantità e tipologia di persone, veicoli e animali, tempi di attesa presso servizi ed esercizi pubblici, flussi di persone (dislocazione, quantità, movimento) per favorirne la distribuzione omogenea, misurazione dei veicoli su strada (velocità, distanza mutua, occupazione di corsia, densità, tipologia, portata).

SORVEGLIA:
qualsiasi tipo di terreno (terra, asfalto, neve, cemento, pietra, ecc.), persone, veicoli e animali, corpi estranei.

RILEVA
incidenti, sovraffollamento, uso scorretto di mezzi di trasporto, accesso in aree critiche, ammaloramento e ostacoli su strade, fumo, incendi, atti vandalici, affissioni abusive.

SERAPHIC SECURITY

## SICUREZZA DEL BROWSER AZIENDALE SU ANY BROWSER

La sicurezza dei browser web è una pietra miliare del lavoro ibrido. Seraphic Security offre una protezione dagli attacchi per consentire una navigazione sicura ai dipendenti o agli appaltatori, oltre a controlli di governance avanzati per applicare le policy aziendali sui dispositivi gestiti e non gestiti. 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.
È possibile consolidare le molteplici funzionalità di sicurezza e governance di diverse soluzioni in un'unica piattaforma di sicurezza del browser aziendale.

I VANTAGGI DI SERAPHIC:
Fornisce un controllo coerente. Seraphic Security consente alle aziende di configurare il comportamento del browser e di implementare le politiche DLP in modo uniforme, indipendentemente dal browser utilizzato. Gli amministratori mantengono un controllo di visibilità a grana fine, gli utenti mantengono il loro browser preferito.

Nessuna firma, ML/AI o informazioni sulle minacce. La tecnologia brevettata di Seraphic Security offre una protezione senza precedenti contro un'ampia gamma di attacchi, tra cui sfruttamento, attacchi basati sul web e phishing. Fortifica i browser quando sono più vulnerabili: durante lo sfruttamento 0-day/non patchato N-day e durante le "ore d'oro" prima che i siti di phishing vengano categorizzati.
Una prevenzione degli attacchi che non dipende da feed in ritardo rispetto alle minacce.

TRASPARENTE PER GLI UTENTI:
A differenza di altri strumenti e infrastrutture di sicurezza, la soluzione Seraphic per la sicurezza del browser aziendale è veramente "dietro le quinte". Poiché non è necessario isolare il browser su un sistema remoto per garantire la protezione e non è necessario reindirizzare o smontare il traffico di rete per ottenere visibilità.
Non c'è alcun impatto sulle prestazioni, quindi non c'è alcun impatto sulla produttività.

GTB Technologies
Data Security that Works™

## GTB: DATA LOSS PREVENTION (DLP) - Data Protection that Works ™

Le soluzioni brevettate Next Generation of Data Protection di GTB mantengono i dati al sicuro on-premise, off-premise, inclusi endpoint Windows, Linux e Mac insieme al cloud, eseguendo scansione locale e monitoraggio in tempo reale con rilevamento accurato delle impronte digitali fuori rete.

GTB DATA PROTECTION PLATFORM
1. Rilevamento accurato dei dati delle impronte digitali (strutturati, semi e non strutturati) su tutti i moduli. Nessun limite al numero di campi;
2. Sistema di classificazione integrato sensibile al contenuto, molti obiettivi, incluso l'archiviazione nel cloud;
3. Funzionalità OCR sia per i dati in movimento che per i dati inattivi;
4. Scanner cloud nativi, per oltre 75 account cloud;
5. Unique File Share Auditing that's focused on the End User/ File share.

GTB DATA PROTECTION
Distribuzione semplificata.
Manutenzione ridotta, pronto all'uso.
Agente leggero o senza agente.
Non è richiesto alcuno schema di classificazione dei dati; i dati sensibili sono al centro.
Costruito per rilevare e rispondere all'esfiltrazione di dati.
Rilevamento completo dei dati, prevenzione e mitigazione dell'esfiltrazione dei dati, compresi quelli provenienti da minacce interne - estremamente difficile da aggirare.
Tempi di risposta drasticamente ridotti.
Possibilità di correggere la classificazione errata dei dati.
Capacità di prevenire l'esfiltrazione dei dati nel cloud.

ULTRARED

## ULTRARED: Piattaforma di gestione continua dell'esposizione alle minacce (CTEM) / Continuous Threat Exposure Management Platform (CTEM)

CTEM è una piattaforma multi-tool progettata per proteggere i tuoi assets in base alle vulnerabilità e alle minacce più importanti per la tua azienda.
Il Continuous Threat Exposure Management (CTEM) è un insieme di processi e funzionalità che consentono alle aziende di valutare in modo continuo e coerente l'accessibilità, l'esposizione e la sfruttabilità delle risorse fisiche e digitali di un'impresa.
ULTRARED consente di implementare e automatizzare un programma CTEM con 1 soluzione.
Soluzione all-in-one, per implementare un programma CTEM (Continuous Threat Exposure Management) al fine di :
- Eliminare il lavoro manuale, Fornire visibilità sulla superficie di attacco, Ridurre i falsi positivi, Comunicare il rischio ai dirigenti

ULTRA RED è il primo e unico fornitore CTEM. Un approccio completamente nuovo alla sicurezza informatica utilizzando una profondità di scansione senza pari per la mappatura della superficie di attacco, processi di convalida automatizzati, combinati con l'arricchimento della cyber intelligence.

VISIBILITÀ
Gestione della superficie di attacco esterna (EASM) Gestione della superficie di attacco delle risorse informatiche (CAASM) Scoperta, inventario e categorizzazione senza agenti delle tue risorse conosciute e sconosciute in meno di 3 clic. Servizi di protezione dai rischi digitali (DRPS)Trova tutti i casi di compromissione degli account sul deep web/dark web, sui social media e sui marketplace di app per la rimozione e la riparazione immediate.

VULNERABILITY MANAGEMENT (VM)
Visualizza tutte le vulnerabilità reali e prioritarie associate alle tue risorse attraverso la nostra funzione di rilevamento ricorsivo automatizzato. Filtriamo i falsi positivi per te e generiamo soluzioni politiche immediate, difendibili e attuabili

BREACH AND ATTACK SIMULATION (BAS)
Metti alla prova le tue difese perimetrali contro tutti i vettori di minacce conosciuti basati su Internet in un ambiente sicuro e protetto.

CONTINUOUS THREAT INTELLIGENCE (CTI)
Rimani al passo con la risoluzione delle vulnerabilità e con l'ottimizzazione del livello di sicurezza attraverso nuove e continue informazioni sulle minacce.

# IMHOTEP

## GESTIONE DEI PROCESSI, AFFIDABILITÀ DEI PROCESSI, METODOLOGIA E POLICIES. LA PRIVACY ON LINE

Il regolamento europeo ha eliminato il concetto di misure minime di sicurezza, inserendo al suo posto il concetto di sicurezza delle informazioni. Imhotep, seguendo queste direttive, si caratterizza per la sua gestione delle regole anche relativamente alle procedure di disaster recovery e piano di continuità operativa.

Implementa una gestione basata su:
Regole: Una minaccia è un'azione potenziale, accidentale o deliberata che può portare alla violazione di uno o più obiettivi relativi alla sicurezza e non solo, e quindi causare un danno all'azienda.

Documentazione: è possibile consultare tutta la manualistica come ad esempio: Registra informativa, Registra consenso, Nomine.

Struttura organizzativa: è possibile manutenere la struttura organizzativa che deve gestire le problematiche di Continuità Operativa.

Br@inIT
cyber security solutions
+39 06 84386162
sales@brain-it.it

ISO Stars EU
EN ISO 9001:2015