www.brain-it.it | www.andip.it | Associazione Europea Protezione Dati | www.tagdistribuzione.com | www.digitalbrainit.it

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 così 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.

ammune.ai

INNOVATIVA SOLUZIONE ISRAELIANA DI PROTEZIONE API BASATA SU INTELLIGENZA ARTIFICIALE

Le caratteristiche principali:
Ammune.ai è pioniera nell'applicazione di una nuova tecnologia di "apprendimento senza supervisione" denominata Ammune ™.
Ammune™ contiene un modello di apprendimento non supervisionato che monitora e analizza i dati in tempo reale, identificando e bloccando anche attacchi subdoli e furtivi e mitigandoli efficacemente senza una previa conoscenza dei parametri del modello di attacco.

Soluzione automatica INLINE che protegge qualsiasi interfaccia API anche durante un traffico molto elevato e con un livello assoluto di precisione.
SOLUZIONE CLOUD NATIVA CON SCALABILITÀ ELASTICA INTRINSECA

MODELLO DI DIFESA ZERO TRUST:
Esecuzione di DPI completi del traffico HTTP/s (richieste e risposte) alla risoluzione API come parte dell'analisi complessiva del traffico AI/ML, presupponendo che tutto il traffico sia potenzialmente dannoso.

PROTEZIONE IN LINEA, ALTAMENTE ACCURATA:
Identificazione del traffico dannoso con elevata precisione in tempo reale, utilizzando la tecnologia avanzata AI/ML.

SOLUZIONE AUTOMATIZZATA OUT-OF-THE-BOX:
Soluzione Plug & Play che inizia a proteggere API e app subito dopo la sua implementazione, quasi senza bisogno di intervento umano nel tempo.

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.

EYE-TRACK

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.

senhasegura®

FULL PRIVILEGE LIFECYCLE PAM AUTOMATION AND SECURITY PLATFORM

PROBLEMA:
La Mancanza di controllo sui privilegi delle credenziali diminuisce la sicurezza e non scoraggia gli attaccanti.

SOLUZIONE:
Scopri e centralizza tutti i privilegi delle credenziali per creare una autenticazione forte, autorizzazione e responsabilità per i suoi usi.

IMPATTO:
Riduce la superficie a rischio di attacco eliminando le credenziali non necessarie.

Presente nel quadrante Gartner 2021 come challenger.

BrandShield®

INNOVATIVA TECNOLOGIA DI RILEVAMENTO DELLE MINACCE ONLINE A DANNO DEL BRAND

Dalla protezione del marchio alla caccia alle minacce online. Basata sull'intelligenza artificiale, Brandshield è una soluzione tecnologica anti-contraffazione e anti-phishing.
La solida tecnologia di BrandShield 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.
BrandShield monitora e identifica phishing online, furti d'identità, vendite contraffatte, violazione del marchio e abuso del marchio su più piattaforme.

I VANTAGGI DI BRANDSHIELD:
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.

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