spritzmatter

your cybersecurity partner for innovation

LA NOSTRA IDENTITÀ

CyberSecurity

Offriamo una serie di servizi per il miglioramento della sicurezza informatica per le aziende.

Intelligenza Artificiale

Integra la potenza dell'Intelligenza Artificiale con sicurezza all'interno dei tuoi asset aziendali.

La nostra missione

Siamo una spin-off dell' Università di Padova, specializzata in soluzioni avanzate di cybersecurity.

La nostra missione è garantire un ambiente digitale sicuro per le aziende, proteggendo i dati e assicurando la continuità operativa.

Utilizziamo tecnologie innovative come l'intelligenza artificiale e siamo costantemente aggiornati sulle ultime tendenze per sviluppare soluzioni all'avanguardia.

Università degli Studi di Padova

Spritz Matter è uno SPIN-OFF dell'Università di Padova

Scan for more information

www.spritzmatter.com

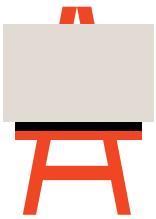
info@spritzmatter.com

Migliora la tua postura cyber

LA NOSTRA OFFERTA

Vulnerability Assessment
Un' attività mirata per mettere in risalto le minaccie informatiche degli asset aziendali (infrastruttura IT, Web App) e identificare una lista di remediations correttive.

Penetration Test
Un team di esperti che simuleranno un attacco informatico contro asset aziendali per identificare potenziali vulnerabilità e sfruttarle, conducendo attacchi che valutino la resilienza dei sistemi.



Laboratorio di Phishing
Un laboratorio interattivo con l'obiettivo di preparare al meglio i propri dipendenti nel riconoscere minaccie di spam e phishing.

Sistema di Difesa Antiphishing
Un sistema antiphishing da integrare all'interno dei tuoi asset aziendali. Grazie all'integrazione di sofisticati sistemi di Intelligenza Artificiale, la nostra soluzione permette di identificare anche le email di phishing piu' pericolose.

Secure AI Fast Prototyping
Un team di esperti dedicato per integrare all'interno dei tuoi processi aziendali soluzioni di Intelligenza Artificiale.

spritzmatter
your cybersecurity partner for innovation

Università degli Studi di Padova

Spritz Matter è uno SPIN-OFF dell'Università di Padova

Vulnerability Assessment

In cosa consiste. Il Vulnerability Assessment (VA) è un'analisi non intrusiva che serve a identificare e valutare le vulnerabilità di un sistema informatico, come reti, applicazioni o dispositivi aziendali. In pratica, si tratta di un "check-up" della sicurezza che aiuta a scoprire punti deboli che potrebbero essere sfruttati da hacker o malware per attaccare l'azienda.

Perché è utile?
Investire in un Vulnerability Assessment significa:

- Prevenire attacchi: Identificando le criticità prima che vengano sfruttate.
- Risparmiare tempo e risorse: Un attacco può causare danni economici, reputazionali e legali. Prevenire è sempre meno costoso che riparare.
- Garantire conformità: Aiuta a rispettare normative di sicurezza e protezione dei dati
- Rafforzare la fiducia: Con clienti e partner, dimostrando un impegno concreto verso la sicurezza.

Un'azienda sicura è un'azienda più forte. Il Vulnerability Assessment è il primo passo per proteggere il tuo business!

Quali aziende dovrebbero investire in un Vulnerability Assessment?

Il Vulnerability Assessment è essenziale per tutte le aziende, ma è particolarmente cruciale per quelle che:

- Gestiscono dati sensibili: Aziende che trattano dati personali, finanziari o sanitari, come banche, ospedali, studi legali e società di e-commerce.
- Hanno infrastrutture digitali complesse: Organizzazioni con reti aziendali estese, cloud o sistemi IoT, spesso presenti nel settore tecnologico, manifatturiero o della logistica.
- Sono soggette a normative stringenti: Settori regolamentati, come il finanziario, l'assicurativo o l'energetico, che devono rispettare standard di sicurezza specifici (GDPR, ISO 27001, NIS2, ecc.).
- Operano in settori strategici: Aziende che forniscono servizi essenziali, come utility, telecomunicazioni o fornitori della pubblica amministrazione, spesso nel mirino di attacchi cyber.
- Start-up e PMI innovative: Realtà in crescita che puntano sul digitale e sull'innovazione, ma che non possono permettersi di subire perdite economiche o di reputazione a causa di un attacco.

In sintesi: Se la tua azienda utilizza sistemi informatici, raccoglie dati o dipende da processi digitali, un Vulnerability Assessment è un passo fondamentale per proteggere il tuo business.

Penetration Test

In cosa consiste. Il Penetration Test (PT) è un'attività avanzata di sicurezza informatica che simula un attacco hacker ai sistemi aziendali per verificarne la resistenza. In altre parole, esperti di sicurezza (noti come ethical hackers) agiscono come veri cybercriminali per scoprire e sfruttare vulnerabilità, permettendo di identificare e risolvere i punti deboli prima che possano essere utilizzati da attaccanti reali. Il Penetration Test è più avanzato del Vulnerability Assessment perché, oltre a individuare le vulnerabilità, simula veri attacchi hacker per testare la reale resilienza dei sistemi, valutando l'impatto pratico delle falle di sicurezza.

Perché è utile?
Investire in un Penetration Test significa:

- Identificare e capire l'impatto delle vulnerabilità: Simulando attacchi reali, scopri quali debolezze e punti critici possono essere sfruttate e con quali ripercussioni.
- Quantificare i rischi: Comprendi l'impatto e la portata delle potenziali conseguenze di un attacco riuscito.
- Rafforzare la conformità e aumentare la fiducia in clienti e partner, dimostrando un impegno concreto verso la sicurezza.

Un Penetration Test non è solo un test, ma una vera e propria strategia per anticipare le minacce e proteggere il tuo business.

Quali aziende dovrebbero investire in un Penetration Test?

Il Penetration Test è essenziale per tutte le aziende, ma è particolarmente cruciale per quelle che:

- Gestiscono dati sensibili: Aziende che trattano dati personali, finanziari o sanitari, come banche, ospedali, studi legali e società di e-commerce.
- Hanno infrastrutture digitali complesse: Organizzazioni con reti aziendali estese, cloud o sistemi IoT, spesso presenti nel settore tecnologico, manifatturiero o della logistica.
- Sono soggette a normative stringenti: Settori regolamentati, come il finanziario, l'assicurativo o l'energia, che devono rispettare standard di sicurezza specifici (GDPR, ISO 27001, NIS2, ecc.).
- Operano in settori strategici: Aziende che forniscono servizi essenziali, come utility, telecomunicazioni o fornitori della pubblica amministrazione, spesso nel mirino di attacchi cyber.
- Start-up e PMI innovative: Realtà in crescita che puntano sul digitale e sull'innovazione, ma che non possono permettersi di subire perdite economiche o di reputazione a causa di un attacco.

In sintesi: Se la tua azienda utilizza sistemi informatici, raccoglie dati o dipende da processi digitali, sviluppa software o hardware, un Penetration Test è un prezioso strumento per individuare e mitigare minacce prima che possano causare danni.

Laboratorio di Phishing

In cosa consiste. Il laboratorio di phishing è un workshop della durata di 3 ore, ideata per educare i dipendenti a riconoscere e difendersi dagli attacchi di phishing, una delle minacce informatiche più diffuse.

Struttura del laboratorio

1. Parte Teorica (1 ora):
    - Introduzione al phishing: Cos'è, come funziona e quali sono le principali tecniche utilizzate dai cybercriminali.
    - Segnali di allarme: Analisi di casi reali per identificare gli indizi tipici di una mail di phishing (linguaggio, link sospetti, richieste urgenti).
    - Best practice: Consigli pratici per evitare di cadere nella trappola e comportamenti da adottare in caso di sospetto.
2. Parte Pratica e Gamification (2 ore):
    - I partecipanti accedono a una piattaforma interattiva progettata per simulare scenari reali.
    - Attraverso una modalità gamificata, i dipendenti devono analizzare e classificare una serie di email come phishing o legittime, accumulando punti per ogni risposta corretta.
    - Simulazioni realistiche con livelli di difficoltà crescente, che mettono alla prova le competenze apprese.

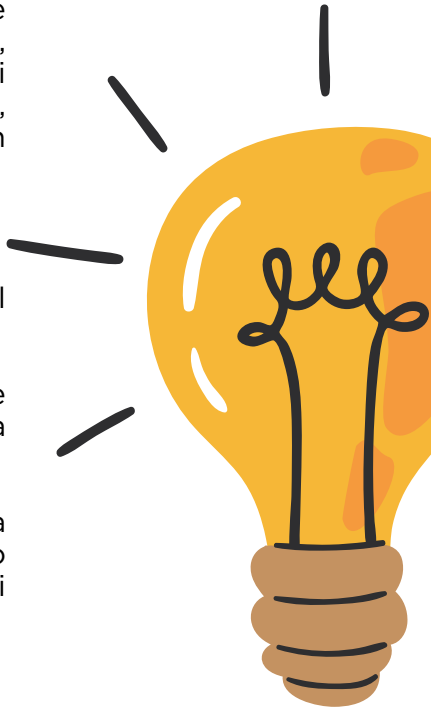
Perché sceglierlo? Il phishing rappresenta oggi una delle principali minacce alla sicurezza aziendale, con un impatto potenzialmente devastante sul business. Il nostro laboratorio fornisce ai vostri dipendenti gli strumenti e le competenze necessarie per riconoscere e rispondere correttamente ai tentativi di phishing, rafforzando così il primo livello di difesa della vostra organizzazione: il fattore umano.

- Approccio pratico che combina teoria e simulazioni reali, permettendo ai dipendenti di sviluppare le capacità di identificare i tentativi di phishing e aumentando la loro consapevolezza.
- Solida base di teoria e utilizzo della gamification per rendere la formazione sul phishing un'esperienza interattiva, garantendo un maggiore coinvolgimento e un migliore apprendimento.
- Workshop strutturato con simulazioni realistiche di crescente complessità, che permettono ai partecipanti di mettere alla prova le proprie competenze in un ambiente sicuro e controllato.

Investire nel rafforzamento delle competenze dei tuoi dipendenti riduce i rischi e protegge l'azienda da minacce, potenziali perdite economiche e danni reputazionali.

Sistema Antiphishing

In cosa consiste. Il nostro sistema antiphishing on-demand è una soluzione flessibile e avanzata che si integra facilmente nei tuoi asset aziendali, offrendo una protezione immediata e personalizzata contro le minacce di phishing. Grazie all'uso di sofisticati algoritmi di Intelligenza Artificiale, questa soluzione non si limita a identificare le email dannose, ma fornisce un supporto diretto e continuo ai tuoi dipendenti.



Come funziona?

- Analisi on-demand: Quando un dipendente ha dubbi su un'email sospetta, può inoltrarla al nostro servizio dedicato.
- Feedback personalizzato: Il nostro sistema analizza l'email e restituisce un responso rapido, indicando se si tratta di phishing o di una comunicazione legittima.
- Educazione continua: Oltre al feedback, il servizio fornisce una spiegazione dettagliata sui motivi per cui l'email è considerata sicura o pericolosa, aiutando i dipendenti a migliorare la loro capacità di riconoscere potenziali truffe.

Perché sceglierlo? Il nostro servizio antiphishing on-demand è la combinazione perfetta tra tecnologia avanzata e supporto umano. Riduce drasticamente il rischio di attacchi informatici, educa i tuoi dipendenti in tempo reale e rafforza la resilienza della tua azienda contro una delle minacce informatiche più comuni.

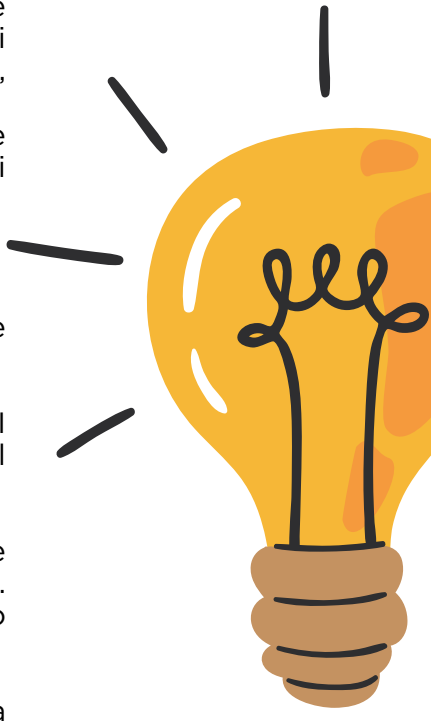
Cosa include l'abbonamento?

- Analisi On-Demand: Ogni volta che un dipendente è incerto riguardo un'email sospetta, può inoltrarla per un'analisi approfondita da parte del nostro sistema di Intelligenza Artificiale, che fornirà un feedback immediato, spiegando se l'email è legittima o phishing.
- Flessibilità: Puoi utilizzare il pacchetto di analisi per qualsiasi email sospetta e personalizzarlo in base alle tue esigenze.
- Supporto continuo: Ogni analisi è accompagnata da spiegazioni chiare e istruzioni per migliorare la consapevolezza dei dipendenti e prevenire futuri attacchi.
- Aggiornamenti periodici: Manutenzione e aggiornamenti regolari per garantire che il sistema sia sempre in grado di rilevare le minacce più recenti e sofisticate.

Secure AI Fast Prototyping

In cosa consiste

Il nostro servizio di Fast AI Prototyping è progettato per aiutare le aziende a sviluppare soluzioni di Intelligenza Artificiale su misura, ottimizzate per le loro esigenze specifiche. Dalla creazione di algoritmi personalizzati all'integrazione nei sistemi aziendali esistenti, ci occupiamo di ogni aspetto, garantendo performance elevate e massima sicurezza.
La nostra filosofia si basa sull'adozione del modello "AI on-premise", che consente alle aziende di mantenere il pieno controllo sui propri dati sensibili senza compromessi sulla privacy o conformità normativa.



Come funziona

- Analisi iniziale: partiamo con un workshop dedicato per comprendere le esigenze aziendali, definire i requisiti e identificare le sfide specifiche.
- Progettazione della soluzione: Disegniamo una strategia AI personalizzata che sfrutta le tecnologie più innovative, garantendo al contempo conformità agli standard di sicurezza e regolamentazione.
- Sviluppo della PoC (Proof of Concept): Creiamo un prototipo funzionale che dimostra la fattibilità tecnica e il valore aggiunto della soluzione. Questo include l'addestramento di modelli AI, la raccolta e il trattamento dei dati, e la validazione preliminare.
- Iterazione verso l'MVP (Minimum Viable Product): Una volta validata la PoC, espandiamo la soluzione verso un MVP, integrandolo nei flussi aziendali e ottimizzandolo per la scalabilità e le performance operative.

Perché sceglierlo

- Personalizzazione totale: Ogni soluzione è costruita su misura per adattarsi perfettamente alle tue necessità operative.
- Sicurezza: Il nostro approccio on-premise ti consente di mantenere il controllo completo sui tuoi dati, eliminando i rischi legati alla gestione da parte di terzi.
- Velocità ed efficienza: Dal concetto iniziale al prototipo, lavoriamo per ridurre al minimo i tempi di sviluppo senza sacrificare qualità o sicurezza.
- Innovazione continua: Sfruttiamo le tecnologie AI più recenti per offrire soluzioni all'avanguardia, competitive e orientate al futuro.

Perche' Scegliere Noi. Siamo il partner ideale per aziende che cercano soluzioni AI su misura, combinando innovazione, sicurezza e velocità. Grazie al nostro approccio Fast AI Prototyping, sviluppiamo rapidamente prototipi personalizzati mantenendo un focus rigoroso su compliance e protezione dei dati sensibili, grazie al modello AI on-premise. Con un team esperto e multidisciplinare, offriamo tecnologie all'avanguardia, garantendo performance elevate e soluzioni progettate per rispondere alle tue esigenze uniche. Collaboriamo con trasparenza, coinvolgendo il tuo team in ogni fase per costruire insieme un futuro digitale sicuro e innovativo.