SICURANEXT

Cyber security for everyone

www.sicuranext.com | *info@sicuranext.net*

SicuraNext

CHI SIAMO

SicuraNext si occupa di **cyber security** con l'obiettivo di trovare **una soluzione definitiva** al problema principale dell'era informatica: **il cyber crimine.**

Il nostro **team** è formato da **giovani talenti** esperti in cyber security.

Siamo in grado di offrire **soluzioni concrete pensate ad hoc,** grazie a un'analisi strutturata e personalizzata dei singoli casi.

Guardiamo all'innovazione con un **approccio moderno e personale.** Investiamo costantemente nella **ricerca e nello sviluppo** delle nostre competenze per essere pronti ad affrontare le nuove sfide che il mercato e l'ambiente informatico presentano e per **anticipare le future criticità.**

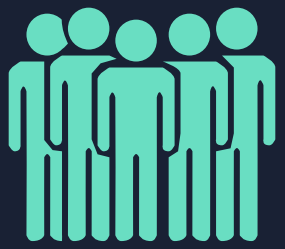
Certificazioni:
UNI EN ISO 27001:2013
UNI EN ISO 9001:2015

MISSION

Il nostro obiettivo è:
- **offrire un servizio innovativo di cyber security** gestita a 360° grazie a tecnologie all'avanguardia;
- **mantenere il pieno controllo del perimetro informatico** aziendale e dei dati inerenti a utenti, processi e tecnologie;
- **garantire** la massima **protezione del business e la reputazione** del cliente.

Società in
forte crescita

Team composto
da +50 persone



Rete
commerciale
distribuita
in tutta Italia

Oltre 300 clienti
in Italia

80% PMI
20% Enterprise

Cosa offriamo

OCTOFENCE

- New generation SOC
- Cyber Threat Intelligence (CTI)
- Log Management
- Web Application & API Protection

MANAGED SERVICE

Security Operation Center (SOC) gestito per conto del cliente

SERVICE OFFENSIVE

- Vulnerability Assessment
- Network Penetration Test
- Web Application Penetration Test

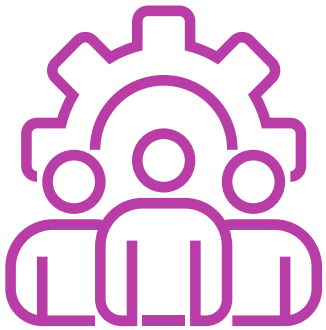
SICURALEARN

Piattaforma cloud di formazione aziendale a tema cyber security

OCTOFENCE

LA CYBER SECURITY SUITE PER LA PROTEZIONE DELLE PMI

Suite completa di tecnologie evolute per la **sicurezza informatica** della tua azienda



Team dedicato di analisti esperti per garantire un servizio gestito a 360°

Monitoraggio costante e sempre attivo, con **presidio garantito 24/7/365**

OCTOFENCE

SECURITY OPERATION CENTER (SOC)

SOC è l'acronimo di Security Operation Center ovvero un **centro operativo** tramite il quale vengono garantiti i **servizi di gestione, analisi, monitoraggio e difesa della sicurezza IT** di un'azienda.

Grazie a un team di professionisti, **il SOC analizza l'intero flusso dei dati** ed esercita un **controllo su tutti i dispositivi aziendali** – compresi quelli cloud e di terze parti – individuando e contrastando gli attacchi e le minacce alla cyber security prima che possano avere un impatto sull'azienda.

SMART DETECTION

Rilevazione in tempo reale delle minacce grazie all'unione dei *Cyber Security Feed*, *Log di sistema* e *Machine Learning*.

SISTEM ADVISORING IN TEMPO REALE

Notifiche IRT e interventi rapidi per fermare le minacce sul nascere con soluzioni repentine ed efficaci

ESPERTI E SOFTWARE DEDICATI

Analisti ed ethical hacker lavorano all'unisono con i nostri sistemi

TEAM DEFENCE

Professionisti e tecnologie per la **sicurezza difensiva** e il monitoraggio delle informazioni.

TEAM OFFENCE

Team specializzato nella **sicurezza offensiva** fisica e tecnologica.

TEAM CONSULTING

Team di **consulenza** per l'ottenimento di **certificazioni informatiche** di cyber security

OCTOFENCE

AUTOMATIC REMEDIATION

Il servizio garantisce un **intervento automatico e istantaneo del sistema** in risposta a predeterminate condizioni.

AGENT

L'agent raccoglie le informazioni di sicurezza del dispositivo e le invia al SOC che, in caso di minaccia in corso, **interviene tramite l'agent isolando completamente o parzialmente la macchina o l'utenza compromessa.**

INTEGRAZIONE CON IL CLOUD

Tramite un collegamento al cloud è possibile **monitorare** l'eventuale presenza di abusi di utenze privilegiate o **abusi sul sistema** e **reagire** di conseguenza, intervenendo in modo mirato e velocemente.

Il servizio è in grado di **riconoscere l'eventuale accesso** a una casella di posta elettronica da parte di un **IP malevolo** e reagisce con un **cambio password automatico** e con l'invio di una segnalazione al team IT.

OCTOFENCE

INTERVENTO SOC

In caso di **minacce critiche**, all'analisi e all'individuazione **segue l'intervento immediato di uno specialista**.

In caso di impossibilità di rimedio automatico, l'analista contatta il cliente fornendo assistenza e proponendo la soluzione di mitigazione più adatta.

OCTOFENCE

CYBER THREAT INTELLIGENCE (CTI)

CTI è l'acronimo di **Cyber Threat Intelligence** e rappresenta **l'insieme di teorie, procedure e strumenti per la raccolta e la condivisione di informazioni sulle minacce informatiche.**

L'obiettivo principale della CTI è la **creazione di strategie preventive**, tattiche di intervento e sistemi di monitoraggio.

DATA&CREDENTIAL LEAKAGE DETECTION

Rilevamento di credenziali trafugate che possono compromettere account e servizi

EARLY WARNING

Servizio di **notifica di attacchi in corso** per prevenire ripercussioni di business sul cliente

BRAND REPUTATION MONITORING

Individuazione delle **minacce che possono compromettere la reputazione** del cliente e brand abuse

VIP PROTECTION

Protezione da frodi grazie al monitoraggio di account, carte di credito e numeri di telefono

DOMINI

Monitoraggio di domini omografici e cloni usati per attacchi di phishing

DARK WEB

Controllo attivo del perimetro del cliente **sul dark e deep web**

OCTOFENCE

WEB APPLICATION & API PROTECTION (WAAP)

WAAP, acronimo di **Web Application & API Protection,** rappresenta l'**evoluzione del classico Web Application Firewall** (WAF) as a service.

Il WAAP non si limita a proteggere siti e applicazioni web dalle minacce elencate nella OWASP Top 10 ma va oltre; riesce a intercettare Bad Bot, mitigare attacchi DoS L7 o applicare uno strato di Virtual Patching per attenuare exploit di vulnerabilità non ancora corrette.

OWASP Top 10 Application Security Risks

- SQL Injection (SQLi)
- Cross Site Scripting (XSS)
- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)
- PHP Code Injection
- Java Code Injection
- HTTPoxy
- Shellshock
- Unix/Windows Shell Injection
- Session Fixation
- Scripting/Scanner/Bot Detection
- Metadata/Error Leakages

OCTOFENCE

WEB APPLICATION & API PROTECTION (WAAP)

SECURITY HEADERS

Aumenta la sicurezza degli utenti agendo direttamente sul loro browser

FREE SSL CERTIFICATES

Completa **gestione dei certificati SSL** senza costi aggiuntivi

BAD BOT DETECTION

Identifica le minacce elencate nella "OWASP TOP Automated Threats"

REPUTATION DATABASE

Blocca anonymous browsing, botnet, spammer, abusers e altre sorgenti malevoli

VIRTUAL PATCHING

Applica patch su vulnerabilità senza toccare il codice sorgente

LEAKED PASSWORD

Interagisce con *Have I Been Pwned?* per identificare password presenti in **data breach pubblici**

CACHE&PERFORMANCE

Incrementa e migliora le performance riducendo il ritardo nella risposta utilizzando tecniche di cache, compressione e minificazione dei file

DoS L7 PROTECTION

Protegge dalle diverse **tipologie di attacchi volumetrici** a livello applicativo

CUSTOM RULESET

Utilizzo di un **RuleSet dedicato** in caso di CMS come WordPress, Joomla, Drupal, ecc...

SICURALEARN

CYBER SECURITY AWARENESS

Sicuralearn è una piattaforma di e-learning ideale per il personale non specializzato delle organizzazioni pubbliche e private.
Il sistema si fonda su metodologie di formazione che tengono conto delle **modalità di apprendimento digitale** che risultano maggiormente efficaci ed è stato progettato per coinvolgere tutta l'organizzazione in un **percorso** di apprendimento educativo e stimolante, caratterizzato da un approccio "a rilascio costante e graduale".

PROBLEMA

Più del 90% degli attacchi Cyber sono riconducibili ad errori umani e all'interazione tra utente e dispositivi digitali.

OBIETTIVO

Trasformare il comportamento degli utenti e sviluppare una **consapevolezza del rischio digitale**.

SICURALEARN

CYBER SECURITY AWARENESS

SICURALEARN AWARENESS

Piattaforma avanzata di e-learning per coinvolgere tutta la forza lavoro in un programma formativo efficace.

- Servizio Cloud su base annuale;
- Apprendimento cognitivo;
- Programma didattico in formazione continua;
- Lezioni video presentate da un coach;
- Impatto 0 su HR e IT/SEC
- Elevato coinvolgimento dell'utente;
- Gamification pervasiva.

CAMPAGNE PHISHING

Piattaforma adattiva di allenamento anti-phishing, che produce risultati efficaci grazie alla sua metodologia avanzata e alle caratteristiche di automazione e di intelligenza artificiale.

- Servizio Cloud su base annuale;
- Allenamento esperienziale;
- Programma di attacco simulato in formazione continua;
- Simulazione di attacco personalizzato sulla base del profilo comportamentale dell'utente;
- Impatto 0 su HR e IT/SEC
- Aumento graduale e costante della resistenza agli attacchi phishing;
- Reportistica con analisi degli indicatori di rischio.

SicuraNext

IL NOSTRO VALORE AGGIUNTO

MADE IN ITALY

Servizio **monitorato e gestito in e dall'Italia** da un team di esperti

SERVIZIO COMPLETO

Formula ***chiavi in mano*** e gestione **24/7/365** con supporto dedicato

TECNOLOGIA ALL'AVANGUARDIA

Aggiornamento costante delle tecnologie e delle fonti di informazioni

RISPARMIO

Servizio *all-in-one* a una frazione del costo rispetto alla formazione di un team e una struttura in-house

VISIONE GLOBALE

Monitoraggio a 360° della sicurezza dell'infrastruttura e dell'immagine aziendale

RISPOSTA PROATTIVA

Notifiche coerenti e interventi tempestivi per ridurre al massimo le minacce verso il cliente

CI HANNO SCELTO

LATO SOC

ALTRI SERVIZI

SICURANEXT

GRAZIE PER L'ATTENZIONE

www.sicuranext.com | info@sicuranext.net | 0121 393642| C.so Vinzaglio 2 - 10121 Torino