MANAGED DETECTION AND RESPONSE SERVICE

Oltre le tecnologie: le competenze umane per combattere i cyber criminali.

Con l'evoluzione delle tecnologie, si è verificata un'evoluzione anche degli attacchi informatici, che utilizzano tecniche di evasione avanzate, repliche, cifratura dei dati e intelligenza artificiale: **le sole licenze antivirus non sono più sufficienti e nessuna organizzazione è immune**.

Ecco perché offriamo un **servizio di Managed Detection and Response**, gestito da **esperti di cyber sicurezza** che monitorano i sistemi **h24** per **365 giorni** all'anno ed agiscono proattivamente in caso di attacco.

Si stima che entro il 2025, il 50 % delle aziende si affiderà ad un team di Managed Detection and Response (MDR), per ovviare le tecnologie con una "*battaglia uomo a uomo*".

VANTAGGI PER LA TUA AZIENDA

ESPONENZIALE AUMENTO DELLA SICUREZZA DIGITALE

TEAM ESPERTO IN CYBER ATTACCHI DEDICATO H24

RISPOSTA PIU' COMPLETA ALLE MINACCE ZERO DAY

DRASTICA RIDUZIONE DEGLI INCIDENTI DI SICUREZZA

OFFERTA COMPLETA DI CYBERSECURITY AVANZATA

MANAGED DETECTION AND RESPONSE

I PUNTI DI FORZA

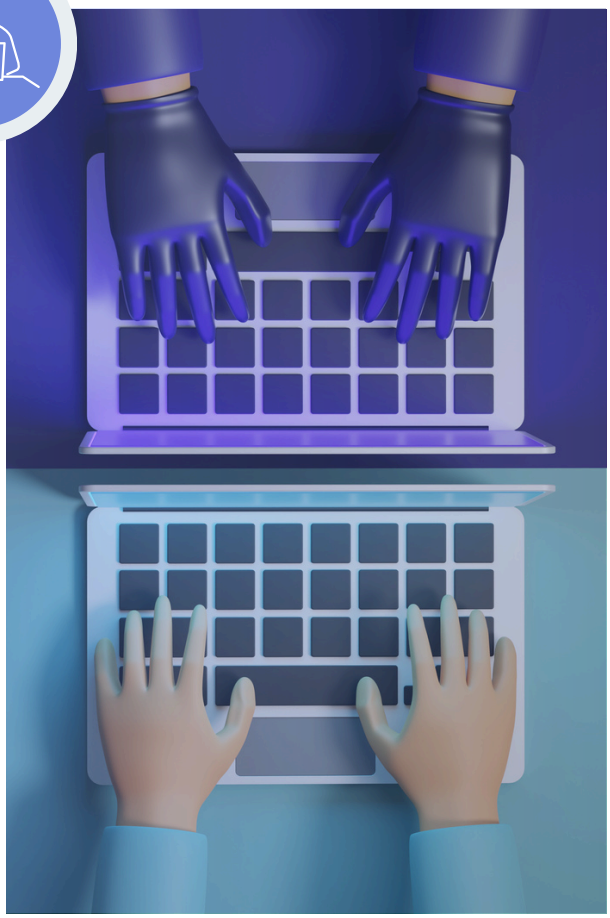
Il servizio MDR è la risposta completa alle minacce zero day: la combinazione di avanzate tecnologie di analisi, threat intelligence e le competenze di un vero e proprio **team di professionisti di cybersecurity** aumenta significativamente il grado di efficienza della sicurezza aziendale.

La soluzione offerta mira a rilevare gli attacchi che potrebbero eludere le difese tradizionali, ed a **rispondere tempestivamente in caso di attacco**, grazie ad un vero e proprio team di esperti in sicurezza informatica, il **Security Operation Center**, che **agisce** mitigando l'attacco, prima che possa compromettere l'intera infrastruttura IT.

DISPONIBILITA' DEL SERVIZIO 24/7 - 365 GG/ANNO

MITIGAZIONE DEL RISCHIO E REMEDIATION

HELP DESK ZUCCHETTI INFORMATICA 08.30 - 18:00



GESTIONE DELLA SICUREZZA ISOLAMENTO DELLE MINACCE H24

TEAM PROATTIVO E SPECIALIZZATO IN ANALISI/RISPOSTA CHE AGISCE IMMEDIATAMENTE CON L'ISOLAMENTO DEI DEVICE

RISPOSTA IMMEDIATA IN CASO DI EVENTO DI SICUREZZA TRAMITE AUTOMAZIONE E SISTEMI DI QUARANTENA

REMEDIATION DA REMOTO INCLUSA IN TUTTI I LIVELLI DI SERVIZIO

SECURITY AWARENESS E SERVIZI ADD ON

Formazione aziendale sulla cybersecurity e tutti i servizi correlati per la sicurezza IT.

Il **90%** delle minacce informatiche è ancora causato da errori umani: **sensibilizza la cultura della sicurezza informatica nella tua azienda** con il nostro servizio di Security Awareness.

La formazione aziendale è sempre un tassello importante per supportare la tua impresa ad evolvere, adeguandosi ai nuovi scenari: con il nostro **corso online sulla cybersecurity** scoprirai l'**importanza della sicurezza informatica nelle PMI** e la sua funzione, non solo come **necessità** ma anche come **investimento nel futuro** della tua attività.

VANTAGGI PER LA TUA AZIENDA

- SENSIBILIZZAZIONE DELLA CULTURA AZIENDALE SULLA SICUREZZA INFORMATICA
- AUMENTO DELLA CONSAPEVOLEZZA DEI RISCHI
- RIDUZIONE DEGLI ERRORI UMANI IN FASE DI ATTACCO

SECURITY AWARENESS E SERVIZI ADD ON

I PUNTI DI FORZA

Per promuovere una **cultura della sicurezza informatica** più consapevole all'interno della tua azienda e per informare collaboratori e utenti sui **rischi** e le **possibili tipologie di attacco** a cui potrebbero essere esposti durante l'"attività lavorativa, proponiamo un **percorso di formazione in modalità on demand**, caratterizzata da mini video ottimizzati per l'apprendimento e test delle conoscenze.

PIATTAFORMA E-LEARNING ADATTA A TUTTI [MAX. 160 MIN]

POSSIBILITA' DI RICHIEDERE FORMULE CON SIMULAZIONI DI ATTACCHI PHISHING

ATTESTATO FINALE PER I PARTECIPANTI

I SERVIZI ADD ON

VULNERABILITY ASSESSMENT

Attenta scansione delle tecnologie presenti all'interno di un perimetro o di un'infrastruttura informatica con lo scopo di ottenere un inventario completo delle vulnerabilità presenti. Reportistica in ottica di compliance o certificazioni

PENETRATION TEST

Simulazione di attacco dall'esterno del perimetro aziendale verso gli indirizzi IP pubblici, attraverso i quali vengono esposti portali WEB, server FTP o scambio dati, server di posta o terminatori VPN.

WAAP

Attenta scansione delle tecnologie presenti all'interno di un perimetro o di un'infrastruttura informatica con lo scopo di ottenere un inventario completo delle vulnerabilità presenti.

ZUCCHETTI Informatica