

Vigilant Shield

La sicurezza della tua azienda,
seguita giorno e notte.

Specialisti controllano accessi, posta e computer, intervengono sulle minacce e affiancano il responsabile IT nelle azioni di miglioramento.

CHE COSA FA PER LA TUA AZIENDA

Dai segnali di rischio alle azioni concrete

Per le aziende che usano Microsoft 365: specialisti controllano in tempo reale i segnali di sicurezza degli accessi, della posta e dei computer inclusi nel servizio. Quando individuano una minaccia, la analizzano, avvisano i referenti e intervengono secondo le autorizzazioni concordate.

01 **Controllo giorno e notte**

Il centro operativo di sicurezza segue le segnalazioni 24 ore su 24, tutti i giorni, anche nei festivi. Distingue le anomalie dai possibili incidenti e verifica che i dati di controllo continuino ad arrivare. Adegua le regole per ridurre le segnalazioni inutili.

02 **Interventi per limitare il danno**

Gli specialisti possono interrompere immediatamente un accesso sospetto o isolare dalla rete un computer colpito da un attacco, nei limiti concordati. Svolgono le azioni correttive previste, verificano il risultato e informano l'azienda.

03 **Informazioni chiare per chi decide**

Il consulente AI Defender aiuta a tenere aggiornato ciò che è coperto dal servizio, mantiene i registri degli eventi e degli incidenti e prepara sintesi comprensibili per la direzione. Affianca il responsabile IT nelle priorità emerse.

Come interveniamo sulle minacce

Un esempio: credenziali email aziendali rubate

Immagina che un estraneo rubi i dati di accesso alla posta di un dipendente e riesca a entrare nella sua casella. Il servizio può rilevare segnali anomali e attivare questo percorso:

- | | | |
|-----------|------------------------|--|
| 01 | Verifica | Gli specialisti analizzano il segnale e valutano se si tratta di un accesso legittimo o di un possibile accesso abusivo. |
| 02 | Intervento | Quando previsto dalle autorizzazioni, interrompono gli accessi sospetti e applicano le misure necessarie, per esempio il cambio della password. |
| 03 | Comunicazione | Informano i referenti aziendali attraverso i canali concordati e indicano le eventuali attività da svolgere internamente. |
| 04 | Tracciamento | Documentano ciò che è accaduto e gli interventi effettuati. Il consulente aggiorna i registri e aiuta l'azienda a comprendere le priorità successive. |
| 05 | Lezioni apprese | Specialisti, consulente e responsabile IT ricostruiscono come è avvenuto l'accesso. Definiscono correzioni, responsabili e scadenze; verificano poi l'attuazione e l'efficacia delle misure. |

Esempio illustrativo: le azioni dipendono dai sistemi collegati, dai permessi disponibili e dalle procedure concordate.

Un messaggio sospetto? La tua segnalazione protegge tutti.

Se un dipendente segnala un'email sospetta, gli specialisti la analizzano. Se risulta dannosa, possono cercarla e rimuoverla anche da tutte le altre caselle aziendali coinvolte e incluse nel servizio. Verificano l'esito e gli eventuali segnali di compromissione, secondo i permessi e le procedure concordate.

Che cosa ricevi

La mappa del servizio

Utenti, computer e servizi coperti, referenti e modalità di intervento.

Resoconti tecnici

Riepiloghi periodici e resoconti degli incidenti, con azioni ed esiti.

Registri e sintesi per la direzione

Incidenti e lezioni apprese: correzioni, responsabili, scadenze e verifiche.

Un servizio definito insieme

Come si parte

Conosciamo il tuo ambiente. Individuiamo utenti, computer e servizi da seguire e verifichiamo le licenze disponibili.

Concordiamo come lavorare. Definiamo chi contattare, quali interventi autorizzare e quali attività restano al responsabile IT.

Verifichiamo il funzionamento. Colleghiamo i sistemi, proviamo il percorso di segnalazione e risposta e avviamo i resoconti periodici.

Che cosa viene precisato nell'offerta

Il controllo tecnico è previsto 24 ore su 24. Il supporto del consulente ha orari e impegno concordati. L'offerta conferma sistemi inclusi, licenze, tempi di intervento, frequenza dei resoconti e costi.

Sono controllati direttamente i computer attivati nel servizio e collegati alla piattaforma. Osservare gli accessi di un utente non significa proteggere automaticamente ogni computer o telefono che utilizza.

Protezioni aggiuntive per posta e accessi, gestione di rete, telefoni e server, ripristino dei dati e indagini specialistiche sono attività da concordare a parte. La gestione quotidiana dei computer resta al personale informatico dell'azienda.

Parliamone: info@myma.sm

Piccolo glossario

AI	Artificial Intelligence: intelligenza artificiale. È la sigla nel nome AI Defender; le valutazioni e gli interventi del servizio restano affidati agli specialisti.
SOC	Security Operations Center: centro operativo di sicurezza. È il gruppo di specialisti che analizza le segnalazioni e gestisce gli interventi tecnici.
MDR	Managed Detection and Response: servizio gestito di rilevazione e risposta alle minacce. È il tipo di servizio descritto in questa brochure.
PC	Personal Computer: computer utilizzato per lavorare, portatile o fisso.
IT	Information Technology: informatica. Il responsabile IT segue i sistemi informatici aziendali.
Lezioni apprese	Lessons learned: ciò che impariamo da un incidente per correggere le debolezze e ridurre il rischio che si ripeta.
Server	Sistema che mette dati e applicazioni a disposizione di più utenti.
Incidente informatico	Un evento che compromette o mette concretamente a rischio dati, accessi o funzionamento dei sistemi.