

# Cyber Defense 365

*Per offrire alla tua azienda un ambiente IT più sicuro e protetto*



La protezione, l'analisi e le strategie di reazione all'interno di una corretta progettazione della sicurezza informatica sono attività fondamentali non trascurabili per un dipartimento IT.

Una solida pianificazione e attuazione delle misure di sicurezza facilita la protezione del sistema informativo aziendale anche se, per essere ancor più attenti, è importante poter accertare costantemente il livello di protezione applicato e pianificare le eventuali azioni di remediation. Questo approccio consente di minimizzare la superficie di attacco e la vulnerabilità.

Con una profonda conoscenza delle minacce e una comprovata esperienza decennale nell'ambito della sicurezza IT, Microsys ha sviluppato Cyber Defense 365, una serie di servizi che sfruttano anche i servizi di Microsoft Azure, studiati per pianificare e migliorare la Security Posture di un'azienda, in particolare:

- introduce un approccio strutturato alla sicurezza
- mantiene costante il livello di attenzione
- organizza la protezione negli ambiti identità, accessi, dispositivi, dati e infrastruttura
- La creazione di strumenti atti a gestire in modo sicuro le attività amministrative di infrastruttura con credenziali privilegiate
- protegge il Modern Workplace

## **Awareness**

Workshop tecnico, rivolto ai dipartimenti IT, per la valutazione dei rischi sul tema sicurezza. E' possibile estendere l'attività anche a ruoli di business  
Obiettivo: creare maggiore consapevolezza sul tema della sicurezza e mappare le soluzioni e gli strumenti Microsoft

## **Project services**

- Security Assessment, Gap Analysis e Remediation Plan
- Selezione e prioritizzazione dei servizi Microsoft da abilitare per la protezione, controllo e gestione della sicurezza
- Avvio del servizio complessivo di gestione e controllo
- La creazione attraverso Microsoft Azure dei pc virtuali a disposizione per le attività amministrative di infrastruttura con le credenziali privilegiate

## **Managed services**

Gestione e monitoraggio periodico in modalità Security Operations Center (SOC), con review trimestrale o quadrimestrale, per preservare costantemente le attività di protezione eseguite e valutare i rischi a cui si è esposti.

La soluzione prevede due gruppi di lavoro a supporto:

**Blue team** - composto da specialisti costantemente aggiornati:

- Responsabili della progettazione della sicurezza (identità e accessi, dispositivi e dati)
- Organizzano le attività di controllo
- Pianificano le strategie di remediation
- Eseguono il monitoraggio e i controlli periodici
- Allertano in caso di criticità

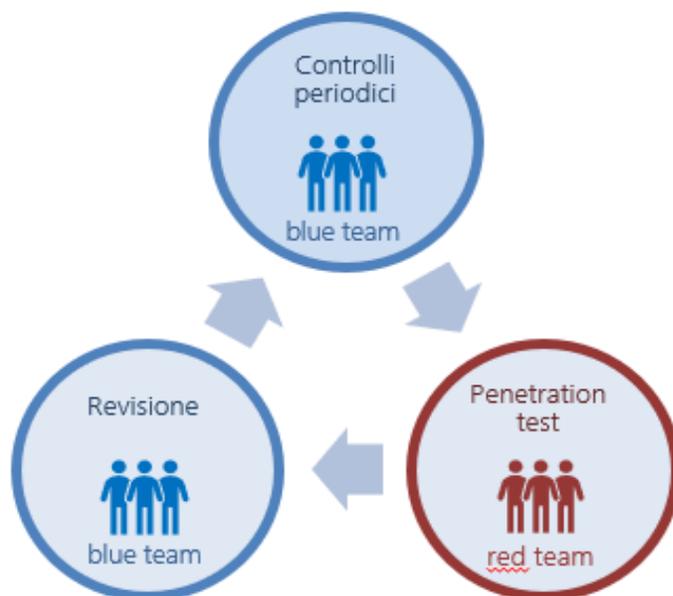


**Read Team** - gruppo di lavoro gestito da una terza parte per:

- Eseguono test per verificare le vulnerabilità (External network, Internal network, Wi-Fi network, Corporate Workstation, Web Application, Mobile Application, campagna di Phishing)
- Creano la reportistica dettagliata sulle vulnerabilità

### Perchè Cyber Defense 365?

- Per diffondere la cultura della sicurezza in azienda
- Pre creare procedure di controllo e remediation
- Per verificare le vulnerabilità
- Per avere il supporto da parte di un team di professionisti esperti e altamente competenti sul tema



Per ulteriori informazioni

Visitare il sito [www.msys.it](http://www.msys.it)

Contattare Chiara Zaninello, e-mail [chiaraz@msys.it](mailto:chiaraz@msys.it) telefono +39 02 303 707 01