

# Cyber Defense 365

## Protect, Detect, Respond



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

Una solida pianificazione delle misure di sicurezza può effettivamente contribuire a semplificare la protezione del sistema informativo aziendale, attraverso misure preventive costantemente verificate e riverificate ed aggiornate per minimizzare la superficie d'attacco.

Con conoscenza delle minacce sulla sicurezza ed esperienza nell'ambito, Microsys ha sviluppato Cyber Defense 365, una suite di servizi per prevenire e difendersi dalle minacce informatiche. La soluzione permette di:

- Introdurre un approccio strutturato alla sicurezza
- Mantenere alto nel tempo il livello di attenzione
- Focalizzare la protezione sull'identità, gli accessi, dati e dispositivi per garantire la migliore sicurezza a supporto del lavoro in mobilità

La soluzione Cyber Defense 365 una suite di servizi:

<b>Awareness</b>	Workshop tecnico, rivolto al dipartimento IT ed al business dell'azienda per: <ul style="list-style-type: none"><li>• Sensibilizzare l'azienda sul tema della sicurezza IT</li><li>• Creare maggiore consapevolezza</li><li>• Identificare le soluzioni Microsoft a supporto della gestione della sicurezza</li></ul>
<b>Project Services</b>	Attività di assessment ed analisi per definire una roadmap di interventi ed iniziare il processo di evoluzione della Security Posture (protect): <ul style="list-style-type: none"><li>• Selezione ed abilitazione dei servizi Microsoft per il controllo e la gestione della sicurezza (detect)</li><li>• Avvio del servizio di gestione e controllo della sicurezza (respond)</li></ul>
<b>Managed Services</b>	Gestione e monitoraggio giornaliero tramite un Security Operations Center (SOC), con review trimestrale o quadrimestrale delle politiche di sicurezza

La soluzione presume due gruppi di lavoro a supporto:

**Blue team**, composto da figure specialistiche costantemente aggiornate:

- Responsabili del monitoraggio e dei controlli periodici di sicurezza (su identità, accessi, dispositivi e dati)
- Gestione degli allarmi, criticità e revisione dei processi di controllo



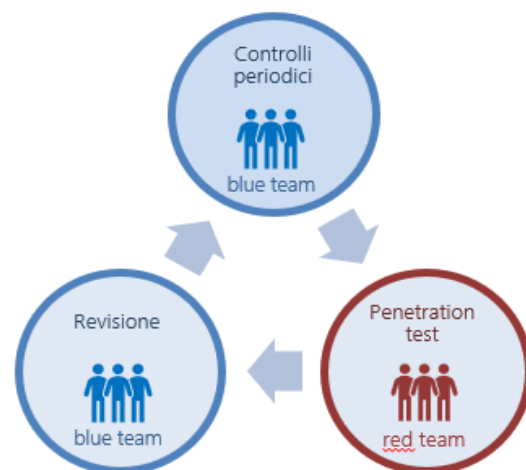
**Red Team**, gruppo di lavoro esterno per:

- Penetration Test per simulare e prevenire gli attacchi (external network, internal network, Wi-Fi network, corporate workstation, web application, mobile application, campagna di phishing)
- Creazione della reportistica dettagliata sulla vulnerabilità e le criticità constatate



## Perchè Cyber Defense 365?

- Diffondere la cultura della sicurezza in azienda
- Aumentare la protezione delle identità e dei dati aziendali
- Aiutare a strutturare gli investimenti e il piano aziendale sulla sicurezza informatica
- Essere costantemente seguiti o affiancati da un gruppo di professionisti esperti e competenti sul tema



Per ulteriori informazioni  
Visitare il sito [www.msyst.it](http://www.msyst.it)  
Contattare Chiara Zaninello, e-mail [chiaraz@msyst.it](mailto:chiaraz@msyst.it)  
telefono +39 02 303 707 01