HORNETSECURITY

365 TOTAL PROTECTION

AI-POWERED, ALL IN ONE M365 SECURITY, BACKUP & GRC

Stai correndo tra le conversazioni di Teams in ufficio e soprattutto quando sei in giro?

FANTASTICO! I CYBERCRIMINALI LO ADORANO.

Quante volte tu e i tuoi colleghi preferite le chat di Teams alle e-mail? La comodità di una conversazione veloce in tempo reale spesso batte le e-mail più lente, rendendole una scelta sempre più popolare per fare le cose in azienda.

Microsoft Teams è perfetto per discutere o condividere rapidamente informazioni, soprattutto quando sei in viaggio e usi l'app mobile. Più siamo veloci, più possiamo fare in un dato lasso di tempo, aumentando la nostra produttività e raggiungendo gli obiettivi con maggiore facilità.

Ma questo è solo un lato della medaglia.

Più ci concentriamo sul portare a termine le cose velocemente, meno siamo propensi a prestare attenzione ai dettagli e più cose iniziano a sfuggirci, comprese le misure di sicurezza come non cliccare su link ricevuti, anche se inviati da contatti apparentemente sicuri.

E i criminali informatici ne approfittano.

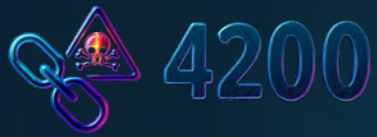
UN ATTACCO INFORMATICO SU TRE UTILIZZA UN ACCOUNT COMPROMESSO

Uno studio del 2025 mostra che gli attacchi basati sull'identità costituiscono il 30% degli attacchi totali. Gli hacker non hanno più bisogno di violare i sistemi: basta che effettuino l'accesso utilizzando credenziali valide rubate con un attacco AITM (adversary-in-the-middle) o acquistate sul dark web.

LASCIA CHE AI.MY ANALIZZI I LINK IN TEAMS PER INDIVIDUARE POTENZIALI RISCHI

1000 dipendenti

12% dei quali contiene link



links potenzialmente dannosi

Probabilmente ti stai già proteggendo dai link dannosi nelle e-mail grazie a soluzioni come Advanced Threat Protection. Ma con sempre più persone che preferiscono chat in tempo reale veloci e convenienti, devi dare a Microsoft Teams la stessa protezione.

TEAMS PROTECTION DI HORNETSECURITY, BASATO SULL'AI CYBER ASSISTANT, AUTOMATIZZA TUTTA LA SICUREZZA PER TE.

TEAMS PROTECTION protegge un tenant dagli account compromessi internamente scansionando tutti i messaggi contenenti URL e inviando immediatamente un messaggio di avviso nella conversazione tramite il bot AI Cyber Assistant. Teams Protection utilizza la tecnologia AI utilizzata in Secure Links di Hornetsecurity:

Modelli intelligenti analizzano le caratteristiche chiave degli URL e delle pagine (ad esempio reindirizzamenti, percorsi dei file, script, ecc.) per identificare i contenuti dannosi.

Algoritmi di apprendimento automatico supervisionati e non supervisionati analizzano più di 47 caratteristiche degli URL e delle pagine web, cercando comportamenti dannosi, tecniche di offuscamento e reindirizzamenti URL.

Deep learning: i modelli di Computer Vision analizzano le immagini per estrarre le caratteristiche rilevanti usate negli attacchi di phishing, inclusi loghi di marchi, codici QR e contenuti testuali sospetti incorporati nelle immagini.

Gli amministratori possono eliminare intere conversazioni contenenti messaggi dannosi e **impedire ai mittenti di accedere a Teams**. Possono anche utilizzare la funzione **di correzione automatica che elimina automaticamente le chat in cui è stato trovato un messaggio dannoso** se la chat è stata creata meno di 10 minuti prima dell'invio del messaggio dannoso.

LA PROTEZIONE DI TEAMS FA PARTE DEL NUOVO PIANO 365 TOTAL PROTECTION

PLAN 4

Il nuovo piano 365 Total Protection 4 è potenziato da AI Cyber Assistant, un potenziamento automatico della sicurezza che **supporta gli utenti finali e gli amministratori nelle loro operazioni quotidiane**, garantendo comunicazioni sicure e un carico di lavoro alleggerito. AI Cyber Assistant si evolve continuamente grazie alla nostra tecnologia di apprendimento automatico, fornendo un supporto inestimabile.

365 TOTAL PROTECTION

AI-POWERED, ALL IN ONE M365 SECURITY, BACKUP & GRC

PLAN 4

INCLUDES 1 + 2 + 3

			POWERED BY AI CYBER ASSISTANT		
SECURITY AWARENESS	PERMISSION MANAGEMENT	DMARC REPORTING & MANAGEMENT	AI RECIPIENT VALIDATION	TEAMS PROTECTION	AI EMAIL SECURITY ANALYST
PHISHING & ATTACK SIMULATION	PERMISSION ALERTS	ENHANCED EMAIL REPUTATION & DELIVERY	COMMUNICATION PATTERN ANALYSIS	CHAT-BASED THREATS MONITORING	AI ANALYSIS OF USER REPORTS
ESI® REPORTING	PERMISSION AUDIT	EASY DNS MANAGEMENT & OPTIMISATION	SENSITIVE DATA CHECK	AI PHISHING DETECTION & RESPONSE	AI RESPONSE & AWARENESS

PRONTO A METTERTI AL PASSO CON I TEMPI?

Scopri oggi il futuro della sicurezza informatica con una **PROVA GRATUITADELLA** soluzione più completa per Microsoft 365 sul mercato.