Cybersecurity

CYBERSECURITY SENZA TECNICISMI: IL GLOSSARIO PER TUTTI!

TeamSystem

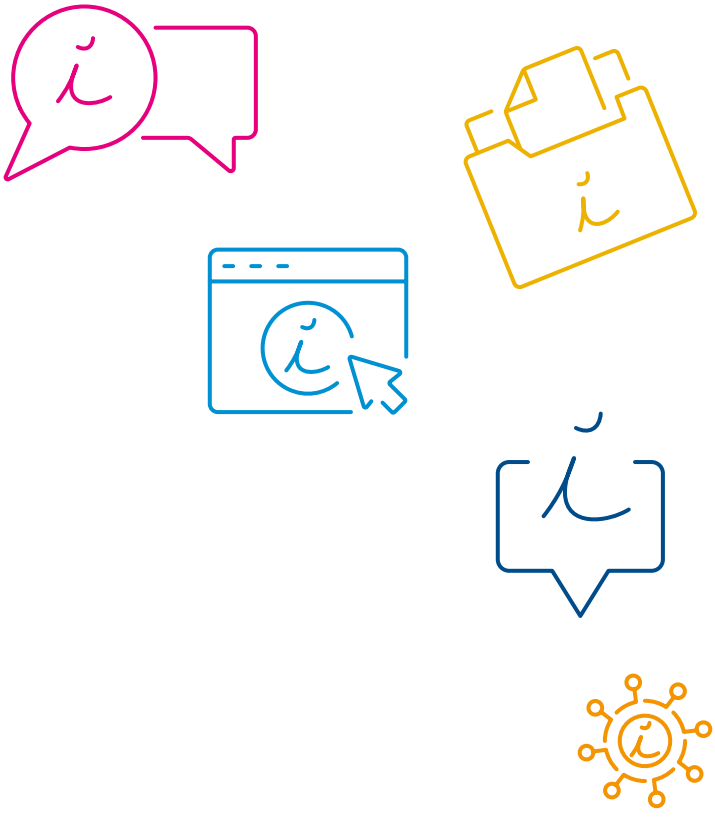
L'impresa che semplifica la tua.

Cybersecurity senza tecnicismi

Il glossario per tutti!

Autenticazione a due fattori (2FA)	Un meccanismo di sicurezza che richiede due forme di identificazione per accedere a un account, come una password e un codice inviato via SMS o generato da un'app. Aggiunge un ulteriore livello di protezione contro gli accessi non autorizzati.
Backup	Una copia di sicurezza dei dati conservata in un luogo sicuro, che può essere ripristinata in caso di perdita o danneggiamento.
Crittografia	Una tecnica di protezione dei dati che li rende illeggibili a chi non possiede la chiave per decifrarli. È usata per proteggere le informazioni sensibili durante la trasmissione o quando sono archiviate.
Cyber Threat Intelligence (CTI)	La raccolta e l'analisi di informazioni sulle minacce informatiche, per anticipare e prevenire attacchi futuri. Include la ricerca di dati compromessi sul dark web e su altre fonti.
Dark Web	Una parte nascosta di internet, accessibile solo tramite software specifici, dove avvengono spesso attività illegali, inclusa la vendita o lo scambio di dati rubati.
Firewall	Un sistema di sicurezza che monitora e controlla il traffico in entrata e in uscita di una rete, bloccando eventuali tentativi non autorizzati di accesso.
Leak	La divulgazione non autorizzata di dati sensibili, come email, password o altre informazioni personali, che possono finire online o essere venduti su piattaforme nascoste.
Malware	Software dannoso progettato per infiltrarsi, danneggiare o rubare informazioni da un sistema informatico. Può includere virus, trojan, spyware e ransomware.
Password manager	Un'applicazione che aiuta a creare, conservare e gestire password complesse in modo sicuro, evitando di doverle ricordare tutte manualmente.
Patch di sicurezza	Aggiornamenti rilasciati dai fornitori di software per correggere vulnerabilità o falle di sicurezza nei sistemi operativi, nelle applicazioni o nei dispositivi.
Phishing	Una tecnica di frode online in cui un attaccante si finge un'entità affidabile (come una banca o un servizio online) per ingannare le vittime e farsi consegnare informazioni sensibili, come password o dettagli della carta di credito.

Ransomware	Un tipo di malware che blocca l'accesso ai dati o ai sistemi dell'utente, chiedendo un riscatto (solitamente in criptovalute) per ripristinare l'accesso.
Rotazione delle password	La pratica di cambiare periodicamente le password per ridurre il rischio che vengano compromesse.
Vulnerabilità	Una debolezza o falla in un sistema informatico o in un software che può essere sfruttata da attaccanti per comprometterne la sicurezza.
Asset	L'insieme degli asset aziendali esposti a Internet che possono essere potenziali punti di ingresso per attacchi informatici. Questi includono siti web, server, DNS, indirizzi IP e altri servizi pubblicamente accessibili.
Asset type	Risorse tecnologiche come server, siti web, servizi DNS, email e indirizzi IP associati a Internet, che possono essere bersagli di attacchi informatici se non adeguatamente protetti.
IP	Un identificatore numerico assegnato a ciascun dispositivo collegato a una rete che utilizza il protocollo Internet. Gli indirizzi IP esposti possono diventare bersagli di attacchi.



OFFICINE BONFIGLIOLI

VERS.01 - MAR.2025

TeamSystem

teamsystem.com