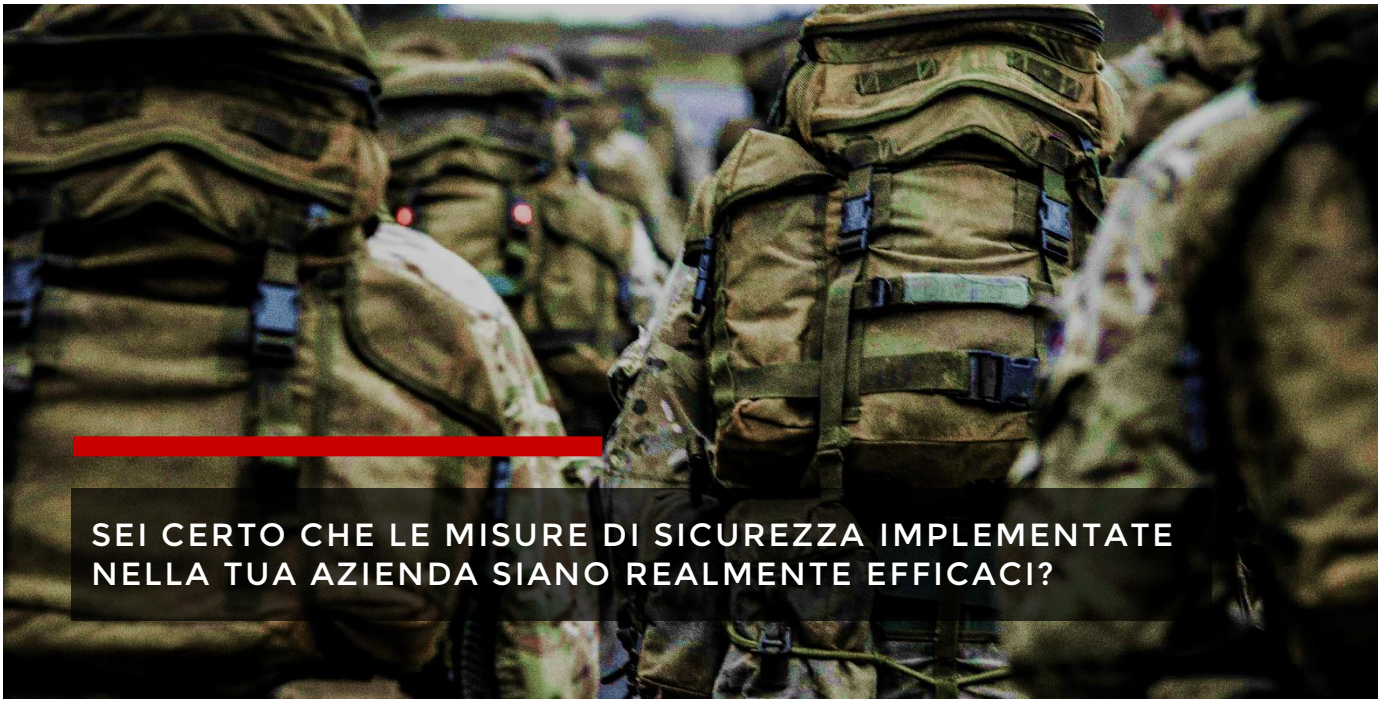
RED TEAM

OFFENSIVE SECURITY



Guardando le aziende con occhi di un "hacker" e simulando un vero attacco, il servizio Red Team di IMQ Intuity aiuta i propri Clienti a verificare se la loro strategia di sicurezza è efficace nel contrastare un attacco informatico di ultima generazione.

Incarnando il processo mentale dei veri attaccanti e utilizzando le loro stesse tecniche, il servizio **Red Team** di IMQ Intuity esplora tutti gli aspetti della *Security Posture* aziendale: Network Infrastructure, Application Security, Human Behavior, Physical Security Control e Business Process.

Per il Cliente rappresenta l'opportunità di aumentare la propria sicurezza e di affinare le proprie capacità di Detection & Reaction, acquisendo una maggiore consapevolezza delle tecniche e procedure usate dai veri attaccanti.

IL SERVIZIO RED TEAM SIMULA UN VERO ATTACCO INFORMATICO ELUDENDO LE TECNOLOGIE ED I SERVIZI DI SICUREZZA DEL CLIENTE

Sede operativa: IMQ Intuity, via A. Ceron 2, 35129 Padova | 049 817 0850 | info@intuity.it | www.intuity.it

TIPOLOGIE DI ATTACCO

OSINT
IMQ Intuity grazie all'utilizzo di particolari tecniche quali l'Open Source INTelligence (OSINT), esegue un'approfondita ricerca di informazioni relativamente all'azienda che possono essere utilizzate per la preparazione di un attacco o che rappresentino esse stesse un rischio per il business.

INFRASTRUCTURE ATTACK
Il Red Team cerca di violare la sicurezza aziendale sfruttando vulnerabilità riconducibili all'infrastruttura o, come sempre più spesso accade, presenti nelle applicazioni di tipo web.

HUMAN ATTACK
Guardare le aziende con gli occhi dell'hacker significa considerare anche il fattore umano come una vulnerabilità da sfruttare, per questo il servizio di Red Team include attività di Social Engineering, quali campagne di Phishing, Impersonation, Baiting.

PHYSICAL ASSESS
Talvolta un accesso non autorizzato ad aree o locali può esporre l'azienda a rischi significativi, per questo il servizio di Red Team si prefigge di verificare l'efficacia dei controlli che l'azienda ha introdotto. (Attività non prevista nel servizio Hack In A Day)

PROCESS EVALUATION
I risultati ottenuti dal servizio di Red Team consentono di validare con dati oggettivi anche l'adeguatezza dei processi aziendali dal punto di vista IT, evidenziando le criticità che hanno un impatto sulla sicurezza.

WHITEBOARD ATTACK
Tale attività viene svolta attraverso un «gioco di ruolo» in cui attaccanti (specialisti IMQ Intuity) e difensori (Cliente), seduti attorno ad un tavolo, si sfidano per raggiungere i rispettivi obiettivi, utilizzando le proprie strategie. (Attività non prevista nel servizio Hack In A Day)

IL METODO

La modalità d'attacco del servizio Red Team è di tipo **BlackBox** che non prevede la condivisione iniziale di informazioni relative al target e alcun tipo di autorizzazione o informazione d'accesso. Questo tipo di modalità permette a IMQ Intuity di **"vedere" il target così come lo vedrebbe un attaccante esterno.**

Il confronto diretto con il Red Team di IMQ Intuity consente al Cliente di elevare la propria attenzione nei confronti di reali incidenti di sicurezza, di testare le proprie capacità di rilevare un'attività anomala e di bloccarla.

Il **servizio Hack In A Day** simula un attacco informatico della **durata di un giorno**, utilizzando i principali metodi operativi del Red Team.

Il servizio permette di dimostrare e documentare quali vulnerabilità aziendali un "hacker" potrebbe sfruttare in una sola giornata di attività e quali potenziali danni potrebbe recare al business, all'infrastruttura o alle persone.

L'obiettivo del servizio è quello di poter fornire ai propri clienti una **prima visione del livello di protezione aziendale** dal punto di vista della sicurezza informatica e di capire dove intervenire al fine di migliorarla.