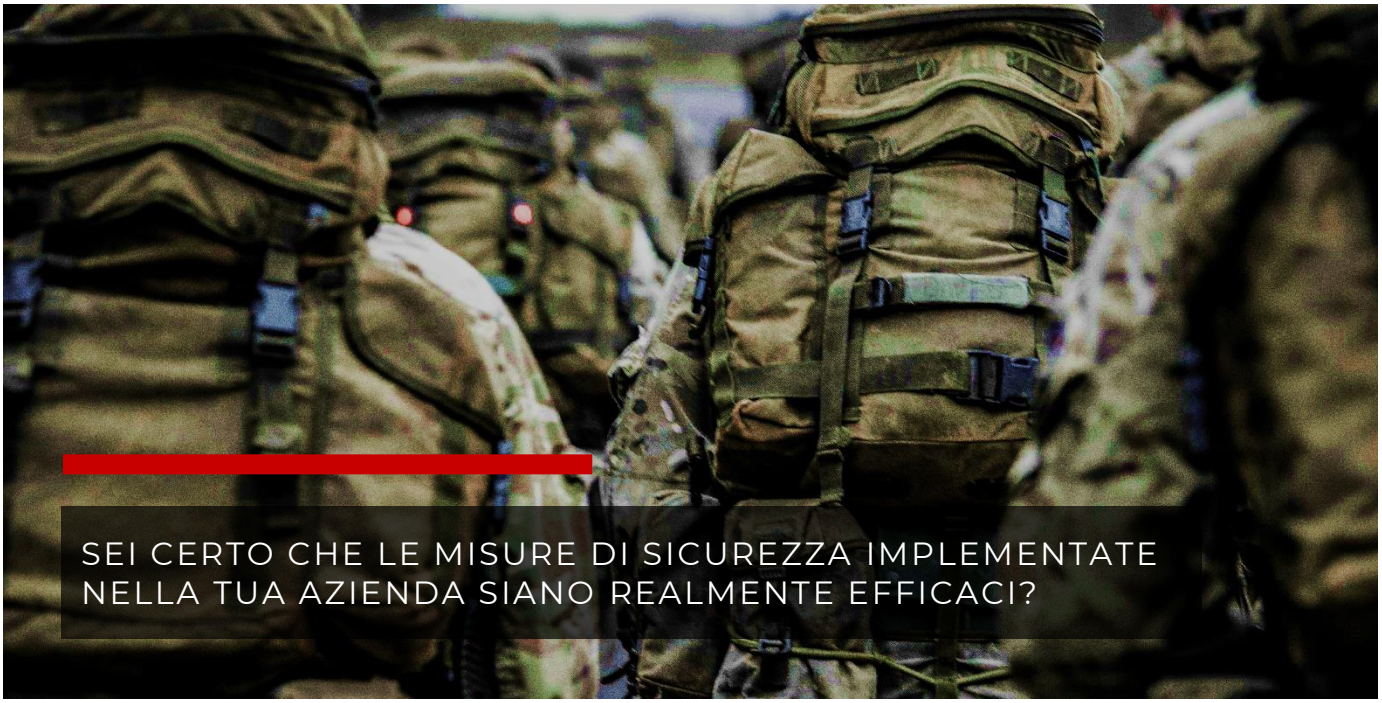
RED TEAM

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

IMQ INTUITY SRL | info@intuity.it | intuity.it/
Sede Operativa Via A. Ceron 2, 35129 | +39 049 817 0850 | **Sede Legale** via M. F. Quintiliano, 45 - 20138 Milano

TIPOLOGIE DI ATTACCO

OSINT

IMQ Intuity ed ITI Sistemi grazie all'utilizzo di particolari tecniche quali l'Open Source INTelligence (OSINT), eseguono 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 ACCESS

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.

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 ed ITI Sistemi) e difensori (Cliente), seduti attorno ad un tavolo, si sfidano per raggiungere i rispettivi obiettivi, utilizzando le proprie strategie.

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 ed ITI Sistemi di "vedere" il target così come lo vedrebbe un attaccante esterno.

Il confronto diretto con il Red Team 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.

BENEFICI

EFFICACY: Valutare l'efficacia delle misure tecnologiche ed organizzative in essere.

REACTION: Misurare le potenzialità di reazione di fronte a tentativi di intrusione o incidenti di sicurezza.

AWARENESS: Avere una conoscenza più ampia e dettagliata del livello di sicurezza della propria organizzazione.

IMPROVEMENT: Migliorare la propria sicurezza con un piano correttivo basato su evidenze oggettive.

TI DIAMO LA POSSIBILITÀ DI DARE UNO SGUARDO AL FUTURO, PER COMPRENDERE CIÒ CHE POTREBBE ACCADERE.