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, per poter reagire tempestivamente nel caso di un attacco reale.

VI DIAMO LA POSSIBILITÀ DI DARE UNO SGUARDO
A CIÒ CHE POTREBBE ACCADERE IN FUTURO.

IL METODO

La modalità d'attacco del servizio Red Team è di tipo *BlackBox,* ovvero non prevede la condivisione iniziale di informazioni relative al target né alcun tipo di informazione d'accesso da parte del cliente. 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 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 FRAMEWORK TIBER-EU\IT

IMQ Intuity esegue attività di Red Team dal 2016, tra le prime aziende in Italia ad integrare nei suoi servizi di simulazione di attacco tutti gli aspetti di *Social Engineering* e test di sicurezza fisica. Dal 2018 IMQ Intuity recepisce le indicazioni del **Framework TIBER-EU,** adeguando di conseguenza i suo servizio di Red Team.

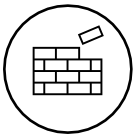
Sede Operativa: Via Brunello Rutoli, 6 35129 | Padova
Sede Operativa: Via Nazionale, 230 CAP 00184 | Roma
Sede Legale: Via M. F. Quintiliano, 45 - 20138 | Milano

Tel: 049 817 0850
E-mail: info@intuity.it

TIPOLOGIE DI ATTACCO

THREAT INTELLIGENCE

Gli specialisti di IMQ Intuity, grazie all'utilizzo di particolari tecniche di *Threat Intelligence*, eseguono un'approfondita ricerca di informazioni sull'azienda. Queste ultime possono essere utilizzate per la preparazione di un attacco o possono rappresentare esse stesse un rischio per il business. L'attività prosegue con la ricerca di eventuali minacce e di potenziali *Threat Actor*.



INFRASTRUCTURE ATTACK

Il Red Team cerca di violare la sicurezza aziendale sfruttando vulnerabilità riconducibili all'infrastruttura IT o, come sempre più spesso accade, presenti nelle Web Application.

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 Vishing, Smishing, 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 al suo interno.

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 e quindi sul business aziendale.

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.

FULL ATTACK O SCENARIO?

E' TOP SECRET, MI RACCOMANDO!

IMQ Intuity «attacca» le aziende nella loro interezza, perché è questo che fanno i criminali. È possibile comunque focalizzare l'attacco su un ambito specifico: una simulazione di attacco limitata ad **uno o più scenari predefiniti**. Questo tipo di esercizio ha come obiettivo principale quello di testare in maniera approfondita uno specifico contesto, normalmente indicato dal cliente.

RED TEAM CONTINUATIVO

Il Mondo sta cambiando, le minacce informatiche cambiano con esso. Per essere sempre aggiornato sul panorama delle minacce informatiche e per avere una più esaustiva e completa visione di ciò che potrebbe accede al tuo business, puoi scegliere il servizio Red Team erogato in modalità continuativa.

PURPLE TEAM

A volte il Red Team può evolvere in servizi di tipo **Purple Team**. Il Purple Team è un momento di condivisione di esperienze fra il Red Team e il Blue Team. IMQ Intuity ha sviluppato una suite di servizi Purple Team che permette alle aziende di «addestrare» il proprio Blue Team facendosi trovare pronto nel caso di un attacco reale.

Sede Operativa: Via Brunello Rutoli, 6 35129 | Padova
Sede Operativa: Via Nazionale, 230 CAP 00184 | Roma
Sede Legale: Via M. F. Quintiliano, 45 - 20138 | Milano

Tel: 049 817 0850
E-mail: info@intuity.it