«La Sicurezza non è solo una sfida tecnologica.
Se così fosse la tecnologia l'avrebbe già vinta molto tempo fa.
La Sicurezza è una sfida di persone, una sfida sociale e organizzativa.
È una sfida Culturale».

ABOUT US

Stiamo vivendo un'era di evoluzione tecnologica che, pur creando nuove opportunità per le aziende, le espone anche a nuovi pericoli.

È tanto importante conoscere quali benefici l'evoluzione porta con sé, quanto avere una chiara consapevolezza di quali sono i rischi a essa connessi.

IMQ Intuity propone un approccio diverso alla Cyber Security, modificando lo status-quo che vede nella soluzione tecnologica l'unico modo di affrontare il problema, quest'ultimo invece sempre più legato all'uomo e al contesto sociale in cui esso opera.

Tale obiettivo può essere raggiunto attraverso la consapevolezza che la sicurezza informatica deve essere approcciata da un punto di vista culturale, mettendo le persone al centro del processo di sicurezza aziendale, approccio noto anche come *People Centric Security*.

Concentrarsi solo sulla tecnologia è sempre una strategia perdente, poiché un approccio alla Cybersecurity di tipo *Technology-Centric*, verrà inevitabilmente aggirato da un nuovo comportamento umano.

CERTIFICAZIONI DEL PERSONALE E AZIENDALI

- eLearnSecurity **Web application Penetration Tester**
- eLearnSecurity **Web application Penetration Tester eXtreme**
- eLearnSecurity **Certified Professional Penetration Tester**
- Pentester Academy **Certified Red Teaming Expert**
- EC-Council **Certified Ethical Hacker**
- PRINCE2® **Projects in Controlled Environments**
- Offensive Security **Certified Professional**
- Offensive Security **Wireless Professional**
- ISACA **Certified in Risk and Information Systems Control**
- European Security Academy **OSINT & Darkweb Investigations**
- EC-Council **Certified Incident Handler**
- **ISO27001 Lead Auditor**
- Offensive Security **Experienced Penetration Tester** (OSEP)

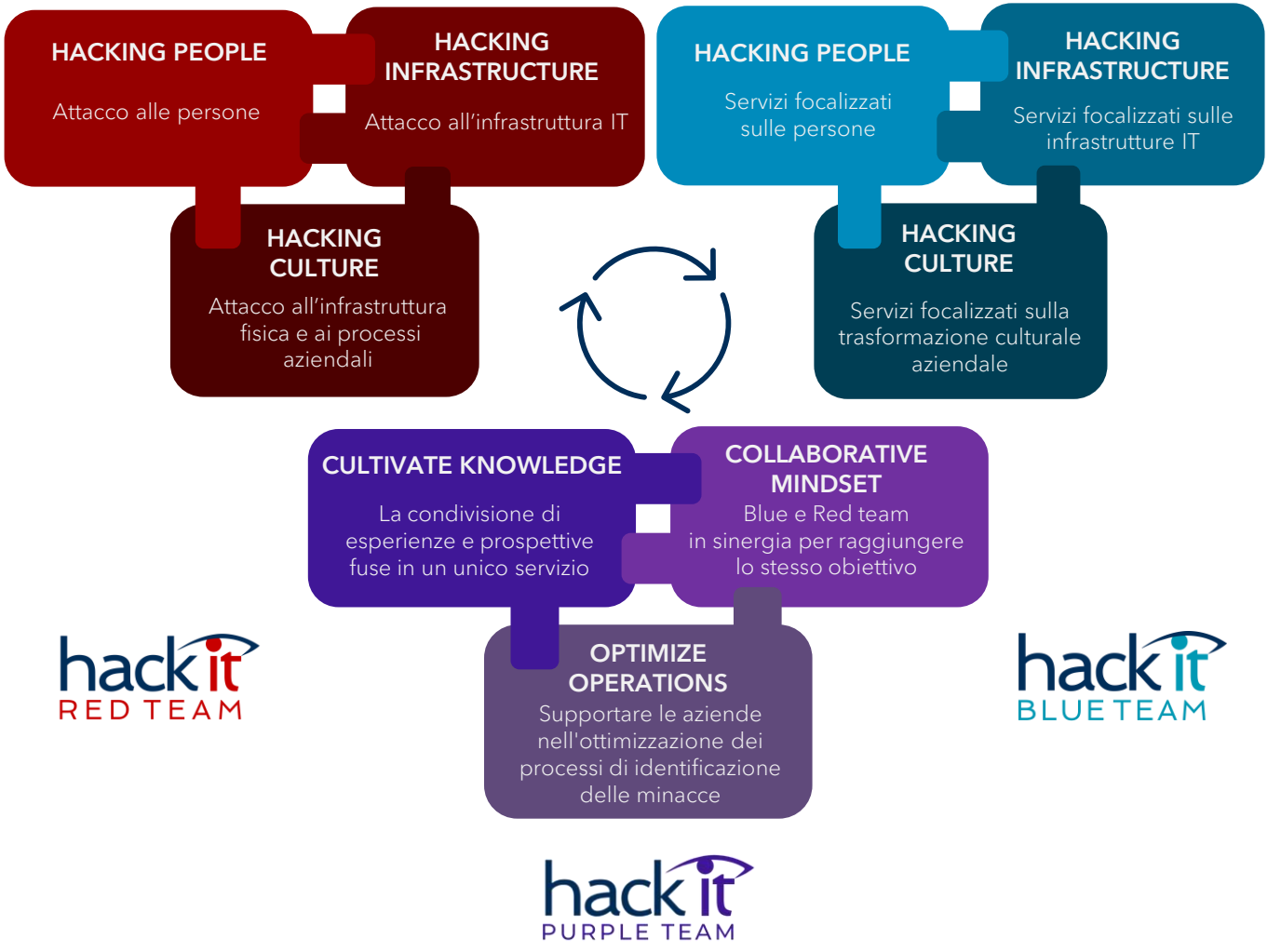
TURN THE MAP AROUND
GUARDARE AL BUSINESS ATTRAVERSO GLI OCCHI DI UN HACKER

Guardare le aziende attraverso gli occhi di un hacker significa considerarle come un insieme interdipendente di **Tecnologia, Persone, Sicurezza Fisica** e **Processi**.

Ognuno di questi elementi ha le sue vulnerabilità e chi attacca lo sa.

Cerca periodicamente il modo più efficace raggiungere il suo scopo, talvolta sfruttando le debolezze della tecnologia, ma sempre più spesso sfruttando quelle umane.

Solamente con questo approccio è possibile realizzare un'appropriata difesa, senza trascurare nell'analisi alcun tipo di vulnerabilità, sia essa umana o tecnologica.



D.R.E.A.M.
A TRANSFORMATION PROCESS FOR A «HIGH RELIABILITY SECURITY CULTURE»

Crediamo nella cultura della sicurezza come principale strumento per contrastare il rischio «cyber», per questo motivo abbiamo sviluppato D.R.E.A.M., un percorso di trasformazione per le aziende.

Crediamo nella capacità dell'uomo di comprendere il proprio ruolo in questa sfida quotidiana che sempre più travalica la sfera professionale ed entra nella vita privata. Crediamo che parlare del problema della cybersecurity e delle sue conseguenze, coinvolgendo tutti, condividendo informazioni e imparando dagli errori sia il modo migliore per affrontarlo.

D.R.E.A.M.

non è un servizio, piuttosto una visione che pone le radici in quello in cui crediamo e si sviluppa attraverso quello che facciamo

DIAGNOSIS
Evidenziare le lacune nella cultura della sicurezza informatica della propria azienda con l'obiettivo di incentivare il cambiamento.

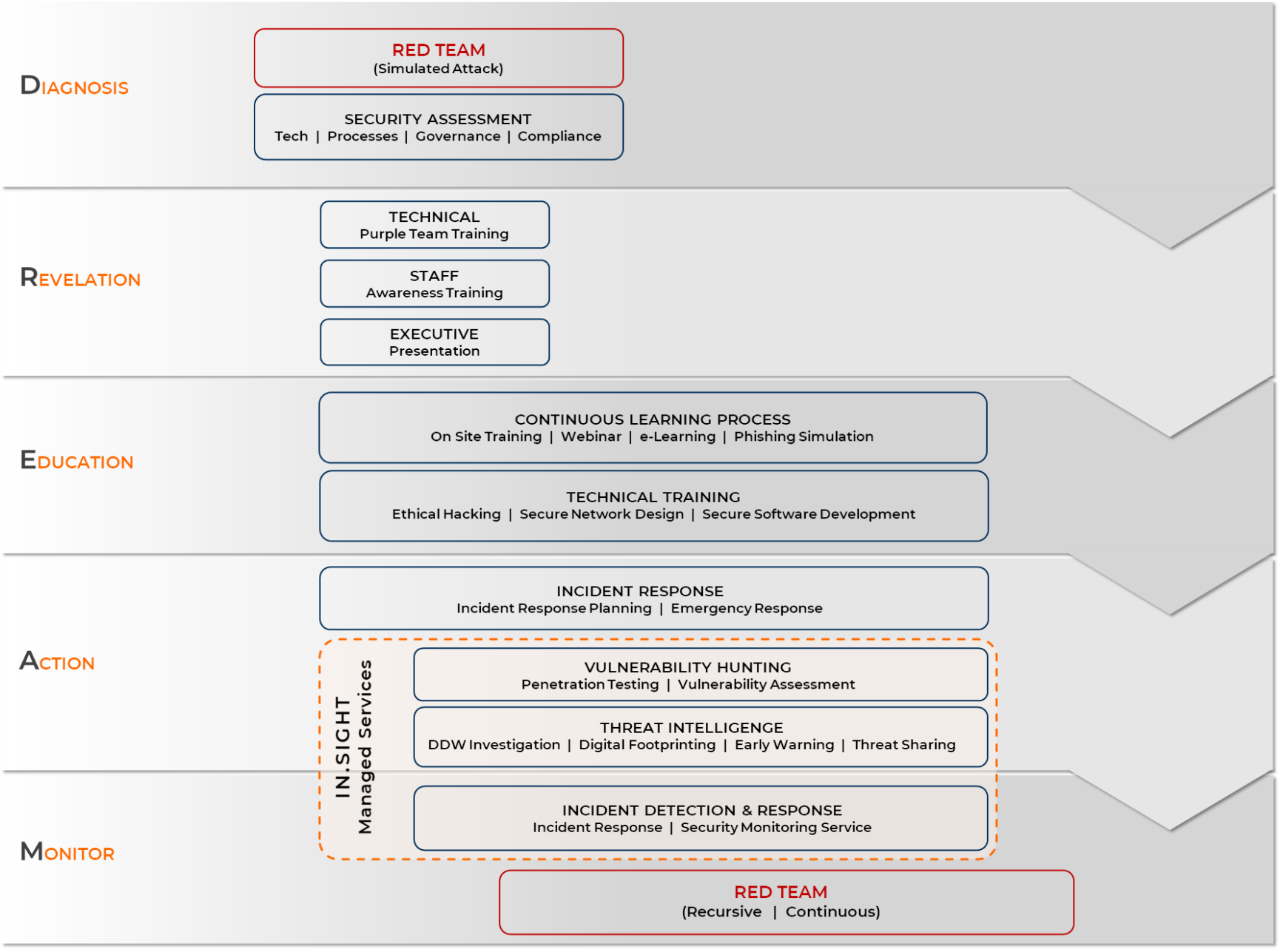
REVELATION
Condividere i risultati per motivare il personale a svolgere un ruolo attivo nella protezione dell'azienda dalle minacce informatiche.

EDUCATION
Migliorare la conoscenza e la consapevolezza sulla sicurezza informatica coinvolgendo ciascun membro dell'azienda.

ACTION
Aumentare il livello di protezione dell'azienda introducendo strumenti e processi a supporto.

MONITOR
Verificare i miglioramenti introdotti nelle fasi precedenti aumentando le capacità di *Detection & Reaction*, al fine di innescare un processo di miglioramento continuo.

IL PROCESSO DI TRASFORMAZIONE: D.R.E.A.M.



hack it
RED TEAM

Il servizio **RED TEAM** di IMQ Intuity aiuta i clienti a capire se la loro strategia di sicurezza è efficace nel contrastare un attacco informatico, guardando le aziende con gli occhi di un hacker.

Incarnando il processo mentale e utilizzando le stesse tecniche dei veri attaccanti, il servizio Red Team 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 ampliare la propria consapevolezza sulle tecniche e procedure, nonché di affinare le proprie capacità di *Detection & Reaction*.

**Ti diamo la possibilità di dare uno sguardo al futuro,
per comprendere ciò che potrebbe accadere.**

UTILITÀ DEL SERVIZIO RED TEAM PER IL BUSINESS

EFFICACY Valutare l'efficacia delle misure tecnologiche e 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.

COSA FACCIAMO DURANTE LA SIMULAZIONE DI ATTACCO RED TEAM

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 possano 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 ATTACK

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 messo in campo in questo senso.

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 di IMQ Intuity) e difensori (Cliente), seduti attorno a un tavolo, devono sfidarsi e, ognuno con i propri strumenti e strategie, raggiungere I rispettivi obiettivi.

hack it
BLUE TEAM

I servizi **BLUE TEAM** di IMQ Intuity permettono ai clienti di aumentare la propria sicurezza e di essere *compliant* a standard internazionali, regolamenti interni o normativi.

Consentono di acquisire la piena consapevolezza del problema e di capire come questo impatta nella propria realtà, di gestire tutti gli aspetti di sicurezza con approccio moderno e proattivo e di implementare una strategia di protezione efficace.

OBIETTIVI DEI SERVIZI DI BLUE TEAM

PROTECTION
Garantire la sicurezza aziendale:

correggere le vulnerabilità più critiche, rafforzare i presidi tecnologici, monitorare e rispondere a situazioni di rischio.

COMPLIANCE
Aderire correttamente a normative e standard richiesti:

ISO27001, PCI-DSS, AgID, internal compliance.

AWARENESS
Aumentare la consapevolezza interna sul problema:

rendere il fattore umano un elemento chiave per la sicurezza del business.

IMPROVE INFRASTRUCTURE

VULNERABILITY ASSESSMENT & PENETRATION TEST
Verifichiamo come le vulnerabilità tecnologiche possono essere sfruttate e quali conseguenze possono avere per il business. Testiamo sistemi, Wi-Fi, applicazioni, applicazioni e source code.

WEB E MOBILE APPLICATION VULNERABILITY ASSESSMENT & PENETRATION TEST
Cerchiamo eventuali vulnerabilità presenti all'interno delle applicazioni Web Mobile aziendali.

DoS/DDoS
Testiamo applicazioni e infrastruttura per capire il livello di resilienza nei confronti di attacchi DoS/DDoS.

EDUCATE PEOPLE

SOCIAL ENGINEERING
Sfruttiamo le vulnerabilità umane per generare un attacco verso l'azienda e fornire evidenza delle criticità riconducibili alle persone, tramite tecniche di *phishing, impersonation, baiting, tailgating o piggybacking*.

SECURITY AWARENESS
I servizi di training di IMQ Intuity hanno l'obiettivo di fornire ai dipendenti le competenze basiche per affrontare il problema della minaccia cyber con cognizione e autonomia, attraverso percorsi formativi rivolti a personale tecnico e non tecnico, anche attraverso tecniche di *gamification*.

ADVISORS/CONSULTANCY
Aiutiamo le aziende ad approcciare alla cybersecurity in modo corretto, indirizzando il cliente verso il percorso più ottimale e specifico per le proprie esigenze.

ENHANCE PROCESSES

INCIDENT RESPONSE PLAN
Per avere successo, le aziende devono adoperarsi per prevenire gli attacchi informatici. Allo stesso tempo, devono essere preparate al peggior scenario: un hacker può compromettere le difese. In questo caso una risposta veloce ed efficace può evitare all'azienda un potenziale disastro.

IN.SIGHT (INCIDENT, DETECTION & RESPONSE)
Offriamo servizi di rilevamento e gestione degli incidenti di sicurezza.

THREAT INTELLIGENCE
Studiamo i fenomeni che potrebbero rappresentare un rischio per un'azienda o per uno specifico settore.
Aggiorniamo i nostri clienti o le loro tecnologie con le più recenti scoperte in ambito cybersecurity, in modo da proteggerli ancora prima che il problema si manifesti.

SECURITY ASSESSMENT
Servizio sviluppato secondo il modello CIS20 che permette di ottenere una valutazione sul livello di sicurezza informatica aziendale, rapportabile anche ad altri standard: ISO27001, NIST, PCI DSS.

hack it
PURPLE TEAM

Il **PURPLE TEAM** nasce dall'idea che deve sussistere necessariamente un **dialogo continuo,** una **comunicazione efficace** tra le due squadre.

Il Purple Team integra le tattiche offensive del Red Team alle strategie di difesa del Blue Team in **un'unica narrazione che massimizza l'efficacia dei risultati**.

La condivisione delle informazioni fra i due team, permette uno scambio di prospettive che promuove il miglioramento continuo.

OBIETTIVI DEI SERVIZI DI PURPLE TEAM

Grazie all'attività di Purple Teaming, le attività di Red Team assumono una valenza formativa rilevante, in quanto tutte le azioni svolte possono essere **spiegate, discusse, provate** assieme.

Il cliente ha la possibilità di capire immediatamente cosa funziona e cosa deve essere migliorato nella sua infrastruttura.

hack it
PURPLE TEAM

PURPLE TEAM REPLAY

A seguito di un'attività di Red Team eseguita in modalità *BlackBox*, le attività simulate durante l'attacco vengono riproposte in un clima collaborativo, coinvolgendo il Blue Team del cliente.

PURPLE TEAM SCENARIO BASED

Una cellula del Red Team conduce una serie di attacchi sulla base di scenari concordati in fase di kick-off con il cliente. Il Blue Team del cliente verifica in tempo reale la propria capacità di *Prevention, Detection & Reaction* e, se presente, l'efficacia delle procedure dell'*Incident Response Plan*.

WHITEBOARD ATTACK SIMULATION (TABLE-TOP)

L'attività si svolge come un gioco di ruolo tra Red Team e Blue Team e prevede la simulazione di attacchi svolti in maniera teorica, senza quindi un impatto sulla reale operatività aziendale. Formulando differenti scenari, i team si confrontano in una simulazione *Table-top*.

PURPLE TEAM TRAINING

Training «hands on» su tecniche d'attacco condotte sull'infrastruttura del cliente, in un *Cyber Range* e alla lavagna. Affiancandosi ad una cellula di Red Team, il cliente avrà la possibilità di assistere alla simulazione di differenti tipologie di attacco.

SEDE LEGALE - MILANO
Via Marco Fabio Quintiliano, 45 CAP 20138

SEDE OPERATIVA - PADOVA
Via Brunello Rutoli, 6 CAP 35129

SEDE OPERATIVA - ROMA
Via Nazionale, 230 CAP 00184

UAE - DUBAI
Building 6WA Office 819
FZCo Dubai Airport Free Zone PoBox 371233

GERMANIA - MONACO
GMBh Lepoldstraβe, 240 PLZ 80807

info@intuity.it
Tel. +39 049 817 0850
WWW.INTUITY.IT