PURPLE TEAM

ATTACCO VS DIFESA

Red Team e Blue Team sono in conflitto continuo con l'obiettivo di rendere le difese dell'Azienda sempre più robuste e reattive. Mentre il Red Team ha lo scopo di attaccare dando evidenza dei rischi e delle minacce alla quale si è esposti, il Blue Team ha un perimetro da difendere e monitorare verificando l'impatto che un danno può avere sul business aziendale.

Nel mondo reale chi difende non sa mai chi, quando e da dove attaccherà e non è certo se i tempi di detection e reaction siano adeguati.

CONDIVIDERE DIVERSE PROSPETTIVE

Il Purple Team nasce dall'idea che il dialogo continuo tra le due squadre possa aumentare l'efficacia degli strumenti e dei processi di difesa tramite un percorso culturale comune.

Simulando un attacco, il Red Team condivide in tempo reale col Blue Team il "quando ed il come" dell'azione offensiva.

Questo consente al Blue Team di poter misurare "se e quando" riesce ad identificare l'attacco.

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.

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

SERVIZI PURPLE TEAM

PURPLE TEAM REPLAY

A seguito di un servizio IMQ Intuity Red Team (Simulazione d'Attacco al Business) eseguito in modalità BlackBox, le attività simulate durante l'attacco vengono riproposte in un clima collaborativo, coinvolgendo il Blue Team del cliente.
Le caratteristiche e gli obiettivi del servizio vengono concordati con il cliente.

PURPLE TEAM SCENARIO BASED

Una cellula del Red Team di IMQ Intuity conduce una serie di attacchi sulla base di scenari concordati con il cliente in fase di kick-off. 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 il rischio di un impatto sulla reale operatività aziendale. Attraverso la formulazione di differenti scenari, i team si confrontano in una simulazione *Table-top* discutendo delle possibili azioni da intraprendere, verificando inoltre l'efficacia dell'*Incident Response Plan* aziendale.

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.

BENEFICI PER LA TUA AZIENDA

Lo scopo è fare tesoro delle criticità rilevate (su infrastrutture fisiche, IT, processi e persone) durante le attività di simulazione di attacco Red Team e condividerle con il Blue Team, trasformandole al contempo in consapevolezza e cultura condivisa.
In particolare, il Red Team spiegherà le dinamiche delle tecniche utilizzate e descriverà al Blue Team l'approccio correttivo su quanto riscontrato.

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