PURPLE TEAM

OFFENSE & DEFENSE

Red Team and Blue Team are constantly conflict with the goal of making the Company's defenses more robust and responsive. While the Red Team aims to attack by highlighting the risks and threats to which the company is exposed, the Blue Team has a perimeter to defend and monitor by verifying the impact that damage can have on the business.

In real world, those who defend never know who, when and from where they will be attacked, in addition it is not certain if the detection and reaction times are adequate.

SHARING DIFFERENT PERSPECTIVES

The Purple Team was conceived from the idea that the continuous dialogue between the two teams can increase the effectiveness of the defense tools and processes through a common cultural path.

Simulating an attack, the Red Team shares in real time with the Blue Team the precise "when and how" of about the offensive action.

This allow the Blue Team to measure "if and when" it can identify the attack.

The Purple Team integrates the Red Team's offensive tactics with the Blue Team's defense strategies into a single narrative that maximizes the effectiveness of the results.

The sharing of information between the two teams allows an exchange of perspectives that promotes continuous improvement.

Headquarter: Via Brunello Rutoli, 6 35129 | Padova
Headquarter : Via Nazionale, 230 CAP 00184 | Roma
Registreded Office: Via M. F. Quintiliano, 45 - 20138 | Milano

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

PURPLE TEAM SERVICES

PURPLE TEAM REPLAY

Following an IMQ Intuity Red Team (Business Attack Simulation) service performed in *BlackBox* mode, simulated activities performed during the attack are repeated in a collaborative atmosphere, involving the customer's Blue Team.

The characteristics and objectives of the service are agreed with the customer.

PURPLE TEAM SCENARIO BASED

A cell of IMQ Intuity Red Team conducts a series of attacks based on some scenarios, previously agreed during the kick-off with the customer. The Blue Team of the customer verifies in real time its ability to *Prevention, Detection & Reaction* and, if present, the effectiveness of the procedures of the *Incident Response Plan*.

WHITEBOARD ATTACK SIMULATION (TABLE-TOP)

The activity takes place as a *role-playing game* between Red Team and Blue Team and involves the simulation of attacks carried out in a theoretical manner, without therefore the risk of an impact on the real business operations. Through the formulation of different scenarios, the teams are confronted in a *Table-top* simulation discussing the possible actions to be taken and verify the effectiveness of the company's Incident Response Plan.

PURPLE TEAM TRAINING

Training «hands on» on attack techniques conducted on the customer's infrastructure, in a *Cyber Range* and on the blackboard. Alongside a Red Team cell, the customer will have the opportunity to witness the simulation of different types of attack.

BENEFITS FOR COMPANIES

The aim is to take advantage of the critical issues detected during the Red Team attack simulation activities and share them with the Blue Team, transforming them into awareness and shared culture.

In particular, the Red Team will explain the dynamics of the techniques used and will describe to the Blue Team the corrective approach to the findings.

Headquarter: Via Brunello Rutoli, 6 35129 | Padova
Headquarter : Via Nazionale, 230 CAP 00184 | Roma
Registreded Office: Via M. F. Quintiliano, 45 - 20138 | Milano

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