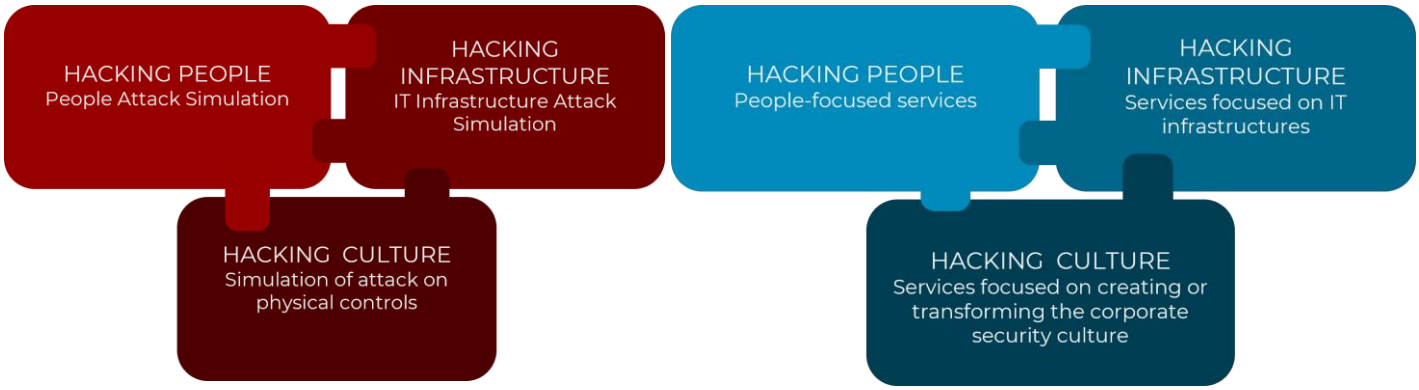
PURPLE TEAM

OFFENSE & DEFENSE

Very often, attackers and defenders do not speak the same language, as they have opposite roles.

While the **Red Team** aims to highlight the risks related to the business and know the impact that a threat can have on the business, the **Blue Team** has a perimeter to defend (sometimes unknown) and aims to monitor and protect against cyber threats that could compromise the business.

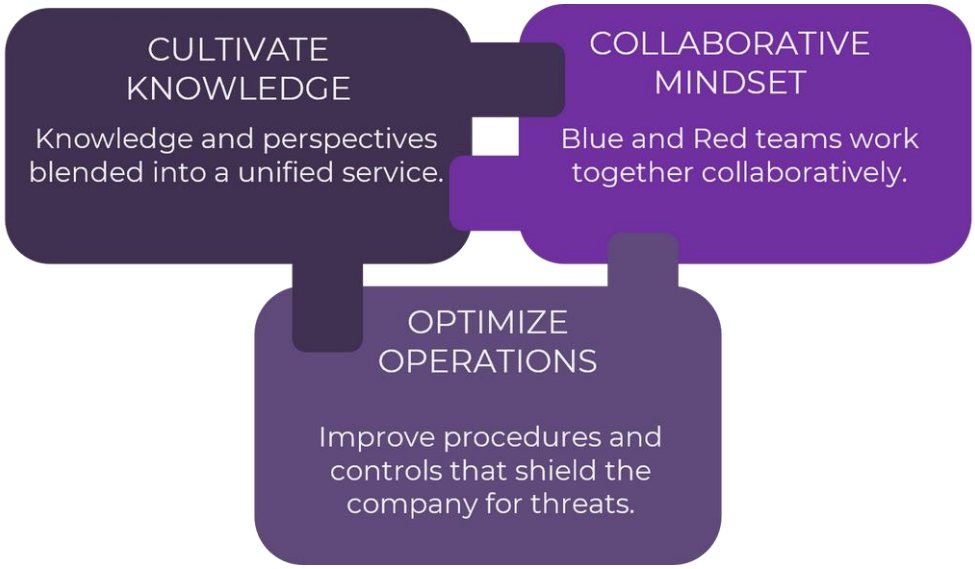


SHARING DIFFERENT PERSPECTIVES

Purple Team service was born from the idea that there must necessarily be a continuous dialogue and effective communication between the two teams.

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 activities of Red Teaming, if delivered with the presence of the customer's Blue Team group or if shared during a special session, assume a relevant educational value, as all the actions can be **explained, discussed, tried together**.

The customer has the opportunity to immediately understand what works and what needs to be improved in its infrastructure and processes. For IMQ Intuity, the Purple Team represents the moment when the **skills and the point of view of those who have the attacker's mindset, meet with those who have the responsibility and competence of the company's defense.**

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