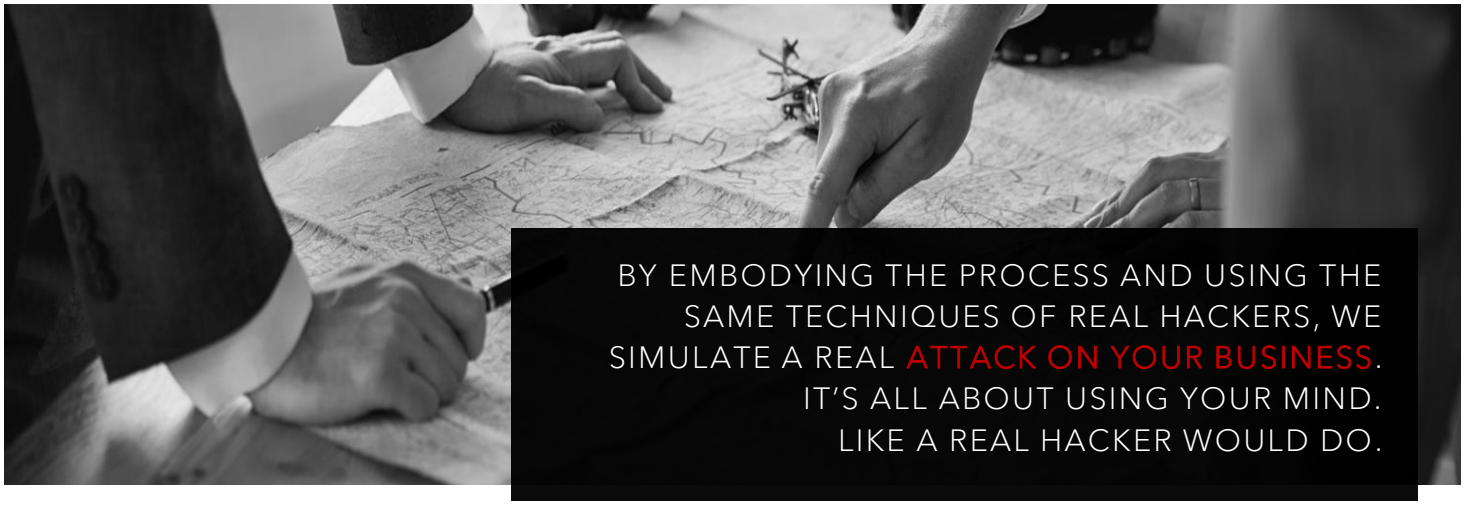
RED TEAM

OFFENSIVE SECURITY



By looking at companies with the eyes of a "hacker" and simulating a real attack, IMQ Intuity Red Team helps its customers to verify if their security strategy is effective in countering a last generation cyber attack.

By embodying the mental process of the real attackers and using their own techniques, the IMQ Intuity Red Team service explores all aspects of the company's Security Posture: *Infrastructure, Application Security, Network Human Behavior, Physical Security Control* and *Business Process*. For the customer it represents the opportunity to increase their security and to improve their *Detection & Reaction* skills, acquiring a greater awareness of the techniques and procedures used by the real attackers, in order to be able to react quickly in the event of a real attack.

WE GIVE YOU A CHANCE TO TAKE A LOOK
TO WHAT MAY HAPPEN IN THE FUTURE.

THE METHOD

The Red Team method of attack is *BlackBox*, that is, does not provide for the initial sharing of target-related information or any type of customer access information. This mode allows IMQ Intuity to "see" the target as an external attacker would. The direct comparison with the Red Team allows the customer to raise their attention to real security incidents, to test their ability to detect an abnormal activity and to block it.

THE TIBER-EU IT FRAMEWORK

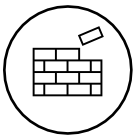
In IMQ Intuity, the **Red Team** Exercise has been running since 2016, among the first companies in Italy integrating the cyber attack simulation with physical infrastructure security tests and Social Engineering techniques. Since 2018, IMQ Intuity Red Team has implemented the indications of the *TIBER-EU Framework*, adapting its Red Team service accordingly.

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

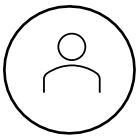
Tel: 049 817 0850
E-mail: info@intuity.it

TYPES OF ATTACK

THREAT INTELLIGENCE
IMQ Intuity' specialists, using specific threat intelligence techniques, perform an in-depth research of the company information. These can be used to prepare for an attack, or they can be a risk to the business. The activity continues with the search for possible threats and potential *Threat Actors*.



INFRASTRUCTURE ATTACK
The Red Team tries to breach corporate security by exploiting vulnerabilities linked to IT infrastructure or, as is increasingly the case, vulnerabilities present in Web Applications.



HUMAN ATTACK
Looking at companies with the eyes of the hacker also means considering the human factor as a vulnerability to be exploited, so Red Team service includes *Social Engineering* activities, such as Phishing campaigns *Vishing, Smishing, Impersonation, Baiting*.

PHYSICAL ACCESS
Sometimes, unauthorized access to some areas can expose the company to significant risks, so Red Team service aims to verify the effectiveness of the controls that the company has introduced.

PROCESS EVALUATION
The results obtained by Red Team service, allow to validate with objective data also the adequacy of business processes from the IT point of view, highlighting the critical issues that have an impact on security and therefore on the business.

WHITEBOARD ATTACK
This activity is carried out through a «role-playing game» in which attackers (IMQ Intuity' specialists) and defenders (client), sitting around a table, challenge each other to achieve their respective goals, using their own strategies.

FULL ATTACK OR SCENARIO?

THIS IS ABSOLUTELY TOP SECRET!

IMQ Intuity «attacks» companies in their entirety, because that's what criminals do.
However, it is possible to focus the attack on a specific field: an attack simulation limited to one or more predefined scenarios. This type of exercise has as its main objective to thoroughly test a specific context, normally indicated by the customer.

ONGOING RED TEAM

The world is changing, cyber threats change with it. To keep up to date on the cyber threat landscape and to have a more comprehensive and complete view of what could access your business, you can choose the Red Team service provided on an ongoing basis.

PURPLE TEAM

Sometimes the Red Team can evolve into Purple Team type services. The Purple Team is a moment of sharing experiences between the Red Team and the Blue Team. IMQ Intuity has developed a suite of Purple Team services that allows companies to «train» their Blue Team by being ready in the event of a real attack.

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

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