«Security is not a technology challenge.
If it were, technology would have fixed the problems a long time ago.
Security is a people challenge, a social and organizational challenge.
It's a **Cultural** challenge».

ABOUT US

We are living in an era of technological evolution that, while creating new opportunities for companies, also exposes them to new dangers.

Having a clear awareness of the risks inherent in technological evolution is just as important as understanding the benefits.

IMQ Intuity proposes a different approach to cybersecurity, challenging the status-quo of technology as the solution to a problem that is more and more linked to human actions and the social context in which they take place.

This objective can be achieved through the realization that IT security must be approached from a cultural point of view, putting people at the center of the corporate security process, also known as People Centric Security.

Focusing only on technology is always a losing strategy because a technology centric approach to cybersecurity will inevitably be bypassed by uncontrolled human behavior.

PERSONNEL & COMPANY CERTIFICATIONS

- 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 **Experienced Penetration Tester** (OSEP)
- 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

LOOKING AT THE CUSTOMER'S SECURITY THROUGH THE EYES OF A HACKER

Looking at businesses through the eyes of a hacker means considering them as an interdependent set of **Technology, People, Physical Security and Processes**.

Each of these elements has its own vulnerabilities and the attacker knows them, periodically trying the most effective way to exploit them, traditionally focusing on technological weaknesses but increasingly exploiting human ones.

This is the only approach that can build a viable defense that considers all vulnerabilities, both human and technological.

HACKING PEOPLE
People Attack Simulation

HACKING INFRASTRUCTURE
IT Infrastructure Attack Simulation

HACKING CULTURE
Attack Simulation on physical controls

hack it RED TEAM

HACKING PEOPLE
People-focused services

HACKING INFRASTRUCTURE
Services focused on IT infrastructure

HACKING CULTURE
Services focused on creating corporate security culture

hack it BLUE TEAM

CULTIVATE KNOWLEDGE
Knowledge and perspectives blended into a unified service

COLLABORATIVE MINDSET
Blue e Red team work together collaboratively

OPTIMIZE OPERATIONS
Improve procedures and controls that shield the company for threats.

hack it PURPLE TEAM

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

We believe that security culture is the best tool to counter cybersecurity risks. That's why we've developed **D.R.E.A.M.**, a transformation path for companies.

We believe in a person's ability to understand their own role in this daily challenge that increasingly transcends the professional sphere and enters the realm of private life. We believe that the best way to understand the impact of a problem is when we personally experience it. We believe that, sharing information and learning from mistakes is the best way to grow.

D.R.E.A.M.

is not a service, but rather a vision rooted in our beliefs and crafted by what we do

DIAGNOSIS
Highlight gaps in your company's IT security culture with the goal of encouraging change.

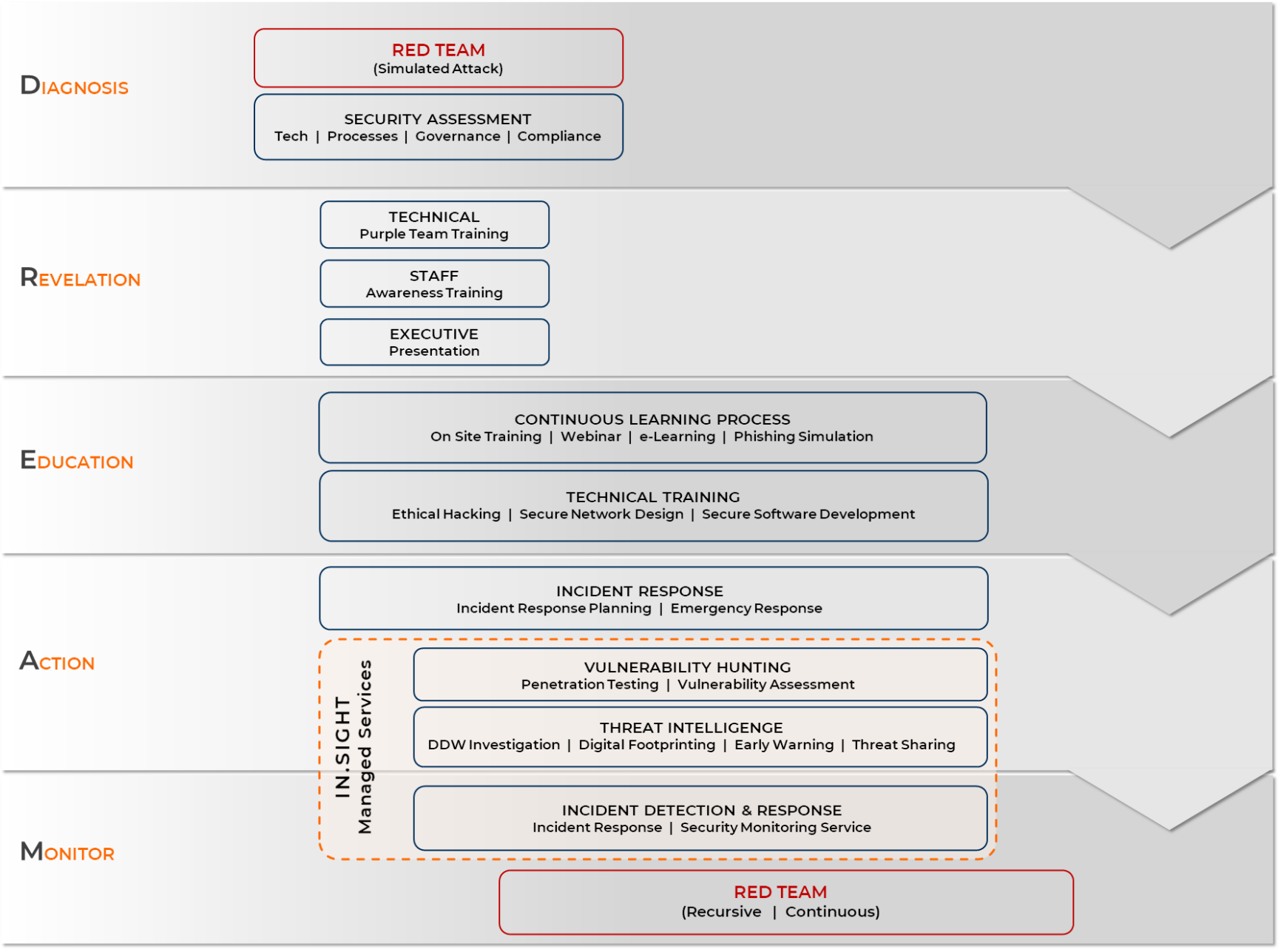
REVELATION
Share results to motivate staff to play an active role in protecting the company from cybersecurity threats.

EDUCATION
Improve knowledge and awareness of cybersecurity by involving each member of the company.

ACTION
Increase the company's level of protection by introducing supporting tools and processes.

MONITOR
Verify improvements introduced in the previous steps to increase detection and reaction capabilities to trigger a continuous improvement process.

THE TRANSFORMATION PROCESS: D.R.E.A.M.



hack it
RED TEAM

IMQ Intuity's **RED TEAM** service helps customers determine if their security strategy can effectively counter a cutting-edge cyber attack by looking at the customer's security through the eyes of a hacker.

Adopting the techniques and mental processes of real attackers, IMQ Intuity's Red Team service explores all aspects of the corporate security setup: *network infrastructure, application security, human behavior, physical security, and business processes*.

For the client it represents an opportunity to broaden their awareness of the techniques and procedures used by attackers, with the ultimate goal of increasing their security and refining their detection and reaction skills.

We give you the chance to take a look into the future, to understand what might happen.

WHAT IT MEANS FOR YOUR BUSINESS

EFFICACY Evaluate the effectiveness of existing technological solutions and organizational measures.

REACTION Measure reactions to intrusion attempts and other security incidents.

AWARENESS Obtain a broader and more detailed understanding of your organization's security level.

IMPROVEMENT Improve your security with a corrective plan based on objective evidence.

WHAT WE DO DURING A RED TEAM SIMULATION ATTACK

OSINT

IMQ Intuity, thanks to particular techniques such as *Open Source INTelligence (OSINT)*, performs in-depth research on the company and its employees to understand the target, to prepare an attack and to determine whether the company exposes information that presents a business risk.

INFRASTRUCTURE ATTACK

The Red Team tries to penetrate corporate security by exploiting vulnerabilities in the IT infrastructure or, as is increasingly the case, in web-based applications.

HUMAN ATTACK

Looking at a company through the eyes of a hacker also means trying to exploit the human factor, which is why Red Team service includes *Social Engineering* activities such as *phishing, impersonation*, and *baiting campaigns*.

PHYSICAL ATTACK

Unauthorized access to the premises can expose the company to significant risks. The Red Team service uses various techniques including Social Engineering techniques such as impersonation to test the effectiveness of the company's physical security.

PROCESS EVALUATION

The results obtained from the Red Team service provide objective data that can be used to assess the adequacy of IT business processes, highlighting critical issues that have an impact on security.

WHITEBOARD ATTACK

The objective is to assess the client's ability to react in a series of simulated scenarios that represent real situations. This activity is carried out through a role-playing game in which attackers (IMQ Intuity) and defenders (client) sit around a table and challenge each other.

hack it
BLUE TEAM

IMQ Intuity's **BLUE TEAM** services allow you to increase your security as well as your compliance with standards and regulations.

It brings you up to speed on your current issues and how they impact your reality, helping you manage all aspects of security with a modern and proactive approach and implement an effective protection strategy.

WHAT IT MEANS FOR YOU BUSINESS

PROTECTION
Ensure corporate security:

correcting the most critical vulnerabilities, strengthening technological devices, monitoring and responding to risk situations.

COMPLIANCE
Correctly comply with the required regulations and standards:

ISO27001, PCI-DSS, AgID, internal compliance.

AWARENESS
Increase internal awareness:

make the human factor a key element for the security of the business.

IMPROVE INFRASTRUCTURE

VULNERABILITY ASSESSMENT & PENETRATION TEST
We look at how technological vulnerabilities can be exploited and what consequences they can have for your business. We test systems, Wi-Fi, apps, and source code.

WEB E MOBILE APPLICATION VULNERABILITY ASSESSMENT & PENETRATION TEST
We look for vulnerabilities in your company's web and mobile applications.

DoS/DDoS
We test applications and infrastructure to assess the level of resilience against DoS/DDoS attacks.

EDUCATE PEOPLE

SOCIAL ENGINEERING
We exploit human vulnerabilities to launch an attack on the company and provide evidence of critical people-related issues using *phishing, impersonation, baiting, tailgating and piggybacking techniques*.

SECURITY AWARENESS
IMQ Intuity's training services provides employees with the basic skills to face cybersecurity threats knowledgeably and autonomously, with training courses aimed at both technical and non-technical personnel, often employing *gamification*.

ADVISORS/CONSULTANCY
We help companies correctly approach cybersecurity, directing them towards the specific path that best matches their own particular needs.

ENHANCE PROCESSES

INCIDENT RESPONSE PLAN
Organizations have to do their best to prevent cyber attack to succeed, at the same time they need to be prepared for the worst-case scenario: a hacker can breach the defenses. In this case a quick and efficient response can save the business from a disaster.

IN.SIGHT (INCIDENT, DETECTION & RESPONSE)
We offer services for the detection and management of Security incidents.

THREAT INTELLIGENCE
We study phenomena that could pose risks to a company or to a specific sector. We update our customers and their technologies with the latest cybersecurity findings to protect them before a problem even arises.

SECURITY ASSESSMENT
Our service is developed according to the CIS20 model to assess the level of corporate IT security, which can also be compared with other standards such as: ISO27001, NIST, PCI DSS.

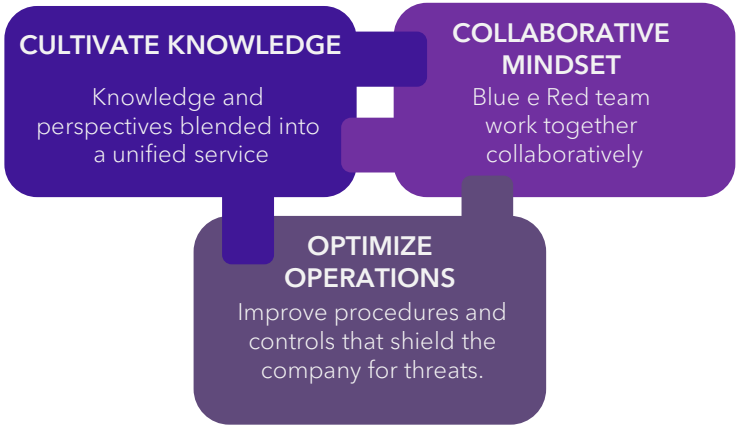
hack it
PURPLE TEAM

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.

GOALS OF PURPLE TEAM SERVICE



Thanks to Purple Teaming activities, the Red Team exercise assumes a relevant educational value, as all the actions carried out can be **explained**, **discussed, tested together.**

The customer has the opportunity to immediately understand what works and what needs to be improved in its infrastructure and processes.

hack it
PURPLE TEAM

PURPLE TEAM REPLAY

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

PURPLE TEAM SCENARIO BASED

A cell of IMQ Intuity Red Team conducts a series of attacks based on some scenarios, previously 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 without the risk of an impact on the real business operations. By formulating different scenarios, teams compare in a T*able-top* simulation.

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.

REGISTERED OFFICE - MILAN
Via Marco Fabio Quintiliano, 45 CAP 20138

OPERATIVE HEADQUARTER - PADUA
Via Brunello Rutoli, 6 CAP 35129

OPERATIVE HEADQUARTER - ROME
Via Nazionale, 230 CAP 00184

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

GERMANY - MUNICH
GMBh Lepoldstraβe, 240 PLZ 80807

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