

CONTACTS

c/o Università Politecnica delle Marche,
Engineering Department,
Via Brece Bianche,
60131 Ancona
P.IVA 02906880428
Tel. +39 071 2205423
E.mail info@ancharia.net
Sito www.ancharia.net

COMPANY INFORMATION

Innovative startup
Established: 2021
Business development phase: growth
Share capital: € 10,000

TEAM

1 Ethical Hacker
1 CTO
1 Crittograph
1 Electronic Engineer
1 SIEM expert
1 Blockchain expert
1 Company focused on business posture
1 Company focused on medical software

MAIN VISION

Ancharia aims to analyze, test and secure computer networks. The aim is to help companies to face the threats of cyberspace

MARKET OPPORTUNITIES

Cyber threats have increased tenfold since 2019. In 2020 thanks to the pandemic, cybercriminals have found fertile ground for their activities also thanks to smart-working which has contributed to extending the corporate cyber perimeter. Ransomware is one of the main cyber threats, an extremely profitable type of cyber attack, confirmed by the Clusit 2021 Report: ransomware in 2018 represented 23% of all malware, in 2019 they became almost half (46%) and in 2020 they reached 67%. In practice, two-thirds of the attacks are ransomware.

Cybersecurity market

Revenue in the cybersecurity market from 2018 to 2025, by segment (in billion U.S. dollars)

Source: Statista



THE SOLUTION

We test networks using controlled simulations of hacker attacks. We provide reports in Italian that can be understood even by those unfamiliar with the technical language. We guide the customer through a step-by-step process by bridging the gap with European cybersecurity standards.

THE COMPETITIVE ADVANTAGE

Ancharia is the only reality in the Marche region totally focused on cybersecurity. We do nothing else, we are highly specialized in offering services focused on accompanying our customers through a complete path of securing their business.

BUSINESS MODEL

We offer cybersecurity-oriented services, according to the SaaS model (Software as a Service / Service as a Service)

CYBERSECURITY

Cyber Risk Assessment

We evaluate corporate posture through frameworks recognized by the European and International community.

Phishing Campaign

We test employee maturity through what is considered the main attack vector used by cybercriminals to compromise companies.

Awareness

Corporate training using Social Engineering techniques and practical demonstrations remotely and in person.

Vulnerability Assessment

We carry out periodic scans that provide a detailed report on the vulnerabilities present within a company.

Penetration Test

More concrete simulations of an attack with the aim of highlighting all the criticalities of a network and then being able to remedy the flaws found. We provide the customer with detailed reports in Italian.

WAPT

Penetration test of web applications, or portals and websites.

Malware Analysis

Malicious payload analysis to understand the intentions of cyber criminals in detail.