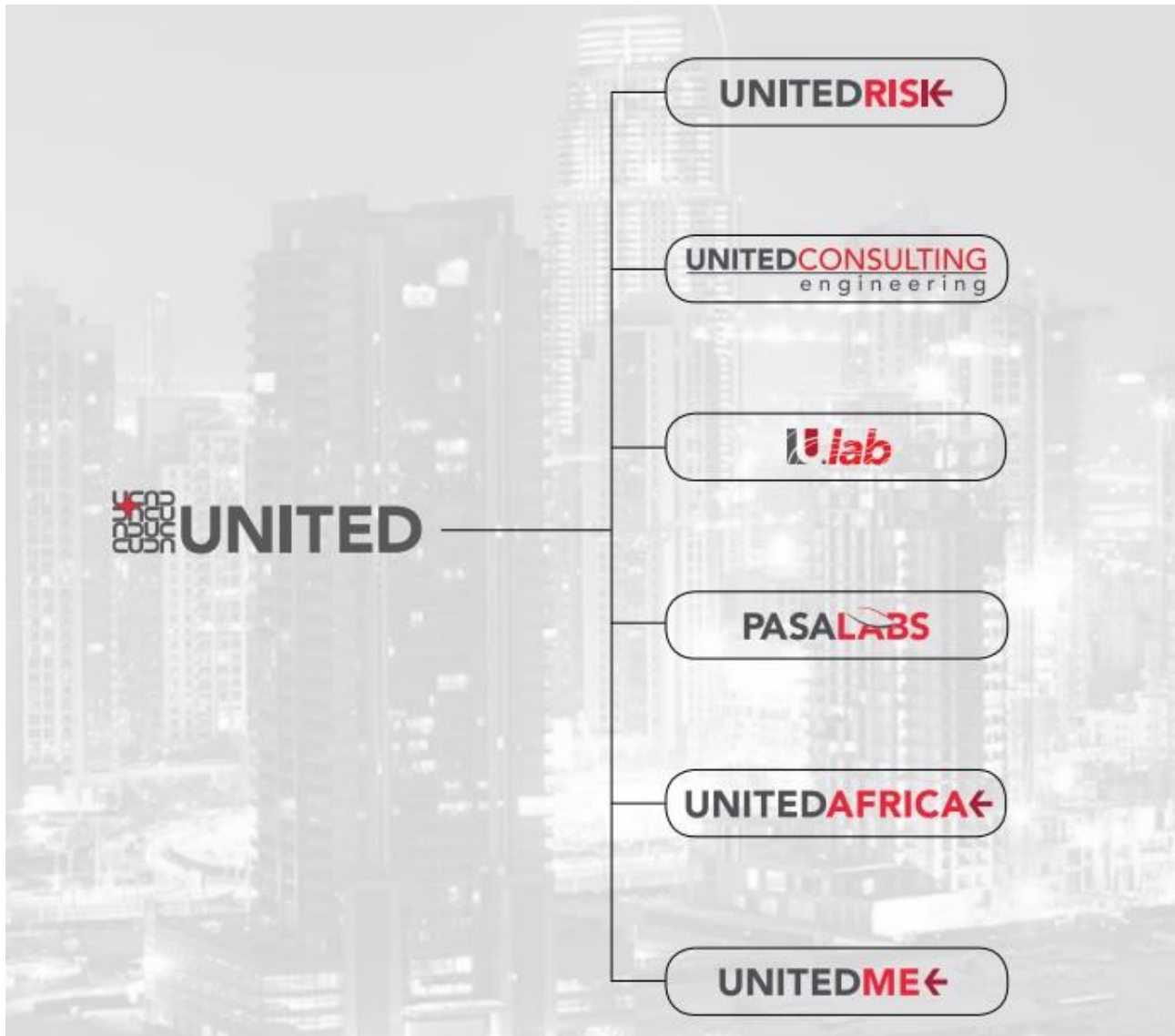


UNITED GROUP

United S.p.A. is an international experienced Italian Group and our mission is to guarantee an integrated and coordinated response to both organization and individual security requests.

Our Group operates throughout Italy with United Risk Management S.p.A., United Consulting Engineering Srl and U.lab Srl. Abroad, we are working through our legal entity in Africa, based in Senegal (Dakar), and another one in the United Arab Emirates, based in Abu Dhabi.

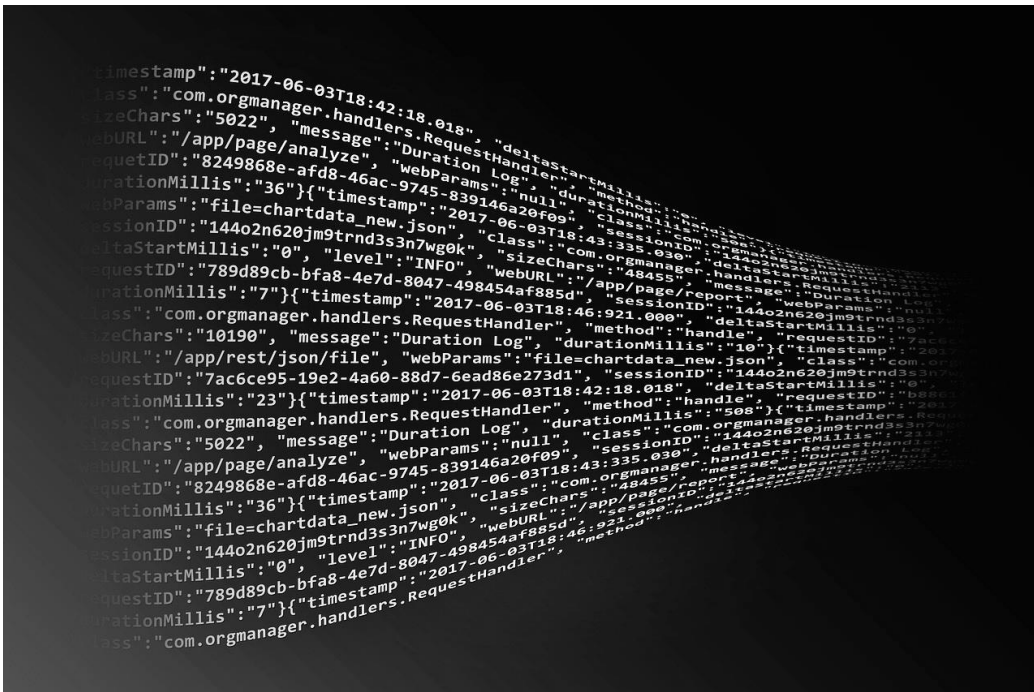


CYBER THREAT - INTELLIGENT PLATFORM

Millions of cyber-attacks are happening around the globe every day. Cyber threats and attacks are becoming more common, sophisticated and damaging. A company's digital infrastructure plays a critical role in blunting cyber-attacks but maintaining its effectiveness can be a challenge.

Often, the effort required to upgrade infrastructure and train staff can be costly and time-consuming. Next-generation architectures offer "self-defending" capabilities that can increase an organization's odds of surviving an attack with only limited damage.

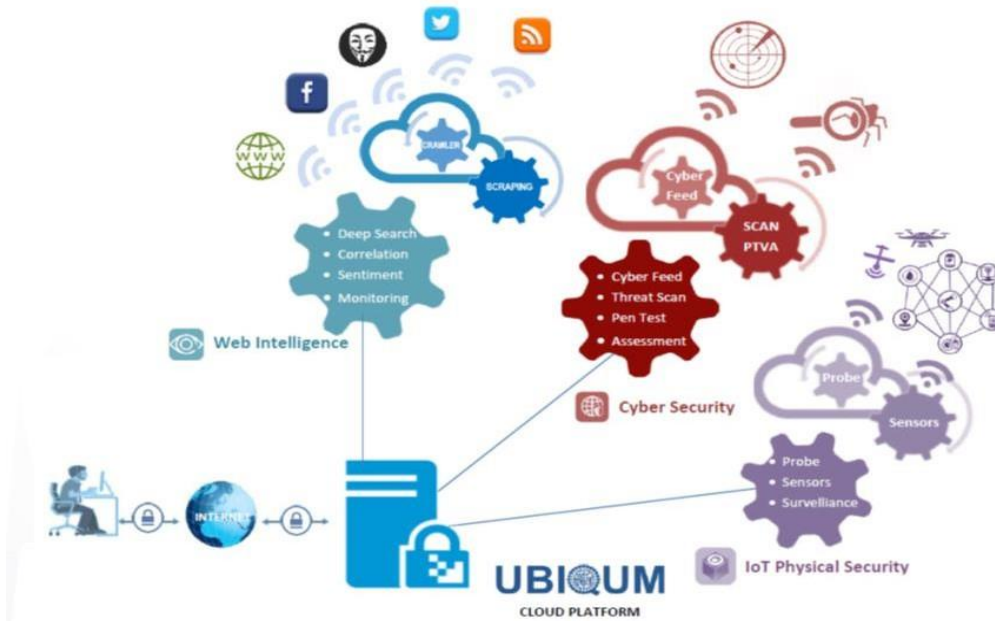
United together with an Italian partner has developed an exclusive technology to effectively counter and prevent new Cyber threats: Ubiquim, a cloud platform able to perform real-time analysis of threats and vulnerabilities in the customer's ICT infrastructure.



Using UBIQUIM platform we offer 2 services

Using our Cyber Security Platform Ubiquim we offer continuous Penetration Test and Vulnerability Assessment Service (PTVA) in the "Follow Up" mode of the identified critical corporate assets that includes intranet / extranet network infrastructure, host, network and domain services.

Through the non-invasive installation of a PTBOX appliance based on the SENSO proprietary technology, when connected to the customer's local ICT infrastructure, our Cyber Division experts can perform remote PTVA activities. Due to this remote PTBOX service, it is possible to guarantee the monitoring (24x7x365) of critical assets in the different locations (even geographically distant) with real-time updates of any anomalies and / or critical issues.



1. EXTERNAL CHECK - UBIQUUM RISK Assess & RISK Manage

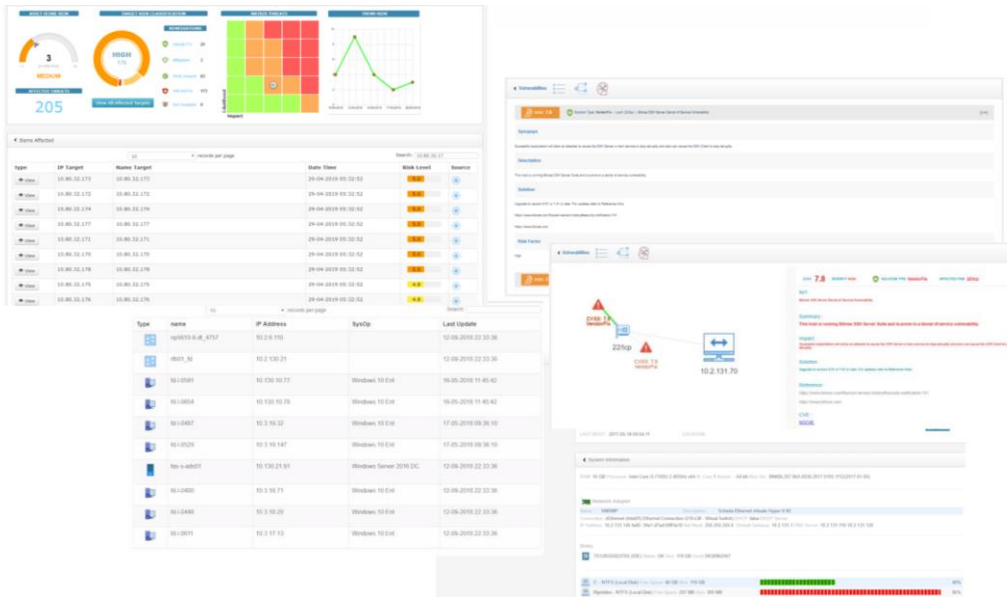
The PTVA (Penetration Test and Vulnerability Assessment) service takes a picture of the level of IT security currently implemented by our client. The PTVA service provides for the execution of in-depth tests using Ethical Hacking. It is based on attack techniques aimed at identifying vulnerabilities not known or, in any case, not detectable by means of automatic scanning and analysis tools. It is carried out by qualified professionals and in compliance with internationally recognised methodologies, such as, for example, the OSSTMM (Open Source Security Testing Methodology Manual), adapted to the specific needs of the client and the attack scenario.

The PTVA service is carried out from outside (External Penetration Testing) and / or from inside (Internal Penetration Testing), in "Gray Box" mode to simulate different attack scenarios. At the end of the PTVA activities, the gap analysis will be performed to verify any critical issues issued by the IT stress test, the compliance with the corporate ICT security criteria and the regulations in place, including that relating to the new European regulation (GDPR) on sensitive data.

To complete the gap, analysis will be carried out using the Security Assessment which will develop the remediation plan, including indications and guidelines (e.g. system update and hardening, control and monitoring process implementations, etc.) needed to harmonise the processes of security with the requirements of the GDPR. Furthermore, we will check your Internet connection and Domain Hosts (mail server, DNS, Web server, etc.) to verify their reputation and trust.

GDPR Compliance Check

As part of UBIQUUM Cyber Scan, we check your GDPR compliance and identify the risk level of IT assets for GDPR compliance.



This will be provided by means of a detailed report and you will have access to real-time information in the case of UBIQUUM RISK Manage & UBIQUUM Cyber Monitor.

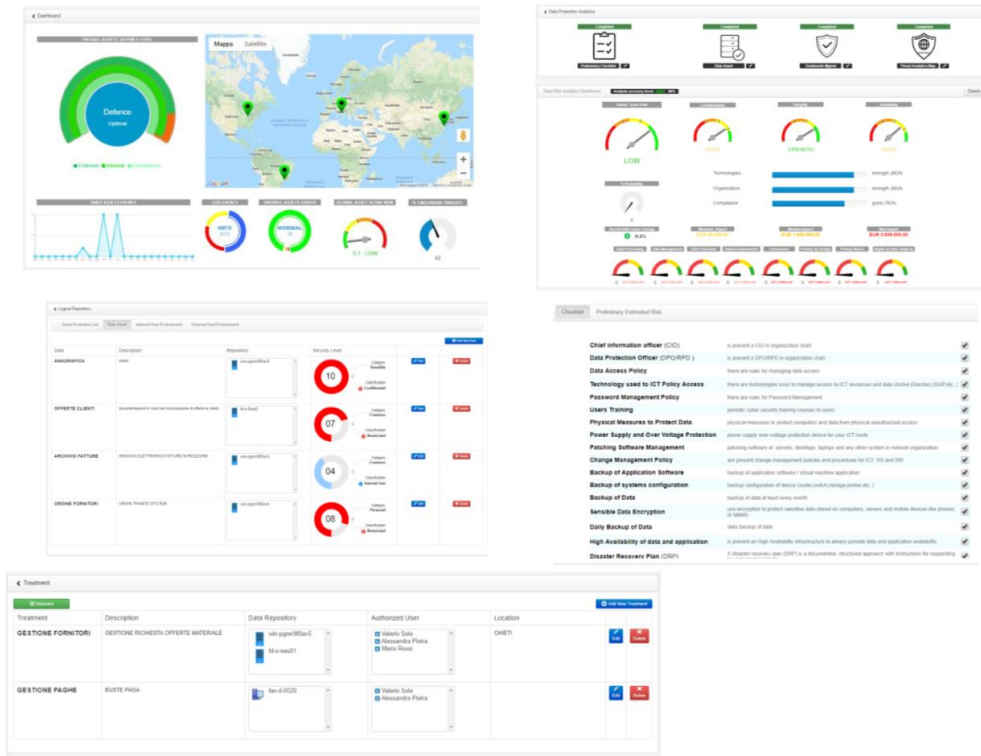
INTERNET Computer Check

For all our services, we analyze computer configuration and browser for secure Internet connection, recommending the security level based on use; we also check your Internet connection and Domain Hosts (mail server, DNS, Web server, etc.) to verify their reputation and trust.

2. INTERNAL CHECK - UBIQUUM Cyber Scan & Cyber Monitor

This service provides a general view of the security of our client through a detailed cyber security check for one month. We will install a probe in the network and, using our unique technology, we will conduct the required testing and will provide a detailed report with list of vulnerabilities and remediation plan.

Using our “Ubiquum” Cyber Security platform, we provide full-time monitoring of all IT infrastructure with a defined priority setting, to optimize resources and intervention times, for greater efficiency. This stage allows to supervise the status of architectures, devices, applications, connection systems and user access, as well as the status of the hardware and software inventory of the customer's ICT system. The full-time monitoring of ICT systems allows to minimize anomalies and critical events that can lead to possible user down-time. Monitoring activities are carried out 24x7x365. The customer can check the status of its ICT system in real time through a detailed dashboard.



IoT & Ubiqum Platform

Thanks to the exclusive and proprietary technology, specifically designed for the development of physical computing applications, UBIQUUM is able to control IoT sensors for monitoring physical environments and for controlling their security (datacenters, industrial plants, reserved areas, etc.). Cyber platform allows to acquire heterogeneous information from environmental sensors (eg temperature, humidity, smoke, radioactivity, audio, video, access control, or any other infos coming from a IoT devices.), correlate them and process them on their own platform of deep learning.

Monitor physical devices has never been so easy, the plug and play sensors can connect directly to the PT-BOX or to an x-server concentrator, simply turn them on or connect them to an ethernet network (also PoE). In a short time and without the need to carry out new wiring or connection infrastructures it is possible to realize environmental monitoring systems for small offices or complex offices, even geographically distributed.

This approach is used also to control sensitive and personal data/papers wared in the cupboard or specific areas. All IoT are linked to Cyber Security Platform Ubiqum and are constantly monitored.

