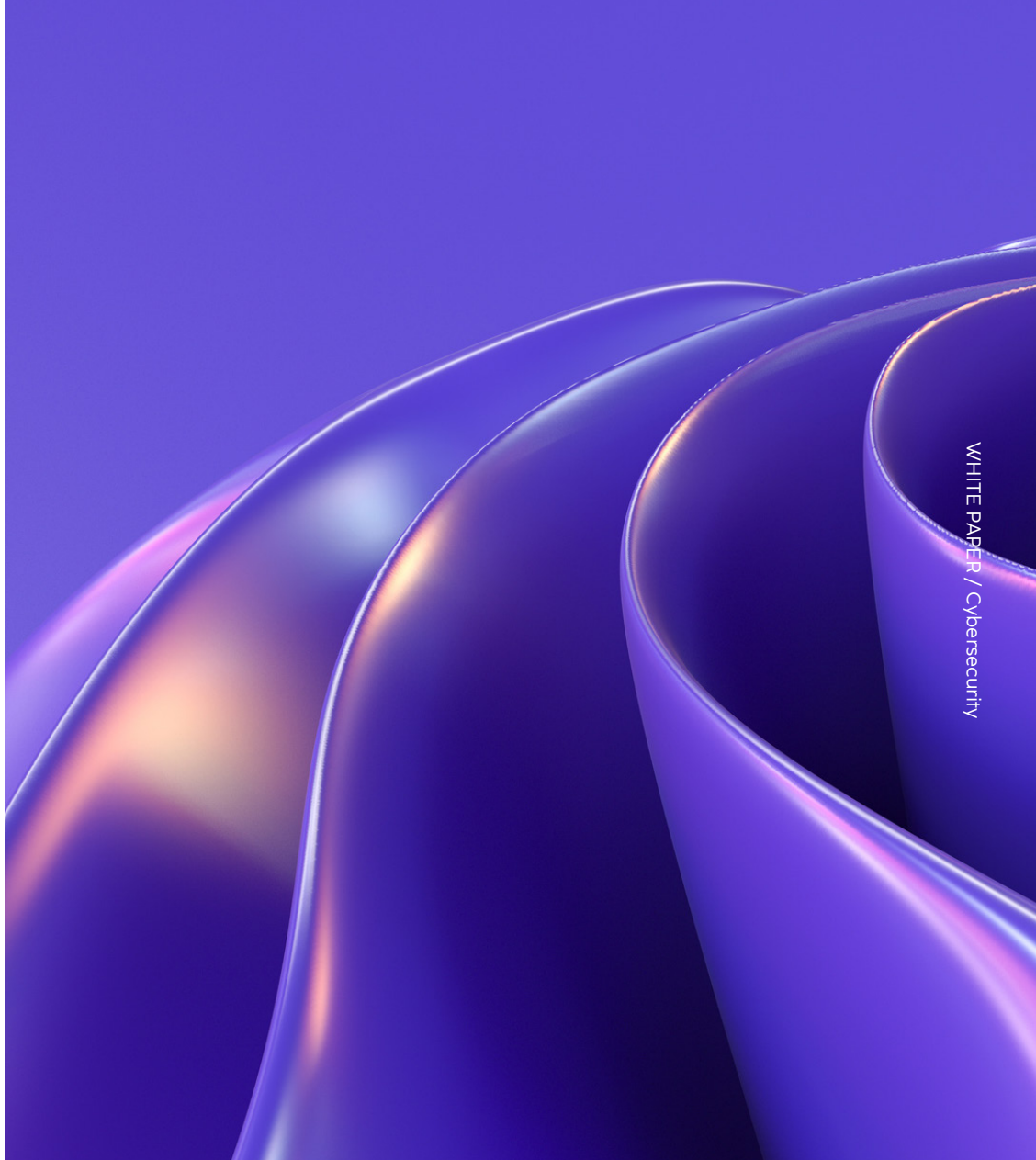
WHITE PAPER

Cybersecurity



Authors

Elio Di Sandro
Cybersecurity Offering Manager

ENGINEERING
elio.disandro@cybertech.eu

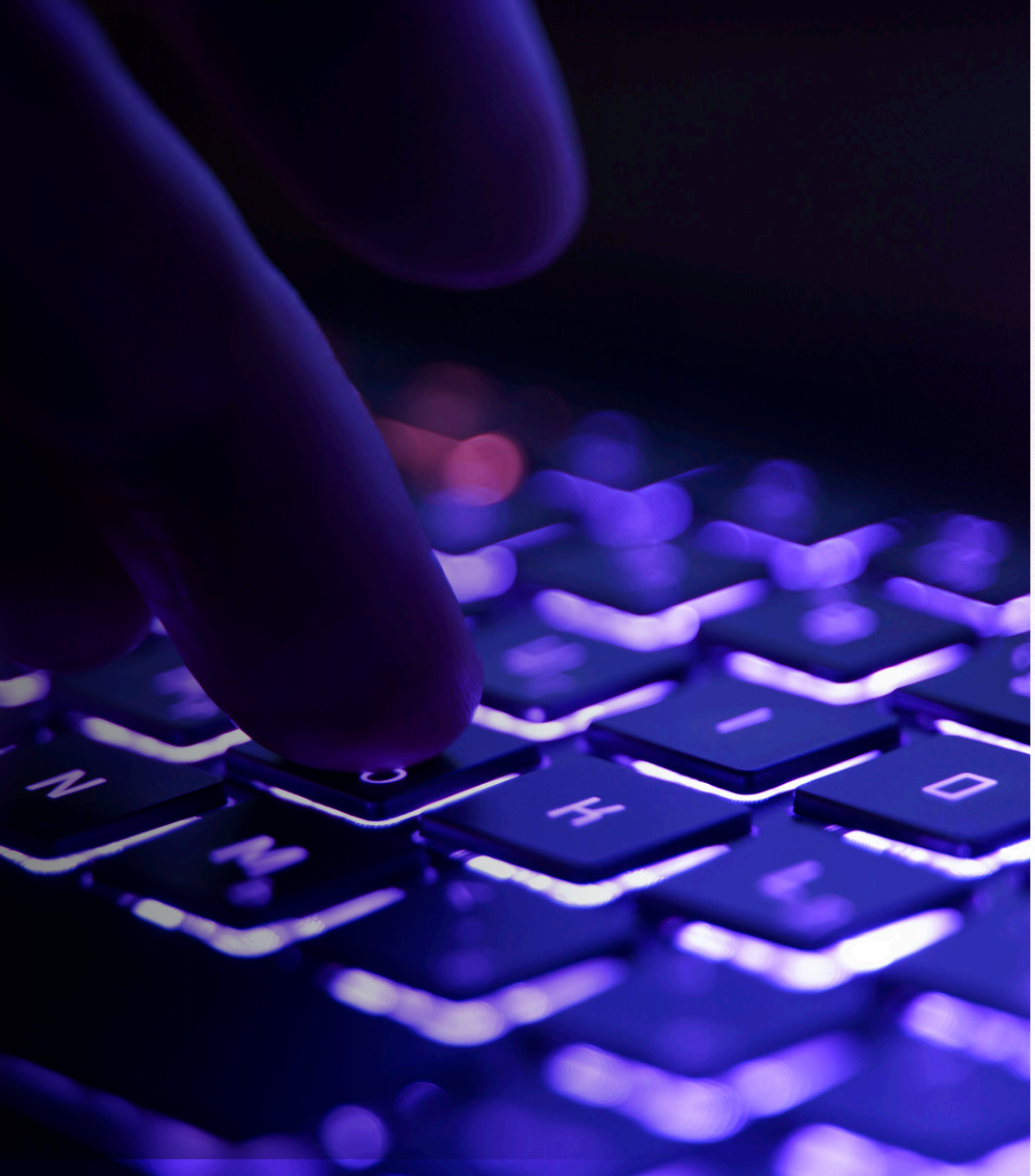
Mara Di Ciocco
Cybersecurity Offering Manager

ENGINEERING
mara.diciocco@eng.it

Paolo Roccetti
Head of cybersecurity Research Unit Engineering R&D

ENGINEERING
paolo.roccetti@eng.it

Index



01

A Secure Business Is A Business That Can Grow

The world we live in is evolving rapidly: **innovation** is bringing improvements to the ways we live and work at an unprecedented speed. However, to the extent that technology is simplifying life, vulnerability to cyber attacks is also increasing.

The **Digital Transformation** imposes two fundamental and divergent imperatives on businesses:

- to **enable** and grow business by implementing online services that securely interact with employees, customers and partners, and by making their structure more efficient and agile so as to respond quickly to new market demands
- to **protect** the business from violations, data breaches and improper access with controls that safeguard data wherever it is located (mobile devices, laptops, data centre and cloud)

Cybersecurity is the structured collection of technologies, skills and processes capable of preventing, detecting and effectively reacting against attacks on people, data, applications and infrastructure.

With the exponential growth in the amount and value of data (code, text, images, infographics, video, signals), the importance of adopting Cybersecurity corresponds directly. Neglecting certain fundamentals, such as continuous Cybersecurity protection and Cybersecurity awareness among employees, can generate significant costs in the long run.

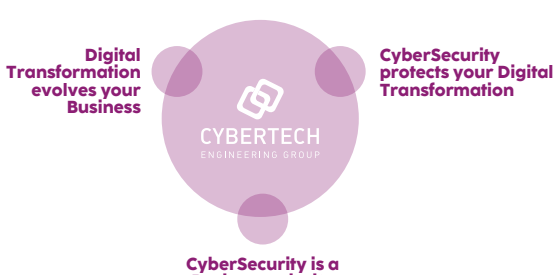
This is why cyber protection should become a "**must-have**", rather than a "**nice to have**" in the decision-making process.

> This change of mindset requires the enhancement of a Cybersecurity culture in every aspect of business, harnessing a mix of experience, expertise and the right technologies

> to ensure a secure and controlled digital transformation.

Since it is impossible to achieve complete security, it is therefore necessary to define a cybersecurity strategy by selecting and balancing where and how to focus interventions, using an approach based on the priority of risk mitigation.

In this scenario, Cybersecurity is not only a business issue, but an essential requirement for the growth and evolution of any company.



02 Modern Cybersecurity Goes Far Beyond Passive Defense

In today's context, characterised by increasing and changing cyber threats to companies, public authorities and operators of critical infrastructures, Cybersecurity is at the centre of the all stakeholders' agenda, in the various roles involved, at both strategic and operational levels.

Cyber attacks often result in substantial business impacts related to business interruption, financial loss and reputational damage.

In a rapidly evolving digital ecosystem, there will be an increasing need to anticipate and address Cybersecurity challenges to stay ahead of the curve, with a focus on enhancing resilience (cyber resilience).

Cybersecurity priorities and drivers that populate the agendas of these stakeholders include multiple themes, such as:

Block cyber attacks

Protect against advanced malware, targeted, persistent and silent attacks, and Cybersecurity threats from within.

Address skills shortage issues

Ensure effective, 24x7 security operations despite the shortage of expertise, both within the company and on the market.

Manage ever-changing technological complexity

Know how to manage multiple products, each addressing a security domain, with limited integration capacity that is being updated continuously.

Manage the growth of digital identities

Ensuring continuous and selective zero trust access control to systems, data and applications in a context where digital identities are dispersed, in volume, variety and dissemination.

Secure critical data

Protect intellectual property in the various stages of discovery, classification, allocation of risk of loss or undue manipulation of data, hardening of data repositories, control of access to information, and all this for both structured and unstructured data.

Protect critical infrastructures

Start from the identification of critical assets, unique to each business context, and prioritise investments in a risk management logic.

Protect the extended perimeter

Secure, in a zero-trust logic, data and applications now distributed in the Hybrid Multi-cloud, B2B, B2E, B2C ecosystems, including IoT.

Create widespread cyber culture and keep up with regulatory compliance

Raise awareness to increase the Cyber Posture of the entire system and leverage operational mandates and comply with general and industry requirements (GDPR, PSD2, PCI/DSS, NIS2, DORA, ...).

Cybersecurity is about reducing risksand increasing awareness

$9,2 Trillion

2024 ESTIMATED COST OF CYBERCRIME WORLDWIDE

$4.45 M
AVERAGE COST OF A DATA BREACH IN 2023 ($3.86 M in ITALY)

+25 BN
ESTIMATED IOT-CONNECTED DEVICES INSTALLED GLOBALLY BY

277
AVERAGE DAYS TO IDENTIFY AND CONTAIN SECURITY BREACHES

80%
OF COMPANIES EXPERIENCED ONE OR MORE DATA BREACH IN 2023

82%
BREACHES INVOLVED DATA STORED IN THE CLOUD (PUBLIC OR PRIVATE)

+3.5 M
THE ESTIMATED NUMBER OF UNFILLED POSITIONS IN CYBERSECURITY TODAY

Top 3 Business Impacts

Business Interruption

Financial Losses

Reputational Damage

The main threats come from:

Malware, Ransomware, Misconfigurations, Phishing/ Social Engineering, Identity Theft, Insider Attacks.

Data displayed represents our elaboration of data coming from multiple sources; Engineering Observatory 2022; Market Reports

03 Governance, Incident Response And Data Protection: Our Cyber Intelligence

Cybertech Engineering's Cybersecurity Company

Engineering ensures constant Cybersecurity protection. Choosing our approach to Cybersecurity allows to focus on growing your business, because as your partners, we can train employees, monitor networks, safeguard data and prevent cyber threats before they impact your organization.

Our continuous investment in people and research also ensures that our approach to security is constantly evolving in a way that is aligned to the complexity of our world.

We have the vision, resources and experience to protect your organisation as it embarks on its digital journey.

We enable a secure Digital Transformation for your organisation.

We protect data, networks and infrastructure, and ensure a secure digital space for employees, customers and partners.

We are a member of the European Organisation for Security (EOS) and the European Cyber Security Organisation (ECSO)

300+
CYBERSECURITY SPECIALISTS

550+
INDIVIDUAL CERTIFICATIONS

450
CLIENTS

20+
COUNTRIES WHERE WE HAVE CLIENTS

20 PB
OF DATA PROTECTED

22K
SERVERS

1
SOC CERTIFIED ISO27001/2017

3
SOC CONTROL ROOMS:ROME, ZURICH, BELGRADE

50+
0-DAY (WITHOUT CVE OR IN BUG BOUNTY PROGRAM)

35+
OFFICIAL CVE RELEASES

3
DATA CENTER TIER IV, AGID, ISO27001/ 2013, TIA-942

1
VULNERABILITY ASSESMENT LAB ISO17025/2018

30+
ETHICAL HACKER

For a comprehensive and effective **investment strategy**, it is crucial to enhance people, processes and technologies. But how can this be done sustainably?

The **risk management** approach is the answer:

- Identify the attack surface and key assets for business operations
- Contextualise the risk and prioritise remediation actions based on the types of attacks occurring in the sector
- Enrich the defense portfolio by testing responses to unexpected events
- Remediate identified weaknesses, both technological and process-related
- Evaluate and measure, with a view to continuous improvement, the actions necessary to support the evolution of the company

Addressing Cybersecurity challenges requires a holistic approach and multi-layered "defense-in-depth" security, integrating both vertical and cross-cutting solutions to impact devices, identities, data, technology infrastructures, workloads, and application services deployed in the cloud, as well as to orchestrate technologies, processes, and skills according to reference standards, modern market methodologies and best practices.

The goal is to become adaptive and resilient to cyber risk, looking at security as **proactive prevention**, **early detection**, **rapid response**, **and advanced security analytics**.

Digital transformation therefore requires a new multidimensional and transversal approach to Cybersecurity, capable of deploying skills based on advanced threat detection and effective protection technologies. Each approach must harmonise with the knowledge and processes already present in the company, to ensure that defense is fully aligned with other activities.

In order to facilitate an adequate understanding and mitigation of the cyber risk, enabling the application of countermeasures in a logic of risk reduction and control driven by business priorities both in the organisational and technological spheres, we have designed a three-pillar approach to Cybersecurity:

Govern Digital Identity

To dynamically control access to key applications and data in a 'Zero Trust' logic, anticipating compliance while keeping audit, IT, and Line of Business (LOB) perspectives aligned.

The modern paradigm of digital identity governance is based on a Zero Trust logic, with a centralised control and enforcement system able to authenticate, authorise and connect (with continuous and granular verification) digital identities now dispersed among users (both internal to the company, including administrator access, and external from customers and third parties), IoT-connected devices and APIs, to applications and services distributed between on-premises and - increasingly - in the Cloud.

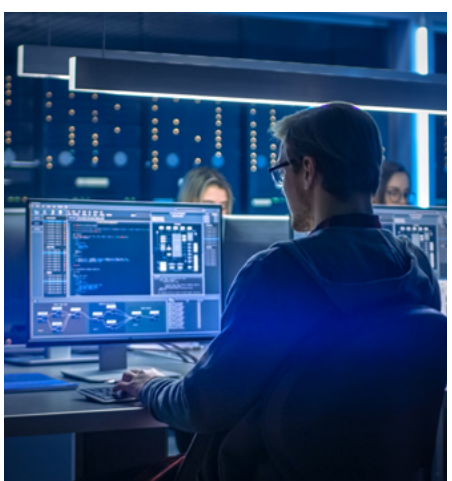
Block Cyber Attacks

To intercept and stop advanced, persistent and insider threats, leveraging Security Operations with advanced data analysis and automation features.

Together with an adequate orchestration of Cybersecurity technologies, processes and skills we ensure effective and orderly counter and response to security incidents.

A "fluid" and continuously evolving security perimeter requires a multidimensional defense, with progressive safeguards capable of intercepting threats along the "kill chain".

This is where the **Intelligence and Automation Driven Security Operation Centre (ADSOC)** comes in, providing a centralised, Artificial Intelligence-driven, and Process Automation-intensive system to integrate and orchestrate the different levels and safeguards of security, consolidating qualified alerts, incident detection, and response and recovery actions into a unified view.



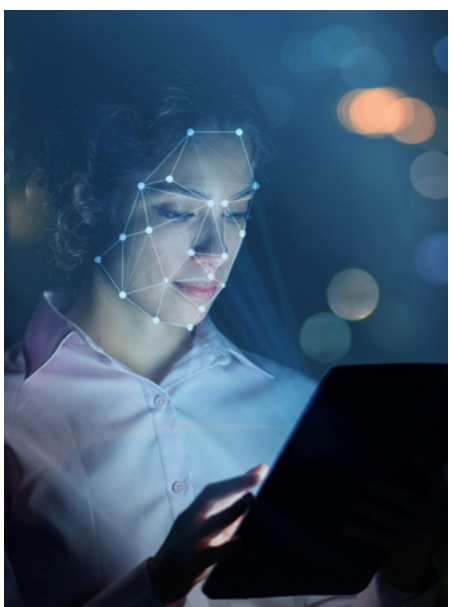
Safeguard Data

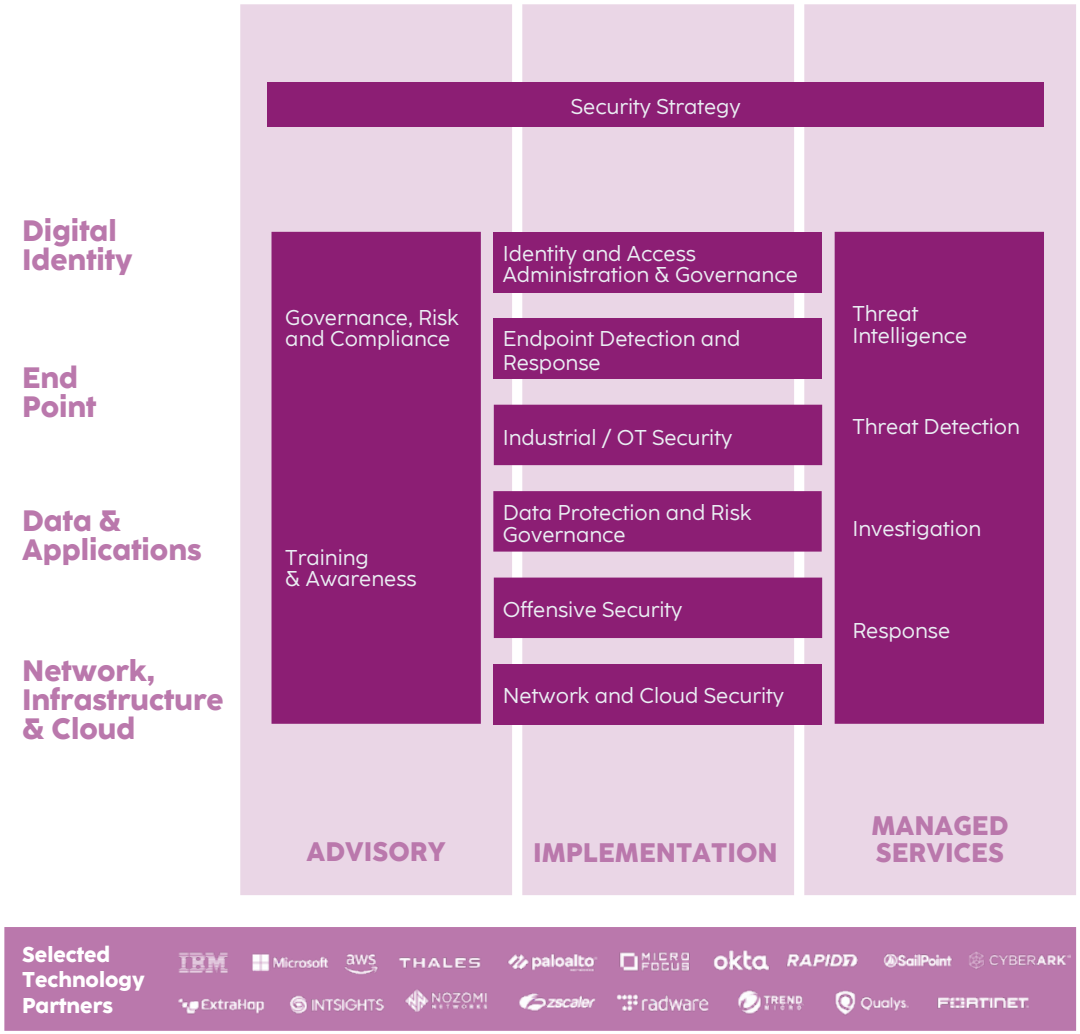
To control the risk of undue access and manipulation of data, protect the brand and enable digital business across the B2E, B2C, B2B business ecosystem, hybrid cloud workloads and an organisation's most important assets.

For a company running a digital business, data is one of its most important assets.

Today, however, data security is being challenged by the fact that more and more information (both structured and unstructured) is being modified, shared, stored locally or in the cloud, and with processes that, if poorly managed, can generate vulnerabilities.

New privacy regulations are also creating increasingly stringent requirements on how to manage data, especially when it relates to individuals.





Finally, thanks to high investments in technology and resources, we have designed a comprehensive, modular and highly flexible service portfolio using the best-of-breed solutions in the market.

04

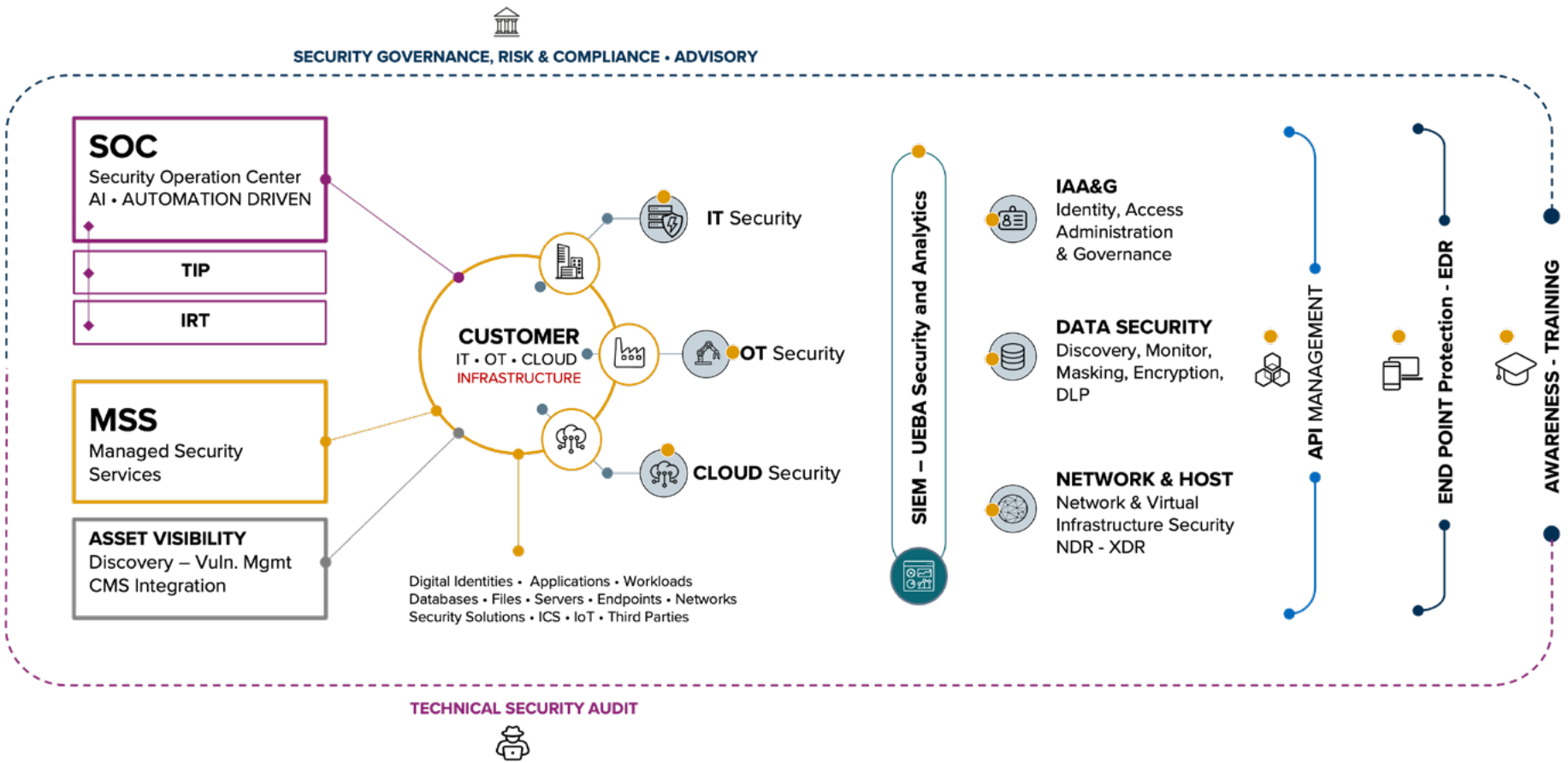
Integrated Multilevel Solutions Provide Security For The Entire Organisation

Integrated Multilevel Solutions Provide Security For The Entire Organisation

In line with our approach, we have positioned and developed our expertise and solutions in various domains of cybersecurity within a solid technological framework. These services include implementation and support, as well as managed services through the Security Operations Center (SOC).

A complete technology architecture organised in a logical structure, to offer solutions within an integrated, cross-functional framework. For our customers, we build and implement integrated, multi-layered Cybersecurity solutions to support the secure delivery of new digital services, while protecting access to apps and data within the mobile, IoT and cloud-connected enterprise. In this way we help organisations to:

- **improve** visibility, control and block the growing threat-cyber surface, achieving adaptive and contextualised security
- **understand** the flow of information and improve capabilities to prevent, detect and respond to cyber threats
- **safeguard** data to support the Digital Transformation journey



The architecture of our services and solutions revolves **around the technological perimeter of our clients**, which includes IT infrastructure, Operational Technology (OT), and Cloud technologies. Our services and solutions are centered around this core, starting with:

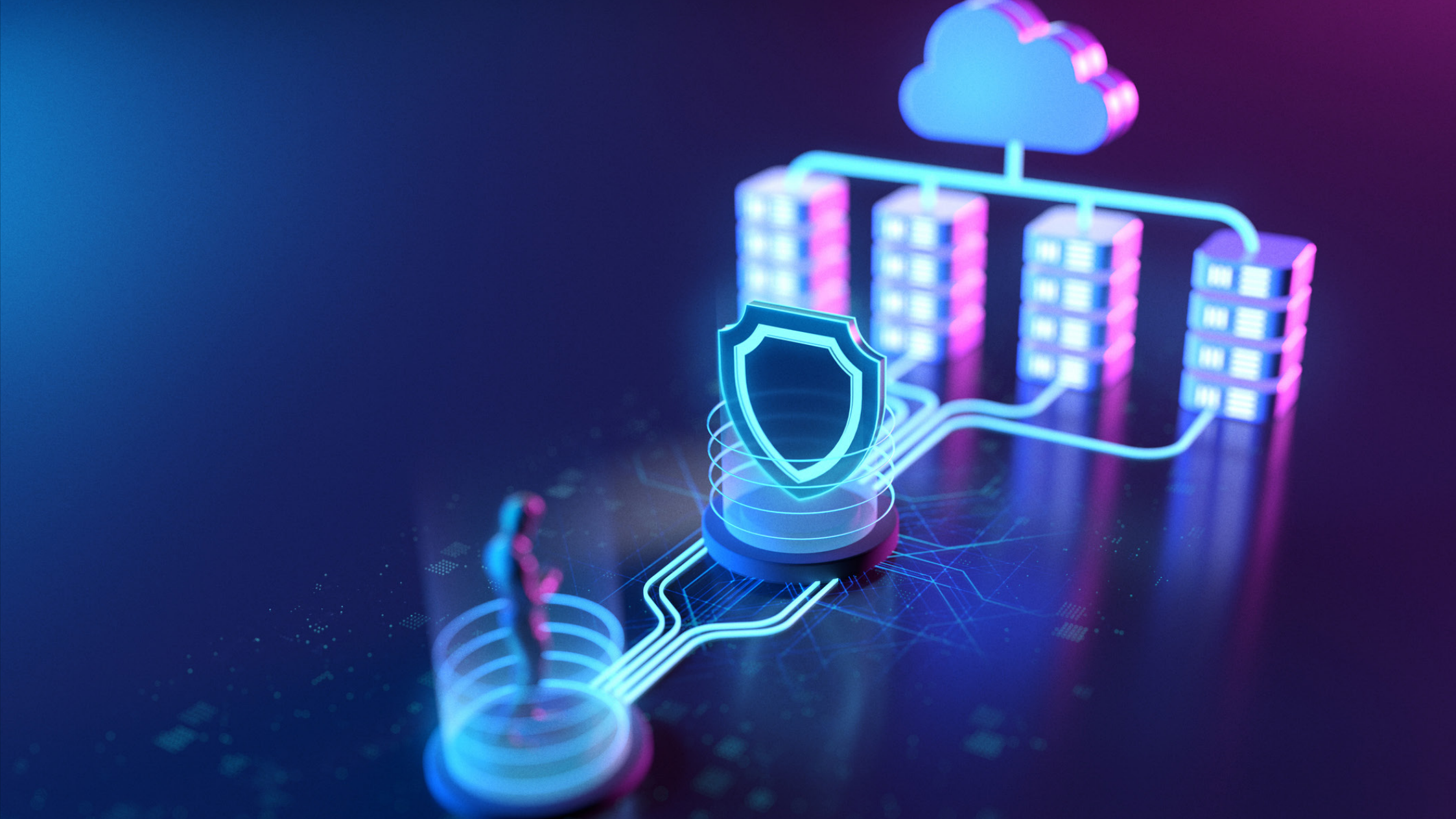
- **Advisory and Governance Risk & Compliance** services to orchestrate the client's security strategy
- **Security Information and Event Management (SIEM)** services, including activities related to Identity & Access Management (IAM), Data Security, Network & Host, as well as API Management and Endpoint Security
- Managed services, starting with a Security Operations Center (SOC) founded on **Artificial Intelligence and automation**, supported by advanced Threat Intelligence and Incident Response services
- **Managed Security Services (MSS)** for security asset discovery and visibility, including Vulnerability Management services
- Services aimed at increasing **cybersecurity skills** and **awareness**
- **Technical Security Audit** services, including Vulnerability Assessment and Penetration Testing (VA/PT).

Focus On

Our SOC Framework, A mesh-like approach

Our SOC Framework aligns with reference standards such as the **NIST Cybersecurity Framework** and draws inspiration from the composable **Mesh approach introduced by Gartner**. It aims to create a collaborative ecosystem of security tools that operate beyond the traditional perimeter, while aligning SOC processes and organization.

According to the principles of the Mesh, in the architectural framework of our SOC, **the control points and security measures are brought closer to the assets to be defended and integrated into a central**, multi-layered platform that hosts analytics, automation, orchestration, and dashboarding/reporting functions.



05 New Technologies Enable To Face New Threats

The proliferation of technological solutions and the interconnection of devices and networks will continue to characterise our development, unfortunately also creating more opportunities for cyber attackers.

Six trends for Cybersecurity up to 2030:

01 / LACK OF SKILLS

The labour market's demand for professionals in this field will continue to increase, and there is already a shortage of qualified personnel. The widening gap could soon lead us to a situation where there are not enough experts to protect critical infrastructure and respond to attacks.

Responding to the Cybersecurity skills shortage will require:

- a combination of short-term and long-term strategies, adopted and supported by public and private organisations, including promoting education and training,
- developing apprenticeship and mentoring programmes, incorporating different skills and approaches,
- using automation and artificial intelligence tools, and retaining existing talent.

02 / INCREASING THE "DEPTH" OF TECHNOLOGICAL SOLUTIONS

In line with advances in automation and autonomy, technological solutions will be increasingly pervasive in our professional and personal lives.

This development, both vertical and horizontal, has the counterproductive effect of increasing the problem of skills shortages.

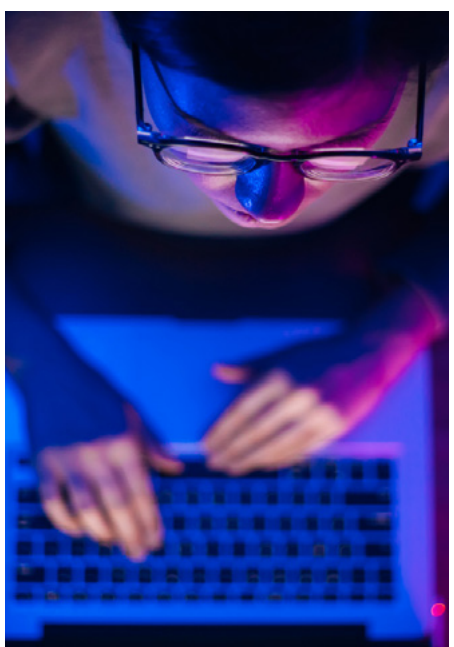
- It will become progressively necessary to balance technological advances with governance and orchestration skills, delegating the more routine activities, but without running the risk of disrupting the autonomy-control balance

03 / INFORMATION WARFARE

The increasing conduct of law enforcement operations in cyberspace by states poses a significant threat to global security: hackers now have the resources and skills to launch sophisticated attacks on critical infrastructures and government systems. Moreover, the legal status of this new field is still unclear. Under this pressure, governments in many countries have already issued operational national security policies to protect their cyber infrastructures, but companies also need to strengthen their security measures to reduce the risks of an attack on a nation-state.

Dealing with this evolving threat will require a proactive and multi-faceted approach that involves:

- developing threat intelligence,
- implementing a thorough defense strategy,
- conducting regular vulnerability assessments,
- implementing access controls,
- developing incident response plans and promoting collaboration between public and private stakeholders.



04 / ARTIFICIAL INTELLIGENCE

Continuous development in the field of AI has also made new tools available to cybercriminals, which could be used to launch more sophisticated and complex attacks: artificial intelligence could be used to generate convincing phishing emails or to exploit vulnerabilities in computer systems. Responding to these new attacks developed through the use of AI by cybercriminals will require an approach that works on several dimensions, including:

- developing AI-based defenses,
- implementing access controls,
- conducting regular vulnerability assessments,
- training employees,
- promoting collaboration,
- developing incident response plans
- regularly updating security measures

05 / INTERNET OF THINGS (IOT) AND CONNECTED DEVICES

The increase in intelligence and connectivity of our physical world through IoT, combined with the spread of the 5G network, creates progressively fluid defense perimeters by introducing new threat-cybers, whose impacts on civil society will be increasingly significant, as in the cases of attacks on critical infrastructures that we are already seeing today. Addressing the Cybersecurity challenges arising from the deployment of IoT devices requires a multi-layered approach, including:

- secure design, strong authentication and access control,
- continuous monitoring, segmentation, isolation
- incident response planning.

06 / QUANTUM COMPUTING

Quantum computers could potentially breach many of the encryption methods currently used to protect data: as quantum computing becomes more widespread, computer security experts need to develop new encryption methods that can resist attacks.

- Addressing the possible threat of quantum computing will require a combination of research, development and planning: by taking a proactive approach and investing in quantum-resistant technologies (Quantum-resistant cryptography, Quantum key distribution, Quantum-safe network infrastructure and Post-quantum security planning), organisations will be able to better protect their data and systems.

For all the trends described, Europe has taken and is taking concrete steps towards a strategy to increase resilience to cyber-attacks, focusing on building greater capacity and coordinating response and prevention processes. However, it is imperative that businesses also strengthen their security measures to increase overall system resilience.

06 Our Innovation Network

Engineering actively contributes to research in the field of cybersecurity, also through participation in European and national initiatives.

We promote innovation by managing projects on emerging topics such as the relationship between AI and cybersecurity, the protection of critical infrastructure, the security of IoT environments, and privacy preservation techniques.

We provide a concrete contribution as the prototypes realized by our laboratory are based on real use cases and developed to meet the needs of various markets including energy, transportation, and healthcare.

Focus On

ENGINEERING HAS BEEN A EUROPEAN PLAYER IN CYBERSECURITY SINCE 2007.

Engineering has been a European player in Cybersecurity since 2007. In the European Security Organisation (EOS), we have promoted a coordinated approach to Cybersecurity with the adoption of a concerted strategy.

Together with the major security players in Europe, our efforts to promote an action plan at European level reached an important milestone with the Cybersecurity private public partnership between the European Commission and industry players through the ECSO, the European Cyber Security Organisation.

Over the last few years, Engineering has directed its research activities in Cybersecurity towards three directions

- **new approaches to train employees and civil servants to detect malicious cyber attacks;**
- **integrated and continuous cyber risk assessment in IT and OT contexts, especially on critical infrastructures;**
- **prioritization of investment decisions based on the economic impact of cyber threats and their increasing contextualisation.**

Engineering Group collaborates with the main national research bodies (including the Research Observatory of the Politecnico di Milano and Clusit) and with the European Cybersecurity Agency, ENISA.

The cooperation of ENISA members to create the European Cybersecurity Certificates, which will be valid throughout Europe for products, processes and services, is of particular importance.

RESEARCH PROJECT / SMART ENERGY & UTILITIES

CyberSEAS – Cyber Securing Energy dAta Services:

The dramatic increase in the attack surface of a modern electrical network makes it essential to protect transmission and distribution systems from cyber attacks that can disrupt operational continuity and cause serious security incidents. The project, coordinated by Engineering, considers the challenges and constraints arising from the presence of decentralized renewable energy sources and legacy systems in the energy supply chains.

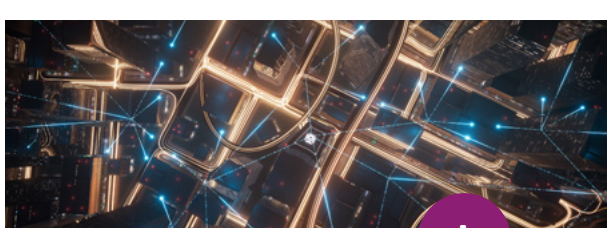
The solution involves innovative models of involvement for producers/distributors and consumers in complex attack scenarios, offering an open ecosystem of customizable security solutions to prevent, detect, and manage cyber attacks, including social engineering. The CyberSEAS solutions are validated through experimental campaigns on pilot infrastructures in Italy, Croatia, Slovenia, Estonia, Romania, and Finland.

RESEARCH PROJECT / DIGITAL INDUSTRY

CERTIFY – aCtive sEcurity foR connecTed devIces liFecYcles:

In IoT contexts, any security modification caused by a vulnerability or an insecure update in the supply chain of a device can jeopardize the entire system. IoT security management must encompass the entire lifecycle of products and requires continuous monitoring and certification to ensure a high level of security in line with the recent European Cybersecurity Act (CSA).

CERTIFY provides a methodological approach and technological and organizational solutions to manage IoT security, including design, assessment, and continuous security monitoring, timely detection, mitigation, and reconfiguration, secure Over-The-Air (OTA) IoT updates, and continuous sharing of security information. Additionally, CERTIFY enables decentralized collaboration among IoT actors and the protection of IoT infrastructures from a wide range of attacks.



RESEARCH PROJECT / DIGITAL DEFENSE, AEROSPACE & HOMELAND SECURITY

ENCRYPT – A scalable and practical privacy-preserving framework:

Recent technologies available to facilitate privacy-preserving big data processing (such as homomorphic encryption, differential privacy, secure multi-party computation, trusted execution environment, etc.) are not yet widely adopted in practice.

ENCRYPT develops a scalable, practical, and adaptable privacy protection framework validated in the healthcare sector for threat intelligence information exchange and in the financial sector for cross-border financial data exchange.

Engineering is part of the project with a methodology and prototype that enable data controllers to have an integrated and continuous estimation of privacy and cybersecurity risks, following a combined approach to personal data protection.

RESEARCH PROJECT / DIGITAL INDUSTRY

KINAITICS – Cyber-kinetic attacks using Artificial Intelligence:

The proliferation of Artificial Intelligence opens the door to new types of attacks, but at the same time, it has the potential to broaden the spectrum of classical cybersecurity tools to protect against these new threats.

Based on specific approaches dedicated to four main use cases (finance, CBRN, computer simulations, health), the KINAITICS project aims to produce a series of AI-enhanced tools.

These tools will advance the current state of the art in attack and defense and will be integrated into an operational framework capable of simulating cyber events to train cyber experts and include their reactions in the analysis. In the project, Engineering aims to evolve prototypes for protection against social engineering techniques and monitoring of cyber threats, including new AI-based functionalities.

RESEARCH PROJECT / E-HEALTH

ERATOSTHENES – IoT Trust and Identity Management Framework:

There are many recent challenges posed by IoT networks: device heterogeneity, system security, lack of common mechanisms for evaluating device reliability, and a reference framework for managing identity, privacy, training, and security protocols in IoT environments.

ERATOSTHENES supports organizations in forecasting, monitoring, and updating the security of their ICT systems, with a particular focus on IoT environments. It also develops inter-ledger mechanisms to share and track cybersecurity information in a network of IoT devices.

Engineering leads the integration of the framework and participates in the validation across three pilots in the automotive, healthcare, and Industry 4.0 domains, providing a solution for intrusion detection in the IoT context.

RESEARCH PROJECT / DIGITAL DEFENSE, AEROSPACE & HOMELAND SECURITY

CitySCAPE – City-level Cyber-Secure Multimodal Transport Ecosystem:

With its progressive digitalization, the transportation sector has become increasingly interconnected, with a growing centralization of fleet and passenger control and management services. However, this centralized architecture increases vulnerability to cyber attacks.

The CitySCAPE project, in which Engineering is a partner, has developed a modular toolkit that can be integrated into any multimodal transportation system to assess the impact of an attack in both technical and financial terms, detect suspicious traffic data values, and identify persistent threats. It combines external knowledge and internally observed activities to improve the predictability of zero-day attacks.

The solution is being tested on use cases involving ticketing applications, computer fraud, and location data in the regional transportation system in the municipalities of Tallinn (Estonia) and Genoa (Italy).

07

KEY TAKEAWAYS

Our Cybersecurity Fabric

key ta

1

Cybersecurity is a tool of Digital Transformation: as such, it is an integral part of the company's growth strategy

2

It is not just about technology: Cybersecurity is a priority and a business decision in its own right, and people and processes are essential components of it

3

It is impossible to achieve total security: instead, it is necessary to deeply understand the risks in order to correctly prioritise investments

4

Risk assessment is continuously changing and is linked to market and company development, as well as the evolving landscape of cyber threats. Therefore, it must be updated to retain its value.

keaways

5

You have to know what you are defending: each company has its own particular reference system, its own interpretation of critical assets (buildings, vehicles, computers and networks, but also trade secrets, marketing plans and pricing strategies) and risk acceptability

6

Prevention is the other side of defense: the study of the evolution of threats and the constant analysis of one's own vulnerabilities, also from the attacker's point of view, are constituent components in the Cyber resilience plan

7

Identity-first security, i.e. the conscious management of digital identities: in a digital world without a perimeter, the identification of users and the correct management of their permissions, in ZeroTrust logic, is the basis on which to build any defense strategy

8

Measuring is the first step to improvement: understanding Cybersecurity achievements and sharing evidence with the entire company is necessary to define improvement actions and raise overall security performance

9

A regulatory environment and standards are allies: compliance mandates, standards and methodologies improve the position of individuals and the value chain ecosystem

10

Resilience and reaction to cyber-attacks must be trained: check the resilience of communication plans, isolation procedures and the underlying accountability system to minimise potential damage

www.eng.it

Engineering Group

@LifeAtEngineering

@EngineeringSpa