

CYBERSECURITY

Protect and enable your company's Digital Transformation through Cybersecurity.



WHAT WE ARE TALKING ABOUT

1	What is cybersecurity?	6
2	What does cybersecurity mean for your company?	9
3	Our approach and our solutions	13
	Governance of digital identities while anticipating compliance	18
	Blocking cyber attacks through the construction of intelligence-led security activities	22
	Safeguarding data to grow the business while protecting the brand	28
4	Our reference architecture for cybersecurity	29
5	What will the future of cybersecurity look like?	31
6	Engineering as an active player in the European cybersecurity strategy	36

AUTHORS

Paolo Roccetti

Head of cysec research unit
Engineering R&D

✉ paolo.roccetti@eng.it

[in](#) [Paolo Roccetti](#)



Paolo leads the cybersecurity research team and coordinates EU and national cybersecurity initiatives, especially cyber risk management for local public administrations, the impacts of cyber attacks on intangible assets, and the use of social engineering techniques and their mitigation.

Pablo Canestro

Sales Specialist, Engineering D.HUB

✉ pablo.canestro@eng.it

[in](#) [Pablo Canestro](#)



In 27 years Pablo has held positions in business development, sales and consulting for leading ICT companies in digital encryption, multimedia solutions, mobile services, and cybersecurity. He joined Engineering D.HUB in 2018 to strengthen and develop the solutions of the cybersecurity team.

Elio Di Sandro

Director of Offering & Solutions,
Cybertech an Engineering Company

✉ elio.disandro@cybertech.eu

[in](#) [Elio di Sandro](#)



With over 35 years of experience in the IT industry, Elio has held technical, commercial, and managerial roles in Italy, Europe, and the US, successfully managing international software and IT services business units. Today he is responsible for the range of IT security services and solution portfolio at Cybertech.

Marco Tulliani

Global Chief Security Officer
Engineering Group

✉ marco.tulliani@eng.it

[in](#) [Marco Tulliani](#)



Marco is a security transformation programme expert with over 22 years of experience in leading global change programmes, delivering sustainable best-in-class practices in Italy, Europe, and Latin America with a focus on information security. He was Chief Information Security Officer at AXA Italy and Chief Security Officer at BNL BNP Paribas Bank.

AT A GLANCE

The world we inhabit is changing. More dramatically and more rapidly. New technological frontiers make it possible to connect everything and everyone. This transformation is driving innovation at an unprecedented speed and bringing hitherto unimaginable improvements to the way we live and work.

But this new world of opportunity needs to be protected: only the right blend of experience, skills, and technology will ensure a safe and controlled transformation.

According to all leading international analysts, the number of serious cyber threats has increased exponentially in recent years and is set to grow further.

For a company that wishes to embark on the road to digital transformation, this trend poses an important question: how can we make sure that the digital world is a safe place for customers, employees, and partners?

Engineering guarantees constant cybersecurity. Companies who choose our approach to cybersecurity will benefit from a partner who can train employees, monitor networks, safeguard data, and prevent cyber threats before they impact the business, allowing the company itself to focus on growing its business.

With over **300 specialists** dedicated to cybersecurity, already protecting over **20 petabytes of data**, we have one of the most significant cybersecurity hubs in Europe. Our ongoing investment in people and research also ensures that our approach to security is constantly evolving in a way that corresponds to the complexity of our world. We have the vision, resources, and expertise to protect your organisation as it embarks on its digital journey.

ADVISORY

450 clients
1 soc certified
 ISO27001/2017

WE MANAGE

22,000 servers

20+ Client countries

Our company specialises in cybersecurity services

300+ specialisti in Cybersecurity

550+ Individual certifications

IN MORE THAN
370 categories

TECHNOLOGY & IMPLEMENTATION

3 certified datacenters
 Tier IV, AGID,
 ISO27001/2013, TIA-942

1 security training school

WE SAFEGUARD MORE THAN

20 petabyte of data

MANAGED SECURITY SERVICES

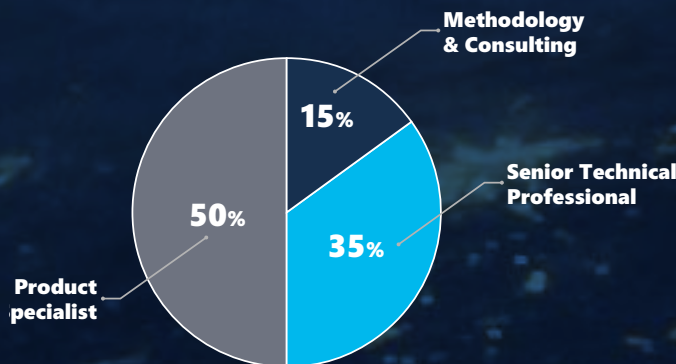
1 Vulnerability Assessment Lab
 ISO17025/2018

OUR RESEARCH AND INNOVATION ACTIVITIES IN THE FIELD OF CYBERSECURITY

We have pursued research activities in three directions:

- new approaches to train public and private employees to intercept malicious cyber attacks;
- re-assessment of risk and prioritisation of investments based on the economic impact of cyber threats;
- increased contextualisation of cyber threat intelligence.

Engineering is a member of the European Organisation for Security (EOS) and the European Cyber Security Organisation (ECSO)





As Chief Security Officer, with responsibility for more than 12,000 employees and over 450 customers worldwide, my job is to ensure the integrity and confidentiality of data for our stakeholders and our Group as well as the availability of our IT resources on a continuous basis.

From my point of view, security must have a 'holistic' approach, and organisations must now turn their attention to this if their priority is a concrete strengthening of their security position. What is at stake here is the opportunity to adopt a customised approach in defining security measures towards our customers, third parties, and other stakeholders through an analysis of their risk profile on an ongoing basis. This analysis will enable the evolution of security baselines, and proactively 'synchronise' companies with their reference ecosystem.

Marco Tulliani

Global Chief Security Officer Engineering Group

1 WHAT IS CYBERSECURITY?

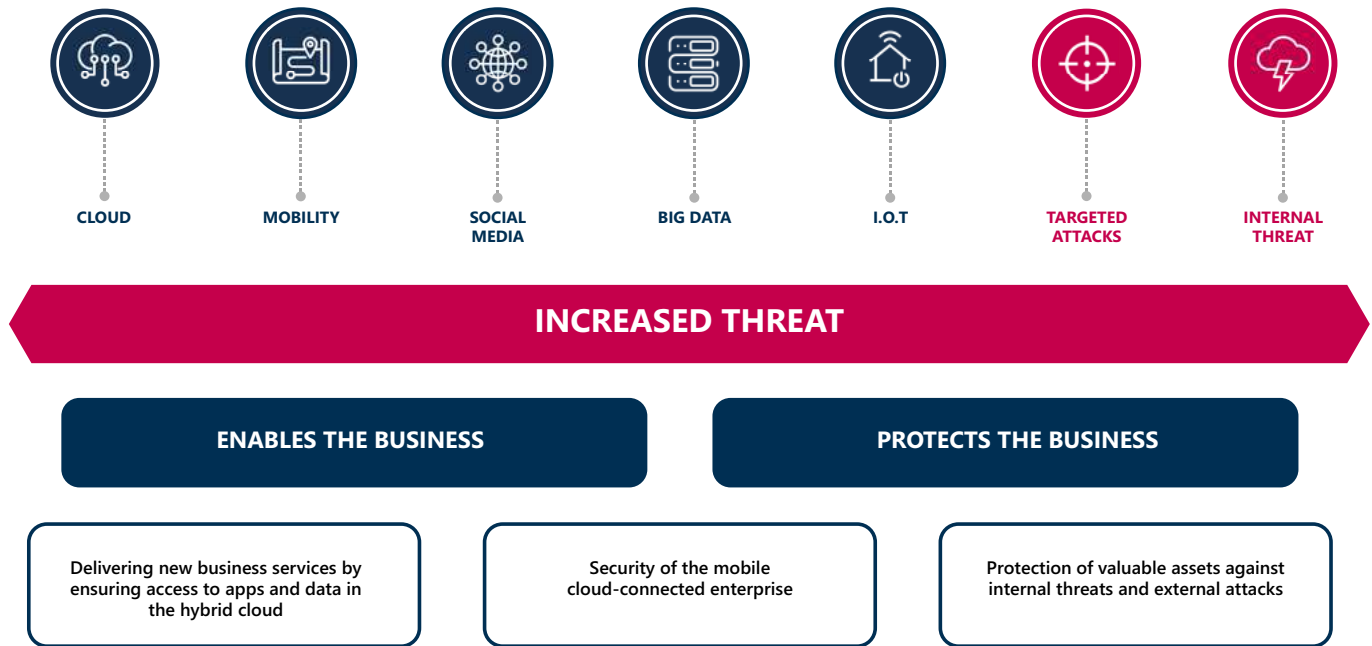


In the context of digital transformation, we define cybersecurity as the set of technologies, skills, processes, and structures required to protect data, applications, and infrastructure from unauthorised access, damage, or attack.

The importance of adopting cybersecurity directly corresponds to the exponential growth in the amount and value of data (code, text, images, infographics, video, signals).

Digital transformation imposes two fundamental and divergent imperatives on companies:

- **to enable and grow the business**, implementing online services that interact securely with employees, customers and partners, and making its structure more efficient and agile to respond quickly to new market needs.
- **protecting the business from violations**, data breaches, and unauthorised access with controls to safeguard data wherever it is located (mobile devices, laptops, data centres and clouds).



In this context, cybersecurity is a fundamental component of the risk management strategy and an enabling agent for digital transformation. Going beyond IT security programmes, it is in fact a structured collection of technologies, skills and processes, capable of effectively preventing, detecting, and reacting to attacks on people, data, applications, and infrastructures.

Attacks are inevitable, and when they occur, cybersecurity professionals, from security professionals down to the CISO, must be prepared. **A strategy is needed to ensure that an organisation's data and key assets remain safe - one that helps them understand and decide where and how to invest.** As with fire safety procedures, teams need to be prepared to act efficiently and quickly: who needs to be called? What part of the business should be isolated? How should the attack be communicated to customers, employees and partners?

The cybersecurity strategy thus becomes an integral part of a business organisation and ranges from prevention and detection to reduce the occurrence of cyber attacks, to mitigation to react to the occurrence of the attack.

2 WHAT DOES CYBER- SECURITY MEAN FOR YOUR COMPANY?



Cybersecurity is a business priority: digital transformation makes your business evolve, and Cybersecurity is essential to protect this transformation. But it is impossible to achieve a degree of total security, and it is therefore necessary to balance risks and investments to be able to protect your business.

To protect and simultaneously enable its digital business within an ecosystem of customers, partners, and employees, a company must implement a holistic approach to cybersecurity, with a strategy that encompasses three dimensions: people, processes, and technology.

More than 90 per cent of cyber attacks exploit people, e.g. using social engineering techniques, to gain access to a company's most important assets. The trend in recent years also shows a proliferation of ransomware attacks. These can entail the encryption and/or theft of corporate data, or a demand for the payment of a costly ransom to obtain decryption keys and to prevent the online publication of data (e.g. in cases of theft of personal data and/or trade secrets, resulting in so-called 'double extortion').

The pandemic brought with it a surge in cyber attacks, with hackers initially exploiting the general climate of fear and uncertainty, and an upward trend in attacks that is now a characteristic of the 'New Normal'. On the one hand, the increased use of remote working allows hackers to exploit known vulnerabilities, which can be traced back to access to services that companies have necessarily found themselves exposed to through virtually protected channels (such as VPNs), but in any case through devices that are not always sufficiently protected, and are directly connected to the Internet, which is intrinsically not secure.

On the other hand, **we have the increase in online services**, another trend driven by the pandemic, but with an acceleration that has now become structural and affects several sectors, from retail (and e-commerce in general) to home banking, from services for citizens to those for health: all this has put and continues to put a strain on portals and application services exposed on the Internet, with attack vectors that have now learned to exploit the supply chain, outside the perimeter of the organisation.

Several studies, both at national and international level, show that attack vectors are now concentrating on the one hand on telework, and on the exploitation of vulnerabilities in protocols and remote desktop clients, and on the other hand on the insertion of Trojans, malware, ransomware, and backdoors through fraudulent sites as well as phishing and smishing attacks.

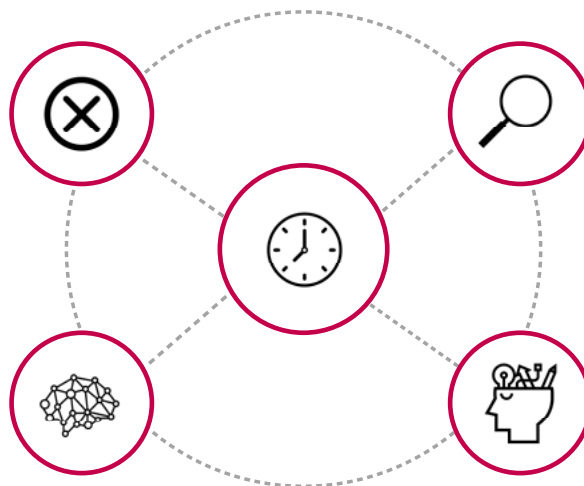
In this polarisation of attack vectors, it is interesting to note that the characteristics of a computer breach can often be traced back to insufficient attention to basic aspects in the management of and access to networks and systems, and to poor hygiene in the general security position of a company and its users, such as incorrect system configurations, high access permissions not orientated to the principle of least privilege, poor network segmentation, open ports (which are open to too many protocols), vulnerabilities that are known but not dealt with, careless user navigation, and the use of weak credentials without MFA.

MISCONFIGURATION / BAD HYGIENE

- Clear Text Passwords
- Over Permissive Credentials
- Faulty Group Policies in AD
- Credentials in Memory
- Misconfigured DHCP

NETWORK ACCESS

- Poor Network Segmentation
- Overly Permissive Access
- Open Ports / Protocols



VULNERABILITIES

- Newly Discovered Vulnerabilities
- Vulnerabilities with Threat (EK)
- Malware with Updated EK of New Vul.

USER ACTIVITIES

- Violation of Corporate Policy
- Access of Compromised Web Sites
- Use Strong Credentials that Can Be Scraped

Precisely because of this growth and evolution of cyber attacks, accompanied by inadequate attention to basic defence principles and practices, **an effective cybersecurity strategy must be an integral part of the corporate organisation** and consist of prevention, interception, and mitigation of the attack.

Preventing a cyber attack starts with a 360° analysis of one's digital and physical world. This inventory must consider risks relating to:

- **tangible assets**, which are not only devices or networks, but also smart buildings, logistics, and factories
- **intangible assets** (often more at risk than tangible assets) including trade secrets, marketing plans, pricing strategies, roll-out deadlines.
- **internal staff, third parties, and customers** who often use company systems with timelines and processes outside the company perimeter.

The inventory, however, is only the first step in a verification process that must never stop. Indeed, ever-evolving connectivity creates an inherently dynamic level of vulnerability, requiring a dynamic identification and classification of one's assets to prioritise what needs to be protected.

An effective prevention strategy therefore has continuous staff training as its most important barrier to attacks. It is the company's task to spread a cyber-aware culture so that all employees (even those who are not ICT experts) feel part of the cybersecurity processes.

The interception of a cyber attack relies on the timely interpretation of a range of information, the importance of which must be recognised immediately. It is therefore essential for teams to have access to threat-cyber intelligence from a variety of sources that can provide manageable data in terms of relevance, quality, and timeliness. Even more fundamental, then, is access to contextualised information about the company and its activities and the ability to act on this.

Mitigation of a cyber attack is driven by two criteria: efficiency and speed. Teams must be prepared to act, knowing who to call and which part of the business needs to be isolated. They must also know the protocol for communicating the attack to customers, partners, and employees.

OUR CYBERSECURITY CHECK LIST

- Cybersecurity is not just about technology: it is a strategy in its own right.
- Have an awareness of how your company operates and don't let anyone else define what is important to protect.
- Make people part of your cybersecurity strategy.
- Perform a 360° analysis of the most important assets and keep it up to date.
- Assets concern everything that is essential: buildings, vehicles, computers, networks, but also trade secrets, marketing plans, pricing strategies etc.
- Uncover the cascading effects of asset damage: how quickly can it spread? Where will it stop?
- Invest in security awareness: training staff, working with customers and partners.
- Prepare for cyber attacks with: expert support, communication plans, asset isolation, redundant processes.
- Manage the identities of system users: information on identities is everywhere. Keep up with regulatory changes, put in place dynamic controls.
- Share and review European and global trends: understand how performance is going, set annual targets to improve cybersecurity.
- Consider cybersecurity as a tool of the digital transformation, making it part of the company's growth strategy.
- Set a target on the reporting delay, analyse how it is improving, compare with trends to understand the level of performance. Choose solution and service providers using clear criteria to ensure consistency in the means employed.

3 OUR APPROACH AND OUR SOLUTIONS





“

For a cruise line, security is a priority. We have to ensure the safety of our guests and crew members.

For us, IT security goes far beyond traditional IT security, also covering operational technology - in particular all systems related to navigation, from the bridge to the engine room. We need to be able to rely on a specialist partner who can cover all aspects of security, but also appreciates the importance of this as much as we do.

Franco Caraffi

IT Director - Carnival Maritime Information Technology - Costa Group

In the changed landscape of the New Normal, which is characterised by growing and evolving cyber threats to companies, public bodies, and critical infrastructure managers, the economic impact of these threats and their impact on the availability of services for businesses, public administration, and citizens has brought cybersecurity to the centre of the agendas of organisational managers in the various roles involved and at both strategic and operational levels. Cyber defence is a matter of concern for the Chief Security Officer (CISO) as well as those responsible for governance, risk management, regulatory compliance (GRC), IT operations, the Chief Information and Technologies Officers (CIO and CTO), and those responsible for application architectures, up to the business lines.

Cybersecurity priorities and drivers that populate the agendas of these stakeholders encompass multiple themes, including:

1. **Blocking cyber attacks** and protecting against advanced malware as well as targeted, persistent, and silent attacks, and cybersecurity threats from within.
2. **Addressing the problem of a lack of IT security expertise**, both within the company and in the market, which limits effective 24x7 security operations or at least drives up associated costs.
3. **Governing the growth** - in volume, variety and dissemination - of digital identities, which are now dispersed in B2B, B2E, and B2C ecosystems, including IoT, in a zero-trust logic, thus guaranteeing continuous and selective control of access to systems, data, and applications distributed in the hybrid multi-cloud.
4. **Keeping up with general and sector-specific** regulatory compliance (GDPR, PSD2, PCI/DSS, NIS, etc.)
5. **Securing critical data** and protecting 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.

Today, in order to deal with these cybersecurity priorities in a structured way, a holistic approach is required. This must combine vertical solutions in the various security domains that impact devices, identities, data, technological infrastructures, workloads and application services distributed in the cloud, with transversal capabilities to integrate and orchestrate different technological and process solutions according to cybersecurity reference standards and modern methodologies and market best practices. These capabilities, however, refer to a multi-dimensional and multi-level model where different technological platforms collaborate and offer progressive barriers to ensure that companies are adaptable and resilient, allowing them to better control cyber risks, which grow and change over time.

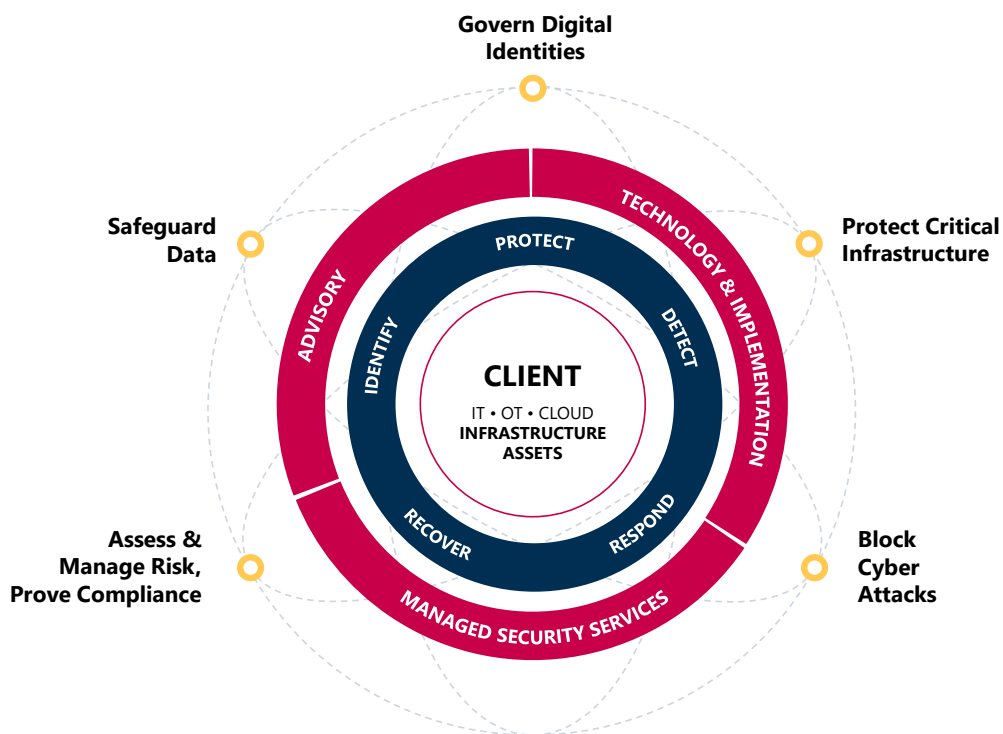
In essence, to become adaptable and resilient to cyber risks, organisations need to regard security not only in a preventive manner, but also and above all with the capacity for early detection, rapid response, and predictive analysis. They must exploit the capabilities of continuous monitoring, control, automation, and advanced security analytics, which today are made available by multiple security technologies at all levels of the IT stack, and which must be orchestrated to act synergistically on several levels.

This is our precise approach to cybersecurity: it is multi-dimensional and encompasses the solutions and capabilities we introduce to support organisations, combining strong specialisation in the various areas influencing security with transversal and operational security capabilities through a 24-hour SOC and shared service centre.

With regard to the cybersecurity agenda of organisations and the expected value results, from our observatory - and with the capabilities and solutions we deploy - we usually aggregate the priorities and drivers we identify according to three dimensions.

One dimension centres on the control of digital identities and access to infrastructures, especially applications and data, through the emerging zero-trust architectures.

In contrast to the 'identity-centric' vision, the cybersecurity dimension is equally crucial and focusses on data protection (from the discovery and classification of critical data to cryptography, PKI architectures, Data Loss Prevention, etc.).



In the middle, between the vision of cyber that is adapted to the government of digital identities and the vision that focusses on the defence of critical data, lies the dimension of tackling cyber attacks, which includes technologies and infrastructural security solutions (from network, to systems, to endpoints). Above all, however, it is based on security operations that are effective in blocking attacks. In fact, in order to be effective, experience teaches us that security operations must first of all be characterised by distinctive professional skills in cybersecurity (so-called Hum-Int, or human intelligence), supported by the successful adoption of security analytics and automation tools.

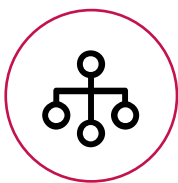
From a business perspective, our approach to cybersecurity is based on three pillars:

- **Governance of digital identities**, to dynamically control access to key applications and data in a 'zero-trust' logic, anticipating compliance while keeping the perspectives of audit, IT, and Lines of Business (LOB) aligned
- **Blocking cyber attacks**, to intercept and stop advanced, persistent, and insider threats by leveraging security operations with advanced data analysis and automation features, and a sufficient ability to orchestrate cybersecurity technologies, processes, and skills to ensure an effective and orderly response to security incidents.
- **Safeguarding data** within the B2E, B2C, B2B business ecosystems, hybrid cloud workloads and an organisation's most valuable assets, controlling the risk of data misuse and manipulation, protecting the brand and enabling digital business.

These three pillars provide an adequate understanding of and mitigation of cyber risks, enabling the application of countermeasures in a logic of risk reduction and control driven by business priorities in both organisational and technological areas.

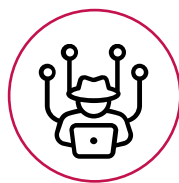
In this way, companies are able to:

- conduct business in a reliable manner, ensuring confidentiality, availability, integrity, and security of information resources together with consistent BC-DC programmes
- maintain continuous and verifiable regulatory compliance
- follow a more secure digital transformation path and adopt the cloud to achieve business growth, brand reinforcement, competitiveness, and greater resilience.



GOVERN DIGITAL IDENTITIES

- **Control Digital Identities w Zero Trust**
- **Get Ahead of Compliance**
 - Dynamically Control Identity ^ Access related Risk
 - Enforce ^ Monitor Access Permissions to App Level
 - Prove Regulatory Confortmity and Align Audit/LOB/IT Perspective



BLOCK CYBER ATTACKS

- **Leverage AI Driven SOC**
- **Automate for Consistent IR**
 - Detect & Stop Advanced & Insider Threats
 - Orchestrate Technologies for Effective IR
 - Leverage Cyber Threat Intelligence/ master Threat Hunting

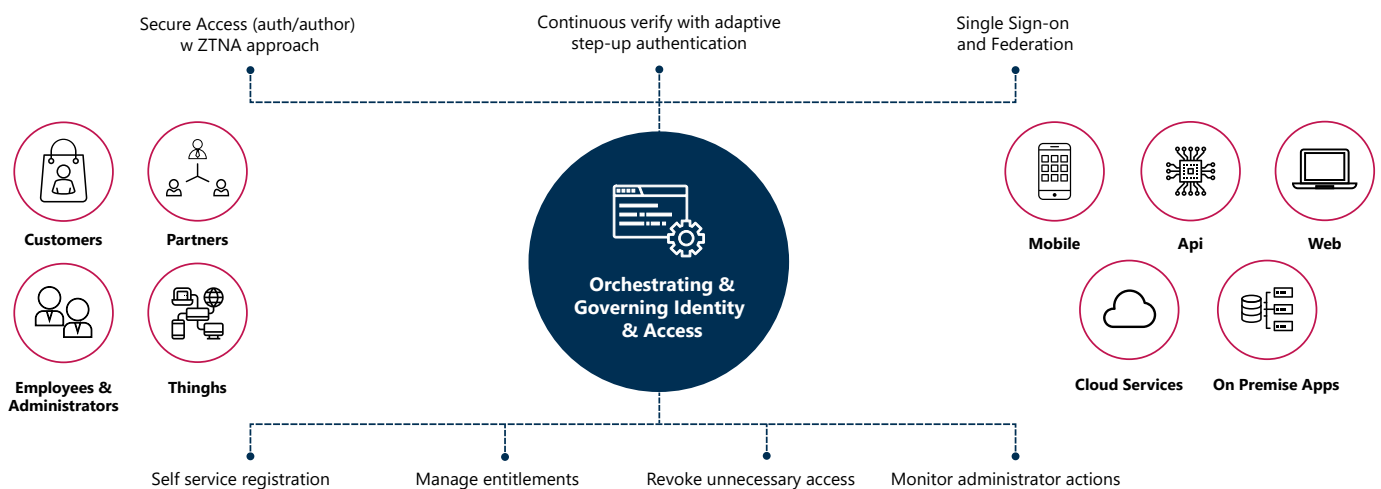


PROTECT DATA

- **Protect Crucial Data and enable Digital Transformation**
 - Secure Hybrid Cloud
 - Protect Critical Assests
 - Assess & Govern Data Risk

Governance of digital identities

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 that are now dispersed among users (both internal to the company – including administrator access, and external – such as customers and third parties), IoT connected devices, and APIs, to applications and services that are located either on-site or (increasingly) in the cloud.



The turning point in the evolution of modern zero-trust identity management architectures is that the core of the system (shown in the centre of the picture) progressively migrates to the cloud, from where it can govern decentralised digital identities that wish to access applications and data that are also distributed in the hybrid multi-cloud.

For this control system in the cloud, 'zero trust' means adopting strong authentication techniques accompanied by dynamic checks during the access session - not only to verify the account, but also the device, the context, and the app to be accessed - applying granular, selective and minimum privilege authorisations.

All this must take place without compromising the user experience and ease of access, through multiple authentication tools, including passwordless.

On the left-hand side of the picture are the multiple digital identities that need to be authenticated and authorised, and whose lifecycle needs to be managed - from internal workforce to system administrators, from external customers to IoT connected devices. On the right are the target systems that these different digital identities access with their form factors (the type of device and target applications) and where they are located (increasingly in the cloud), or the legacy systems that need to remain on-site. The central zero-trust controller then delivers the typical functions of an Identity and Access Management (IAM) system, from identity lifecycle management to single-sign-on via federation, to MFA, with its adaptations for the employee workforce, or for customers and external third parties.

In most surveys, trust in digital identities comes first for any digital transformation initiative. And there are two sides to this trust. One is ease of use, with a user experience that minimises the constraints and need for complex authentication and password storage mechanisms, especially for certain categories of external users such as consumers and customers.

But usability and simplicity of access must not come at the expense of security, and this is the other side of 'trust' in the management of digital identities: it is so essential that modern architectures operate in a logic of 'zero trust'. As we have seen, they continuously verify devices, contexts, and account behaviour throughout the session, applying strong authentication techniques and providing granular authorisations in the logic of minimum privilege.

Identity information is everywhere, attacks are constant, perimeter security cannot provide adequate security, and it is also essential to keep up with changing regulatory requirements.

Hence the need for identity management that utilises zero-trust principles but masks the underlying technological complexity within the centralised control system to allow the user experience to remain as usable and simple as possible.

The following describes the business drivers of any open organisation and some of the challenges they face in the area of Identification and Access Management.

Engaging customers and partners by adopting a zero-trust model that safeguards the user experience

Zero-trust identity and access technologies and processes that combine security and continuous control with an easy user experience must be adopted. Customers want to use their device through a consistent experience across web and mobile platforms. As part of a business ecosystem, partners need secure yet easy access to the information they require. But neither customers nor partners can be completely trusted from a security perspective: centralised policy management, granularity and selectivity in recognising authorisations, and the ability to audit the device and context in which access is initiated (i.e. a zero-trust logic) must therefore be implemented for all users.

Providing secure yet easy access to employees, partners, and customers

Le modalità di doppia autenticazione e le molteplici password si stanno dimostrando sempre più insoddisfacenti. Vengono implementati nuovi modelli di accesso di tipo zero trust, che elevano il livello di astrazione nel cloud, dove viene spostato il punto di controllo ed "enforcement" delle policy: la loro selezione e sicura adozione devono far parte di una strategia. Questo è anche un elemento importante per la qualità della user experience.

Efficiently monitoring the corporate cyber position

Through cost-effective solutions for the integrated and continuous assessment of cyber vulnerabilities and risk at various levels: physical, infrastructural (both IT and OT, Operational Technologies), and organisational. Especially in relation to the most commonly used attack techniques, such as social engineering, in order to periodically assess the preparedness of employees to recognise and report such attacks.

Demonstrating compliance

Managing consent and complying with regulatory requirements relating to Personally Identifiable Information (PII) and data privacy (GDPR) bring into play the dimensions of transparency and accountability.

Adopting identity governance systems for apps increasingly moving to the cloud

With the explosion of cloud-based applications, credential-related cyber risks must be fully managed from the start of any deployment. This applies to all customer, partner, and employee access. When employees leave, for example, their accounts must be logged out of all applications, both on-site and in the cloud. Orphaned accounts represent a risk that needs to be controlled.

Protecting and managing privileged accounts

Internal threats and external attacks are the main risks. External attacks often focus on accounts, especially privileged accounts. When the account is hacked, serious damage can occur. Controls must therefore be put in place to protect what an administrator can do, even after he/she has been authenticated. Extensive controls are needed to limit potential damage from malicious (negligent) users and administrators. Continuous monitoring and documentation can help detect the root causes of a suspected breach.

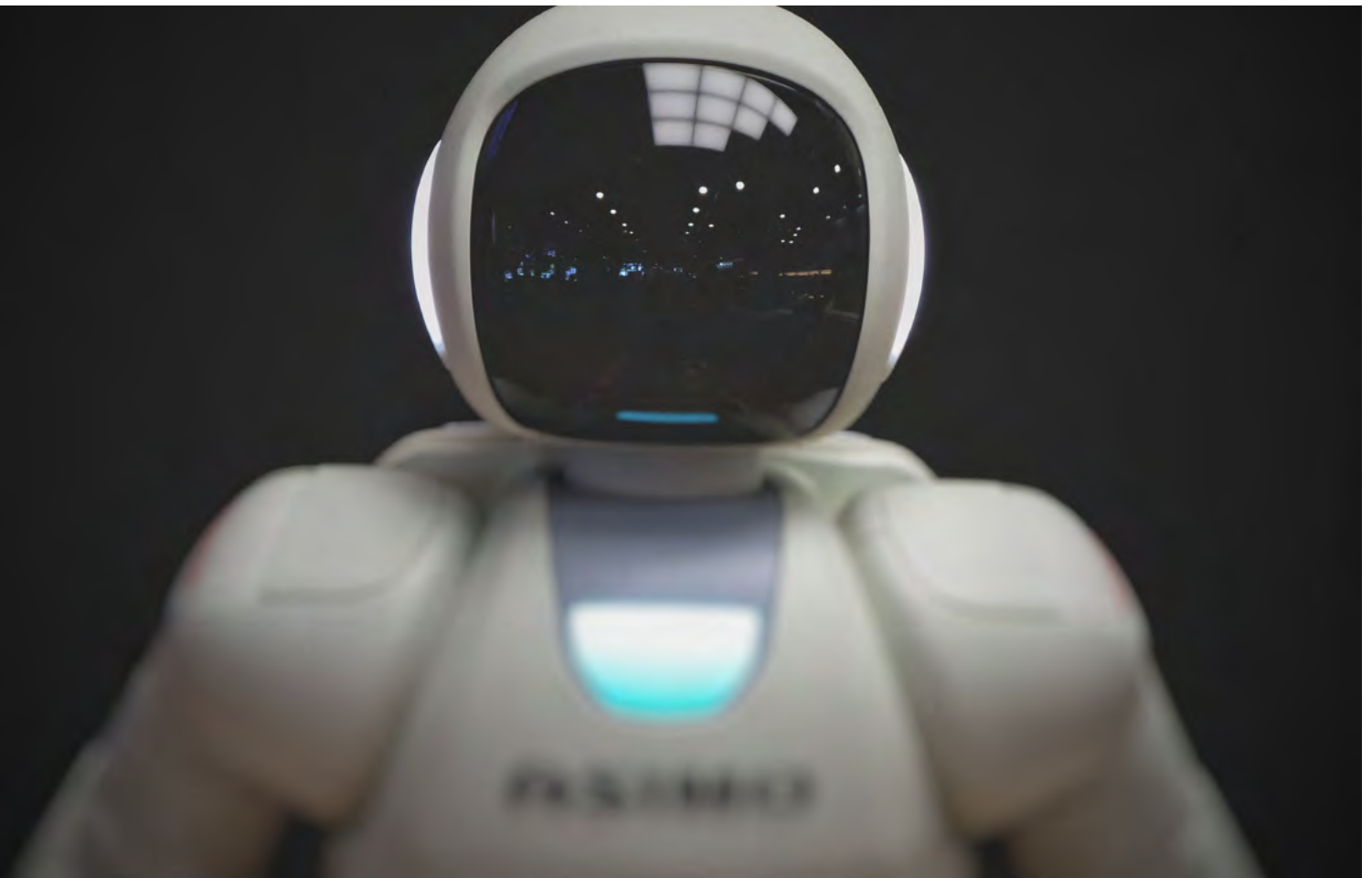


OUR IDENTITY SECURITY PROGRAMME CHECK LIST

In today's 'open' enterprise, digital identities can only be effectively governed by a dedicated security programme, focussing on identity and developed according to the principles of zero trust in order to:

- Establish a centralised zero-trust point of control, mitigating risk within and across companies, verifying regulatory compliance, and enforcing and monitoring access permissions with two-factor authentication (2FA) mechanisms and minimal privilege authorisations
- Anticipate and continuously monitor compliance requirements (GDPR, PSD2, NIS) and evolving government policies
- Align auditors, line of business and IT perspectives
- Use risk analytics and intelligence to represent complex user data and to provide information on hazardous users and internal threats
- Frequently initiate certification and recertification campaigns for access permissions
- Implement identity governance focused on organisational activities and roles, to help managers understand and certify access requests by assessing their nature and impact on the business
- Allow risk and compliance managers to easily obtain audit reports and evidence, manage role mining, reclaim accounts, perform segregation-of-duty (SoD) checks and quickly identify SoD and violations.

Blocking cyber attacks



A 'fluid' and constantly evolving security perimeter requires a holistic approach to the operations necessary to adequately control cyber risks and securely enable digital business.

This is where the Intelligence and Automation Driven Security Operation Center (IASOC) comes in, providing a centralised, AI-driven system that offers high-intensity process automation, for the detection of cybersecurity incidents and response and recovery actions.

The traditional SOC protects the company from the emergence of cyber threats (advanced malware, email compromise, targeted attacks) relying mainly on preventive technologies.

In contrast, the IASOC uses:

- **machine and deep learning as well as the behavioural analysis of users and digital entities**, enriched with threat intelligence, to verify suspicious and dangerous behaviour through an adaptive, knowledgeable, and holistic approach.
- **next-generation network and host security systems**, incorporating preventive protection capabilities, with advanced detection and response algorithms at the levels of the network, the endpoint, and the server (NDR and EDR), combined with cloud security tools, where AI and advanced analytics are embedded throughout the cloud workload stack.
- **SIEM and XDR technologies**, which provide automatic identification of breaches through intelligence and correlation of feeds from the Network Operation Centre, so that the NOC can provide an early warning of processes and assets consuming standard resources (power, memory, bandwidth) due to malicious activity.
- **an architecture designed to automate security activities** across multiple products and easily assign tasks to analysts: the collaborative and interactive interface of the Security Orchestration Automation & Response (SOAR) platform allows security teams to investigate and track analysis and evidence throughout the incident lifecycle, creating a single hub to ensure consistent and compliant response processes.

The adoption of such a level of automation and architecture offers IASOC analysts the following benefits:

- context enrichment and intelligence correlation/fusion
- collection of evidence
- notification, escalation, and reaction through automated processes (digital cyber playbook)
- processing of raw data with analytical algorithms and presentation of results
- removal of manual work and automation in repeatable processes
- time savings and reduced occurrence of errors through more thorough checks.

Finally, Cyber Threat Intelligence (CTI) platforms, in combination with advanced analytics tools, SIEM and the SOAR platform, are the secret ingredient of an intelligent and automated SOC.

The CTI is characterised by many sources, some open community, others commercial, and is responsible for feeding and supporting all the technological components of perimeter security and of the SOC itself, with threat feeds in a machine-readable format that enrich and add precision to the correlation and analytics capacity in the various defence layers.

Apart from the technological component of threat feeds, CTI platforms are useful for:

- adding context and validating security alerts - frequently through SOAR in a standardised and digitised manner on automated playbooks;
- placing the exposed fingerprint of a company under surveillance;
- supporting analysts in the targeted investigation of compromise and attack indicators, adding precision and attribution to known attack patterns and groups;
- performing effective forensic analysis.

All this leads to time savings and greater efficiency in security operations.

INSIGHTS OVERLOAD

Analysts are overwhelmed by alarms and false alarms: 93% cannot sort through all relevant threats.¹

93%

197

INCREASE IN PAUSES

In 2018, companies required 197 days to resolve an incident.²

51%

SKILLS SHORTAGE

51% of companies reported a lack of cybersecurity skills in 2018.³

1 McAfee Threats Report 2016
2 2018 Cost of a Data Breach IBM Study
3 ESG Research 2018

BLOCKING CYBER ATTACKS – SOME USE CASES

The main objective of any cybersecurity strategy is to prevent cyber attacks from succeeding. Let us consider the following use cases. Companies must know how to manage:

ADVANCED THREAT DETECTION

- Identifying threats in real time and escalating this activity to focus on the most critical threats
- Intercepting targeted, persistent and silent attacks
- Avoiding false alarms and minimising the possibility of overlooking real threats
- Identifying threat actors, malware, campaigns and attack vectors exploited to address skills and knowledge gaps and the growing variety of threats.

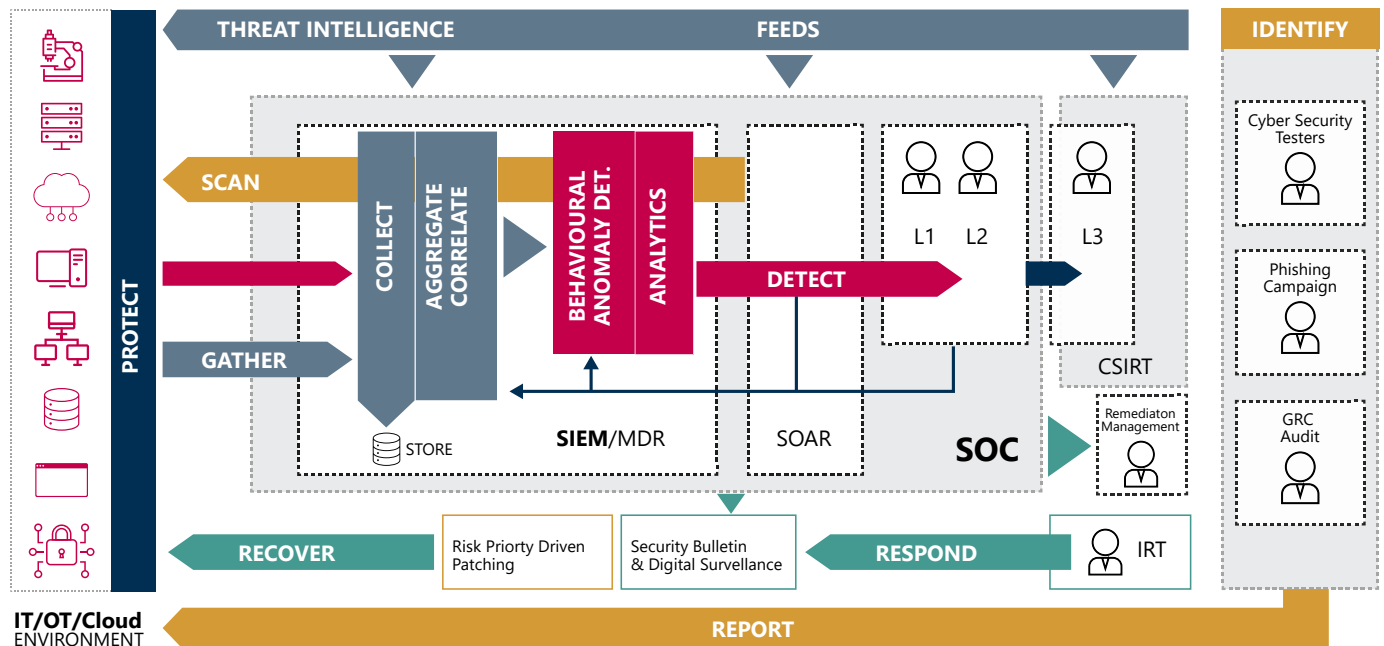
INTERNAL THREATS

- Stolen credentials and compromised accounts
- Misused credentials
- Constant checks to verify that no individuals within the company are stealing data and intellectual property, or abusing customer data
- Preventing users from engaging in activities that put themselves and the company at risk

RESPONDING TO INCIDENTS

- Understanding step by step what happened during a security incident
- Responding quickly and effectively to a security breach or data breach
- Maintaining compliance with security incident reports and regulatory requirements
- Understanding what threats your business is facing, as well as the effectiveness and cost of responding, to put in place actions to continually improve your ability to respond and react to security incidents.

Advanced SOC Framework



The diagram shows the architectural framework of our SOC and Incident Response (IR) services, which we are constantly renewing to keep pace with threats and emerging Tactics, Techniques and Procedures (TTPs) from adversaries.

In addition to the architecture as a whole, the framework includes the building blocks of a modular offering, which is useful for customers who want to increase or modernise the technological, process-related, and skills-based capabilities of their security operations.

In this sense, our SOC continues to enrich its services, especially in the modular offer of:

- **SIEM and next-generation XDR** (Extended Detection and Respond) platforms, based on Advanced Analytics and User Entity Behavioral Analytics (UEBA).
- **Threat Intelligence**, with a series of platforms useful for addressing emerging cybersecurity use cases.
- **Early warning**, both for the management of vulnerabilities, with specific tools for security patching prioritised on the basis of risk, and for early alerting on appropriately validated indicators of compromise that can be traced back to the organisation's exposed digital footprint.
- **Incident Response (IR)**, first of all through the L3 level of the SOC, and then through an emergency SWAT Team dedicated specifically to responding to security incidents. As already mentioned, IR activities are aimed at responding to the attack, mitigating the crisis situation and restoring the correct functioning of information systems. If necessary, they will also include digital forensic investigations and compromise checks for attacks that have already taken place.

And let's not forget the central role played in our SOC by SOAR, the platform for automating and orchestrating processes, which has enabled us to standardise and digitalise them at all levels, from alert analysis to incident response investigations, and which has allowed us to integrate and align these processes with SIEM.

In practice, the adoption of a SOAR platform has made it possible to:

- **reduce the response time to security** alerts once they have been validated by automating repetitive actions, such as opening and assigning tickets, verifying assets, and escalating alerts to the dedicated team. In this context, an example is suspected phishing e-mails sent to a dedicated mailbox: this is automatically scanned by SOAR, which in turn automatically extracts indicators of compromise (IoC), validates them by detonating suspicious digital attachments or artefacts in sandboxes, and then automatically enriches them through Threat Intelligence sources, before finally assigning the ticket to analysts for investigation.
- **improve the quality and uniformity of responses**, as this is managed by a unified and standardised flow. .
- **automatically prioritise the events to be analysed**, to focus on the most important ones first.

The architecture of the SOC also refers to the phases of the NIST Cybersecurity Framework, namely Identify-Protect-Detect-Respond-Recover. These five levels of the NIST framework give a precise idea of the progressive defence through the various stages that a typical attack chain must go through, and which a modern SOC must take into account.

Adherence to the NIST Framework emphasises how technologies, processes, and in general the technological and human components for combating cyber attacks must be aligned with and derived from sector standards, which represent a consolidated reference, offer complete coverage of use cases and control points in the various cybersecurity intervention categories, and are continuously updated. This is precisely the case with the NIST Cybersecurity Framework, as well as its declination in the mapping of adversary TTPs through the MITRE ATT&CK Framework.

In particular, the NIST framework reflected in the architecture of our SOC identifies a set of models and usage practices that we adopt for a structured and effective response to a cyber attack through balanced, synergistic and multi-level actions, involving not only technologies, but also people with their skills and processes.

Safeguarding data

For a company running a digital business, data is one of its most important assets. It is so fundamental that we recommend starting with it when developing a security programme to safeguard your 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 lead to vulnerabilities.

New privacy regulations are also creating increasingly stringent requirements on how to manage data, especially when it relates to individuals. Indeed, data protection is more about regulatory compliance, with tracking and reporting requirements, such as GDPR.

Protecting data therefore becomes a categorical imperative, as data is usually the main target of an attack.

Attention should initially be given to databases, i.e. structured data. But we must also consider unstructured data (documents, Office 365, file systems and shares, images, videos), which is often stored in the cloud. This data is common in organisations and often escapes control. Its existence and distribution across various devices, and its location on-site or in the cloud, is sometimes not even well known.

Technological and process-related solutions that address the issue of data protection can be found on a number of fronts, including:

Identificare il perimetro, attraverso una discovery automatica, e la conseguente classificazione dei dati sensibili o cruciali come Intellectual Property dell'organizzazione.

- **Identifying the perimeter**, through automatic discovery, and consequently classifying sensitive or crucial data as the organisation's Intellectual Property.
- **Attributing and governing** the levels of risk inherent in data (Data Risk Governance).
- **Monitoring and protecting** data access (Data Access Control).
- **Hardening of Repositories**, i.e. securing data containers through data masking encryption algorithms, with (above all) a centralised management of the cryptographic key lifecycle.
- **Adopting Public Key Infrastructure (PKI)** security architectures, applying digital signatures and certificates to protect the integrity and authenticity of critical data.
- **Applying Data Security Analytics algorithms** for early identification of anomalies in data access and processing.
- **Imposing policies** for secure data access and processing.
- **Data Loss Prevention (DLP)**, particularly on endpoints in application use on the machine, stored on disk, and in transit in and especially out of the endpoint.

4 OUR REFERENCE ARCHITECTURE FOR CYBERSECURITY

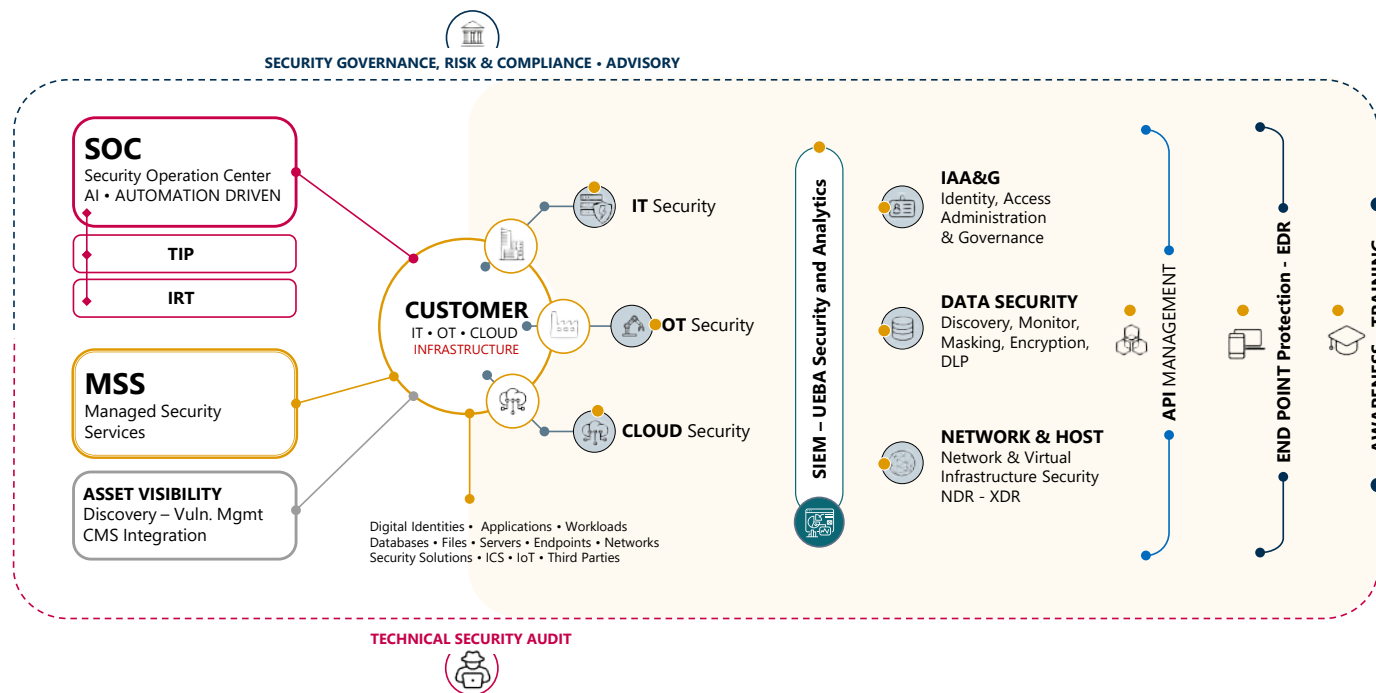


The challenges of the digital transformation call for a new approach to cybersecurity: one that is multi-dimensional, cross-sectoral, and capable of deploying technology-based skills that combine proven techniques for detecting threats (known or unknown) with advanced protection and effective response capabilities. Any approach to cybersecurity must therefore harmonise with the knowledge and processes already in place in the company, to ensure a defence that is fully aligned with other activities.

It is for this reason that **we have developed a reference architecture, through which we have positioned and developed - within a consistent technological framework - our skills and solutions in the various domains of cybersecurity and services (both those relating to implementation and support, and those that are managed through the SOC).**

This is a complete technological architecture, organised in a logical structure, to offer solutions within an integrated and transversal framework. We build and implement integrated, multi-layered cybersecurity solutions for our customers to support the secure delivery of new digital services, while protecting access to apps and data within the mobile world, the IoT, and the cloud-connected business. In this way we help organisations to:

- **improve** the ability to oversee, control, and block the growing surface of cyber threats, achieving an adaptive and contextualised security situation
- **understand** the flow of information and improve the ability to prevent, detect, and react to cyber threats
- **safeguard** their data to support the journey of digital transformation.



5 WHAT WILL THE FUTURE OF CYBERSECURITY LOOK LIKE?



There are six trends that will affect the way we approach cybersecurity. For each of them, Europe is taking important steps towards a concerted strategy to increase resilience to cyber attacks and based on the coordination of response and prevention processes.

1

The first trend directly concerns the information we rely on to act. Intelligence on cyber threats is now widely available, but not always usable. Its usability is hampered first of all by the acquisition of information from other continents, which causes a very risky delay in detecting threats that are spreading ever closer to us. A second obstacle is the huge amount of intelligence data available, which makes its management complex.

For this reason, the timely retrieval and selection of cyber-threat intelligence is a priority. A personalised and smart contextualisation of cyber-threat intelligence needs to be initiated to effectively use this information in all cybersecurity functions: prevention, detection, management, and recovery from attacks, and at various levels: technical and technological, organisational, and supply chain (third party). This contextualisation must be based on increased automation, AI capabilities and a detailed understanding of each organisation's processes and operations. The combination of digital tools with human intelligence is at the heart of future efficiency.





2

The second trend is that we live in a world where sensors and actuators, or so-called Cyber Physical Systems (CPS) are and will become more and more prevalent, with technology and data moving along our networks.

The increase in intelligence and connectivity of our physical world through the IoT, combined with the spread of the 5G network, creates increasingly fluid defence perimeters and introduces new cyber threats, whose impacts on civil society will be increasingly significant, as in the cases of attacks on critical infrastructures that we are already observing today. This will require the continuous updating of authentication methods and data validation, greater attention to IoT protection, and the use of real-time cryptographic transfers.

3

The third trend is greater centralisation through platforms where services offered to users converge with new models of more immersive interaction.

Thanks to voice commands, facial recognition, biometric authentication, and augmented reality, users are increasingly expecting greater fluidity and ease of access to platforms where business services and immersive interaction models converge. This will result in faster authentication modes that are completely secure, despite the absence of passwords.

4

The fourth trend is companies' increased awareness that their exposure to cybersecurity extends to both tangible and intangible assets, and that the economic impact of cyber threats must be quantified like any other risk.

In Europe (as has been the case in America for some time), IT insurance companies are becoming promoters and, in some cases, brokers of cybersecurity products and services.

5

The fifth trend concerns our economies. These are increasingly dependent on the cyber space and this has led to a greater awareness of the need to fully understand and trust the digital devices and processes on which we base our everyday business.

Companies need to reassure customers and citizens that they can handle their data with complete transparency and accountability. The spread of the 5G network, the installation of smart meters in the home, the increasing use of online voting systems, self-driving cars and public transport are just a few examples of how cybersecurity and privacy protection represent challenges that need to be addressed.



6

The sixth and last trend is the use of Artificial Intelligence (AI) and its increasing importance in accelerating decision-making processes and reactions to observed events.

The relationship between AI and cybersecurity is manifold. It is used to counter cyber threats with the help of the enormous processing precision that this new technology offers today. At the same time, AI is widely used by cyber criminals as a tool that facilitates their work: either by allowing the automation of certain phases of the attack (AI-powered cyber attacks), or by increasing the attack surface, especially due to the limited nature of the internal AI models, which are not yet able to handle forged inputs (misuse of AI and Adversarial AI) properly. For this reason, studying the most modern attack techniques and devising innovative countermeasures has become a trend of great importance at present.

In all trends, Europe has taken and is taking concrete steps towards a concerted strategy to increase resilience to cyber attacks, focusing on building greater capacities and coordinating response and prevention processes.

6 ENGINEERING AS AN ACTIVE PLAYER IN THE EUROPEAN CYBERSECURITY STRATEGY

Engineering has been a European player in cybersecurity since 2007. Within the European Organisation for Security (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 commitment to promoting an action plan at European level has 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.

In recent years, Engineering has focused its cybersecurity research activities in three directions: new approaches to train employees and public servants to detect malicious cyber attacks; integrated and continuous cyber risk assessment in IT and OT contexts, in particular on critical infrastructures; and the determination of investment priorities based on the economic impact of cyber threats and their increasing contextualisation.

Engineering Group also cooperates with the European Union Agency for Cybersecurity, ENISA. Of particular importance is the cooperation of ENISA members to create the European Cybersecurity Certificates, which will be valid throughout Europe for products, processes and services.



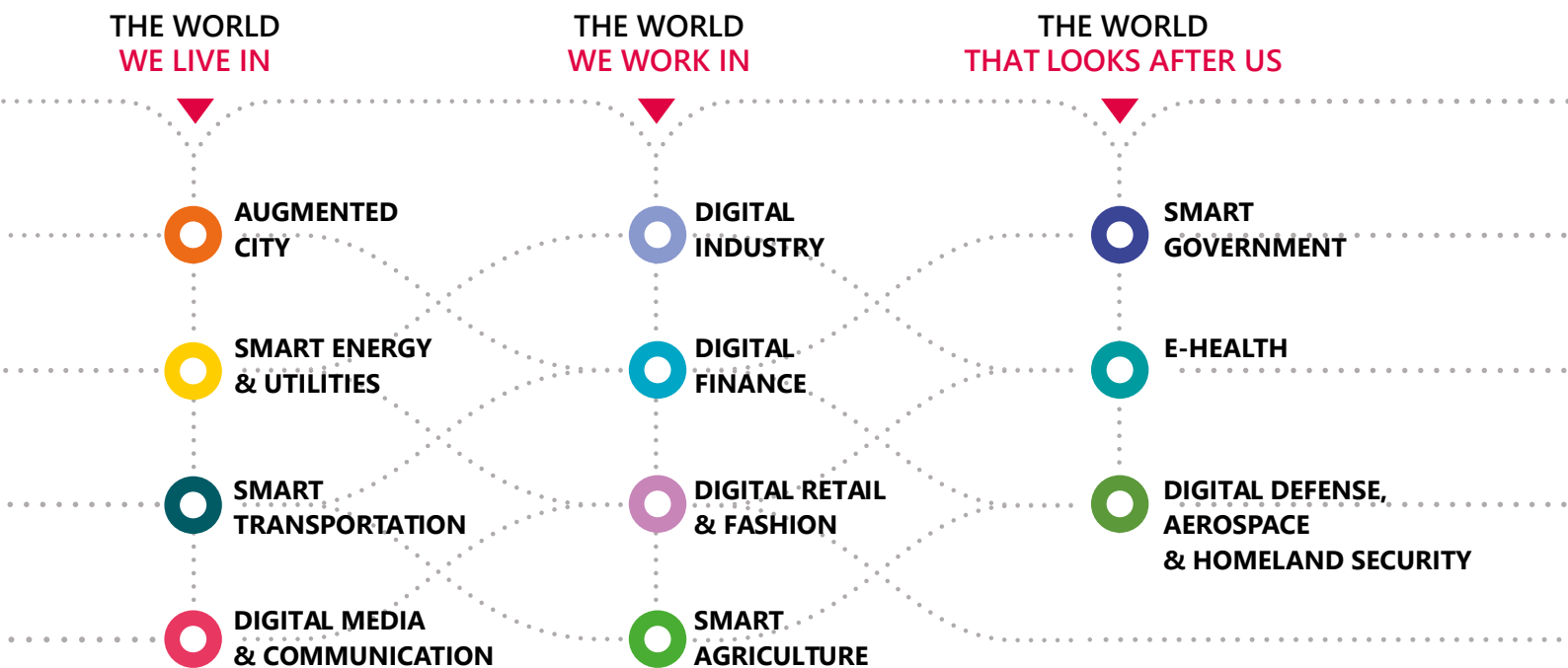
ENGINEERING

Engineering Group is the Digital Transformation Company, leader in Italy and expanding its global footprint, with around 12,000 associates and with over 40 offices.

The Engineering Group, consisting of over 20 companies in 12 countries, has been supporting the continuous evolution of companies and organizations for more than 40 years, thanks to a deep understanding of business processes in all market segments, fully leveraging the opportunities offered by advanced digital technologies and proprietary solutions.

It integrates best-of-breed market solutions, managed services, and continues to expand its expertise through M&As and partnerships with leading technology players. The Group strongly invests both in innovation, through its R&I division, and in human capital, with the internal IT & Management Academy. Engineering is a key player in the creation of digital ecosystems that bridge the gap between different markets, while developing composable solutions that ultimately foster a continuous Business transformation.

www.eng.it/en




CYBERSECURITY

Our point
of view on



DIGITAL TRANSFORMATION	ENGINEERING INNOVATION	ENGINEERING THE NEW NORMAL	WHERE BUSINESS MEETS TECHNOLOGY		
AUGMENTED CITY	DIGITAL DEFENCE, AEROSPACE & HOMELAND SECURITY	DIGITAL FINANCE		AUGMENTED MIXED AND VIRTUAL REALITY	BLOCKCHAIN
DIGITAL INDUSTRY	DIGITAL MEDIA & COMMUNICATION	DIGITAL RETAIL & FASHION		CLOUD	CYBERSECURITY
E-HEALTH	SMART ENERGY & UTILITIES	SMART AGRICULTURE		DIGITAL TWIN	IOT INTERNET OF THINGS
SMART GOVERNMENT	SMART TRANSPORTATION			ROBOTIC PROCESS AUTOMATION	AI & ADVANCED ANALYTICS
			Coming Soon		
DIGITAL WORKPLACE	DIGITAL WASTE	DIGITAL EXPERIENCE: CULTURE & TOURISM	SUPPLY CHAIN	DIGITAL AUTOMOTIVE	PROJECT MANAGEMENT

 www.eng.it

 [@EngineeringSpa](https://twitter.com/EngineeringSpa)

 [Engineering Ingegneria Informatica Spa](https://www.linkedin.com/company/engineering-ingegneria-informatica-spa)