PROSEGUR RESEARCH

Hybrid Security Series

The SOCs of the future: Towards intelligent **integration**

2023

PROSEGUR
SECURITY

PROSEGUR RESEARCH

The SOCs of the future:
Towards intelligent integration

This is an **interactive document**

HOME

HOME

01

Current context: Dynamism and opportunity

01 CURRENT CONTEXT: DYNAMISM AND OPPORTUNITY

Following a global pandemic, military conflicts, and a range of economic, political, and social crises, it has become evident **that the world we live in is marked by complexity, with disruptive changes and emerging hybrid threats** alongside traditional ones, resulting in unprecedented disruptions at all levels. In this context, the European Union Agency for Cybersecurity (ENISA) has highlighted **in its 2030 outlook** that hybrid threats may involve numerous potential actors and dangers, impacting organizations and ultimately society. Presently, any situation, regardless of time or location, has the potential to trigger cascading systemic effects on companies, industries, and even entire nations, with a considerable capacity for destabilization. **This dynamic environment presents new challenges and opportunities** for businesses, making the security sector no exception to global developments.

Confronted with this challenge, **relying on past approaches is no longer a viable option.** Mere adaptation for survival and waiting for the next wave of change is not enough. What is required is an innovative vision to create a future with the advances of society.

Whereas in the past, merely recognizing that something was happening allowed for reactive responses with agility and coordination to address environmental disruptions, today, a certain level of anticipation is required, such as an enhanced situational awareness. The present is only what separates the past and the future, and at this very moment, it is good to reflect, listen, and shift the focus to previously overlooked areas in order to evaluate new ways for evolution and improvement. In this context, botanist Stefano Mancuso emphasizes the remarkable sophistication with which plants perceive their surroundings with a sensitivity several orders of magnitude higher than that of animals. This extraordinary perceptual ability enables them to understand if something is changing in their environment well in advance. This is precisely what the security sector demands: **a transition from reactivity to proactivity, from coordination to integration, and from the past to the future.** Enhancing our ability to understand something as fundamental as our ecosystem needs a reevaluation of our operational methods, information sources, methodologies, and, most importantly, our vision of the future.

Only by understanding the evolving security requirements in a changing world can we anticipate threats and mitigate risks with a vision of sustainability. Taking on this important challenge entails a profound transformation, and within the security sector, **one of the most evolving elements in terms of security is undoubtedly the SOC.**

02

SOCs:
Revisiting the brain

HOME

01
Current context: Dynamism and opportunity

02
SOCs: Revisiting the brain

03
The iSOC: Leading the sector's transformation

04
Learning: The key in the age of change

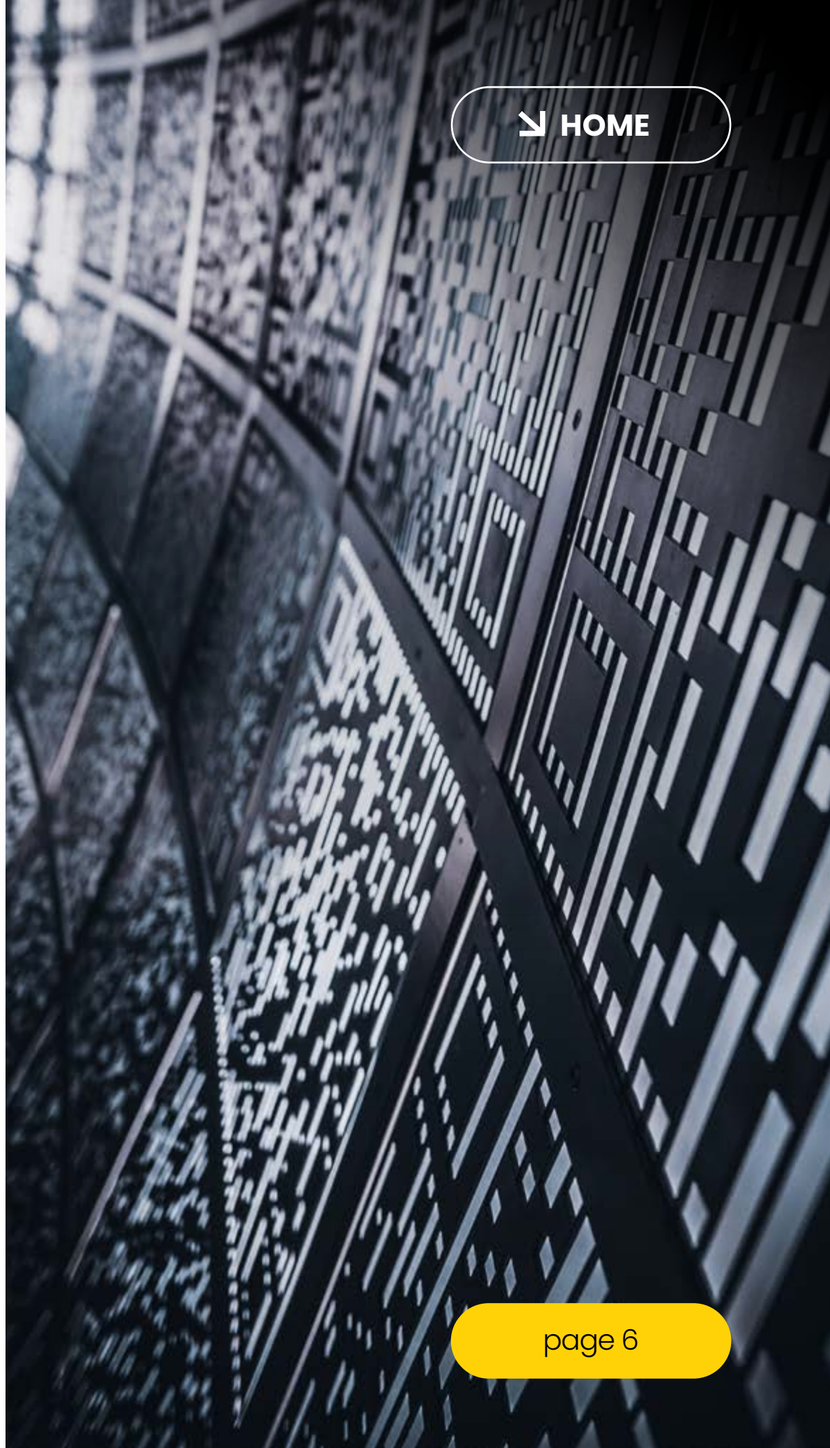
02

SOCS: REVISITING THE BRAIN

2.1.
Approaching the concept

The Security Operations Center, or SOC, is an infrastructure where a company centralizes its security functions to offer security services to other organizations, based on a **set of basic functions and processes that require precise advanced technology:** Firstly, it involves real-time data capture solutions for specific security incidents, which then flow to security teams with the aim of making critical decisions that provide the most appropriate response for each security situation and context. To achieve this, there must be **technological platforms within the SOC** that constantly receive and visualize the information. After an assessment of the situation by the workers present in the SOC, known as operators, a series of mitigation actions will be activated if deemed necessary, which are introduced into repeatable and measurable workflows, for the follow-up which incident management systems are required.

According to **ENISA,** Security Operations Centers (SOCs) should be distinguished from Computer Security Incident Response Teams (CSIRTs): while the SOC provides detection and incident response services through information monitoring, the CSIRT is responsible for all aspects related to cyber incidents, including vulnerability management and the protection of core services and operations, among others.



HOME

HOME

Due to the multitude of tasks, variables, and sources to monitor and business activities to oversee, there are **different types of SOCs** that adapt to the needs of each company and specific operational process.

It's important to note that not all organizations have SOCs to manage their operations and respond to critical incidents, as it's typically an outsourced business activity. In fact, according to some Gartner data, **by 2025, 90% of all SOCs will be at least partially managed externally** by specialized security providers, which falls under the category of security services known as **Security-as-a-Service (SaaS).**

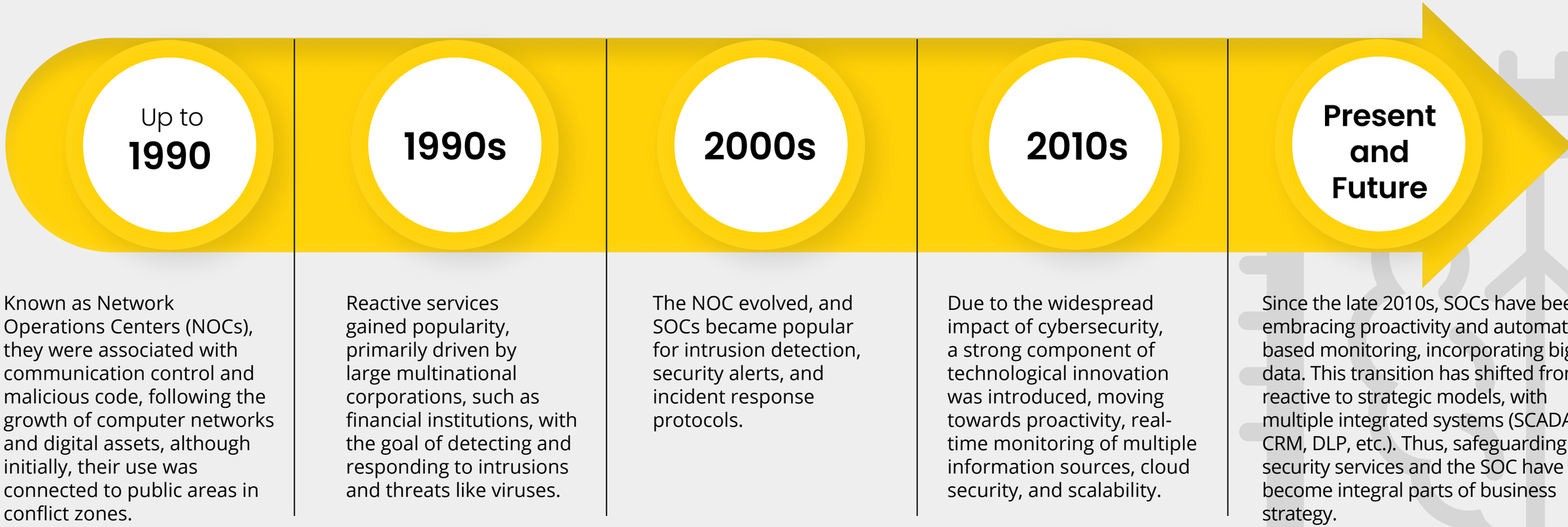
According to *Gartner's typology,* several main categories can be distinguished:

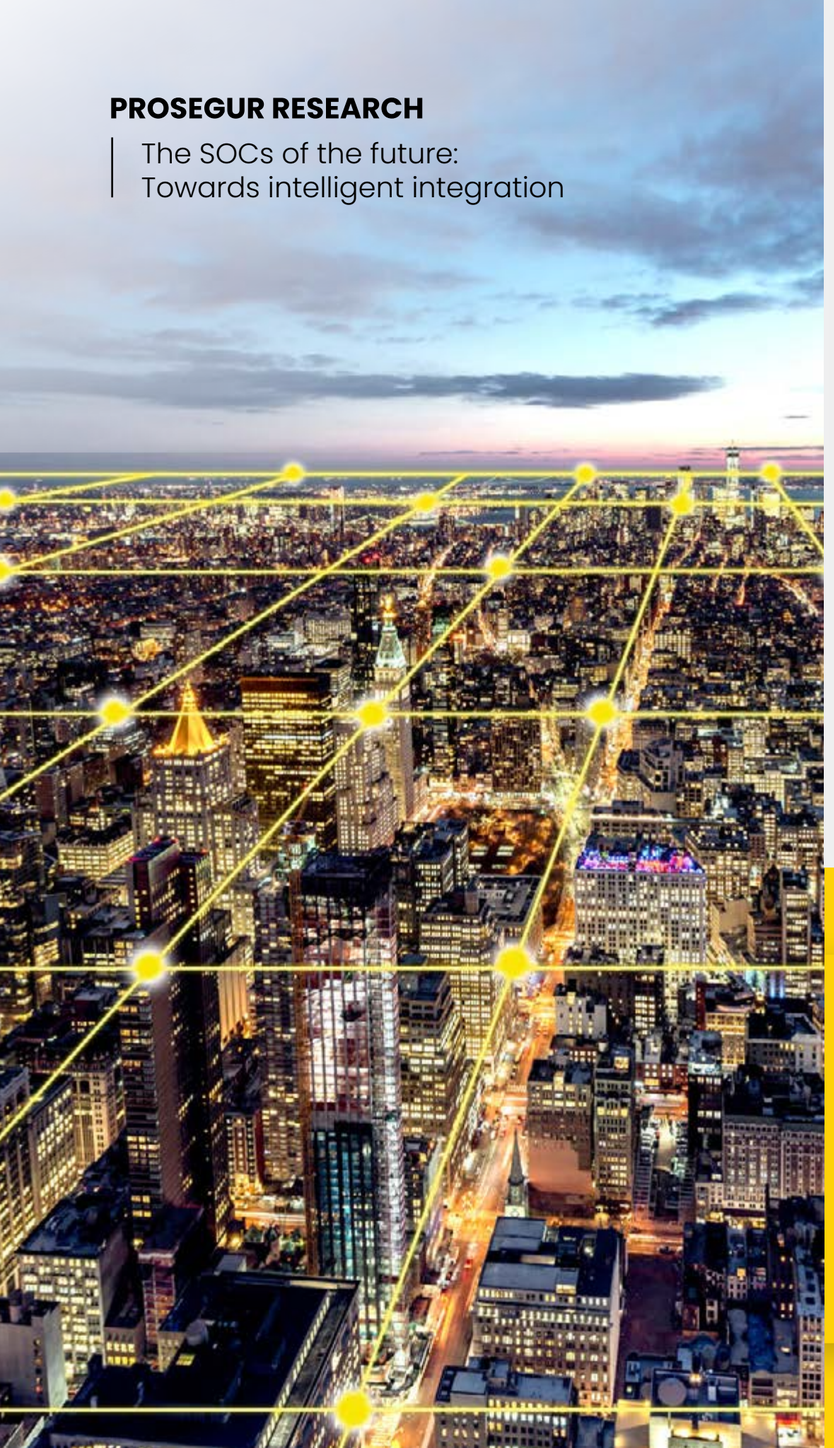
1. **Virtual SOC:** Without associated physical facilities, its component is purely reactive as an incident response.
2. **Dedicated SOC:** Specialized physical infrastructure is provided, with qualified teams to carry out the tasks.
3. **Distributed SOC:** Typically associated with Managed Security Service Providers (MSSPs), combining dedicated and semi-dedicated teams for a specific operation.
4. **Coordination SOC:** Its function is to coordinate other SOCs and teams, aiming to provide expertise on a specific task, not associated with routine operations.
5. **Multifunction SOC:** With the goal of reducing costs, it provides specialized infrastructure and teams for different tasks.

2.2.
Historical evolution

The SOCs, like the security sector, have adapted to changes in the environment and the operational and business continuity needs of organizations. Historically, SOCs have been linked to cybersecurity services, with the rise of operations in cyberspace and the cloud:

Figure 1
Background and historical evolution of the Security Operations Centers (SOCs)
Source: Prosegur Research, 2023





HOME

Thus, the evolution inevitably shifts from the detection of malicious code to the multi-level protection of all central and critical systems within an organization. The wide range of actors and potential threats makes it necessary to reflect on the risks that a company faces today and, accordingly, configure the business processes that require special protection and monitoring. This trend is reflected in the data on the global SOC market value, which, according to Allied Market Research, was over four billion dollars in 2021 and is expected to ***reach ten billion dollars by 2031.***

[1] According to ***DATAMINR.*** Key considerations when building a SOC.

2.3.
Traditional characteristics

Every SOC is based on three fundamental functions - preparation, monitoring, and response - to ensure its proper operation:

1. As part of the **preparation,** having a well-developed business continuity plan is essential, supported by easily actionable protocols and technologies in the event of unforeseen events that impact business operations.

2. Collecting and **monitoring** real-time data from various sources is crucial to trigger relevant alerts in case action is required, including systems, networks, and applications available to the organization, as well as other activities that require surveillance, such as identity and access management to ensure proper authorization for critical resources and/or restricted areas.

3. The presence of advanced protocols, team training, security systems, and the development of mass notification channels are necessary to provide an adequate **response** to a critical event to minimize its impact on the organization's operations[1].

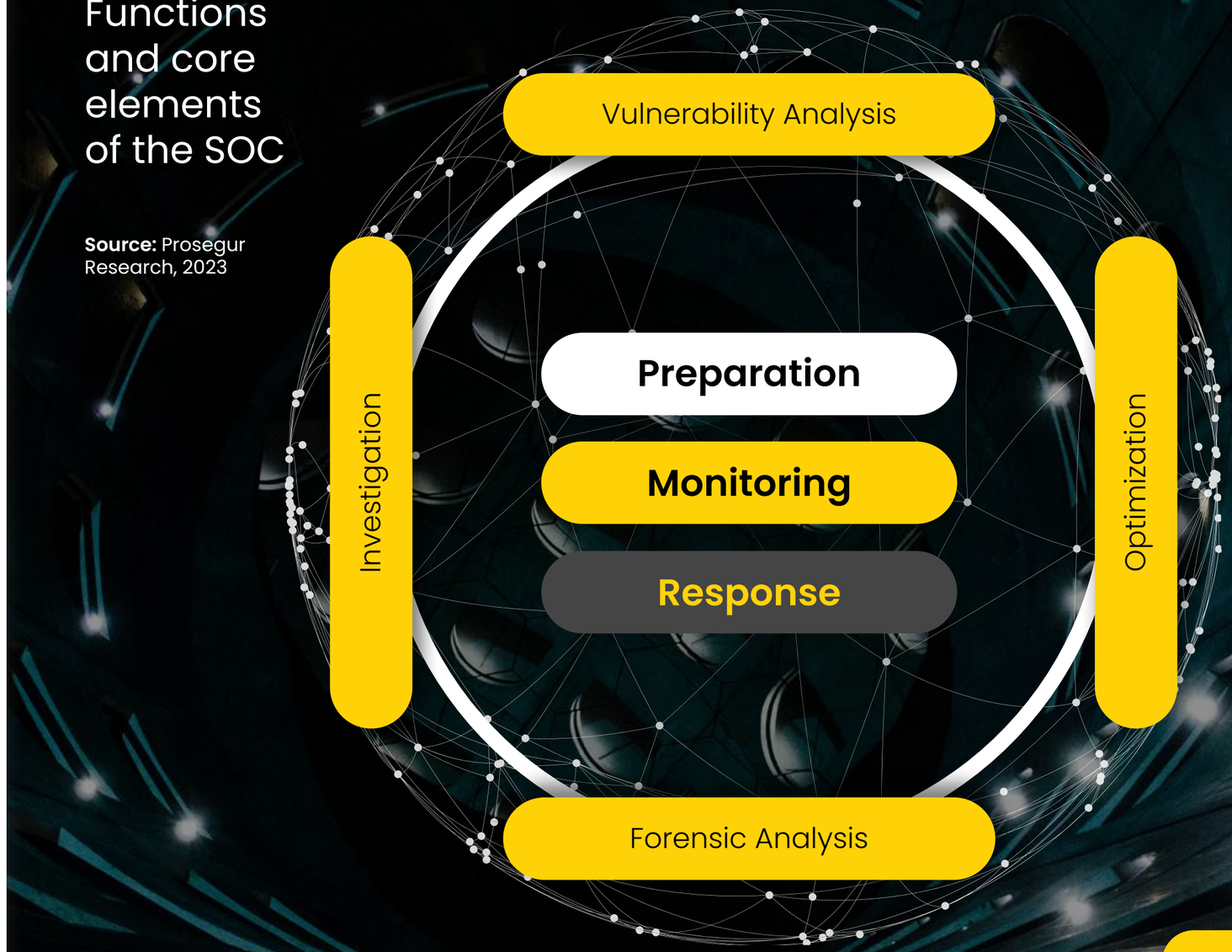
Simultaneously, **the SOC carries out a series of processes to ensure a smooth workflow.** This includes vulnerability analysis for all systems and operations to be protected, incident investigation, and forensic analysis, with the aim of gathering evidence and attempting to prevent future threats as well as an optimization and continuous improvement of all processes and procedures.

In this way, business process management and resilience can be enhanced through SOCs, thanks to real-time detection and monitoring, incident response management, risk and mitigation assessment, continuity planning, training, and awareness. As a result, SOCs hold **significant potential in the realm of business continuity,** which, in turn, is a crucial competitive advantage that strengthens brand reputation.

As a result, SOCs are positioned as a matter of particular interest for the outsourcing and subcontracting of security functions for many companies.

Figure 2
Functions and core elements of the SOC

Source: Prosegur Research, 2023



03

The iSOC: Leading the sector's transformation

HOME

01
Current context: Dynamism and opportunity

02
SOCs: Revisiting the brain

03
The iSOC: Leading the sector's transformation

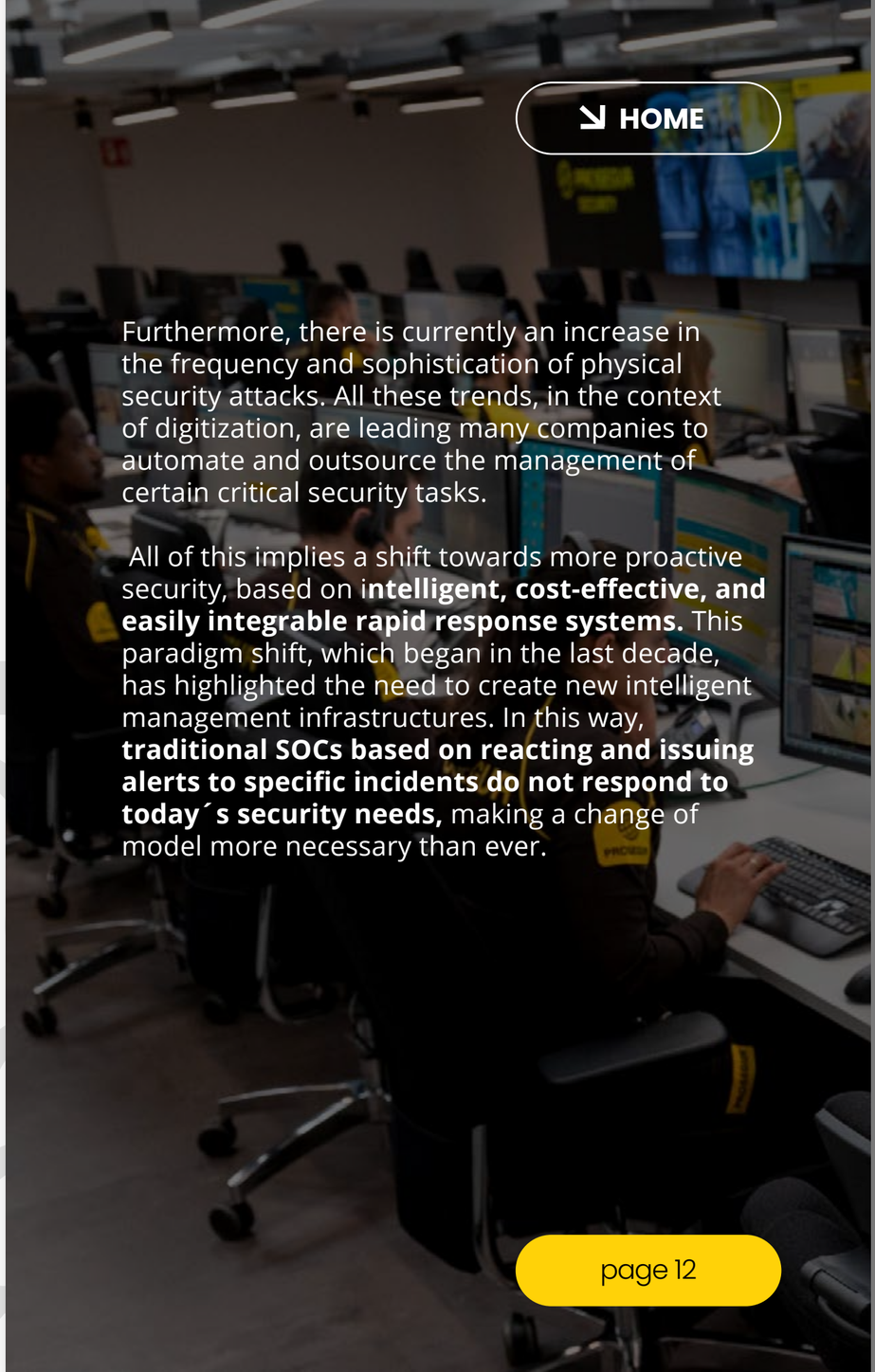
04
Learning: The key in the age of change

THE ISOC: LEADING THE SECTOR'S TRANSFORMATION

3.1.
The Future is already here: Why the traditional SOC is no longer enough

Over the past few decades, we have witnessed exponential growth in the use of technological developments. Consequently, **the world is becoming increasingly digitized, and so is the field of physical security.** This means that security operations increasingly rely on advanced technological solutions, a concept coined as **hybrid security** by Prosegur. All the changes in the business information ecosystem, with the rise of platforms, virtual systems, and cloud services, point towards action rather than reaction. It is no longer just about responding to incidents; it is about **creating proactive prevention-based management procedures.**

Moreover, **expanding security to all levels,** incorporating aspects like the protection of digital assets, corporate reputation, patrimony, legal uncertainties, and environmental effects, makes it necessary to review the protocols, systems, and services that can be offered by a SOC. Therefore, advanced technologies such as remote monitoring, the Internet of Things, interconnectivity, artificial intelligence, sensors, robots, drones, among others, are becoming more frequent in security scenarios.



HOME

Furthermore, there is currently an increase in the frequency and sophistication of physical security attacks. All these trends, in the context of digitization, are leading many companies to automate and outsource the management of certain critical security tasks.

All of this implies a shift towards more proactive security, based on **intelligent, cost-effective, and easily integrable rapid response systems.** This paradigm shift, which began in the last decade, has highlighted the need to create new intelligent management infrastructures. In this way, **traditional SOCs based on reacting and issuing alerts to specific incidents do not respond to today´s security needs,** making a change of model more necessary than ever.

3.2.
From the past SOC to the present and future iSOC

To ensure business continuity, it is necessary to identify and quantify critical business processes, analyzing various relevant measures for each, such as critical operation times, the likelihood of attack, operational impact (economic, legal, commercial, reputational), potential disruptions in each unit, or recovery time in case of disruption, among others.

All of this makes it necessary that SOCs have a distinguishing "i": information of great value, of an international nature and with the capacity to integrate and innovate from an intelligent perspective. In an iSOC, massive data is transformed into intelligence, allowing for risk anticipation and mitigation, as well as making internal and client decisions that enhance their production processes. It leverages the experience to enable high-level, human-like data processing, as advanced data analysis goes far beyond security:

A

It provides **insights for the protection of people and assets,** such as the development of new ways of organized crime, the new targets for theft, hotspots, or suspicious activities in perimeters, among many others.

B

It generates dashboards available to clients, enabling them to enhance their corporate management, such as monitoring workplace safety measures, environmental management, logistics system to prevent fraud or accidents, or public response to various sales strategies, to name just a few.

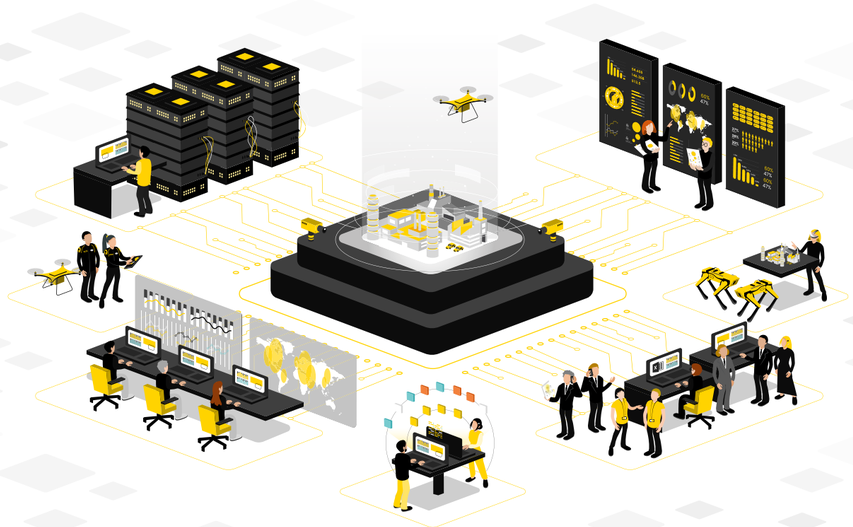
C

It covers the security needs adapted to the requirements of each sector, service, client, or affected individuals, **customizing solutions** without the loss of process automatization capacity and continuous improvement.

In summary, built on the foundation of ***hybrid security,*** i**SOC solutions are born from sophisticated operational strategies based on brain function.** Thus, the iSOC serves as the brain of the model, providing a very agile and realistic knowledge of what is happening in the world, and doing so in an anticipatory manner to boost response efficiency.

HOME

> “Unlike traditional SOCs, which operate in the present, iSOCs are future-oriented.”
>
> **Fernando Abós, CEO of Prosegur Security**



3.3.
What the iSOC brings

In recent years, the escalating threats of physical, cyber, and reputational security, among others, are impacting the business continuity of organizations, causing significant economic losses and damaging their corporate image. Despite Ontic's studies **revealing that 55% of executives are not aware of the physical security threats to their organization or their impact on business continuity,** companies are gradually beginning to view security not just as a cost center but as a valuable organizational asset.

On the other hand, the recent acceleration of technological innovation and connectivity means that it is easier and more cost-effective to hire or develop security services, not only for traditional functions but also for monitoring any organizational process on a large scale in day-to-day operations. Thus, it should be noted that while the design of security services from an iSOC depends on the goals and risk profile of each organization, it always **relies on real-time information to make informed decisions, data analytics, and threat analysis** in order to design appropriate mitigation actions, creating communication synergies and support among different teams and leveraging integrated technological systems.

Therefore, when securing business processes, it is important to adopt a **proactive risk management** approach that aims to create organizational resilience, integrating all relevant aspects within a comprehensive security policy against hybrid threats. However, there are challenging threats to manage, such as firearm attacks, the risk of executive kidnapping, or the combination of traditional threats with new technological components. This necessarily leads to the relevance of integrating new technologies into iSOCs and constantly improving all the processes and operations that comprises them.

If the iSOC is the nerve center of operations, integrating all its elements—people, technology, and data—in an appropriate and innovative manner, understanding the **strategic value of data** today, and staying up to date with the **latest technological innovations in the sector** becomes a critical matter.

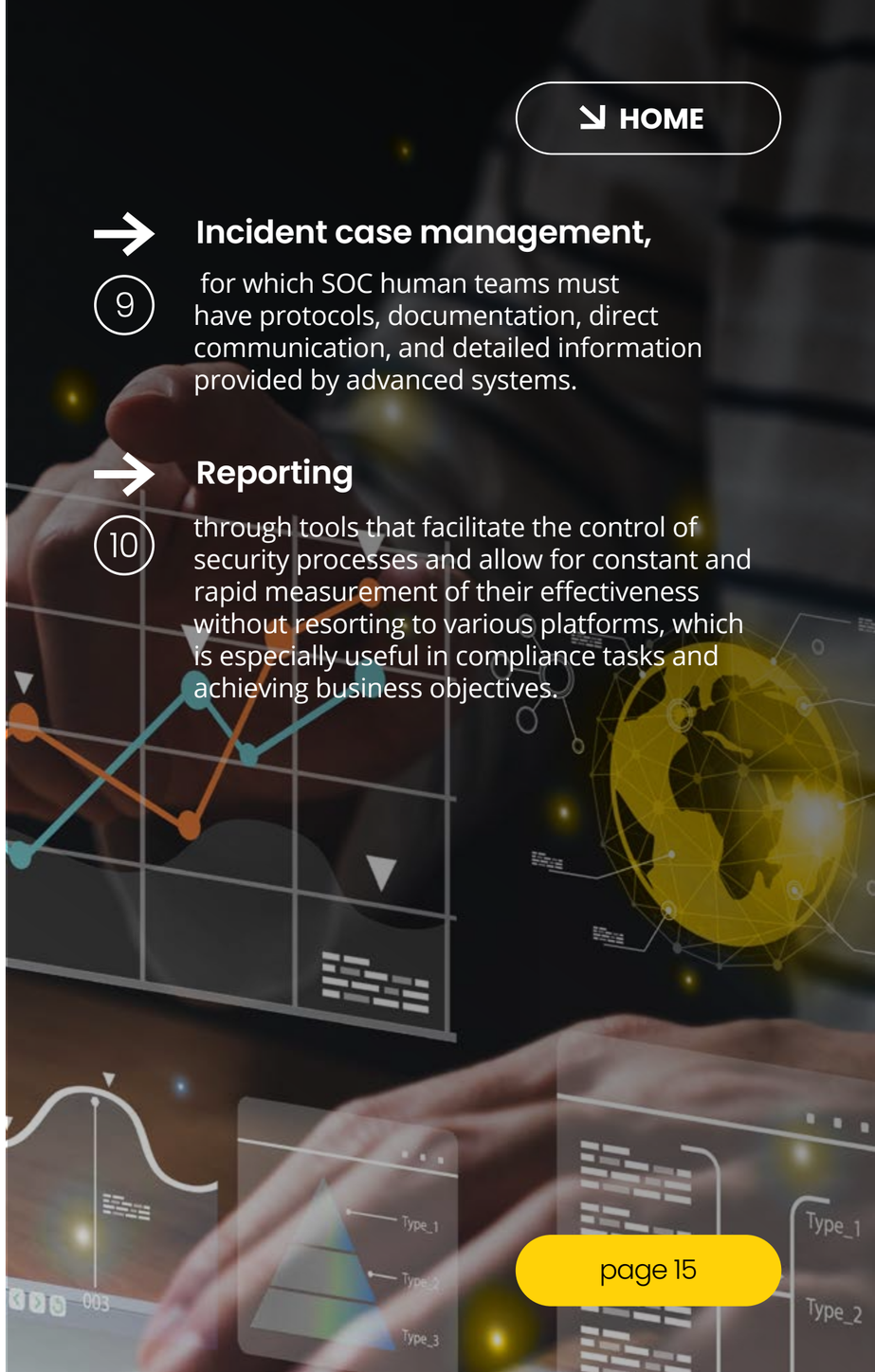
All of this underscores the value of the iSOC in its ability to anticipate threats, as it is designed to evolve constantly in response to a changing world and learn from its own experience. This involves leveraging the expertise of the professionals working there, constantly innovating in their technological tools, and strategically using both internal and external data to generate actionable intelligence for strategic decision-making, managing uncertainty, and anticipating security challenges.

The large volumes of data and their challenging management to obtain **actionable insights** for businesses today pose a significant challenge. To address this, the latest technological developments in security must be employed, and information must be strategically integrated to harness the value of data. This is why a SOC becomes a true iSOC when the level of **integration of all its elements** is maximized and aligns with a way of working and viewing security services as a tailor-made suit. The data transformed into knowledge by technology and human experience is thus the main asset: the entire team, from the top experts to the last security guard, is in constant contact with the information or iSOC technicians to define the appropriate response to any incident.

HOME

The iSOC must be prepared for both the present and the future, and therefore, it has to be revolutionary and transformative, preparing each element of the hybrid security model for change. Beyond the three traditional phases (preparation, monitoring, and response), **the integration of technological systems in the iSOC enables and empowers various security functions:**

1. **Ingestion of data from multiple sources on a large scale,** enabling experts to generate actionable insights, i.e., the ability to implement the results of the workflow.
2. **Rapid and accurate detection of security events,** typically through the use of analytics with machine learning.
3. **Anticipation of security events** with the aim of proactively directing human attention and facilitating the appropriate response process.
4. **Automation of routine tasks,** allowing the acceleration of key daily functions performed within the SOC, such as threat detection and containment.
5. **Organization of data** to connect all elements within the SOC and with external elements to strengthen preparedness for the constant evolution of threats.
6. **Recommendation of individual actions** or specific protocols tailored to each operator and client.
7. **Investigation and prioritization of incidents** to ensure a quick and effective response. Through the management of risk alerts, the "noise" from false or irrelevant alarms can be reduced, and data analytics can also automate the collection and grouping of incidents to facilitate the response.
8. **Comprehensive and coordinated real-time collaboration** and communication through data-based solutions that prioritize strategic information.
9. **Incident case management,** for which SOC human teams must have protocols, documentation, direct communication, and detailed information provided by advanced systems.
10. **Reporting** through tools that facilitate the control of security processes and allow for constant and rapid measurement of their effectiveness without resorting to various platforms, which is especially useful in compliance tasks and achieving business objectives.



HOME

HOME

3.4.
The three pillars of the iSOC: People, technologies, and data

As seen, the iSOC emerges as the true paradigm of intelligent security integration at all levels, incorporating real-time qualitative and quantitative information obtained from an extensive variety of sources, both internal and external: human (HUMINT), public (OSINT), and technological (TECHINT).

Thanks to this, the holistic view of operations provides contextual intelligence to the strategic perspective, and from a sophisticated strategy, the best operational and business continuity decisions can be made. This, in turn, also involves the integration of safety and security, as it allows addressing risks arising from both accidental events (accidents, natural disasters, or environmental damage) and intentional acts (such as theft, intrusions, vandalism, and assaults, among others).

As a result, the iSOC is framed as the brain of the hybrid security, enabling the interrelated elements: security experts empowered with innovative technologies that make strategic use of data, and moving from conceptual to real-world practice.

The hybrid security model is applied on a daily, day-to-day basis at iSOC through people, technologies and its clients' data, because protecting them is its raison d'être. This is why iSOC is the brain in which all valuable information and data is received, processed and analyzed in order to offer innovative and efficient security solutions.

For this reason, the transition from SOC to iSOC in the context of hybrid security is a transformation process. It is not just a question of what the iSOC will look like in the future, but rather to analyze the world from the point of view of the iSOC of the future, which anticipates risks and threats and allows us to respond today.

Our security model for a **hybrid world**

Source: Prosegur Research, 2023.

HOME

A People

The integration and adoption of new technologies across multiple industries are causing the required skills to change rapidly. This does not mean that technical skills have lost their value; rather, digital competencies and purely human skills are gaining special prominence. In this way, interacting with new technological developments, the ability to acquire new knowledge, and self-management or resilience have become fundamental skills **in a constantly evolving work environment,** such as the security sector and the innovations required by iSOCs. Thus, at Prosegur, we are convinced that **human competence is absolutely fundamental and irreplaceable to operate in this world.** Therefore, it is essential to empower workers' skills through the lever of change provided by technology.

Digital Competencies

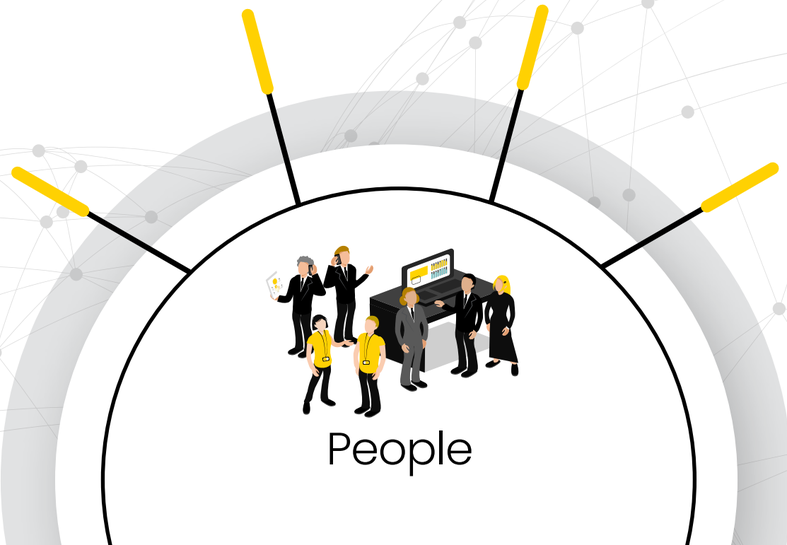
Linked to the handling of organizational technologies: artificial intelligence (AI), virtual reality (VR), blockchain, etc.

Human Competencies

Such as complex problem-solving, critical thinking, creativity, social influence, etc.

Security Experts

Professionals with extensive knowledge and international experience in risk management and security, particularly in challenging environments.



Self-Management

To work in a volatile and ever-changing environment: resilience, stress tolerance, and flexibility.

page 17

B Technology

Understanding that technological systems play a fundamental role in the current iSOC, it is crucial to design and implement an iSOC considering all its elements in detail, always from a perspective of **interoperability** and **interconnectivity.** To achieve this, the iSOC relies on technologies that are thoroughly tested and efficient, steering clear of typical technological hype:

Technologies Acting in the **Physical Environment:** These include cameras, sensors, drones, alarms, networks and systems, robotics, etc. These technologies operate in the physical environment, both to execute tasks and to send information.

Technologies Used for Information Processing and **Analysis and Decision Support:** These include artificial intelligence, machine learning, natural language processing, virtual simulators, GIS models, cloud computing, etc.

In-House Developments for Connecting **Physical and Digital Worlds:** Proproprietary developments such as Genzai, POPS, and Connect are used to interact with inputs from information sources and the end users of the product.

- **GENZAI** is a platform that manages video surveillance cameras as IoT (Internet of Things) devices, processing images and data with an advanced artificial intelligence algorithm. Thus, the iSOC has intelligent connected technology, which allows us to have an amplified understanding of the environment through GENZAI. The automation and autonomous protection that characterizes this tool allows us to anticipate and mitigate risks through the integration of all the technologies deployed in each service.

- **POPS** is the application with which each security guard registers the relevant information of the news and incidents that occur in the client's facilities, allowing a real-time record adapted to the client's requirements, which provides each professional with greater knowledge of the business needs of each company. Having expert professionals connected at all times thanks to POPS allows us to capture contextualized and categorized data for a more efficient and effective response. In addition, their skills and capabilities are enhanced by technology and information to make the best decisions when faced with all types of incidents.

- **CONNECT** is the platform that allows the client to visualize all kinds of data in real time about what is happening in their business. In addition, Prosegur Connect adapts to each client, customizing news, tasks and records according to their needs. Using information in a strategic way to anticipate and adapt possible events to adequately distribute resources brings extraordinary value to each client's business in a unique and exclusive way.

HOME

C Data

The strategic leveraging of data stems from the integration of all these sources worked on by the best security experts and the most innovative applied technologies. Within the iSOC, there are numerous integrated systems, many of which are individually accessible by each analyst or operator. They are typically connected to various corporate and security systems, receiving insights from real-time sources, accessing diverse internal and external communication networks, and utilizing numerous security tools and emergency support solutions.

Combining state-of-the-art technology and professional excellence for intelligent data processing is what enables us to manage on-site and remotely our customers' security services. The data are transformed into intelligence, which allows for risk anticipation and mitigation and a constant flow of feedback between operational and strategic that facilitates better decision making both internally and for our clients.

In summary, **the iSOC is the paradigm of integrating diverse sources, giving rise to the concept of hybrid security.** Thus, input data from guards, sensors, alarms, and cameras, to name just a few, are captured through numerous devices. They are then processed and presented (outputs) through our unique platforms (POPS, Genzai, and Connect) in the form of dashboards, mitigation actions, reports, alerts, or recommendations, enhancing competitive intelligence, products, and services.

HOME

In focus:
The professional in the new security paradigm

One of the paradigms of efficiently integrating human and technological sources revolves around the so-called security expert. Currently, guards carry out a multitude of tasks in various establishments or premises where they perform their professional duties:

- Static and dynamic surveillance.
- Protection of individuals.
- Search for missing persons, such as minors.
- Access management and identity checks.
- Response to incidents such as assaults, aggressions, or vandalism.
- Transportation and protection of valuables.
- Emission and reception of alerts in alarm centers.
- Collaboration and support for law enforcement agencies.
- Assistance in case of falls, health disturbances, or evacuations.
- Detection of prohibited substances or objects.

All these functions are fundamental to carry out true situational awareness, that is, **contextual intelligence** that provides the organization with the opportunity to map the main risks surrounding a facility, geographic point, or industrial sector.

For this purpose, the guard is continuously connected to the iSOC through different devices, such as direct communication tools for issuing alerts and incident reports as they occur.

Additionally, employees are trained and empowered technologically to perform all tasks with the support of cutting-edge and efficient technology.

Therefore, as illustrated in the infographic below, **the guard, as an expert in hybrid security, proactively manages complexity** with the help of powerful technological tools, adapting to various and ever-changing geographical contexts.

HOME

1 MISSIONS

- PATROL THE INSTALLATION
- RESPOND TO AN ASSAULT
- TRANSPORT EXPLOSIVE MATERIALS
- ASSIST IN FIRE EVACUATION
- RESPOND TO NATURAL DISASTERS
- COLLABORATE IN THE SEARCH FOR MISSING PERSONS
- DETECT UNAUTHORIZED SUBSTANCES
- OTHER MISSIONS

2 TECHNOLOGIES

- SMARTPHONES
- SENSORS
- CAMERAS
- GEOLOCATORS
- ROBOTS
- DRONES
- TOTEMS
- OTHER TOOLS

SECURITY EXPERT

START

3 VEHICLE

- CAR
- OFF-ROAD VEHICLE
- MOTORCYCLE
- ARMORED
- TRUCK
- HELICOPTER
- AIRPLANE
- OTHER VEHICLES

4 SCENARIO

- SHOPPING CENTER
- STADIUM
- FESTIVAL
- AIRPORT
- HOSPITAL
- RESIDENTIAL COMPLEX
- JUNGLE
- OTHER SCENARIOS

5 LOCATION

SELECT FROM +30 COUNTRIES ▼ BRAZIL

04

Learning:
The key in the age of change

HOME

04 LEARNING: THE KEY IN THE AGE OF CHANGE

As in the iSOC, diversity and dynamism must be part of the entire company framework, harmonized with the evolution of society and the environment in which it operates. This integrated and intelligent vision in the world allows for a new era of fostering **honesty, networking, and talent:** a leap into authenticity, responding from its raison d'être. What defines an organization is not its level of technological innovation, its size in employees and revenue, or its modern offices; it is its purpose: being able to identify more with where it is going than with where it comes from.

As **Mariana Mazzucato** says, the biggest problem currently is inertia; from Prosegur Research, we are convinced that the challenging future ahead, full of changes and uncertainties, can only be faced with a true **systemic learning character,** following **Donella Meadows'** interesting approach to cultivate positive results. Translating this into the business sphere is not easy; in the words of **Enrique Dans,** "some companies are crazy to keep doing what they were doing and they will crash; others assume that it is a learning process and that talent will go where they are given freedom," and we can add, that freedom will arise from transparency, flexibility, and diversity emanating from corporate culture.

Transparency in organizations to break the addiction of going on autopilot; asking and being accountable to share progress and potential improvements, resisting the temptation to seek certainties, asuming the current times of uncertainty.

Flexibility to go beyond the role, overcome the constraints of guidelines, and incorporate small changes systematically and large changes when they are disruptive; reserve spaces to think and times to act.

Diversity in teams but also to abandon ideological monogamy, expose ourselves to other approaches, and practice promiscuity in learning; we must be able to relate apparently unrelated disciplines and have the courage to analyze our own capabilities, to see what we lack and incorporate it naturally.

The real challenge for organizations will be to absorb all this learning firsthand and transform it into something useful for the entire structure, generating conducive environments for chains of change transmission; what ***Xavier Marcet*** calls "a powerful learning ecosystem." Therefore, the paradigm of intelligent integration is something that surpasses the concept of iSOC, only those companies that understand its importance and embrace **innovation as a mindset of change based on learning will be part of the future.**

Books that have inspired us

- Mission economy
- Designing and Builing Security Operations Center
- AI 2041: Ten Visions for Our Future
- Thinking in Systems
- Link: How Decision Intelligence Connects Data, Actions, and Outcomes for a Better World
- The coming wave
- Everything is going to change: technology and evolution: adapt or perish
- The future of national intelligence
- Next Gen Securlty Operations Center: From Concept to Reality
- Humanistic management
- How to research trends
- Modern Security Operations Center

PROSEGUR
SECURITY

We ensure the safety of individuals, businesses, and the whole society

research@prosegur.com

PROSEGUR **RESEARCH**

www.prosegurresearch.com