

Digital Frontier Guardians

Cyber Resilience in Critical Infrastructures



*A must-read report on cyber security
and resilience in critical environments.*

Summary

A must-read report on cyber security and resilience in critical environments.

This report represents a comprehensive analysis of global cyber challenges in a context of profound geopolitical change, grounded in the history of cyber threats to critical infrastructure, to unravel the formula for strengthening cyber resilience and optimizing cyber defense strategies in critical environments.

It explores security in operational (OT) environments, healthcare, national defense infrastructures, and the protection of 5G and IoT networks by examining real-world use cases. This report provides valuable insights and strategies for safeguarding vital ecosystems, putting the state of cyber security in these high-criticality environments in context and in an understandable way.



INDEX

1. CYBER RESILIENCE FOR CRITICAL INFRASTRUCTURE	4
1.1 Our mission	5
1.2 Dunning-Kruger effect	5
1.3 The sovereign state of the 21st century	6
1.4 The fifth domain: strategic importance	7
1.5 The 21st century sovereign organization	8
2. CRITICAL INFRASTRUCTURES AND THEIR IMPORTANCE	9
2.1 Operators of cyber-sovereign infrastructures	9
2.2 The importance of cyber security in critical infrastructures	11
2.3 Cyber security in critical infrastructures: particularities	14
3. CYBERATTACKS ON INDUSTRIAL OT SYSTEMS: THE TRITON CASE	15
3.1 Global cyber threats to critical infrastructures	17
3.2 Threats from nation-states: limitation of cyber insurance	19
4. CYBER RESILIENCE FORMULA FOR CRITICAL INFRASTRUCTURES	20
4.1 Understanding the organization's cyber security posture	21
4.2 Defending the infrastructure: creating 360° protection around assets	22
4.3 The importance of detection and response for critical infrastructures	24
4.4 Managing the OT security operational center	25
5. CONCLUSION	27

1. Cyber resilience for critical infrastructure

Telefónica Tech's mission as Digital Frontier Guardians is essential.

Contemporary societies heavily depend on critical infrastructures for their day-to-day functioning, and it is our duty to ensure that **these infrastructures are safeguarded in a constantly evolving digital environment.**

Digitalization is advancing at a vertiginous pace, in many cases outpacing the ability to ensure the security of the essential assets and systems that support these critical infrastructures. Cyber security strategies traditionally focused on IT information technologies are not enough to protect cyber-physical systems.

Cyber-physical systems integrate information technologies (IT) and operational technologies (OT) to enable communication and interaction between physical elements and the digital environment. They are used in a wide range of applications, from factories to medical devices, connected cars, military vehicles, and defense systems, among others. In this context, **cyber threats lurk in our critical assets.**

It is essential to understand that while cyber security is already fundamental to the specifications of 5G networks, we must go beyond the native security features of these networks to ensure **comprehensive, end-to-end protection.** In this report, we will explore in detail the challenges and solutions that must be addressed to strengthen critical infrastructure security in the digital age, thus reinforcing our position as Guardians of the Digital Frontier.



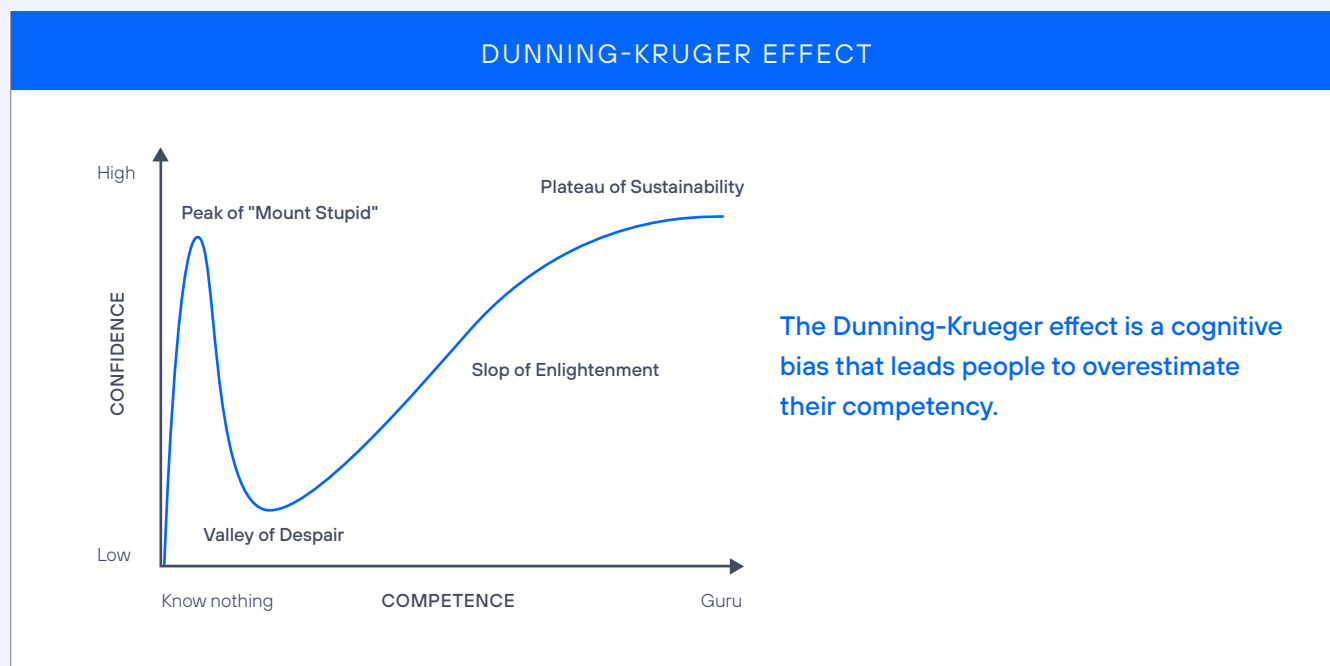
1.1 Our mission

What is our mission as the guardians of this digital frontier where our physical world is going digital?

Our mission is to enable the adoption of digital technologies by people, in processes and on our customers' infrastructures while ensuring their resilience.

1.2 The Dunning-Kruger effect

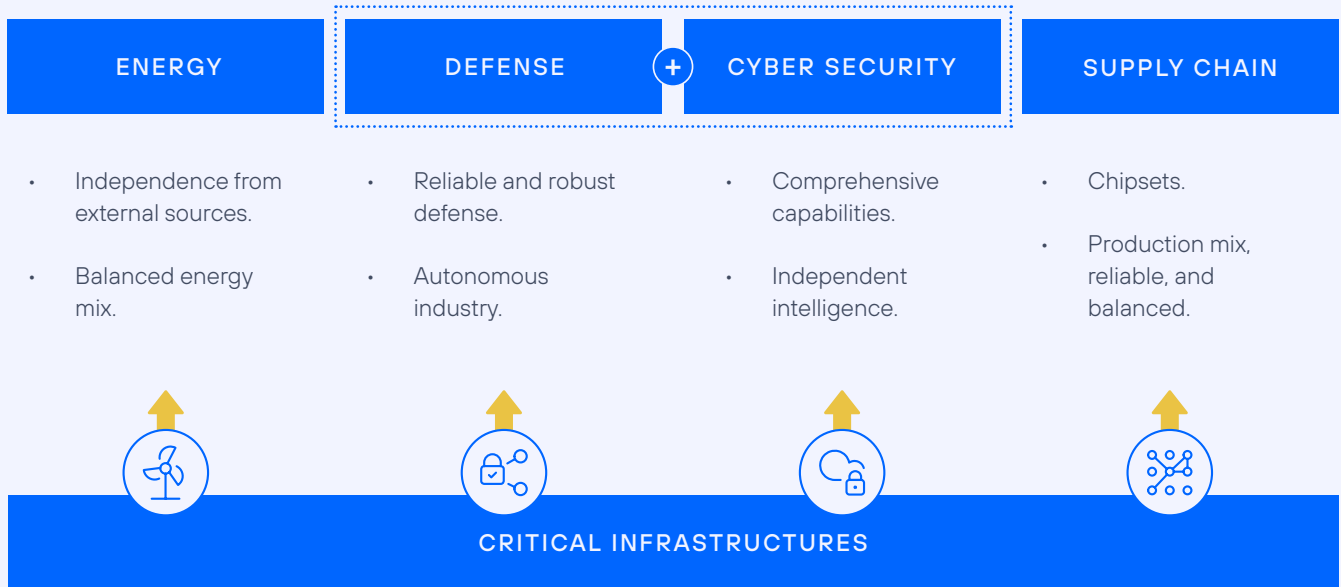
Could it be that, Western nations generally perceived as technologically advanced powers, are inadvertently falling prey to the **Dunning-Kruger effect**? Have we underestimated the capabilities and intentions of our adversaries thus unleashing unprecedented cyber threats and geopolitical turmoil?



If we examine the extent of our naivety in relation to the geopolitical landscape and our cyber adversaries, we discover shocking realities and highlight the consequences of this naivety on critical infrastructures.

1.3 The sovereign state of the 21st century

Do you operate in a sovereign country? Is your organization resilient? Is your infrastructure resilient?



The sovereignty of Western countries is currently challenged on multiple fronts, particularly in the context of the geopolitical tensions they face. This struggle to maintain full sovereignty extends to a number of crucial aspects, among which are:

1. ENERGY SOVEREIGNTY:

Ensuring energy independence is a fundamental pillar of a country's sovereignty. Dependence on foreign energy sources can jeopardize a state's autonomy and security, as well as its ability to respond in times of crisis.

2. DEFENSE CAPABILITY:

A country's defense capability is essential for it to preserve its sovereignty. Investment in and development of capable and modern armed forces are vital for deterrence and protection against potential external threats.

3. CYBER SECURITY CAPABILITIES:

This is a crucial component of a state's sovereignty. Cyber threats can undermine critical infrastructure, defense systems and the privacy of citizens, highlighting the importance of having a robust and effective cyber security strategy.

4. SECURITY OF THE CHIPSET VALUE CHAIN:

Reliance on critical components from foreign suppliers can put security and technological sovereignty at risk.

However, beyond these individual aspects, the key question that arises is the following:

Are our countries capable of protecting their key national infrastructures against global cyber threats?

The reliability of these infrastructures is a crucial element in the protection of a state's sovereignty, as their vulnerability could expose a country to both internal and external threats.

The sovereignty of a state in a world increasingly dependent on advanced technologies depends not only on its ability to withstand traditional threats, but also on its ability to protect its digital assets and ensure the continuity of its critical infrastructures.

It is essential to address these challenges with focus and determination in order to maintain full sovereignty in the modern era. Investment in energy sovereignty, defense, cyber security, and the security of the technological value chain is essential to ensure a state's autonomy and security in today's world.



1.4 The fifth domain: strategic importance

The 'fifth domain' concept refers to cyber security as a new domain of protection and defense in the context of a sovereign state. Traditionally, the four domains of protection and defense have been land, sea, air, and space. However, with the exponential growth of cyber threats, there is growing recognition of the importance of considering cyber security as a fifth domain.

In this fifth domain, cyberspace, sovereign states must develop capabilities and strategies to protect their

critical infrastructures, safeguard the integrity of their information systems, and counter cyber threats that could affect their national security.

This involves implementing policies and regulations, collaborating with the private sector, investing in advanced technologies, and training specialized cyber security professionals. The fifth domain has become an essential component in the protection and defense of a sovereign state in the digital age.

1.5 The 21st century sovereign organization

An organization's ability to protect its key infrastructures against cyber intrusions becomes essential in an increasingly challenging digital environment. In this context, several questions arise:

- **Is your organization able to protect its key infrastructure against cyber intrusions?**
- **Do you have a sovereign cyber infrastructure??**
- **What are we talking about when we talk about being a sovereign cyber infrastructure operator?**

It is important in order to better understand this notion to know the different types of critical infrastructures, their importance and to delve deeper into what it means to be a sovereign cyber infrastructure operator.



2. Critical infrastructures and their importance

Critical infrastructures are the invisible pillars on which the functioning of entire nations is supported, providing essential services. Their importance lies in their ability to support society's economy, security, and quality of life.

Critical infrastructures cover a variety of areas, among which we highlight:

- **Operational Technologies (OT)**
- **Health infrastructures**
- **Security and defense systems**
- **Telecommunications networks and 5G**

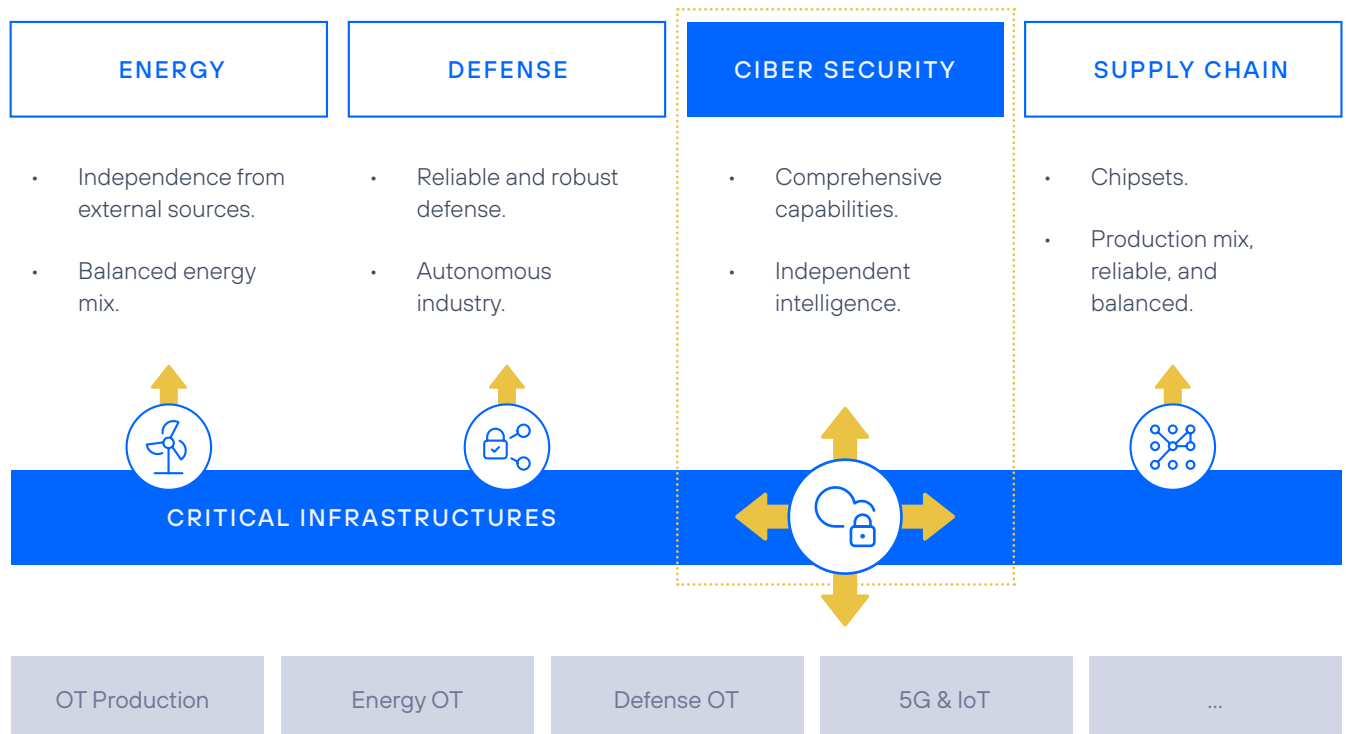


2.1 Operators of cyber-sovereign infrastructures

The concept of a cyber health infrastructure operator addresses an organization's ability to maintain sovereignty over its digital operations and safeguard its critical infrastructures from cyber threats.

This involves:

- Having **full control over its digital assets**, without dependence on foreign vendors or external vulnerabilities.
- Having robust **cyber resilience** measures in place to effectively respond to and recover from cyber threats.
- Ensuring the **integrity and confidentiality of critical data** and sensitive information.
- Ability to **detect and respond quickly to cyber intrusions**, minimizing the impact on their operations.



2.2 The importance of cyber security in critical infrastructures

In sectors where interaction with the end customer is less important, such as industry, mining, agriculture or energy companies, **digitalization has progressed more slowly**, allowing them to maintain a certain distance from the digital transformation.

This lower degree of technological adoption has been closely related to the cyber security needs experienced by these organizations. However, in recent years, several developments have acted as catalysts to accelerate digital transformation in the operational areas of these economic sectors. The objective behind this acceleration is to **automate processes, improve efficiency and agility, and adapt to changes in society's habits and needs**.

This process of accelerating transformation has been accompanied by an increase in the number of cyber security incidents suffered by these industrial sectors.

In this sense, *Figure 1* illustrates this fact by showing the **increase in positions in the ranking of most attacked sectors over the last 5 years**. It can be clearly seen that the **manufacturing sector and the industrial sector have climbed positions**, coming to lead the ranking since 2021, ahead even of the financial and insurance sector, which has traditionally been the leader in cybersecurity investment.

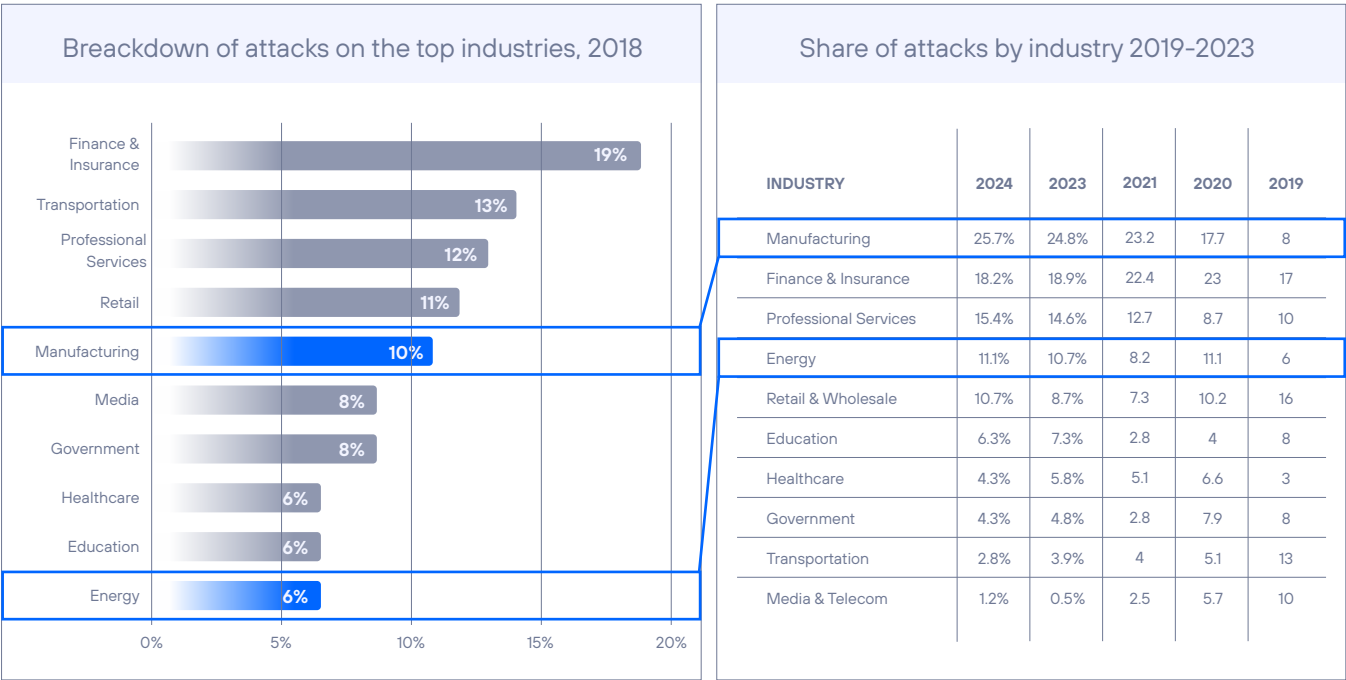


Figure 1. Evolution of the percentage of attacks by sector. Source: X-Force Threat Intelligence.

The healthcare sector also deserves a special mention. Although its position in the above ranking has not changed in recent years, **the sector leads the ranking of industries with the highest cost per incident.**

The **nature of the data it handles undoubtedly makes it particularly sensitive**, an issue that becomes more apparent as its attack surface grows unstoppably due to the digitization of care channels and, especially, to the growing number of connected electromedical devices.

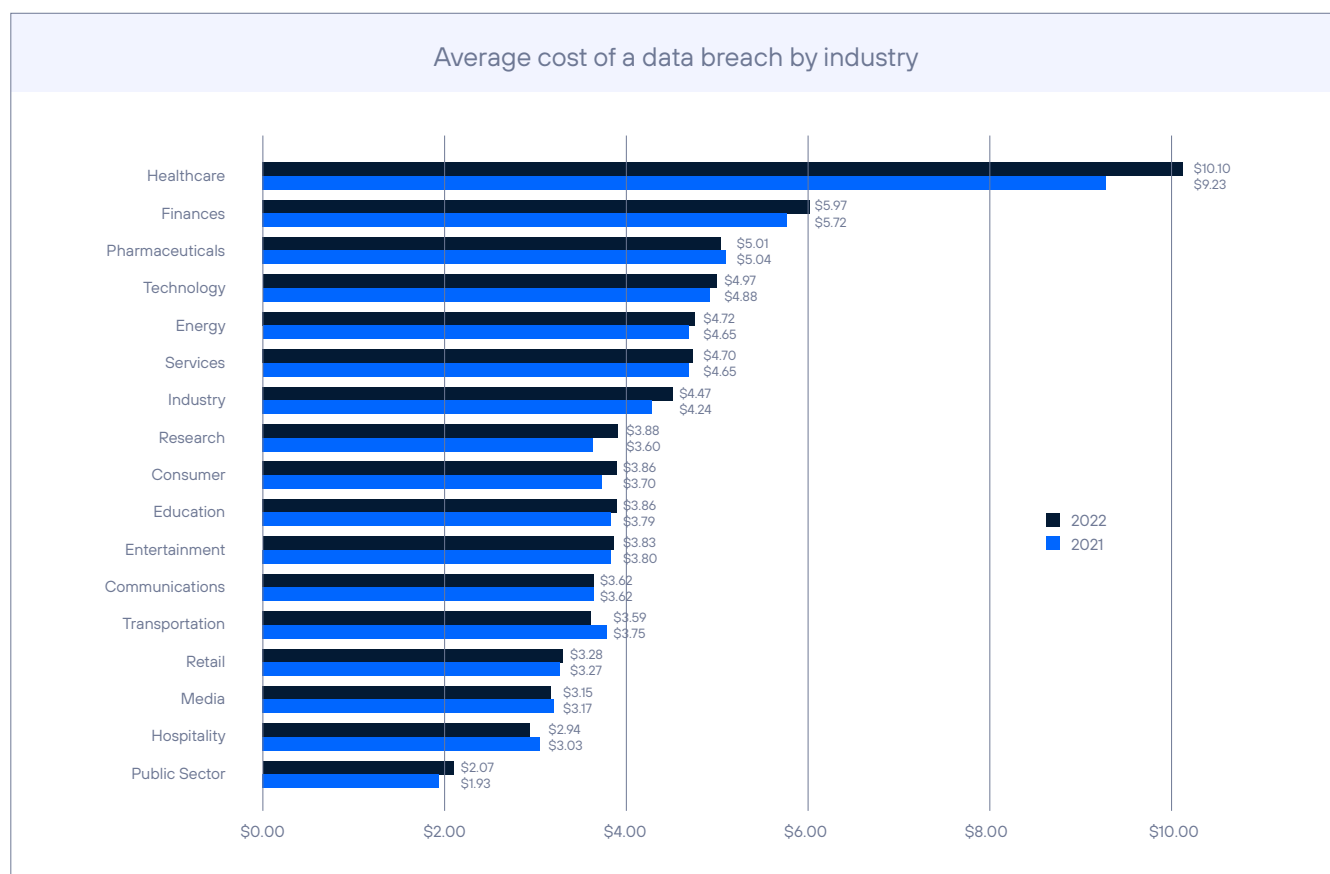


Figure 2. Average cost of incidents by industry. Source: IBM 2022 Report.

Defence is a third sector on the rise as a result of recent geopolitical conflicts. Cyber security has always been an area of interest for the military sector, but for some years now it has been considered a combat domain in its own right, alongside the four traditional ones (land, sea, air and space), and is now considered the 'fifth domain' mentioned above.

When analyzing new-generation weaponry, vehicle and spacecraft from a more technical perspective, the importance of cyber security can be better understood,

as these are connected devices that in many cases can be operated remotely and are therefore **exposed to vulnerabilities that could facilitate the enemy's takeover.**

It is therefore not surprising that this market is expected to grow by 10% over the next few years. The market is also a market in which preference is given to national suppliers and those from allied countries for geopolitical reasons.

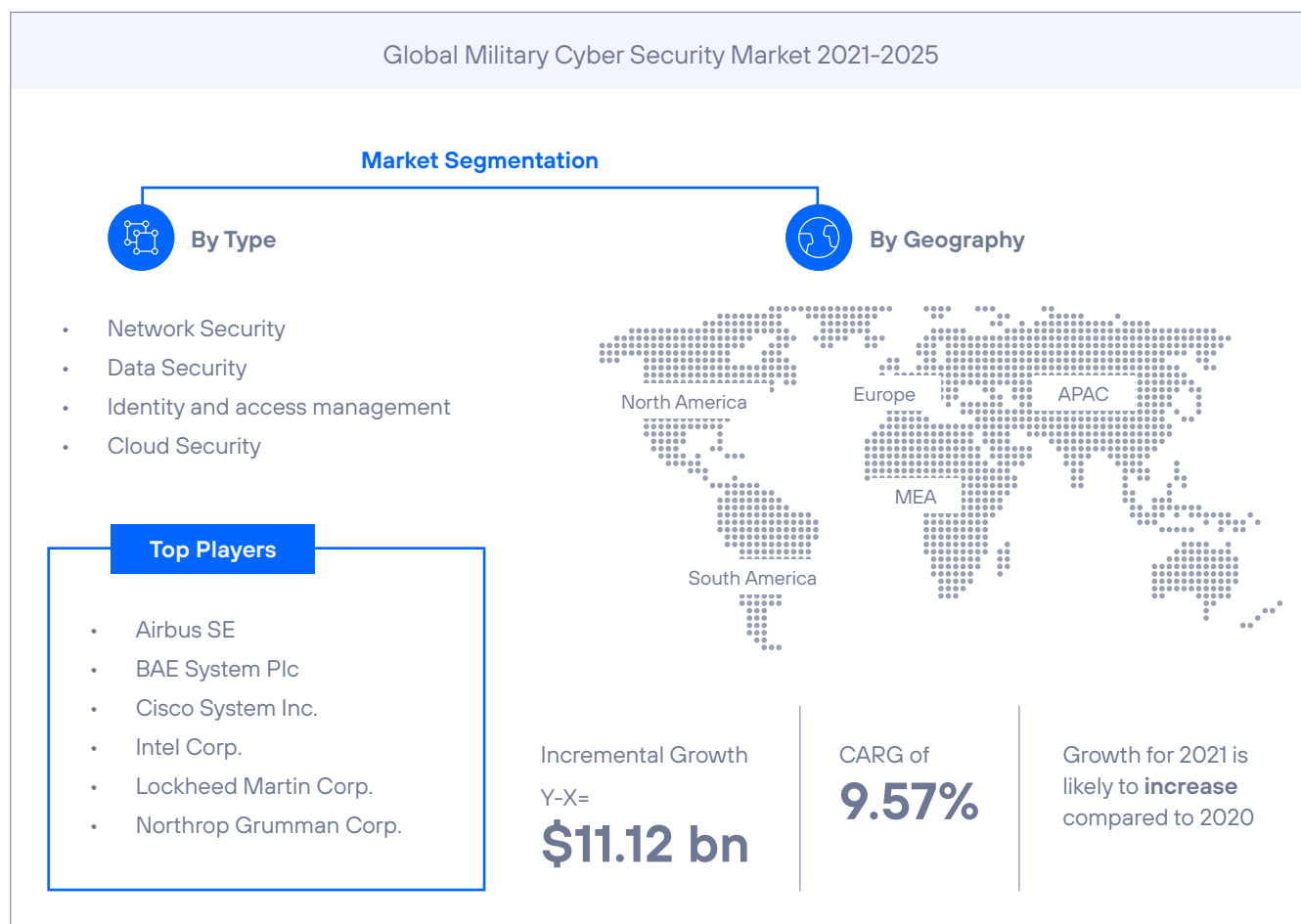


Figure 3. Evolution of the Military cyber security market.

2.3 Cyber security in critical infrastructures: particularities

Critical infrastructures differ from other systems in several fundamental ways that directly impact their cyber security.

- **ORIGEN ANTIGUO:** hardware and software systems used to monitor and control physical processes not designed to connect to the Internet. OT environments often consist of older systems that may have been in operation for many years, making them more susceptible to vulnerabilities and lacking built-in security features.
- **FINALIDAD:** OT systems are designed to ensure the safety, reliability, and efficiency of industrial processes, whereas traditional IT systems focus on data processing and communication.
- **PRIORIDAD:** Unlike IT networks, OT networks prioritize real-time communication and have strict uptime requirements, leaving little room for interruptions or downtime caused by security measures.
- **DIVERSIDAD TECNOLÓGICA:** OT systems encompass a wide range of devices and technologies, such as industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLCs) and specialized machinery. This technological diversity adds an additional layer of complexity to critical infrastructure cyber security.
- **PRIMERO LO FÍSICO:** cyber security of OT systems focuses on protecting critical infrastructures, ensuring the availability, integrity, and security of industrial processes, and preventing potential physical damage or harm caused by cyberattacks.

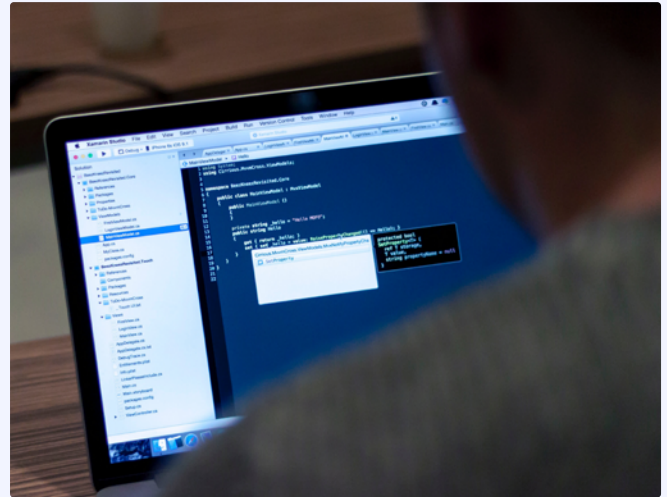
These differences underscore the need to address cyber security in critical infrastructures in a specific way tailored to their unique characteristics. Protecting these systems plays a crucial role in preserving the security, business continuity and integrity of modern society.



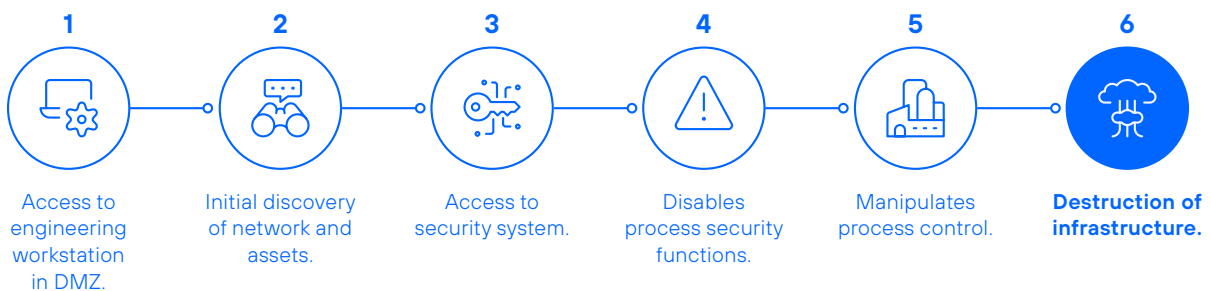
3. Cyberattacks on industrial OT systems: the Triton case

We can illustrate a cyberattack on critical infrastructure through the incident known as the Triton scenario, which took place at a petrochemical facility in Saudi Arabia in mid-2017.

The Triton case represents the **first publicly reported incident demonstrating a targeted attack with a known effect on an operational SIS** (Security Instrumented System). The hackers' activities caused the SIS controller process to shut down, leading to the discovery of the attack.



OT attack scenario (based on Triton)





1. The attack starts with the **compromise of a machine in the corporate network** through phishing techniques, the distribution of an infected flash drive or an internal malicious actor. Since this machine in the IT environment is used to access engineering stations in the OT environment, the attacker proceeds to extract the credentials to connect to one of them using tools like Mimikatz, which can extract passwords stored in memory.



2. Once in the OT environment, the attacker begins to **explore the different assets** found there.



3. The attacker's ultimate goal is to disable safety controllers designed to stop industrial processes when dangerous operating conditions are detected, so at this point it tries to **locate these systems**.



4. After locating the control system, the attacker loads malware specifically designed to remotely **take control of the system and disable the safety functions** capable of stopping the process as soon as it begins to present a risk to physical integrity.



5. With the security system out of play, the attacker proceeds to **manipulate the systems controlling the industrial process**.



6. The changes made by the attacker to the industrial control system have **devastating effects without the security control systems being able to do anything to prevent it**.



3.1 Global cyber threats to critical infrastructures

What are the threats facing critical infrastructures today? The global landscape is dynamic and constantly evolving. Here we share some of the most recent and significant challenges they face:

HUMAN-DRIVEN

Social engineering: These attacks represent a significant threat, as malicious actors attempt to trick employees to gain unauthorized access to systems or confidential information.

Mistakes and oversights: Employee mistakes and oversights can lead to security incidents, including the opening of malicious emails or attachments, loss of devices, or misconfiguration of systems.

Lack of cyber security training: Lack of awareness and training among employees can make them more susceptible to social engineering tactics and less likely to take appropriate security measures.

Privileged access: Employees with privileged access to sensitive systems and data pose a risk, as they may abuse their privileges or fall victim to targeted attacks to gain unauthorized access.

Unwitting collaboration: Employees may unwittingly collaborate in cyberattacks by falling victim to malware or allowing attackers to access systems through their compromised credentials.

ADVERSARY-DRIVEN

Sophisticated cyberattacks: Critical infrastructure systems are increasingly the target of sophisticated cyberattacks, including advanced persistent threats (APTs), ransomware attacks and supply chain compromises. These attacks exploit vulnerabilities in IT and OT systems to disrupt operations, compromise data integrity, and potentially cause physical damage or widespread disruptions.

Nation-state threats: State-sponsored cyberattacks pose a significant challenge to critical infrastructure. Countries engage in cyberespionage, sabotage or disruption campaigns targeting critical sectors, such as energy, healthcare, transportation, and defense. These threats often involve well-resourced and highly skilled adversaries with strategic motivations.

Insider threats: Whether intentional or unintentional, insider threats remain a challenge. Malicious individuals with privileged access can take advantage of their position to cause damage or steal confidential information. Unintentional actions by employees, like falling victim to social engineering attacks or inadvertently introducing malware, can also lead to security incidents.

TECHNOLOGY-DRIVEN

Increasing interconnectivity: Increased interconnectivity between IT and OT systems, along with the proliferation of IoT devices and cloud-based services, expands the attack surface for cyber threats. Critical infrastructures become more vulnerable to cyberattacks as more devices and systems are connected, creating potential entry points for attackers.

Emerging technologies: The adoption of emerging technologies, such as 5G networks, Cloud computing, Artificial Intelligence (AI) and the Internet of Things (IoT), introduces both opportunities and challenges for critical infrastructure cybersecurity. While these technologies improve efficiency and connectivity, they also introduce new vulnerabilities and complexities that must be addressed.

Vulnerabilities of legacy systems: Many critical infrastructure sectors continue to rely on legacy systems that may lack regular security updates or have outdated security protocols. These systems were not originally designed with cyber security in mind and may have inherent vulnerabilities that can be exploited by attackers.

Supply chain risks: The global nature of supply chains introduces cyber security risks. Attackers can attack suppliers, compromise hardware or software components, or inject malicious code during the manufacturing process. Critical infrastructure systems may use compromised components, posing a significant threat to their integrity and security.

ORGANIZATION-DRIVEN

Resource constraint: Executives often face a lack of resources, such as limited budgets, a shortage of qualified cyber security professionals, as well as difficulties in obtaining the necessary technologies and tools. Allocating resources effectively to address cyber security needs within the organization can be a daunting task.

Complex incident response and recovery: Executives must develop and maintain effective incident response and recovery plans to mitigate the impact of cyber incidents on critical infrastructure. This includes timely detection, containment, and recovery measures to minimize disruptions and restore operations quickly.

Limiting cyber insurance: Defining a cyberattack as an act of war can have far-reaching consequences for cyber insurance. It often leads to the exclusion of coverage for damage caused by such attacks, leaving organizations vulnerable to substantial losses. Insurers may also be hesitant to offer coverage for war-related cyberattacks due to their significant and unpredictable nature, resulting in limited availability of suitable policies. If coverage is offered, premiums may increase significantly to reflect the increased risk, making it less affordable for organizations seeking protection.

Addressing these global cyber challenges requires a holistic approach that includes robust cyber security frameworks, ongoing risk assessments, regular security updates, employee awareness and training programs, close collaboration between the public and private sectors, and investment in advanced threat detection and response capabilities.

3.2 Threats from nation-states: limitation of cyber insurance

The combination of some of these threats puts a big challenge ahead of us as we try to protect our critical infrastructures.

Do you think cyber insurance covers your organization from cyberwarfare or state-sponsored cyber operations?

Cyber insurers want to exclude state-sponsored cyberattacks from their policies. This is particularly relevant for critical infrastructure operators. The risk of cyber warfare is systemic in nature; in other words, the risk posed is to an entire system, including all of its component parts, not simply to individual organizations. Given our dependence on digital infrastructures, there is no doubt that a small number of states have in their offensive cyber capabilities the power to cause incalculable economic damage, which the insurance market simply could not withstand. It is against these risks that cyber warfare exclusions are being designed to act.

In *Merk & Co v. Ace American Insurance Company*, the latter already sought to exclude from its coverage damages from the 2017 cyberattack named "NotPetya," which changed the rules of the game. NotPetya was a Russian government-linked malware that caused damage worldwide and resulted in \$3 billion in insurance claims, some of which insurers like Ace, argued that they were excluded. Now, Lloyds, the London-based insurance and reinsurance marketplace has published an explicit exclusion that will be included by default in any future cyber insurance policy.

And why is this important for companies managing critical infrastructure?

The answer lies in the service level agreements (SLA) that these companies often have with their regulator and customers. In the event that the insurer does not provide coverage and, simultaneously, the state does not assume liability as a last resort, **there is a risk that these SLAs will put you out of business.**



4. Cyber resilience formula for critical infrastructures


CTelefónica Tech, as Digital Frontier Guardians, has a formula for cyber resilience in critical infrastructures. It consists of the elements that any organization should have in mind when it comes to protecting its critical infrastructures.

We predicate it this way: **Risk equals the probability of a successful cyberattack multiplied by the impact of the damage that said incident generates.**

$$\text{RISK} = \text{PROBABILITY} \times \text{IMPACT}$$

So, if we consider it as a call-to-action formula,

- First, we must know the **cyber risk our infrastructure is exposed to.**
- Then, **protect our critical infrastructure.**
- Finally, be prepared to **detect, respond to and recover from any cyber security incident.**
- All of this must be **managed and optimized by a specialized OT Security Operations Center.**

1. Know your posture	2. Infrastructure	3. Monitor & React	4. Management
<ul style="list-style-type: none">• Physical security.• Master security plan.• Active inventory.• Vulnerability management.• OT cyber threat intelligence.	<ul style="list-style-type: none">• IT-OT Segregation.• OT segmentation.• Application whitelisting - EDR.• Zone firewall.• Remote access control.	<ul style="list-style-type: none">• Security monitoring.• OT: Integration of cybersecurity equipment, processes and tools for detection and response.• Incident Management.	<ul style="list-style-type: none">• +End-to-end OT security operations management and optimization.
 Identify & Prepare	 Protect	 Detect, Respond & Recover	

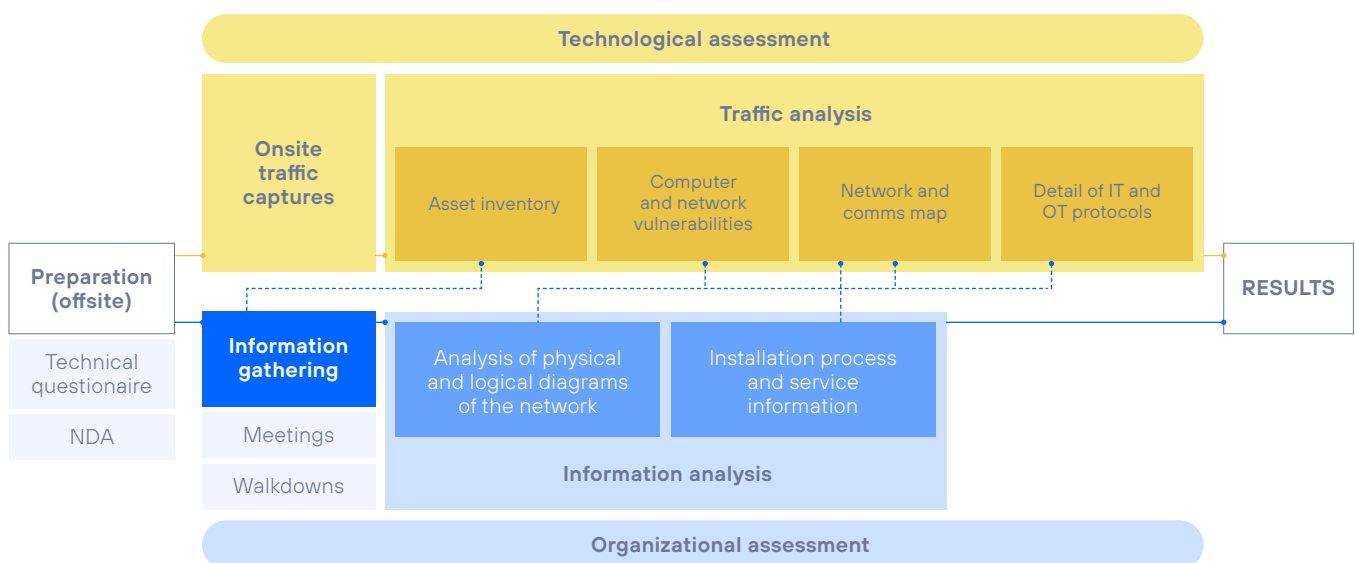
Telefónica Tech is using this formula internally and with our most sophisticated customers to **contribute to the resilience of our critical infrastructures.** Here are some examples of what this means.

4.1 Understanding the organization's cyber security posture

Regarding the first element of our formula, in critical infrastructures we have to:

- **1. Prioritize physical security:** this is an essential component to ensure the protection of assets, facilities, and systems vital to the operation of the infrastructure. It refers to measures and practices aimed at preventing, detecting and responding to threats or physical intrusions that may compromise the integrity, availability, and confidentiality of these infrastructures.
- **2. To have a Security Master Plan:** that allows them to identify and phase the cyber security measures and controls to be deployed, taking into account the needs and priorities of their business and the regulations that apply to them.
- **3. Have a real, fact-based asset inventory:** a survey of the assets of the plant(s) under analysis by capturing traffic and analyzing it using tools capable of interpreting it, identifying the assets, their communication relationships, vulnerabilities in the asset and network configuration and possible malicious activity.
- **4. Manage vulnerabilities:** it is essential to identify and manage the vulnerabilities of the assets that make up the infrastructure, as they are the weak point that attackers can exploit.
- **5. Collect cyber threat intelligence:** once we know our infrastructure and its vulnerabilities, knowing who is interested in exploiting them and how they do it provides useful information to improve detection and response capabilities.

Example of an OT energy cyber security assessment:



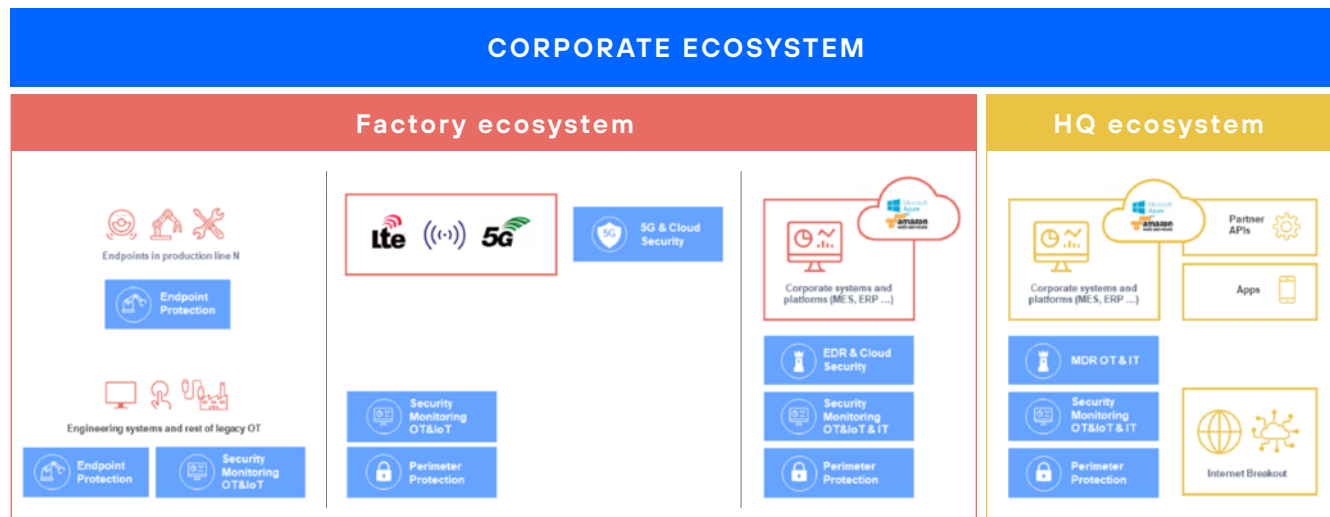
4.2 Defending the infrastructure: creating 360° protection around assets



On critical infrastructures, for the second element of our formula, we need to:

- **1. Apply appropriate IT-OT segregation and OT segmentation:** it focuses on responding to what is usually the first of the proposed cyber security recommendations. The scope of these projects can be divided into two or more phases, always starting with segregation to establish a clear perimeter protection barrier between IT networks and OT networks of an industrial nature. In practice, a complete service should consist of the following phases:
 - Design of secure industrial network architecture.
 - Hardware and software supply.
 - Implementation and configuration of the NGFW (Next-Generation Firewall) and other communication equipment implementing the defined network architecture.
 - Exploitation of the technological equipment implemented in order to provide a service similar in scope to that of any technology included in the Secure Device Management service.
- **2. Apply application whitelisting and endpoint policies:** this allows us to limit the applications that can be executed on the systems that control and supervise production, preventing an attacker from installing malicious software that would allow them to take control of the systems.
- **3. Implement zone firewalls:** as a measure to micro-segment networks to the point of controlling communications between any pair of devices in the industrial environment, provided that the latency requirements of the operating environment allow it.
- **4. Deploy secure remote access control:** operational environments must allow remote access for operators who need to provide monitoring and maintenance functions, but it is critical that this is done in a controlled manner using solutions that ensure that access is done in a secure way.

In the following figure you can see a high-level design of the proposed protection for a 5G private network implementation of another critical infrastructure customer in which you can see:



- Each management zone protected by zero trust policies at the perimeter and endpoints.
- Special security for the cloud and 5G environment.
- OT-specific systems for network monitoring and telemetry of OT and IoT endpoints.



4.3 The importance of detection and response for critical infrastructures

As for the third element of the formula, we need to think about what makes **detection and response in critical** infrastructures so special.

Unlike IT cyber security, **OT cyber security requires a deep understanding of operational processes, the specific industry technologies involved, and the potential impact of a security incident on physical systems.**

Collaboration between IT and OT teams is crucial for effective cyber security in OT environments, as expertise and perspectives from both domains are needed to address the various challenges and requirements of OT systems.

In this case, we suggest designing and preparing with 5 things in mind:

1	2	3	4	5
OT/IoT specific visibility	OT-specific endpoint telemetry	OT system integration	OT-specific guidelines for detection	OT secure response actions

1. OT / IoT specific visibility: It starts with a different approach to collecting endpoint data rather than relying on network traffic alone. This involves adapting traditional agentless IT mechanisms to be secure and effective in OT. A proven, secure, vendor-independent OT-specific agent and an agentless architecture that gathers deep visibility into each endpoint. This combination gathers hundreds of endpoint data such as all installed applications, all users and accounts and their security settings, complete configuration status information, etc. This visibility of endpoint assets is similar to what security managers expect in their IT systems, without causing any risk to OT assets.

2. OT-specific endpoint telemetry: It then adapts the collection of real-time information directly from these assets: logs, syslogs, network flows, device and user behavior, performance statistics, etc. All of this is collected in an OT network-sensitive manner to operate without disruption from bandwidth-limited networks.

3. EOT systems integration: Rather than just sending outbound data to a collector, we need to integrate a wide range of third-party information available to control systems: AV tampering and logs from the various approved OEM (Original Equipment Manufacturer) solutions, whitelist alerts, firewall alerts and detections, backup status data, even process control alarms. Therefore, machine learning engines need to aggregate telemetry from a much broader set of sources to perform accurate detections.

4. OT-specific guidelines for detection: Detection and response is only effective if detections are specifically tied to the environment and provide recommended response actions relevant to that system. The approach identifies OT-specific threats with hundreds of pre-built detections. The detections and response actions must be accurate and enable the "least disruptive response" possible given the threat and the endpoint system itself.

5. Safe response actions in OT: These responses must follow appropriate industrial controls engineering processes in OT. We have to "think safety, but act OT". For detection to be accurate and response to be fast, it must allow "automation" of response actions. However, those actions must go through "local" engineers who know the details of the process before the automated action is initiated. "Act OT" adaptation of DR speeds response but includes critical OT safeguards.

4.4 Managing the OT security operational center

We recommend OT specialization as an umbrella of our formula when it comes to managing critical infrastructure, OT, or IoT security on behalf of our customers or partners. This is what we have done, for example, at Telefónica Tech.

We suggest together with the 3 elements formula for critical infrastructure to focus on:

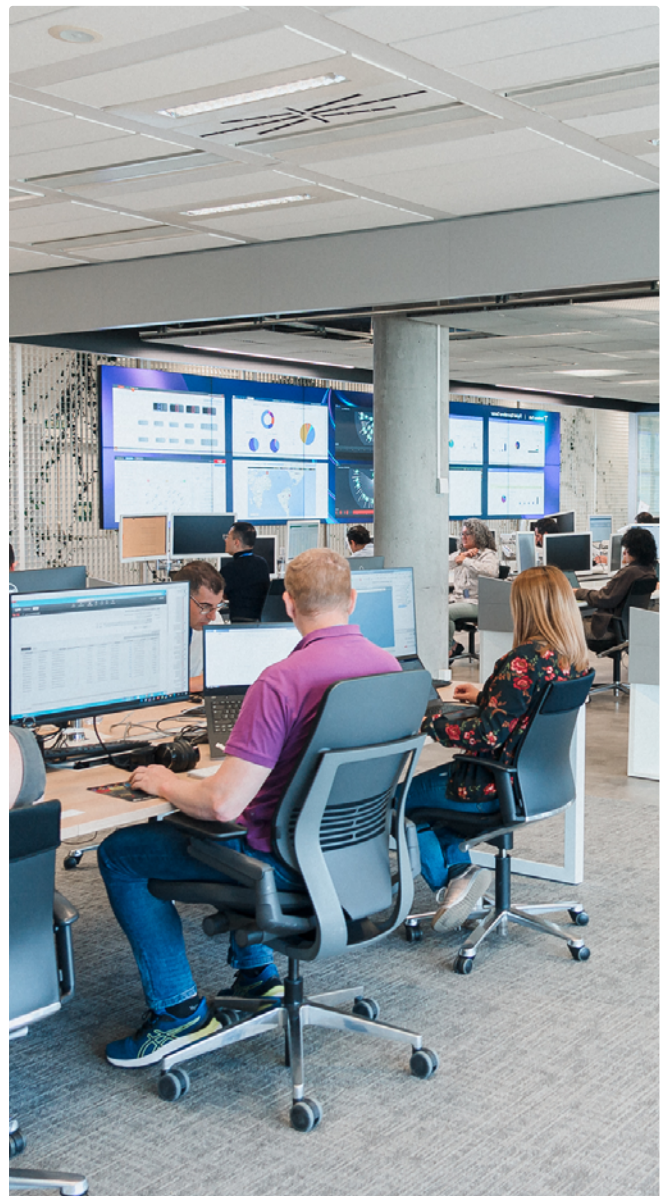
OT security device management: to ensure that devices are active and operating normally, while updated with the latest available software version.

Alert management: this consists of managing alerts generated by the detection of malicious activity in the industrial environment, supervising the health of monitoring equipment and preparing reports on alert generation and processing activity and on changes in assets and vulnerability mapping of the environment.

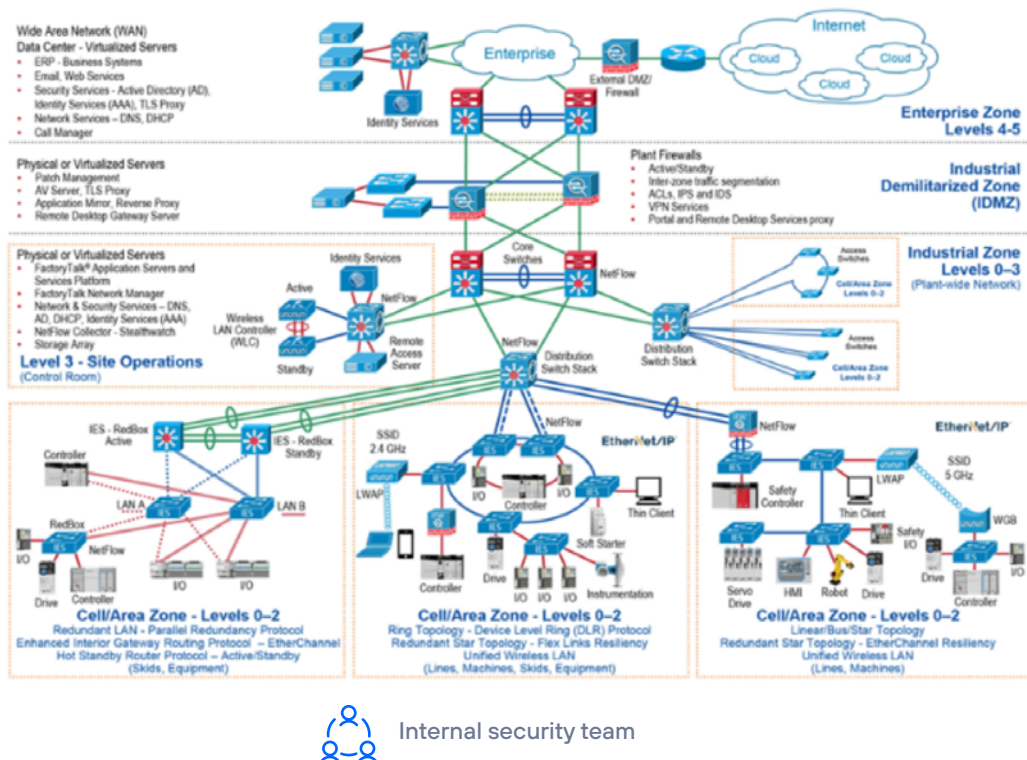
Incident response: in situations where an incident with a materialized impact is discovered, it is essential to respond with agility to contain the damage and remedy the situation with a team specifically prepared for these situations.

Reporting: to update information on the operating environment (i.e. changes in assets and vulnerabilities) and on incident detection and response activity.

Integration with Digital Operations Center (DOC) tools such as orchestration and automation platforms, threat intelligence platforms, customer portals and ticket management, and security monitoring.



Critical Infrastructure Operator Environment



Managed security services partner with OT expertise

OT security appliance management

Proactive health monitoring, monthly fine tuning, upgrades, and support.

Alert management

Alert monitoring, N1 24X7, N2 8X5, recommendations and security incident notification.

Incident response

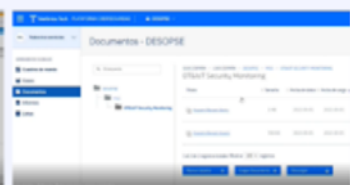
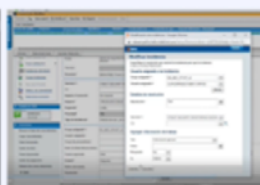
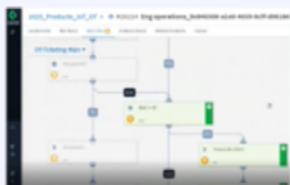
Threat Hunting and incident response in coordination with Infra Operator team.

Reporting management

Weekly device reports, alerts, and relevant information. Monthly risk report from OT security team.

Orchestration and automation platform

Customer portal



Threat intelligence platform

Ticket management and security monitoring

5. Conclusion

The protection of critical infrastructures in an increasingly interconnected digital environment that is exposed to global cyber threats has become a priority. It is therefore essential to understand that cyber security in critical infrastructures goes beyond traditional IT-centric measures. It requires a specific focus on OT operating systems, protection of physical assets and close collaboration between IT and OT systems teams.

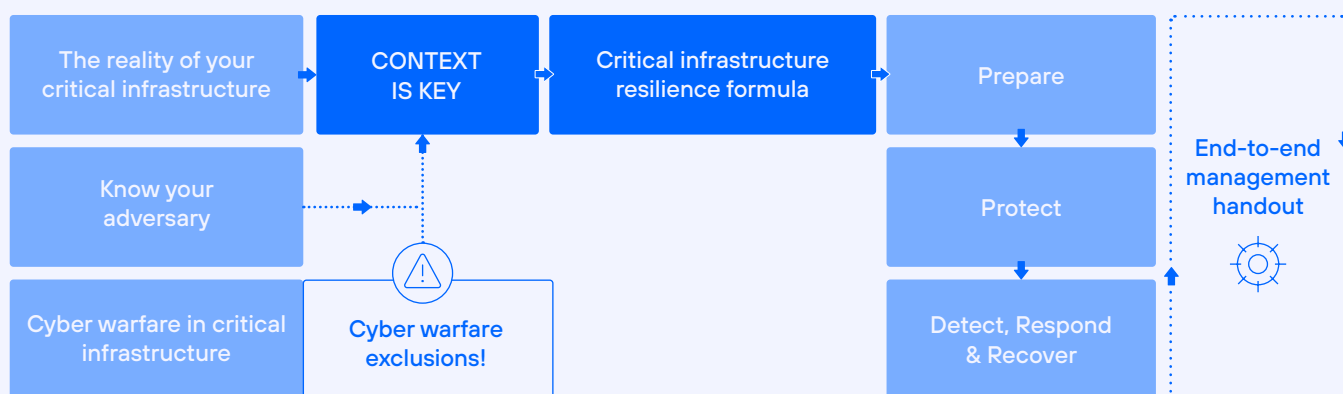
The implementation of measures such as network segregation, application whitelisting and accurate detection and response are key elements to ensure comprehensive protection of critical infrastructures.

The management of the OT security operation center and the integration of emerging technologies such as Artificial Intelligence and the Internet of Things (IoT) are key aspects to strengthen the cyber resilience of infrastructures and strengthen the response capacity of companies and organizations to deal with possible incidents.

Telefónica Tech has the necessary experience and knowledge to offer an end-to-end proposal of products and services specialized in cyber security for critical infrastructures, adapted to the specific needs of each customer. These services range from assessments to identify and analyze risks, monitor assets, detect and respond to potential incidents, to the development of master plans to identify, prioritize, and implement the necessary solutions.

Addressing new cyber challenges and protecting critical infrastructures successfully is only possible through a holistic approach and effective collaboration between the different stakeholders. This is essential to ensure the security, business continuity

and integrity of our societies in a world that is increasingly digitalized and exposed to global cyber threats.





2024 © Telefónica Cybersecurity & Cloud Tech S.L.U. with Telefónica IoT & Big Data Tech S.A.
All rights reserved.

The information disclosed in this document is the property of Telefónica Cybersecurity & Cloud Tech S.L.U. ("Telefónica Tech") with Telefónica IoT & Big Data Tech S.A. and/or any other entity within Telefónica Group and/or its licensors. Telefónica Tech and/or any Telefonica Group entity or Telefónica Tech's licensors reserve all patent, copyright and other proprietary rights to this document, including all design, manufacturing, reproduction, use and sales rights thereto, except to the extent said rights are expressly granted to others. The information in this document is subject to change at any time, without notice.

Neither the whole nor any part of the information contained herein may be copied, distributed, adapted or reproduced in any material form except with the prior written consent of Telefónica Tech.

This document is intended only to assist the reader in the use of the product, service or technology described in the document. In consideration of receipt of this document, the recipient agrees to use such information for its own use and not for other use.

Telefónica Tech shall not be liable for any loss or damage arising out from the use of the any information in this document or any error or omission in such information or any incorrect use of the product, service or technology. The use of the product, service or technology described in this document are regulated in accordance with the terms and conditions accepted by the reader.

Telefónica Tech and its trademarks (or any other trademarks owned by Telefonica Group) are registered service marks.

