NextDefense

Telefónica Tech's NextDefense services

What is Next for Cyber Security Services?

Telefónica Tech

1 | New Launch: NextDefense

Telefónica Tech is pleased to announce the launch of NextDefense, its new brand of advanced managed services.

Telefónica's NextDefense assembles our next-gen security services to help large and mid-size enterprises adopt an effective security program through fully **managed defense in cloud, endpoint, and network.** NextDefense services extend your security operations through **our elite experts**, backed by proprietary threat intelligence, best-in-class technology and automation-driven standardized procedures.

NextDefense provides the core capabilities to support a comprehensive security practice based on the NIST framework, and includes Detection and Response, Vulnerability Risk Management, and Threat Intelligence services.

2 | Context: Cyber Security Today

Billions of euros are spent annually on security technology. Research predicts a worldwide security spending to reach $174.7 billion in 2024 (a CAGR of 8.1% over 2020-2024). Yet, organizations continue to fail and fall victim to cyber-attacks as shown by the latest breach reports and trends:

In 2020, the volume of compromised records jumped by 141% (37 billion), the largest number since 2005. Ransomware literally doubled in 2020, and accounted for 27% of malware incidents reported (Gartner). The pandemic context was leveraged by bad actors (COVID-19 is blamed for a 238% increase in cyberattacks in FinTech in 2020) and is expected to worsen in 2021.It is clear that something is not working well in the industry. We have been looking for a magic pill that can guarantee health, a single magical technology that can prevent all attacks. As it occurs with many acute illnesses, stopping some types of attacks could completely be undertaken with some specific measure. But guaranteeing that our organizations stays cyber-risk-healthy requires a much more thorough, systematic, and constant effort.

NIST has created a very comprehensive framework that explains how such a program should be structured based on the following pillars:

IDENTIFY

- Asset Management
- Business Environmnet Governance
- Risk Assessment
- Risk Management Strategy

PROTECT

- Access Control
- Awareness & Training
- Data Security
- Info Protection & Procedures
- Maintenance
- Protective Tech

DETECT

- Anomalies & Events
- Security Continuous Monitoring
- Detetction Processes

RESPOND

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER

- Recovery Planning
- Improvements
- Communications

Implementing it, however, is no easy feat. Even large multinationals in regulated industries that have relevant experience in risk management and building internal cyber security capabilities are struggling with the complexity and costs involved. Therefore, the outlook for smaller organizations is even more disturbing.

Organizations more than ever are now relying on Managed Security Services (MSS) providers, seeking to outsource SecOps efforts via hybrid operational models, as well as full advisory and turnkey solutions to build their security program from the ground up. In fact, MSS market is estimated to reach $41 billion by 2022 with 16.6% compound annual growth.

3 | From MSS to MDR and Beyond

Considering the challenges above, it is only natural then that Managed Security Services are already transitioning from purely managing security technology towards comprehensive solutions that aim to span the problem entirely.

Organizations are now shifting their focus and demanding their MSS providers to elevate their role and become a strategic partner that can empower their CISOs and help provide tangible business outcomes.

And as the core enabler of those business outcomes, there is Detection and Response, the true backbone of modern security operations. Managed Detection and Response (MDR), as opposed to traditional MSS capabilities for security technology management, focus their efforts on extending security controls via skilled experts that hunt for and eliminate unnoticed threats.

Detection and Response is no easy task, and it is predicted that many organizations will share efforts with specialized partners:

> *"2025, 50% of organizations will be using MDR (Managed Detection and Response) services for threat monitoring, detection and response functions that offer threat containment capabilities."*
> *Gartner*

MDR services providers enhance an organization's security programs, while greatly decreasing the acquisition costs for adopting this capability. By comparison, deploying mature Detection and Response is almost unattainable for mid-sized enterprises, considering the entry barriers to setup this practice and the ongoing costs to maintain the talent and technology.

As a rule of thumb, an average capability for a mid-size organization would require at least 900k€ in personnel, and over 300k€ in licensing and infrastructure. Way far unaffordable for most companies from this segment.

It is even challenging for the largest organizations with the deepest pockets: global talent scarcity (it is predicted to be as big as 3.5 million unfilled jobs globally by 2021) makes it really difficult to attain and retain talent. And on the other hand, the complexity to evolve security technology steadily grows as new business patterns transform (e.g. BYOD, remote work, SaaS, serverless applications, etc.) and company perimeters follow along (unmanaged devices, private/public clouds, OT & IoT, mobile, etc.).

In contrast, leading MDR providers can provide global threat visibility across sectors and geographies, and unlike most organizations, can manage to afford high fixed costs through economies of scale. Large customer bases allow them to support high staffing costs (hiring, training, churn, retention of tier-3 experts, etc.). Besides, these players have made large investments in standardization, automation, and analytics that allow them to cut short the tier-1 costs for the noisiest low-value operations. Further, top vendors' global reach enables them to build strategic relationships with top technology vendors, thus gaining competitive advantages such as volume-based pricing and premium support programs.

Going back to our NIST framework and our mission to support complete security programs, we acknowledge that MDR on their own will not suffice. A modern **Detection and Response** capability is crucial, but an effective security practice will fail if we do not put equal attention to all other security operations areas and the security program as a whole.

In order to also enable the 'Identify' and 'Protect' functions, it is also critical to leverage a **Vulnerability Risk Management** capability. We need to know what to protect, which threats we need to protect them from, and which is our exposure level to them.

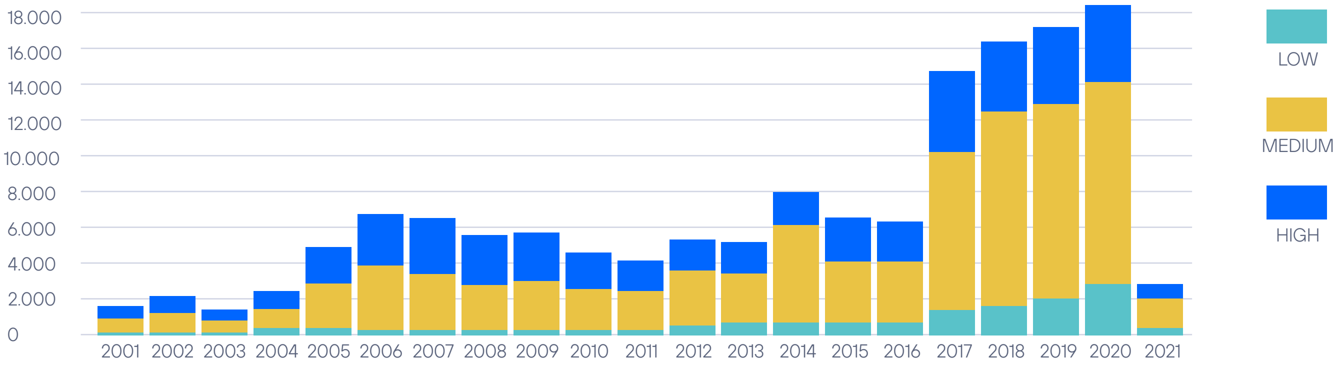
The foundation of a sound security practice is laid in asset inventory, security assessments, and vulnerability management prioritization based on business risk, organizational context, and available threat activity information.

Effective vulnerability management can drastically reduce the burden of detection and response operations, and in most cases even avoid the painful intrusions and data breaches. In fact, according to a Ponemon study, 60% of breaches in 2019 involved unpatched software.

Thus, the challenge for vulnerability management remains on the rise of newly reported vulnerabilities (17,447 vulnerabilities were recorded in 2020, marking the fourth consecutive year with a record number), along with the difficulties for both tracking all assets, detect new security flaws and prioritize the correction of the most urgent ones.

CVSS Severity Distribution Over Time

The visualization is a simple graph which shows the distribution of vulnerabilities by severity over time. The choice of LOW, MEDIUM and HIGH is a based upon the CVSS V2 base score. For more information on how this data was constructed please see the NVD CVSS page.



And to make matters worse, not all vulnerabilities can be found by automatic scanners. Sometimes more subtle flaws exist in specific applications or in whole systems that only human pen-testers or Red Teams can spot.

Lastly, there is a need for a cross-function capability that both helps inform the 'Identify' function, while also extending the 'Detect' function and boost 'Respond' and 'Recovery'. And this is where actionable relevant **Cyber Threat Intelligence** kicks in.

On the strategic side, Cyber Threat Intelligence expands risk management by enabling a better understanding of our adversaries' intent, motives, and capability.

And on the operational side, Cyber Threat Intelligence becomes an extension for security controls to enhance the protection and detection layers. Even when responding to an incident, having information on the attack, actor or campaign can greatly simplify mitigation and remediation by allowing adequate prioritization and proving context information and guidance.

Nevertheless, very few organizations have Cyber Threat Intelligence capabilities available in order to better prepare, detect and respond.

4 | Introduction to Our NextDefense Service

We do believe that most organizations will definitely benefit from a **Detection and Response, Vulnerability Risk Management, or Cyber Threat Intelligence provider.**

But surely they will benefit the most from an **all-in-one partner who can help to build a more comprehensive cyber defense program.**

A partner who can deliver all this as an integrated solution, adapt it to their particular needs, who is nearby and understands their business. A partner who understands technology, has deep insight on the threat landscape, and knows from experience what it entails to protect a digital business. A partner who can innovate and get them ready for everything that is changing in the world today.

And that is exactly the **mission of NextDefense**. Our new brand aggregates our best-in-class operational and technical capability to provide a fully managed solution that combines Detection and Response, Vulnerability Risk Management and Cyber Threat Intelligence.

NextDefense services can be delivered via full turnkey solutions, including the rapid deployment of Telefónica Tech's security technologies that enable advanced detection, hunting and response. This option is best for mid-size to large organizations with lesser security maturity and technology investment deployed.

Additionally, our NextDefense provides bespoke solutions to very mature organizations, based on Telefónica Tech's accumulated expertise over decades providing security services to large corporations and governments. NextDefense bespoke solutions are aimed at organizations with larger security programs and existing technology investments, requiring further integration with their existing stack, SecOps teams, and processes. This offering includes high levels of customization, including custom SLAs and hybrid operations model, with closer engagement and understanding of the customers business.

NextDefense has been designed to help build and support complete effective security programs, enabling the NIST's five security functions. NextDefense fulfills this purpose supported on their **three pillars**:

Detection & Response services, for continuous monitoring, hunting and mitigation of security threats, and breaches. Includes a fully managed turnkey Managed Detection and Response solution, as well as standalone Digital Forensics & Incident Response (DFIR) and proactive Threat Hunting services.

Vulnerability Risk Management services, to gain control over your critical assets through continuous visibility and analysis for faster vulnerability identification and remediation. Includes Vulnerability Scanning, pentesting and Red Team capabilities, as well as Third-Party Risk Monitoring and Security Benchmarking.

Cyber Threat Intelligence services, aim to help you understand your digital risks, providing you with a strategic advantage and situational awareness for better identification and anticipation against threats targeting your digital assets. Includes Digital Risk Protection service, as well as Threat Intelligent Feeds based on Telefónica Tech proprietary feed and our partners' intelligence products.

More information about NextDefense in our web page

About Telefónica Tech

Telefónica Tech is a key holding of the Telefónica Group. The company offers a wide range of integrated technology services, reaching more than 5.5 million customers in 175 countries every day.

Telefonica TECH will host other digital businesses in the future, including in the B2C segment.