Eleven Paths

From MSS to MDR and Beyond

What is Next for Cyber Security Services?

Telefónica CYBER SECURITY COMPANY

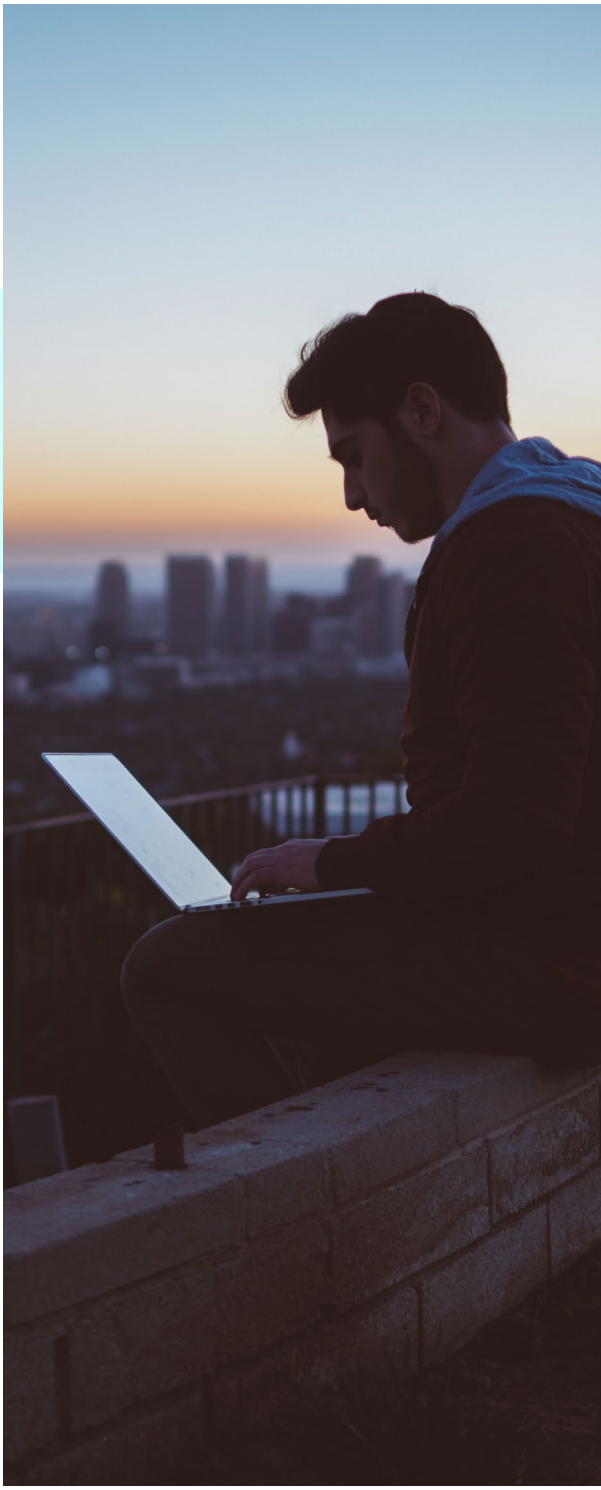
elevenpaths.com

1 | Cyber Security Today

It is our opinion that Cyber Security today is at a crossroad. Despite increased awareness, focus and investment, many organizations are still struggling to implement effective security programs. For example, even after the aftermath of the first global ransomware attacks back in 2017 and the sustained wave that followed, we recently saw a rise in serious ransomware incidents within our customers and it seems that other security providers are reporting the same:

In Q3 2020, Check Point Research saw a 50% increase in the daily average of ransomware attacks, compared to the first half of the year.

(https://blog.checkpoint.com/2020/10/06/study-global-rise-in-ransomware-attacks/)



It is clear that something is not working well in the industry. Billions of euros are being invested to create new technology and partly is intended for diverted security budgets, but still, we are largely vulnerable. Unfortunately, there is a growing awareness and consensus that our ways need to change.

We have been looking for a magic pill that can guarantee health, a single magic technology or action 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 organization is and 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.

The hurdles are enormous: digital transformation is for many a largely uncharted territory with unknown risks. Complex supply chains and partner networks multiply exposures; lack of skilled personnel and skyrocketing costs make any budget look insufficient. Technology paradigm shifts like Cloud, 5G and IoT renders any step forward very quickly outdated; unmanageably large and fragmented cyber security technology supply is impossible for any organization to really follow and evaluate.Security programs built to protect the network and IT are now struggling with the complexity involved into protecting all the business, brand and personnel; cyber and physical risks are all blurred into one continuum. We are seeing an increased need for advisory and outsourcing to help security programs evolve and be made sustainable and future proof.

Looking at smaller organizations, the outlook is even more disturbing. As cybercrime gets more sophisticated and the cost of an attack lowers, any business may be worth the effort. In many cases the prize is not even the small enterprise, it may just be the first step towards some bigger catch. We have talked with many of those organizations and their CISOs and the reality in many cases is that they are starting from scratch after an attack made it clear to everybody that they were not prepared and that procrastination was no longer viable. Such organizations cannot really do it on their own. They require full guidance and comprehensive solutions. We have had some cases that we were even asked to outsource for some of them the CISO function itself.

Various forecasts show the market for managed security services growing at double-digit rates.
One report from Allied Market Research estimates the market to reach nearly $41 billion by 2022, based on a 16.6% compound annual growth rate between 2016 and 2022.

2 | From MSS to MDR

It is only natural then that Managed Security Services are already transitioning from managing technology and protecting perimeters to offering comprehensive threat detection and response services.

2025, 50% of organizations will be using MDR services for threat monitoring, detection and response functions that offer threat containment capabilities.
Gartner

According to Gartner MDR services are defined as:

> *Threat monitoring, detection and response (MDR) services provide customers with remotely delivered modern security operations center (SOC) capabilities to rapidly detect, analyze, investigate and actively respond to threats (e.g., containment or disruption). MDR service providers offer a turnkey experience, with many using a predefined technology stack covering endpoints, networks, cloud services, operational technology (OT)/ Internet of Things (IoT) and other sources, to collect relevant logs, data and other telemetry (e.g., forensic data, contextual information). This telemetry is analyzed via the provider's platform using a range of analytics, threat intelligence (TI) and manual analysis from experts skilled in incident detection and response... Human-performed, threat-hunting services complement real-time monitoring and detection capabilities to find novel and sophisticated threats.*

This approach is definitely a big step forward from traditional MSS that was designed to focus on perimetral security, security technology management, compliance and alert filtering, rather than on what it should be the real outcome of security operations, detection and response.

It also prevents the customer from bearing the burden to build all this capability internally, something that is in many cases out of reach for most organizations due to the lack of knowledge, skills, budget or time. It is not even financially affordable for large organizations with the deepest pockets as we explained before.

Let's run some numbers for an average large enterprise (around 3000 employees) in Europe:

- 8 Level 1 SOC Operators to provide 24/7 monitoring as many technical faults or attacks come when least convenient.
- At least 2 L2 Analysts able to perform 8/5 triage, incident response, threat intel gathering, hunting, detection engineering leveraging frameworks like MITRE ATT&K to fine tune tools.
- At least 1 L3 analyst able to do advanced incident response coordination, investigation, malware analysis, forensics, etc.
- The minimum technology for adequate visibility like and EDR and SIEM to cover 3000 endpoints.
- A team to evaluate among dozens of different products and work towards the solution, plus all the tools track incident and automate tasks, training and support.

It is definitely a program that at current rates in the market will require at least 900K€ in personnel and training, and more that 300K€ in technology, so more than 1M€ annually altogether. **Turn-key MDR services** can definitely provide a much lower barrier of entry and they are the only way for average enterprises to incorporate effective detection and response capabilities into their security programs.

Large enterprises can still benefit from MDR services, albeit in a different way. A turn-key approach will probably fail to fully integrate with the existing capabilities that those organizations have and want to retain internally and really cater to their specific business needs and objectives. They require a threat detection and response offering that is more personalized, that can help fill gaps and lower costs for specific aspects for MDR and integrate it fully into their overall security architecture and existing security operations. Custom SLAs and hybrid workflows that allow handover of tasks between the MDR provider and the customer are mandatory, as well as geographical proximity and close engagement and understanding of the customers security and business.

This is not to say that MSS services are no longer needed. Their functions are still required but should be considered a fact. The limelight in any SOC building and provider selection process should be given to detection and response, something that many organizations and providers still fall short to deliver.

3 | From MDR and Beyond

All this is good but is having an effective detection and response program enough to guarantee the success of a security program? Unfortunately, this is not the case. It is crucial and mandatory but our overall security program will fail if we do not put equal attention to all other security operations areas and the security program as a whole.

Going back to our initial message, there is no single magic pill. We need to be able to perform all the functions detailed in frameworks like the one proposed by NIST, and embed cyber security into our organization's operation and governance.

Our MDR program is doomed to play whack-a-mole and overruns in costs. Fail to meet SLAs or even completely fail to avoid the black-swan event our business fears, unless we have prepared the ground adequately in the Identify and Protect functions.

The foundation is actually laid in asset inventory, risk assessment and management. We need to know what to protect, which **threats we need to protect them from, and which is our exposure to them.**

In a survey of nearly 3,000 IT security professionals, Ponemon Institute found that despite putting more resources towards vulnerability management, organizations are still not able to minimize the risks of an attack. Only half of the respondents said they could quickly detect vulnerabilities and respond to attacks, and only 44% said they could patch it quickly.

Less appealing tasks like tracking assets, patching systems and managing vulnerabilities is wheremany times, the battle is lost, even before having any chance to detect and respond.

In fact, very few attacks are really based on 0-days. The majority of attacks leverage known vulnerabilities that slip through the cracks. It is a difficult task for any organization to track all assets, find their exposures, detect all vulnerabilities and correct them on time. Prioritization of vulnerabilities according to probability and risk is still an open problem for vulnerability management programs. And to make matters worse, not all vulnerabilities can be found by automatic scanners. Sometimes more subtle vulnerabilities exist in specific applications or in whole systems that only pen testers or white hats can find.

Threat Intelligence capabilities to better understand our adversaries is also crucial in the risk management process and should drive the required protection layer to make detect and response viable. It can also help alert us about specific new threats that are emerging and thatcan even be the only way to defend our digital assets such as our brand, reputation, or intellectual property against attacks in the digital space. Even when responding to an incident, having information on the attack, actor or campaign can greatly simplify the response process by allowing adequate prioritization and proving context information and guidance. Nevertheless, very few organizations have threat intelligence capabilities available in order to better prepare, detect and respond.

Protection, even if it can never be perfect needs to help reduce risk and cut down the number of security events to a manageable level so thatthe detection and response function hasa chance of completing its mission.The advent of Cloud, IoT, teleworking while using unknown devices and networks, is an huge challenge.

We do believe that most organizations will definitely benefit from an MDR partner, but will probably do more so from an **all-in-one partner whocan at the same time help building 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.

We believe that a next level of managed services is required, and this is exactly what we are prepared to offer.

Stay tuned at ElevenPaths for what is coming next in cyber defense...

About ElevenPaths

ElevenPaths is Telefónica's cyber security company, part of the Telefónica Tech holding, which brings together the digital businesses with the greatest growth potential in the company.

In a world in which cyberthreats are inevitable, as intelligent managed security services suppliers, we focus on preventing, detecting, responding and diminishing the possible attacks faced by companies. We guarantee the cyberresilience of our customers through 24/7 support entirely managed from eleven i-SOCs around the world with global operational capacity.

We believe in challenging the current state of security, a characteristic that must always be present in technology. We are constantly rethinking the relationship between security and people with the aim of creating innovative products capable of transforming the concept of security. In this way, we manage to stay one step ahead of our attackers, whose presence is increasing in our digital lives.

We work to guarantee a safer digital environment through strategic alliances that allow us to improve the security of our clients. Besides constant collaborations with leading organisations and entities such as the European Commission, Cyber Threat Alliance, Cloud Security Alliance, Cyber Security Alliance, EuroPol, Incibe, OpenSSF, OEA, ISAAC, OCA, FIRST, IoT Security Foundation, Industrial Cybersecurity Centre (CCI) y APWG.

More information:

elevenpaths.com | **@ElevenPaths** | **blog.elevenpaths**