Telefónica Tech

The SOC of the Future

Redefining Cyber Security with AI and automation

paloalto NETWORKS

FROST & SULLIVAN

Index

01

Main challenges in the evolution towards the SOC of the future

Cyber Security managers face an incredibly complex, ever-changing, and ever-evolving landscape when designing Cyber Security strategies for businesses and governments. Cyber Security continues to establish itself as a global priority, driven by the **growth of the attack surface** resulting from the adoption of new technologies such as generative artificial intelligence (GenAI) and migration to public clouds, according to Morgan Stanley's Cyber Security 2025 Outlook study. Despite the use of tools such as artificial intelligence (AI), machine learning (ML) and GenAI by malicious actors, more than 90% of SOCs (Security Operations Centers) still rely on manual processes, according to data from the Incident Response 2024 report published by Unit 42, the team in charge of threat and cyber intelligence research at Palo Alto Networks.

Although the number of ransomware attacks is moderating, t**he overall costs of security breaches continue to rise.** According to the 2024 H2 State of Security Report, published by Telefonica Tech, more than 333 million Cyber Security events were detected in the second half of 2024. In addition, the Incident Response 2024 report also reveals a worrying statistic: 4.1 % of malware attacks in 2023 were aimed at destroying data, five times higher than in the previous year.

The profound digital transformation of companies and governments, reflected in high rates of remote work, cloud adoption or implementation of the Internet of Things (IoT), has a direct impact for those responsible for Cyber Security: **an increasingly hybrid ecosystem, more complex and difficult to protect.** According to the 2024 State of the Cloud Report published by Flexera, 89% of organizations are using multi-cloud infrastructure, and 73% are using hybrid cloud infrastructure.

+90%

of SOCs still rely on manual processes

Source: Incident Response 2024 (Unit 42)

+333 million

Cyber Security events were detected in the second quarter of 2024

Source: State of Security Report 2024 H2 (Telefónica Tech)

Another aggravating factor is the global shortage of Cyber Security talent, which limits and conditions the search for analysts. According to ISC2's 2024 ISC2 Cyber Security Workforce Study, there are nearly 4.8 million unfilled positions in Cyber Security. **This represents a 19.1% growth in the talent gap over the previous year.** The inordinate demand for professionals makes it difficult to recruit and retain them. As a result, it is very difficult for Cyber Security managers to manage and execute a complex security strategy that makes effective use of sophisticated solutions capable of responding to the constant barrage of attacks.

There are also multiple security rules and regulations established by different governments to increase the resilience of organizations, such as **GDPR** (General Data Protection Regulation) in Europe, **ENS** (National Security Scheme), **CRA** (Cyber Resilience Act of the European Union), the **NIS2** directive (European Network and Information Security Directive), and the regulations dictated by the US National Security Strategy. Compliance with these standards requires Cyber Security managers to keep comprehensive records of their information and report incidents, increasing the need for security tools that provide visibility into the Cyber Security ecosystem.

Cyber Security leaders require advanced prevention, detection, and response capabilities to cope with increasingly sophisticated attacks. In order to do so, they must leverage the same tools as their attackers, boosting their security by using AI, ML algorithms and GenAI co-pilots that boost analyst efficiency, reduce the volume of alerts, minimize response times, and improve responsiveness to modern threats. Their security strategies must also be aligned with a key business objective: ensure protection while keeping costs under control. In this scenario, a modern, advanced technology SOC is the solution.

02

Transforming cyber defense: Overcoming threats to improve visibility

The first requirement of an effective Cyber Security strategy is to have full visibility into the ecosystem. However, the factors previously mentioned make this a significant challenge for organizations operating in hybrid and multi-cloud environments. These infrastructures expand the attack surface, increase exposure to threats and add complexity in managing data traffic.

Top Cyber Security challenges for organizations around the world

Figure 1. Source: Voice of the Enterprise Security Customer de Frost & Sullivan.

88%

less investigation time thanks to the use of EDR, which groups alerts and analyzes root causes

Source: Palo Alto Networks

The first step to achieving visibility in most organizations is to deploy EDR (endpoint detection and response) solutions that can detect, investigate, and respond to threats that have breached the perimeter and reached the endpoints. According to Palo Alto Networks, using EDR can reduce investigation time by 88% by grouping alerts and analyzing root causes. However, an EDR does not work in isolation, but is complemented by firewalls, cloud security and identity and access management (IAM), among other solutions, to cover all attack vectors. The challenge arises when these tools operate in independent silos, without sharing information with each other.

The only effective solution is to break down these silos through a platform approach, where all security solutions are integrated and work in a coordinated manner, improving threat detection and response in an efficient way.

03

Borderless Journey: Eliminating security silos for a holistic view

Cyber Security professionals are on constant alert due to the high volume of notifications they receive about potential threats in the environment they must protect.

Security systems generate thousands of alerts about potential threats every day, although many of them end up being false positives. According to the Incident Response 2024 report, 75% of alerts are confirmed cases, 15% are false positives and the remaining 10% are near-misses.

The so-called "alert fatigue" has therefore become one of the biggest challenges for SOCs. The main problem is that investigating every alert in depth is unfeasible. Even by focusing only on the highest priority alerts, the workload is still overwhelming. The urgent leaves no time for the important: developing and maturing the organization's Cyber Security strategy on a large scale.

To make matters worse, the most sophisticated threats have different ways of bypassing security controls, masking their behavior and avoiding generating alerts. Insider attacks, targeted attacks and evasive malware do not show sufficient indicators of risk, but are behavior-based, so traditional security solutions cannot detect them.

Additionally, **the number of 0-day vulnerabilities has shown an increasing trend in recent years,** and the way in which these attacks exploit critical vulnerabilities to infiltrate a system's networks can go unnoticed by most security solutions. According to the 2023 Unit 42 Network Threat Trends Research Report, between 2021 and 2023, exploiting vulnerabilities for attacks increased by 55%.

Number of 0-day vulnerabilities discovered

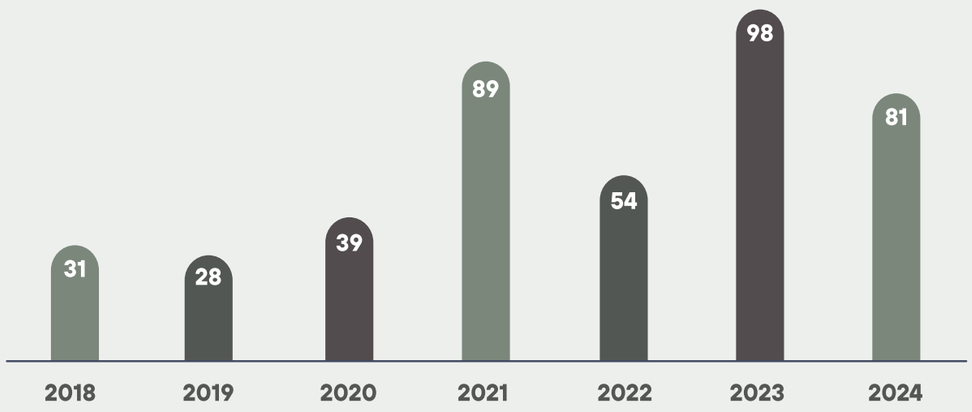


Figure 2. Source: **Zero-Day.cz** Database.

According to the Incident Response 2024 published by Unit 42 of Palo Alto Networks, in 2023 the main access route used by attackers was the exploitation of vulnerabilities in software exposed to the Internet, surpassing phishing as the most common method. This shift reflects a **trend toward automation and mass escalation of attacks by identifying vulnerable systems online.** In addition, previously compromised credentials experienced a notable increase as an attack vector, increasing five-fold in the last two years and highlighting the importance of strong password management and authentication practices.

Among the most prominent incidents in the second half of 2024, analyzed in Telefónica Tech's H2 2024 State of Cyber Security Report, there were attacks that paralyzed businesses for days and caused millions of dollars in losses in key sectors such as technology, finance, automotive, and data management.

An attack can go undetected if analyzed in isolation from different security solutions, such as an EDR, a firewall or a Cloud Workload Protection Platform (CWPP). **Each of these tools might not detect suspicious behavior on its own, but by correlating events and analyzing the context together, it is possible to identify that they are part of the same attack.** This phenomenon resembles the experiment in which a group of blindfolded people touch different parts of an elephant such as its trunk, ears, tusks, tail, and legs. Individually, each person perceives only a fraction of reality, making it difficult to understand what is in front of them. It is only by sharing information and connecting individual pieces that a complete picture emerges. **Similarly, effective Cyber Security requires a unified approach, where all solutions work together to detect and mitigate threats more accurately and efficiently.**

A high-impact case

A healthcare company in the United States, whose platform connects payers, providers, and patients, was the victim of a high impact cyberattack in February 2024. Given its key role in the functioning of the country's healthcare system, the attack paralyzed the sector for days and resulted in millions of dollars in losses for the company. It is estimated that the breach could have exposed the data of 1 in 3 of the country's citizens. To this day, the consequences are still present: customers facing problems with the platform, suppliers with economic losses, and other collateral effects. The cause of the incident was a server without multi-factor authentication, which allowed unauthorized access to the company's systems. This case reinforces the importance of having full ecosystem visibility and applying behavioral analysis to prevent and mitigate attacks of this magnitude.

x5

the increase of previously compromised credentials as an attack vector in the last **2 years**

Source: 2024 Unit 42 Incident Response

Between

2021 and 2023

the exploitation of vulnerabilities for attacks increased by **55%**

Fuente: *2023 Unit 42 Network Threat Trends Research Report*

Extended detection and response (XDR) platforms are based on the principle that **the whole is greater than the sum of its parts**, and therefore seek to unify security and destroy silos, increasing cyber resilience through synergy and communication between security controls.

XDR features **three key pillars: the first is threat detection and response across the entire ecosystem.** To achieve this, XDR's leading solutions collect telemetry from various security controls, including endpoint, network, cloud, identity, email, mobile, IoT, OT, among others. They then analyze and correlate this data, relying on machine learning (ML) and artificial intelligence (AI), discarding false positives, significantly reducing the volume of alerts cluttering the SOC and analyzing the behavior of entities in the ecosystem. In addition, they aggregate alerts and incidents into processes that tell the full story of the attack and provide essential context for analysts.

This entire process allows Cyber Security managers to have almost unlimited visibility into their ecosystem, removing the barriers imposed by hybrid and multi-cloud environments. Correlation and the use of AI and ML to work with the data reduces noise and maximizes the value to Cyber Security analysts, allowing them to focus on the really important alerts. The solution also detects cunning threats that are more than the sum of their parts, or that do not present traditional risk indicators. **XDR is a unified platform that centralizes** multiple security sources within an organization, reducing complexity and providing an effective response to advanced threats.

> "Palo Alto Networks reported that implementing XDR as a core piece in a SOC can achieve up to an **80%** reduction in alert volume, in **addition to a 93%** improvement in detection time and a **90%** improvement in response time."

04

A Multidimensional Path: Extending coverage to third-party data for increased resiliency and flexibility

Full integration of a vendor's security portfolio through an XDR solution is something that can provide organizations with multiple benefits in terms of resiliency, visibility, interoperability, and ease of deployment. For most Cyber Security managers, however, this is an impossibility. According to Frost & Sullivan, more than 7 out of 10 companies work with 5 or more Cyber Security vendors.

Number of security companies that organizations work with around the world

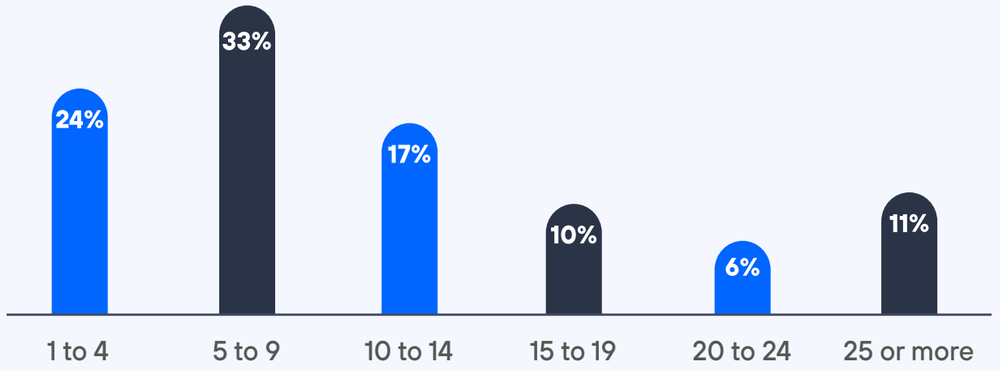


Figure 3. Source: Voice of the Enterprise Security Customer de **Frost & Sullivan.**

This is due to multiple factors, from lack of budget forcing organizations to try to make the most of their security investments, to personal preference and interest in having the best-of-breed solution, to inter-company relationships and multi-year contracts that make it impossible to switch vendors at any time. Despite the flexibility that comes with working with multiple Cyber Security companies, and according to Morgan Stanley's Cyber Security 2025 Outlook, there is a trend toward vendor consolidation.

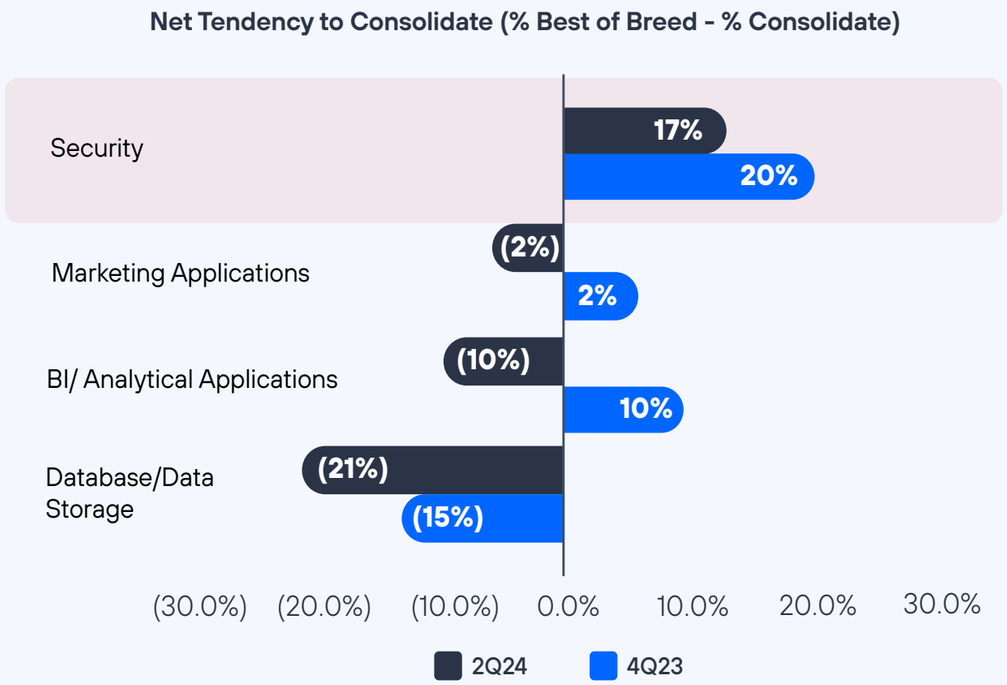


Figure 4. Source: Morgan Stanley Database.

Integrating third-party solutions is twice as essential for companies in critical sectors that make use of industrial technology, such as healthcare, manufacturing, utilities, oil and gas, mining, and government entities. In many cases, the technology that these organizations use for their tasks does not allow the deployment of an EDR or similar solution that can provide visibility into it. Additionally, OT elements often have vulnerabilities that can be exploited by malicious actors to infiltrate the system and move laterally. According to data from Palo Alto Networks, nearly 70% of industrial companies have received a cyberattack specifically targeting OT by 2024, and 25% of companies have had to pause operations due to a security incident.

70%

of industrial companies have received a cyberattack specifically targeting OT in 2024

Source: Palo Alto Networks

25%

of companies have had to put operations on hold due to a security incident

Source: Palo Alto Networks

Two researchers from the Dutch Institute for Vulnerability Disclosure (DIVD), Wietse Boonstra and Hidde Smit, discovered between April and August 2024 six vulnerabilities in the Enphase IQ Gateway device, an essential component of solar panels manufactured and distributed by the Enphase company that serves to transform the direct current produced by the panels into alternating current. The first three of these vulnerabilities enabled an attacker to connect to and take complete control of the device and any other devices connected to it, provided they were both over a public network. According to Enphase, which collaborated with researchers to disclose these vulnerabilities, there are about four million of its systems deployed in more than 150 countries. An attack on this type of infrastructure can generate catastrophic consequences both within an organization and for third parties, causing significant damage, sanctions, increased regulations and a series of negative impacts. **It is therefore essential to maintain visibility and monitoring over these devices, as they are essential to mitigate an attack in the event that a previously unknown vulnerability is exploited.**

In any case, the need for technology integration, logs and third-party data should not be a limit to an XDR solution. **The second pillar of the platform is the integration of third-party Cyber Security solutions.** That is, an XDR platform should not force its users to perform a rip and replace practice of its security controls such as EDR, firewall or cloud. Instead, by design, it should provide direct support to all organizations seeking to unify the management of multiple solutions offered by a variety of security vendors.

The behavioral and identity-based analysis offered by XDR aligns with one of the major industry trends: **moving from a reactive to a proactive approach. Identity data, as well as solutions such as identity and access management (IAM) or identity threat detection and response (ITDR), are essential for faster incident response.** Due to the popularity of techniques such as phishing, man-in-the-middle, data breaches and other types of incidents that result in stolen credentials, these attacks are becoming increasingly common. According to the IBM X-Force Threat Intelligence Index 2024 report, attacks that take advantage of compromised credentials have increased 71% in the last year. According to Palo Alto Networks' Unit 42 Incident Response 2024 report, the average time between compromise and data exfiltration dropped to two days in 2023, compared to nine days in previous years. In 45% of cases, attackers exfiltrate data in less than a day, underscoring the need for rapid response. An example in relation to Black Basta ransomware, **involved attacking 10,000 endpoints in less than 14 hours** from initial access to ransomware execution.

> "Average time between data engagement and exfiltration was reduced to two days in 2023"
>
> Source: *Unit 42 Incident Response 2024 Report*

It is possible to prevent these attacks by immediately revoking the permissions of suspicious users by combining information from the identity environment with behavioral analysis. This can effectively stop security incidents that would otherwise be extremely difficult or even impossible to detect. According to the Incident Response 2024 report, partial or incomplete deployment of solutions such as EDR/XDR is a common cause of attacker success.

XDR and SIEM solutions must be able to integrate cyber threat intelligence (CTI) sources, data and platforms to multiply a SOC's proactive capabilities. According to Frost & Sullivan data, 51% of organizations globally already have a CTI solution in place, so being able to integrate third-party solutions is essential for this step. The Incident Response 2024 report published by Unit 42 of Palo Alto Networks revealed that 20% of incidents are identified by third parties (partners or external). Worldwide, and particularly in Europe, there are initiatives such as information sharing and analysis centers (ISACs), which offer real treasure troves of freely shared threat information. **Having the widest possible breadth of cyber intelligence enables organizations to stay one step ahead of malicious actors and threats,** as it increases predictive capabilities in the face of modern attacks and presents opportunities to modify the security posture, as well as to prepare detections, configurations and automated actions before the attack occurs.

Thanks to this full integration, analysts in a modern SOC will have all the information at their disposal to resolve security incidents in the best possible way, finding the root cause of each intrusion and effectively mitigating the damage of these attacks. **However, the volume of alerts remains excessive, especially as visibility increases exponentially. Therefore, a key component to further empower analysts is critical: automation.**

↑71%

of attacks leveraging compromised credentials in the past year

Source: IBM X-Force Threat Intelligence Index 2024 Report

45%

of cases, attackers exfiltrate data in less than a day

Source: Unit 42 Incident Response 2024 Report

20%

of incidents are identified by third - parties (partners or external)

Source: Unit 42 Incident Response 2024 Report

05
Smart Evolution: AI-driven SOCs

The third pillar of XDR is the automation of tasks and processes to ease the burden on analysts. For a SOC to function effectively in today's context, characterized by numerous and sophisticated threats, as well as a shortage of talent, it is essential to take full advantage of various forms of automation.

The CISO of a company with more than 1,000 employees in the services sector, interviewed by Frost & Sullivan, **stated that the automation capabilities of the XDR platform enabled him to increase the value of his Cyber Security team by 4 times,** reducing the workload of analysts and eliminating the need to hire additional staff following the organization's regional expansion.

The integration of AI and large language models (LLMs), on the other hand, is revolutionizing SOCs, offering innovative solutions to automate alert management, enrich threat analysis, reduce costs and optimize response times. According to Morgan Stanley's Cyber Security 2025 report, it is estimated that 20% to 40% of security analyst tasks can be automated with generative AI, including processes such as log monitoring, alert analysis and patch management.

The integration of AI within a SOC allows to solve the current challenges faced by organizations and provide a response to the constant pressure to reduce time to detection (MTTD) and time to response (MTTR) to threats. According to the Incident Response 2024 report published by Unit 42, AI is capable of reducing MTTD to 10 seconds and MTTR to 1 minute, improving the efficiency and speed of incident management.

> "AI allows to reduce the average detection time to **10 seconds** and the average response time to **1 minute**"

Source: Unit 42 Incident Response 2024 Report

20%-40%

of security analyst tasks can be automated with generative AI

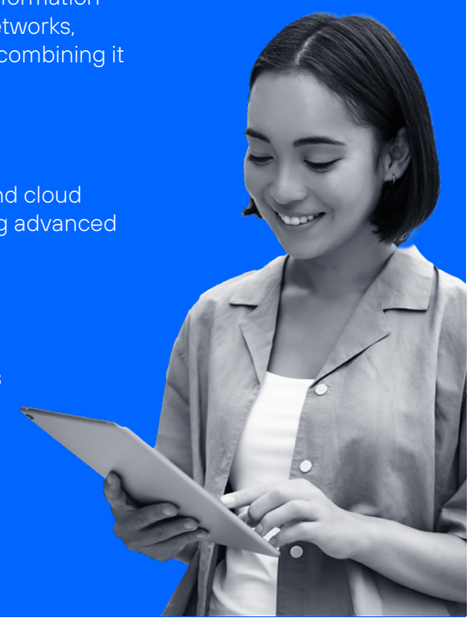
Source: Morgan Stanley Cyber Security 2025 Report

Transformation with AI and LLMs represents an innovative solution for optimizing security in SOCs. Automating alert management reduces repetitive workload, while enriching threat data improves the quality of information for more accurate detection. LLMs can summarize and analyze multiple sources of cyber intelligence, complemented by automated ecosystem data correlation to improve SOC operational effectiveness and provide faster, more efficient responses to incidents.

The SOC market ecosystem faces both demand and supply challenges. Next-generation **security orchestration automation and response (SOAR)** solutions, which integrate LLMs, **are improving ease of use and offering a combination of automation and advanced analytics.**

The architecture of the SOC of the future is based on three fundamental layers:

1. **Data ingestion and processing:** collects information from multiple sources such as endpoints, networks, identity, email, and cloud, processing it and combining it with threat intelligence.
2. **Storage and detection:** uses SIEM, XDR and cloud platforms to store and analyze data, enabling advanced threat detection.
3. **AI response and automation:** incorporates SOAR and advanced AI-based analytics, combining artificial intelligence with human intervention to streamline incident response and optimize operational Cyber Security.



Leading vendors, such as Palo Alto Networks, **have evolved their traditional EDR/XDR solutions into platforms with AI-enabled security co-pilots.** These tools not only allow them to correlate alerts and prioritize investigations automatically but also generate detailed reports and code analysis to identify threats in real time.

A prime example is **Palo Alto Networks' Cortex XSIAM,** which combines advanced endpoint intelligence with orchestration and automated response capabilities, leveraging large volumes of telemetry. This platform helps security analysts optimize their work, reduce response times and make informed decisions, backed by advanced analytics and next-generation AI models.

06

From the future to the present: The Evolution of the SOC with Telefónica Tech and Palo Alto

In the face of an increasingly complex threat landscape and the challenges facing Cyber Security managers, Telefónica Tech and Palo Alto Networks have joined forces to build the SOC of the future, based on visibility, cyber intelligence, artificial intelligence, proactivity, and experience.

As a technology partner in this partnership, Palo Alto Networks brings in its portfolio of solutions, with Cortex XSIAM as the foundation of the modern SOC. This unified platform integrates XDR (with integrated EDR), SOAR, and SIEM capabilities, significantly simplifying SOC management and offering:

- **Ecosystem-wide visibility, detection and response:** It is able to ingest and correlate data from multiple Palo Alto Networks security controls, including EDR, firewalls, Prisma Access, Prisma Cloud and Zero Trust Network Access, among others. This enables you to identify and respond to incidents at any point in the ecosystem.

- **Integration of third-party solutions:** The platform's SIEM capabilities allow you to collect and process third-party data and logs. Its integration with more than 750 security tools extends visibility into complex infrastructures, including OT and IoT devices, providing flexibility and holistic security.

- **Automation and use of AI:** The platform correlates, normalizes and categorizes information from security controls to reduce false positives. It identifies real security incidents through AI and ML models and, with its SOAR capability, automates the response, streamlining threat mitigation in an efficient manner. Its AI continually evolves by training on data from thousands of customer ecosystems, allowing it to generate automation recommendations and further streamline the SOC's work.

In addition, it employs behavioral analysis to identify malicious actors. The solution first establishes a baseline of user behavior, creating a profile that collects typical patterns and activities from logs, authentication and activity on endpoints, networks and cloud environments. **It is able to detect deviations that may indicate malicious behavior** by comparing this behavioral standard to user activity at all times, responding to attacks such as data exfiltration, lateral movement and the use of compromised credentials. This proactive approach strengthens the **resilience of the SOC,** enabling early prevention and avoiding the high cost of managing complex security incidents.

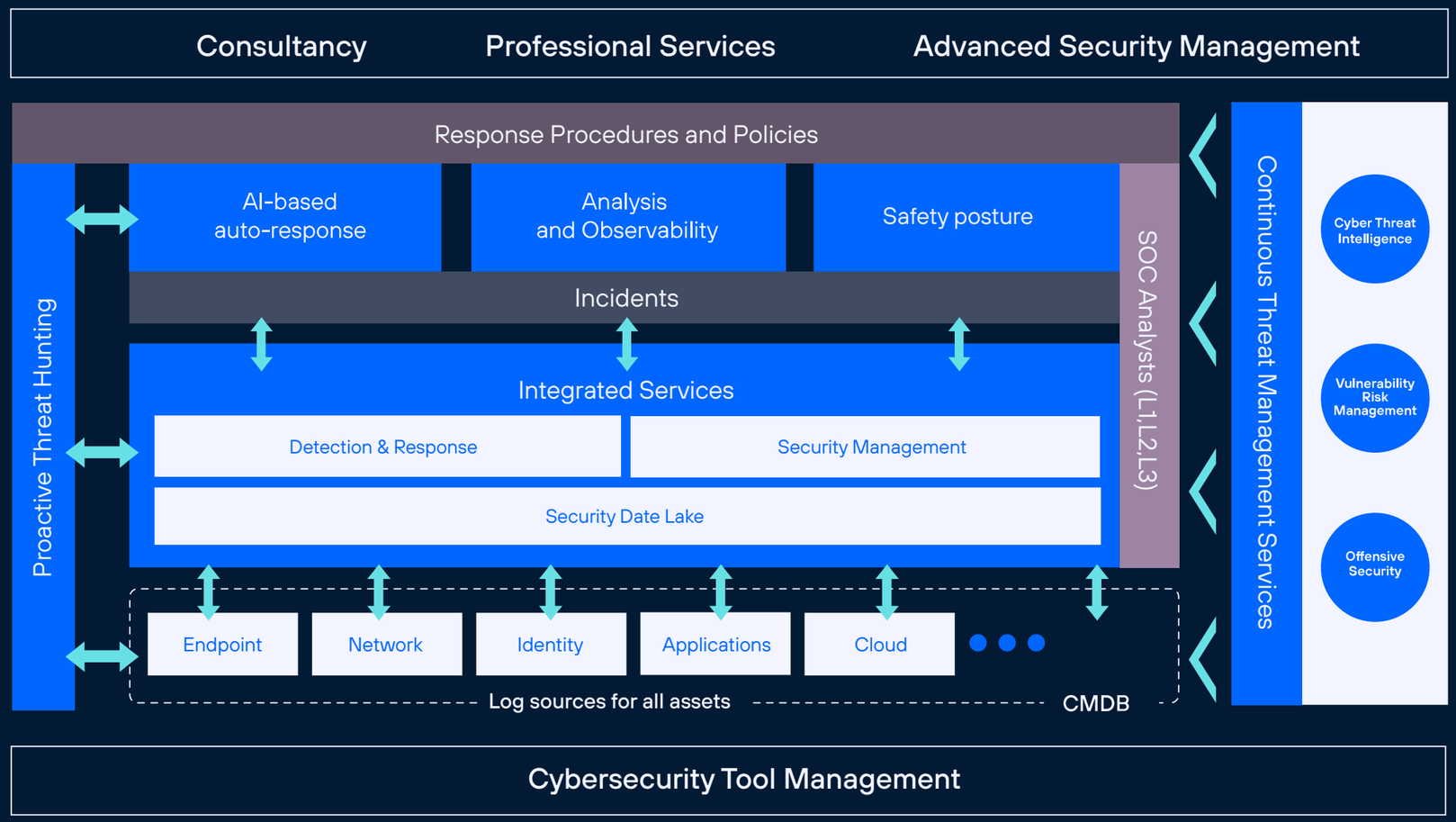
Telefónica Tech, for its part, has NextDefense SOC, the first security operations center designed to take full advantage of Palo Alto Networks technology, including Cortex XSIAM, Prisma Cloud and Prisma SASE.

- NextDefense acts as the key link in Cyber Security management, offering a variety of **services that leverage the value of Palo Alto Networks technology.** Its capabilities include continuous monitoring and management, integration of third-party data sources and cyber intelligence, detection and response in multiple environments, threat hunting, as well as specialized consulting and professional services.

- The effectiveness of a future SOC depends on continuous improvement based on measurement, testing and the implementation of new Cyber Security strategies. Telefónica Tech **offers a full range of services to identify weaknesses in an organization's security posture,** enabling comprehensive management of the ecosystem, vulnerabilities, risks and exposures, while optimizing visibility into the environment. As one of the largest service providers in Europe, it brings its extensive security expertise applied to various industries and sectors. In addition, its experience in resolving tens of thousands of incidents for numerous clients **provides a valuable layer of information for decision-making within the SOC.**

- Telefónica Tech drives **SOC modernization by accelerating AI adoption and automation.** It provides continuous playbook updates tailored to each industry and based on its customers' best practices. Its security posture assessment services help Cyber Security managers define automation strategies aligned with risk, criticality, vulnerabilities and business priorities, facilitating a structured and effective SOC evolution.

NextDefense SOC from Telefónica



Telefónica Tech's approach to managing the SOC of the future facilitates transformation for security managers by combining managed security, consulting, and professional services. Telefónica Tech addresses the most critical Cyber Security challenges by providing holistic protection capable of mitigating the most sophisticated threats by leveraging Palo Alto Networks technology and a joint strategy.

07

Conclusion: Transforming the SOC into a modern, resilient, and proactive unit

We have discussed the steps that a Cyber Security manager must take to drive the evolution of the SOC in an organization.

Security managers must first establish visibility with solutions such as **EDR.** Then expand it across the ecosystem, incorporating external data sources through the deployment of **XDR** and solutions like SIEM. The entire process must be driven by tools where **AI, ML** algorithms and **Gen AI** wizards minimize manual processes, streamline threat response and decrease detection and response time. Finally, the modern SOC must rely on the inclusion of identity data, **user and device behavioral analytics** and cyber intelligence to bolster threat prevention.

Security managers must rely on two types of partners to evolve their SOC: **technology partners,** who provide advanced solutions as the foundation of the SOC architecture, and **security service providers,** who drive the transformation through best practices, assessments, optimized processes and strategic knowledge, providing the necessary expertise to adapt the SOC to a constantly evolving threat environment.

Telefónica Tech and Palo Alto Networks joint proposal offers Cyber Security managers a path to revolutionize SOC with the help of AI

Telefónica Tech, through NextDefense, is leading the evolution of the SOC of the future, offering advanced, proactive security that enables organizations to strengthen their resilience in the face of an ever-evolving threat landscape. As an essential part of this proposition, Palo Alto Networks' Cortex XSIAM extends visibility across the entire ecosystem by ingesting, enriching, and correlating data from multiple security controls, ensuring a holistic approach. It reduces false positives, automates incident resolution and optimizes response times, minimizing operational burden and security costs by integrating artificial intelligence and machine learning (ML).

NextDefense is the only SOC that fully integrates this technology, combining it with the experience and knowledge of its analysts to identify risk surfaces, detect advanced threats and respond quickly and accurately. Telefónica Tech, through services such as threat hunting, vulnerability management and cyber intelligence, closes the continuous feedback loop that drives more robust and predictive security. Finally, it helps Cyber Security managers define their automation and artificial intelligence strategy according to their specific risks through security posture assessments.

The Telefónica Tech Modern SOC, with strategic partnerships and leading technology, is positioned as the ultimate solution to address sophisticated threats, adapt to the complexity of the digital ecosystem and overcome the shortage of specialized talent.

About Telefónica Tech

Telefónica Tech is a global technology integrator, a leader in digital transformation. The company has a wide range of services and integrated technology solutions in Cyber Security, Cloud, IoT, Big Data, and Artificial Intelligence. In all these verticals, we have both our own technologies and the best ecosystems of strategic partners, and this is recognized by both industry analysts and our customers. And all this is also possible thanks to our hubs in Spain, UK, Germany, Brazil and Spain, where we reach more than 5.5 million customers in more than 175 countries.

About Palo Alto

Palo Alto Networks is recognized by industry analysts and thousands of customers as a global leader in Cyber Security. Palo Alto Networks helps companies around the world protect themselves in an ever-changing environment with advanced platforms, leading threat intelligence, and highly trained security professionals. Every day, Palo Alto Networks' SOC, which utilizes Cortex XSIAM®, processes 75 terabytes of data, detects an average of 133 incidents, resolves 100% of them in an automated manner, and achieves an MTTR (Mean Time to Resolution) of 1 minute.Cortex XSIAM has been recognized as a leader and featured in the GigaOm Radar 2023 for Autonomous Security Operations Centers.

About Frost & Sullivan:

Frost & Sullivan is a strategic growth company that helps its customers accelerate their growth and achieve positions of excellence in growth, innovation, and leadership. Its Growth Pipeline -as-a-Service provides the CEO and his growth team with transformative strategies and best practice models to drive the generation, assessment and implementation of high-impact growth initiatives. Frost & Sullivan has more than 60 years of experience collaborating with Global 1000 companies, emerging businesses and the investment community, operating from more than 40 offices on six continents.

If you have any questions and would like to learn more about how we can help you, please

→ CONTACT US

Telefónica Tech

paloalto NETWORKS

FROST & SULLIVAN