Cytomic Services_

Managed Detection & Response (MDR) Service

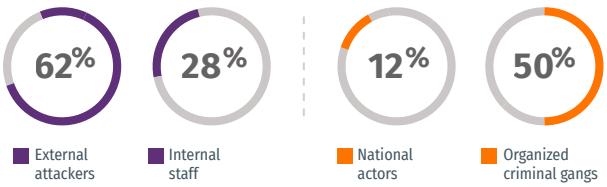
We prevent, discover, and respond to your attackers

Company Cybersecurity_

Cyberattacks are becoming more frequent, more sophisticated, and more critical. The impact on organizations' finances, reputation and competitiveness makes it impossible for any company, large or small, to ignore how important cybersecurity is.

The cybersecurity sector currently works under the assumption that, sooner or later, all organizations will suffer a cyberattack. The only way organizations can protect themselves effectively is to be prepared to react, minimizing economic losses and the damage to their reputation, overcoming the incident without their service being affected.

Who is behind cyberthreats?[1]



What is the cost for companies?

Global cost: **$6 billion[2]**

A security breach costs: **$3.86 M[3]**

However, organizations do not have the resources to carry out this kind of activity. Even if they had the budget for it, it would be impossible for them to hire cybersecurity specialists with the in-depth knowledge in several fields that they need to properly detect and contain threats, mitigate the damage done, and get the company back to normal in the shortest possible time.

The shortage of cybersecurity experts is such that, according to predictions, worldwide there will be be 3.5 million unfilled cybersecurity jobs by 2021[(4)].

In this scenario, where cyberattacks are becoming more frequent, sophisticated and critical, their effects are worsening, and where there are not enough specialized resources, the time needed to detect and respond to these threats is too high. This means that cyberattackers can achieve their goals, extorting companies, exfiltrating their data, and using organizations' assets with ease. In fact, the average time that an attacker spends undetected on a network is 197[(5)] days, while the average time before they are eradicated is 266[(5)] days.

To this we can add the lack of control over new attackers, techniques and vulnerabilities, as well as the absence of continuity plans, which means that organizations are even more likely to be compromised, something that has a huge impact of the business.

The reality of cybersecurity in organizations_

- Organizations tend to disregard the high probability they have of falling victim to hackers, and do not have adequate tools to prevent and defend themselves against such attacks.
- They are unable to detect whether they have been compromised and, as such, are unable to respond and recover properly.
- They do not have continuous risk control and contingency plans.
- Cyberattacks are becoming more frequent and more sophisticated, and the impact on companies' finances, reputation, and competitiveness are constantly increasing.
- They lack specialized Threat Hunting, Threat Intelligence, malware engineers, and data scientists, making it impossible to reduce their exposure to risks and construct a more mature security posture.
- Constant monitoring and analysis of the activity on the organization's assets is the most effective way of detecting the presence of advanced threats.

1 "2018 Data Breach Investigation report". Verizon
2 "2018 Economic Impact of Cybercrime — No Slowing Down". CSIC/McAfee
3 "2018 Study on Global Megatrends in Cybersecurity". Ponemon Institute
4 "Ponemon Institute's cost of a data breach study 2019"
5 Cyber Security Ventures: https://cybersecurityventures.com/jobs/

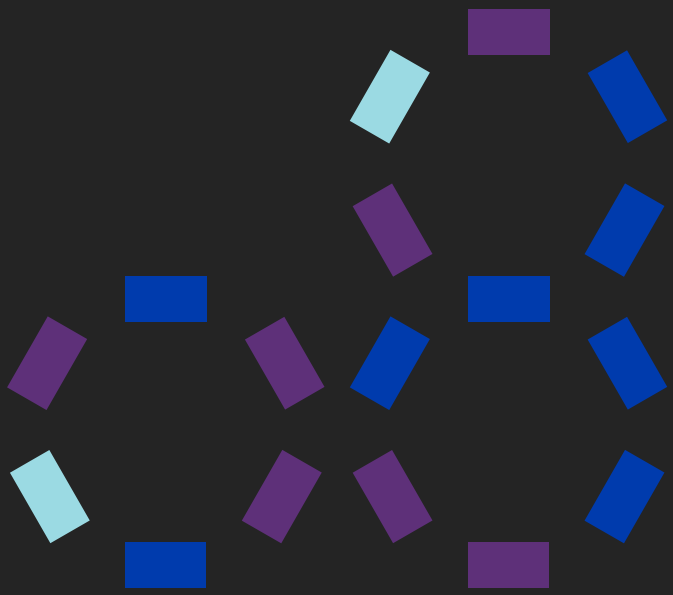
Cytomic MDR Service_

Cytomic MDR is an extension of the organization's security team. It provides comprehensive cover for crucial issues, such as defining protection strategies and defensive, offensive and remediation measures. At the same time, it configures and operates **Cytomic EPDR** and **Cytomic Orion**, the prevention, detection, and response solutions for laptops, desktops, and servers, which are provided from the Cytomic Platform.

The service combines threat intelligence, leading security technology, artificial intelligence, and an expert cybersecurity team. This team has the main national and international certifications in cybersecurity and collaborates as an active member of leading international threat intelligence forums, such as the **Cyber Security Alliance**.

The purpose of this service is to evaluate a range of **malware**, **living-off-the-land**, and **in-memory exploit techniques**, all of which affect our clients. It does this by monitoring activity, detecting **anomalous behaviors**, and investigating incidents. This way, it can determine which machines have been affected and can discover the attack vectors.

Once an intrusion has been confirmed, the Incident Response team establishes response and remediation plans to mitigate any damage. This also includes setting up detection methods to impede future cases.



Benefits_

- Specialized team to increase your maturity and capacity in security and cyber-resilience.
- 4/7 monitoring of all your protected assets, 365 days a year, regardless of where they are located.
- Cloud-native service without investment in infrastructure or licenses. Pay only for what you use and enjoy automatic scalability.
- Reduction of incident detection and response times, minimizing economic, reputational and regulatory damage, as well as recovery time in case of intrusion.
- Threat intelligence and in-house laboratory of experts in malware, evasion techniques, incident investigation and response, and forensic analysis.
- Experience and specialized data analytics technologies specialized in detecting anomalous behaviors and activity in users, applications, and machines.
- Monthly report on security posture, malicious activity prevented or detected, investigated, and remedied by the service, as well as recommendations on avoiding future incidents.

365 DAYS/YEAR

24 x 7

Threat Hunting_

Proactive Hunt for attackers, applying Threat intelligence, data analytics, and our experts' knowledge and experience.

UEBA Detection_

Detection of anomalies via analysis of the behavior of users or other entities in the organization.

Threat Response_

Monitoring and correlation of events. Advanced capabilities for immediate remote incident containment and response.

Inteligencia de Amenazas_

Monitoring and analysis of hundreds of external sources along with sources obtained from the Zero-Trust Application service and other detection technologies

DATA LAKE_

365 days

Endpoint Telemetry

Threat detection and Investigation_

Event monitoring and correlation for suspicious behaviors based on Threat Intelligence and MITRE ATT&CK. Incident Investigation: patient zero, assets impacted, and techniques explored.

Figure 1: Advanced managed service for prevention, detection and immediate response to incidents, combining advanced data analytics on events gathered from protected assets in the organization, threat intelligence from certain external and from Cytomic's own sources with our specialized teams' experience in security, detection and response events.

Main capabilities_

- **Configuration and optimization of security controls.** Ensures effectiveness, personalizing its configuration to obtain optimal protection, detection, and response on the protected assets.
- **Real-time monitoring.** The monitoring of activity on assets, real-time event processing 24/7, 365 days a year along with stored events, allows for the detection of complex attacks by correlating these events with the threat intelligence on the Cytomic platform.
- **Anticipation and detection of threats based on proprietary and third-party intelligence and MITRE ATT&ACK techniques:** Discovery of anomalous behaviors from users, applications and machines, combining the experience of a highly specialized team, platforms, and leading AI technologies, statistical cybersecurity techniques, and internal and external threat intelligence, all in real time.
- **Detection of anomalous behaviors** from users, devices, and applications, using advanced data analysis techniques, entity profiling, and User behavior analytics (UEBA).
- **In-depth analysis:** Study of security incidents to trace the origin of the intrusion, the attacker's path, evasion techniques, persistence or lateral movements used, and evaluate the impact and scale of the incident.
- **Incident response:** Support in identifying and implementing reactive measures to respond to and contain security incidents.
- **Threat Hunting:** Early detection of threats on the network that other detection techniques cannot uncover. This is done by studying the latest hacking techniques, analyzing CVEs and zero-day vulnerabilities, all of which allow the team to establish compromise hypotheses and configure proactive alerts to detect attackers.
- **Lessons learned and reduction of the attack surface:** Revision of weaknesses in systems, discovered either proactively by the team or by analyzing the incident. Recommendations to help implement continuous improvement of the organization's security posture by reducing how exposed it is to present and future threats.

How the service operates_

The service is operated by several teams of cybersecurity experts, who work together to reduce the time needed to detect and respond to attackers who have managed to get onto devices. **The specialized Threat Hunting team** analyzes the behavior of users, applications, and devices to discover any security incident that may have gone unnoticed by other controls, in real time.

To do this, the observe data traffic, the behavior of systems, the origin and destination of connections, and the actions that users and applications usually perform, staying alert to discover anomalous or malicious behavior.

All of this is possible because they use Cytomic's cloud-based platform. The Cytomic Platform processes enormous volumes of information in real time, using artificial intelligence that, with complex statistical models, analysis rules, and a series of next-generation complementary technologies, automates much of the work.

This way, they are able to get ahead of any damage that attackers may cause with malware, malwareless in-memory attacks, or living-off-the-land techniques.

After detection, the **Incident Response team** comes into play. It takes the actions needed to contain the attack and performs exhaustive remediation to eradicate the attacker from the network and return the organization to normal as quickly as possible. This is possible because everything is done remotely from the Cytomic Platform, with no need to travel, meaning that the response is highly effective.

+28 Billion
Events/week/1K nodes protected

1,5 Billion
Events in the Data Lake/1K nodes protected

750
Binaries classified in intelligence

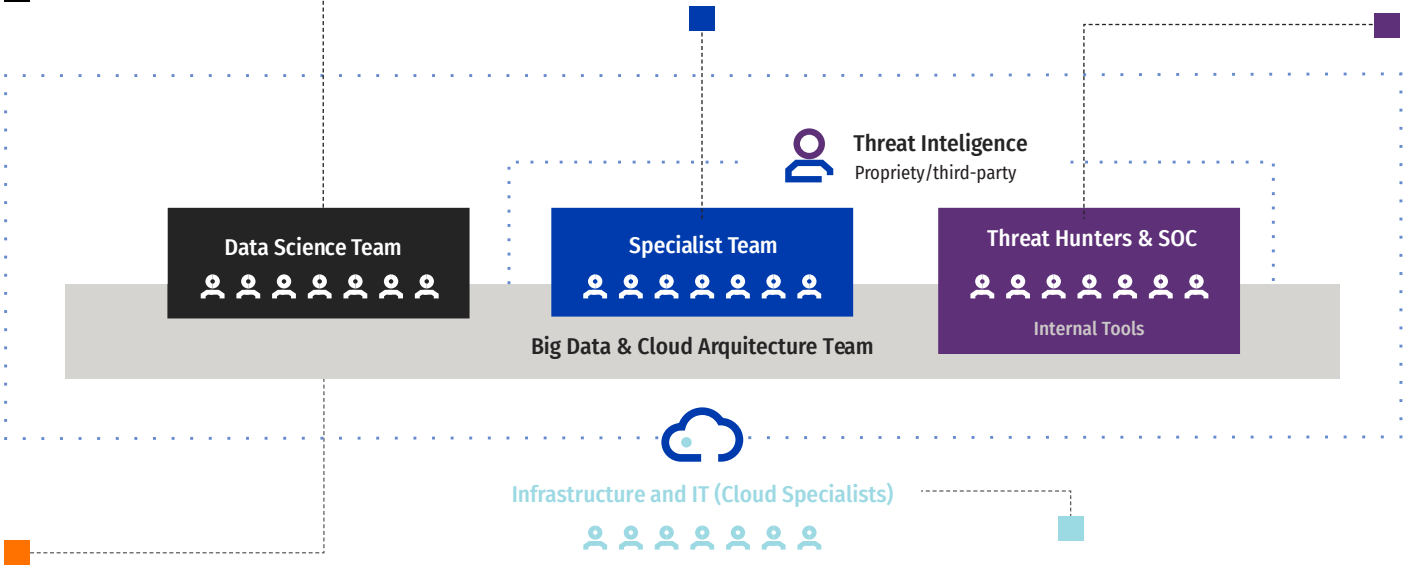
1,2 Trillion
Binarios clasificados en la inteligencia

8,750
Attacks mitigated in the last 12 months/ 1K nodes protected

Security Unit Data Science_

Specialist Unit in threats_

Hunters and team Incident Response_



Application unit and Notebooks specific to other units_

Unit of Big Data & Cloud specialists_

Service Levels_

Cytomic provides multiple layers of managed detection and response services so that the organization can choose the level that best suits its requirements, needs, and structure. This guarantees that it will always get the highest benefit from its investment in Cytomic.

Cytomic's MDR service is offered at two service levels:

	Standard Service	Premium service
Telemetry and incident storage	365 days	365 days
Services operated 24/7	■	■
Notification of operating incidents	■	■
Access to the service portal	■	■
QBR[1]: Practice improvement review	■	■
CSM[2] nominated-single interlocutor	■	■
Prevention, detection and response to malware/malwareless/LotL threats[3], 24x7	■	■
Shared Hunters and security analysts 24x7	■	■
Incident Response upon request[4]	■	■
Dedicated hunters and security analysts 24x7		■
Proactive Incident notification and response[5]		■
Threat Hunting activity report	■	■
Detection of trheats and insider threats with UEBA[6]		■
Initial risk assessment and business context[7]		■
Global plan to improve security posture	Quarterly	Monthly
Flexibility in use cases to be implemented (+800) and real time and retrospective IoCs (+250.000)		■
Service Level Agreement (SLA[8])		■

[1] Quaterly Business Review.
[2] Customer Sucess Manager.
[3] Attackers using **Living-off-the-Land techniques**, without deploying malicious applications, using tools available on devices.
[4] Possibility of unlimited contact with Security Center with "best effort" response commitment
[5] Notification, response, and follow-up of full incident cycle, with remote expert support for resolution.
[6] **Behavioral analysis of users and entities (UEBA)** is a data analytics system that allows suspicious or malicious activity to be identified, whether it is internal personnel or external attackers performing this activity. It applies different advanced machine learning techniques to the activity being monitored, in real time, to trigger an in-depth analysis of what happened.
[7] The **initial evaluation** aims to determine the level of risk and get more detail about the context of the business, understand the IT environment, find out the organization's priorities and usual activities, to be able to offer a personalized service according to the organization's needs. The initial assessment is key in developing an effective detection and remediation strategy, as well as to identify vulnerabilities and weaknesses in the environment

[8] SLA Metrics

	Incident Severity			
SLA Metrics	Critical	High	Medium	Low
Mean time to detect (MTTD)	15 min	1h	6h	24h
Average Notification Time	30 min	2h	12h	48h
Mean time to respond (MTTR)	6h	12h	24h	48h
% compliance	95%	95%	90%	90%
Time to create new use cases	72h (90% compliance)			
Periodic report	5 first days of the period (90% compliance)			

Awards & Recognition_

Common Criteria "EAL2+"
Information Technology Security Evaluation

High "ENS" Classification
Esquema Nacional de Seguridad (Spanish)

Qualified IT Security Product
Centro Criptológico Nacional

Panda Security regularly participates and receives awards for protection and performance from Virus Bulletin, AV-Comparatives, AV-Test, NSSLabs. Cytomic's portfolio shares technologies, platforms, and services with Panda Security's solutions, extending its capacities with its managed threat hunting services and with Cytomic Orion.

AV-Comparatives test Adaptive Defense 360
"This solution classifies all running processes, and registers any kind of malware"

CYTOMIC

More info at_
cytomic.ai

Let's talk_
+34 900 90 70 80

cytomic.ai