Cytomic Services_

Managed Detection & Response (MDR) Service

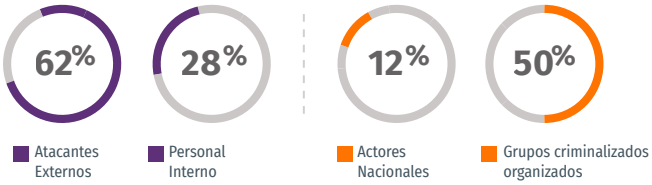
Prevenimos, descubrimos y respondemos a tus atacantes

Ciberseguridad en las empresas_

El continuo incremento, en volumen, sofisticación y criticidad, de los ciberataques y su repercusión económica, reputacional y competitiva de estos en las organizaciones, hace imposible para cualquier empresa, grande o pequeña, ignorar la importancia de la ciberseguridad.

El sector de la ciberseguridad trabaja a día de hoy con la certeza de que todas las organizaciones sufrirán tarde o temprano un ciberataque y que la única estrategia para protegerse de forma efectiva es la de estar preparado para reaccionar, minimizar las pérdidas económicas, el daño a su prestigio y credibilidad frente a sus clientes, socios o proveedores y sobreponerse sin que el servicio se vea afectado.

¿Quién está detrás de las ciber amenazas?[1]



¿Cuál es el coste para las empresas?

Coste global: **$600.000 M**[2]

Cada brecha de seguridad cuesta **$3.86 M**[3]

Sin embargo, las organizaciones no disponen de los recursos para realizar esta actividad, incluso aún disponiendo de presupuesto, les sería imposible contratar especialistas en ciberseguridad con conocimiento profundo en campos diversos necesario para ejecutar una eficaz detección y contención para mitigar el daño y una recuperación y vuelta a la normalidad en el menor tiempo posible.

La escasez de expertos en ciberseguridad es tal que se prevee que en el 2021 habrá 3,5 millones de empleos de ciberseguridad sin cubrir a nivel mundial[4].

En esta realidad, de continuo incremento, en volumen, sofisticación y criticidad, de los ciberataques y su repercusión y de escasez de recursos especializados, los tiempos para detectar y responder a los ciberataques son demasiados altos, las ciberamenazas alcanzan sus objetivos de extorsión, exfiltración de información o instrumentalización de los activos de las organizaciones sin mucha dificultad, al poder permanecer de media 197[5] días en sus redes sin ser detectados, y 266[5] días sin ser erradicados.

A esto se añade, la falta de control del riesgo ante nuevos atacantes, técnicas y vulnerabiliaddes, así como la ausencia de planes de continuidad en las organizaciones, lo que agrave exponencialmente su exposición al compromiso con gran impacto en el negocio.

La realidad de la ciberseguridad en las organizaciones_

- Las organizaciones ignoran la alta probabilidad de ser víctimas de hackers y no cuentan con las herramientas de prevención y defensa necesarias.
- No son capaces de detectar si han sufrido un compromiso y, por tanto, de responder y recuperarse adecuadamente.
- No disponen de control continuo del riesgo y de planes de contingencia
- El volumen, sofisticación y la repercusión económica, reputacional y competitiva de los ciber ataques, sigue una dinámica de crecimiento continuo.
- Faltan recursos especializados en Threat Hunting, Threat Intelligence, Malware reverses y Científicos de datos, imposibilitando reducir su exposición al riesgo y madurar en términos de seguridad.
- La monitorización y el análisis constante de la actividad en los activos en la organizaciób, es la forma más efectiva de detectar la presencia de amenazas avanzadas.

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/

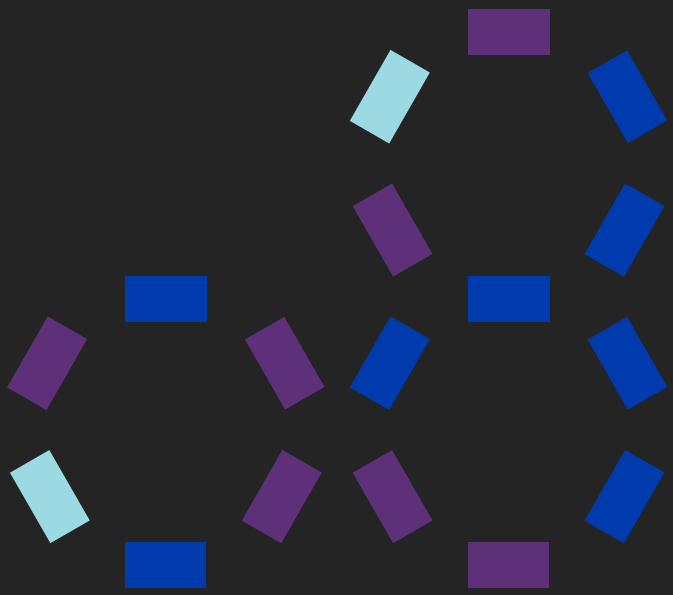
El Servicio Cytomic MDR_

Es una extensión del equipo de seguridad de la organización, dando cobertura integral a temas cruciales como la definición de estrategias de protección y de las medidas defensivas, ofensivas y de remediación, al tiempo que configura y opera **Cytomic EPDR** y **Cytomic Orion**, las soluciones de prevención, detección y respuesta en portátiles, desktops y servidores ofrecidas como servicios desde la **plataforma de Cytomic**.

El servicio combina **inteligencia de amenazas**, **tecnología líder** en seguridad, **inteligencia artificial** y un **equipo experto** en ciberseguridad que cuenta con las principales certificaciones, nacionales e internacionales, en materia de ciberseguridad y que colabora como miembro activo de foros internacionales líder de Inteligencia de amenazas como en **Cyber Security Alliance.**

El objetivo del servicio es evaluar en tiempo real multitud de técnicas malware, living-off-the-land y exploits en memoria, que afectan a nuestros clientes, monitorizando la actividad, detectando comportamientos anómalos e investigando los incidentes, determinando las máquinas afectadas, y los vectores de ataque.

En los casos de intento de intrusión confirmado, el equipo de Incident Response establece planes de respuesta y remediación para mitigar el daño, incluido el establecimiento de métodos de detección para casos futuros.



Beneficios_

- Equipo especializado que multiplica tu madurez y capacidad de seguridad y ciber-resiliencia.
- Monitorización 24×7, los 365 días del año, de todos tus activos protegidos, independientemente de su ubicación.
- Servicio nativo desde la nube, sin invertir en infraestructura ni licencias. Paga solo por lo que usas y disfruta de escalabilidad automática.
- Reducción de los tiempos de detección y respuesta de incidentes, minimizando así el daño económico, reputacional y normativo y el tiempo de recuperación en caso de intrusión.
- Inteligencia de amenazas y laboratorio interno de expertos en malware, técnicas de evasión, en investigación y respuesta a incidentes y análisis forense.
- Experiencia y tecnologías de analítica de datos especializadas en detección de comportamiento y actividad anómala de usuarios, aplicaciones y máquinas.
- Informe mensual de su postura de seguridad, la actividad maliciosa prevenida o detectada, investigada, y remediada por el servicio, así como recomendaciones para evitarlos en el futuro.

365 DÍAS/AÑO

24 x 7

Threat Hunting_

Búsqueda proactiva de atacantes, aplicando Threat Intelligence, analítica de datos conocimiento y experiencia de nuestros expertos.

Detección UEBA_

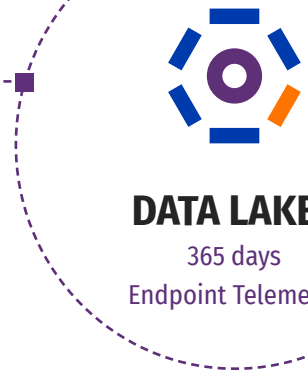
Detección de anomalías mediante el análisis de comportamiento de usuarios y otras entidades de la organización.

Respuesta a amenazas_

Monitorización y correlación de eventos Capacidades avanzadas de contención y respuesta remota e inmediata ante incidentes.

Inteligencia de Amenazas_

Monitorización y análisis de cientos de fuentes externas junto con las propias obtenidas del servicio Zero-Trust Application y otras tecnologías de detección.



DATA LAKE_

365 days

Endpoint Telemetry

Detección e investigación de amenazas_

Monitorización y correlación de eventos en comportamientos sospechosos en base a Threat Intelligence y MITRE ATTACK. Investigación de incidente: paciente cero, activos impactados y técnicas exploradas.

Figura 1: Servicio gestionado avanzado de prevención, detección y respuesta inmediata ante incidentes que combina analítica de datos avanzada, sobre los eventos recogidos desde los activos protegidos de la organización, inteligencia de amenazas de ciertos de fuentes externas y de las propias fuentes de Cytomic con la experiencia en operaciones de seguridad, detección y respuesta de nuestros equipos especializados.

Principales capacidades_

- **Configuración y optimización de los controles de seguridad.** Asegura su efectividad, customizando su configuración para obtener una óptima protección, detección y respuesta en los activos protegidos.

- **Monitorización en tiempo real.** La monitorización de la actividad de los activos, el procesamiento de los eventos en tiempo real, en régimen de 24×7-365d, junto con los almacenados, permite la detección de ataques complejos mediante la correlación de estos con la Inteligencia de amenazas de la plataforma de Cytomic.

- **Anticipación y detección de amenazas en base a Inteligencia propia, de terceros y técnicas MITRE ATT&CK**: Descubrimiento de comportamientos anómalos de usuarios, aplicaciones y máquinas, combinando para ello la experiencia de un equipo humano altamente especializado, plataformas y tecnologías líderes de inteligencia artificial, técnicas estadísticas en ciberseguridad e inteligencia de amenazas interna y externa en tiempo real.

- Detección de comportamientos anómalos en usuarios, dispositivos y aplicaciones aplicando para ello, técnicas avanzadas de analítica de datos, perfilado de entidades y detección de comportamientos outliers (UEBA).

Análisis en profundidad: Estudio de incidentes de seguridad para rastrear el origen de la intrusión, el recorrido del atacante, las técnicas de evasión, persistencia o movimiento lateral utilizados y evaluar su impacto y escala.

- **Respuesta a incidentes**: Apoyo en la identificación e implementación de medidas reactivas con las cuales responder y contener un incidente de seguridad.

- **Threat Hunting**: Detección temprana de amenazas en la red que otras técnicas de detección no son capaces de descubrir, a través del estudio de las últimas técnicas de piratería, el análisis de CVE y vulnerabilidades de 0 días, que permiten al equipo establecerá hipótesis de compromiso y configurar alertas proactivas que detecten a los atacantes.

- **Lecciones aprendidas y reducción de la superficie de ataque**: revisión de las debilidades en los sistemas, descubiertas tanto proactivamente por el equipo o bien en el análisis del incidente. Recomendaciones guías para una mejora continua de la postura de seguridad de la organización mediante la reducción de su exposición a amenazas presentes y futuras.

Cómo opera el servicio_

El servicio es operado por varios equipos de expertos en ciberseguridad que trabajan coordinamente para reducir el tiempo de detección y respuesta de atacantes que hayan logrado llegar hasta dispositivos. **El equipo especializado en Threat Hunting** analizar el comportamiento de usuarios, aplicaciones y dispositivos para poner al descubierto, en tiempo real, cualquier incidente de seguridad que pueda haber pasado inadvertido para el resto de controles.

Observan para ello el tráfico de datos, el comportamiento de sus sistemas, el origen y destino de las conexiones y las acciones que los usuarios y aplicaciones llevan a cabo de forma habitual y se mantienen alerta para descubrir comportamientos y actividad anómala o maliciosa.

Todo ello es posible gracias a que operan la plataforma en la nube de Cytomic. La Plataforma Cytomic procesa, en tiempo real, enormes volúmenes de información apoyándose en tecnologia de inteligencia artificial que, con complejos modelos estadísticos, reglas de análisis y una serie de tecnologías complementarias de nueva generación, automatiza gran parte del trabajo.

De este modo son capaces de adelantarse al daño que pueden ocasionar los atacantes con malware, malwareless en memoria y técnicas living off the land.

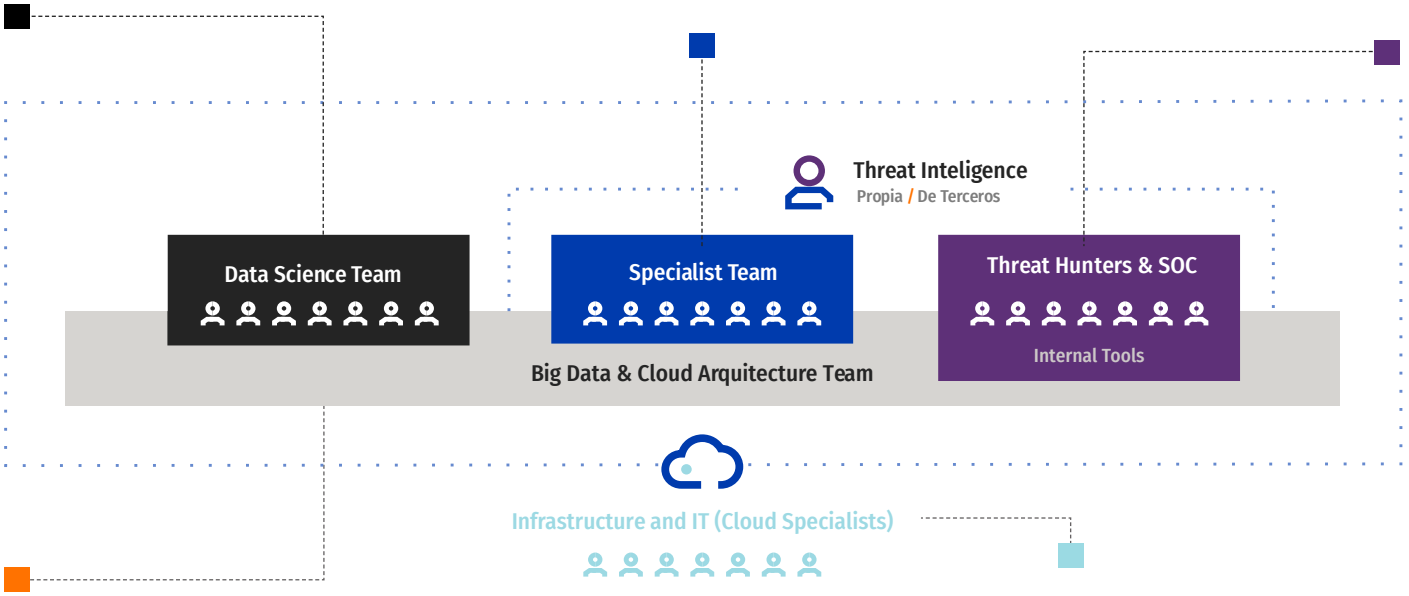
Tras la detección, **el equipo de Incident Response**, entra en juego, realizando las acciones necesaria de contención del ataque y de remediación exhaustiva para erradicar al atacante de la red y la recuperación de la actividad normal de la organización, de forma extremadamente rápida, ya que todo se realiza de forma remota desde la plataforma Cytomic, sin necesidad de desplazamientos, lo cual significaría una respuesta probablemente ineficaz.

+28 Millones	Eventos/semana x 1K nodo protegido
1.500 Millones	De eventos en el Data Lake x 1K nodo protegido
750	Binarios clasificados / semana x 1K nodo
1,2 Billones	Binarios clasificados en la inteligencia
8.750	Ataques mitigados en los últimos 12 meses x 1K nodo protegido

Unidad de Security Data Science_

Unidad de especialistas en amenazas_

Hunters y equipo de Incident Response_



Unidad de aplicaciones y Notebooks específicas para otras unidades_

Unidad de especialistas en Big Data & Cloud_

Niveles de Servicio_

Cytomic proporciona múltiples niveles de servicios getionados de detección y respuesta para que la organización pueda elegir el nivel que mejor se adapte a los requisitos sus necesidades y estructura y así garantiza que obtiene el mayor beneficio de su inversión en Cytomic en cada momento.

El servcio MDR de Cytomic se ofrece en dos niveles de servicios:

	Servicio Standar	Servicio Premium
Almacenamiento telemetría e Incidentes	365 días	365 días
Servicios operados en 24x7	■	■
Notificación incidentes de operación	■	■
Acceso al portal del servicio	■	■
QBR[1]: Revisión mejoras de la práctica	■	■
CSM[2] nominado - interlocutor único	■	■
Prevención, detección y respuesta de amenazas malware/malware-less/LotL[3] en 24x7	■	■
Hunters y analistas de seguridad compartidos	■	■
Respuesta a incidentes bajo petición[4]	■	■
Hunters y analistas de seguridad dedicados 24x7		■
Notificación y respuesta proactivo de incidentes[5]		■
Informe actividad de Threat Hunting	■	■
Detección de amenazas e Insider Threats con UEBA[6]		■
Evaluación inicial de riesgo y contexto de negocio[7]		■
Plan Global de mejora de la postura de seguridad	Trimestral	Mensual
Flexibilidad en casos de uso a implementar (+800) e IOCs en tiempo real y retrospectivo (+250.000)		■
Service Level Agreement (SLA[8])		■

[1] Quaterly Business Review.
[2] Customer Sucess Manager.
[3] Atacantes haciendo uso de **técnicas "Living-off-the-land"**, sin desplegar aplicaciones maliciosas, haciendo uso de las herramientas disponibles en los dispositivos.
[4] Posibilidad de contactar de forma ilimitada con de Centro de seguridad con un compromiso de respuesta"best effort".
[5] Notificación, respuesta y seguimiento del ciclo completo del incidentes con un soporte experto remoto para su resolución.
[6] El **análisis de comportamiento de usuarios y entidades (UEBA)** es un sistema de analítica de datos avanzados que permite identificar actividad sospechosa o maliciosa tanto de personal interno como de atacantes externos. Aplica en tiempo real diferentes técnicas avanzadas de Machine Learning sobre la actividad monitorizada para desencadenar análisis en profundidad de los sucedido.
[7] La **evaluación inicial** tiene como objetivo determinar el nivel de riesgo y profundizar en el contexto del negocio, comprender el entorno de IT, conocer las prioridades y la actividad habitual de la organización, para así poder ofrecer un servicio personalizado acorde con las necesidades de la organización. La evaluación inicial es clave para desarrollar una estrategia de detección y respuesta efectiva, así como para identificar vulnerabilidades y debilidades del entorno.

[8] Métrica SLA

	Severidad Incidente			
Métrica SLA	**Crítica**	**Alta**	**Media**	**Baja**
Tiempo medio de detección (MTTD)	15 min	1h	6h	24h
Tiempo medio de Notificación	30 min	2h	12h	48h
Tiempo medio de respuesta (MTTR)	6h	12h	24h	48h
% cumplimiento	95%	95%	90%	90%
Tiempo para creación nuevos casos de uso	72h (cumplimiento 90%)			
Informe periódicos	5 primeros días del periodo (Cumplimiento 90%)			

Premios y Reconocimientos_

Common Criteria "EAL2+"
Information Technology Security Evaluation

High "ENS" Classification
Esquema Nacional de Seguridad Español

Qualified IT Security Product
Centro Criptológico Nacional

Panda Security participa regularmente y obtiene premios en protección y rendimiento de Virus Bulletin, AV-Comparatives, AV-Test, NSSLabs. El portfolio de Cytomic comparte tecnologías, plataformas y servicios con las soluciones de Panda Security, extendiendo sus capacidades con los servicios gestionados de Hunting y con Cytomic Orion.

AV-Comparatives test Adaptive Defense 360
"Esta solución clasifica todos los procesos ejecutados, registra cualquier tipo de malware"

CYTOMIC

More info at_
cytomic.ai

Let's talk_
+34 900 90 70 80