Cytomic, tu arma de caza contra el cibercrimen_

¿Esperar y ser víctima? o
¿Responder al atacante?

¿Qué es Cytomic?_

Cytomic es una nueva unidad de Panda Security. Su **propuesta de valor diferenciada,** se construye por encima de esta, combinando soluciones de seguridad y servicios gestionados para un eficiente **hunting de amenazas y respuesta a incidentes** en la protección de ordenadores, servidores, entornos virtuales y dispositivos móviles.

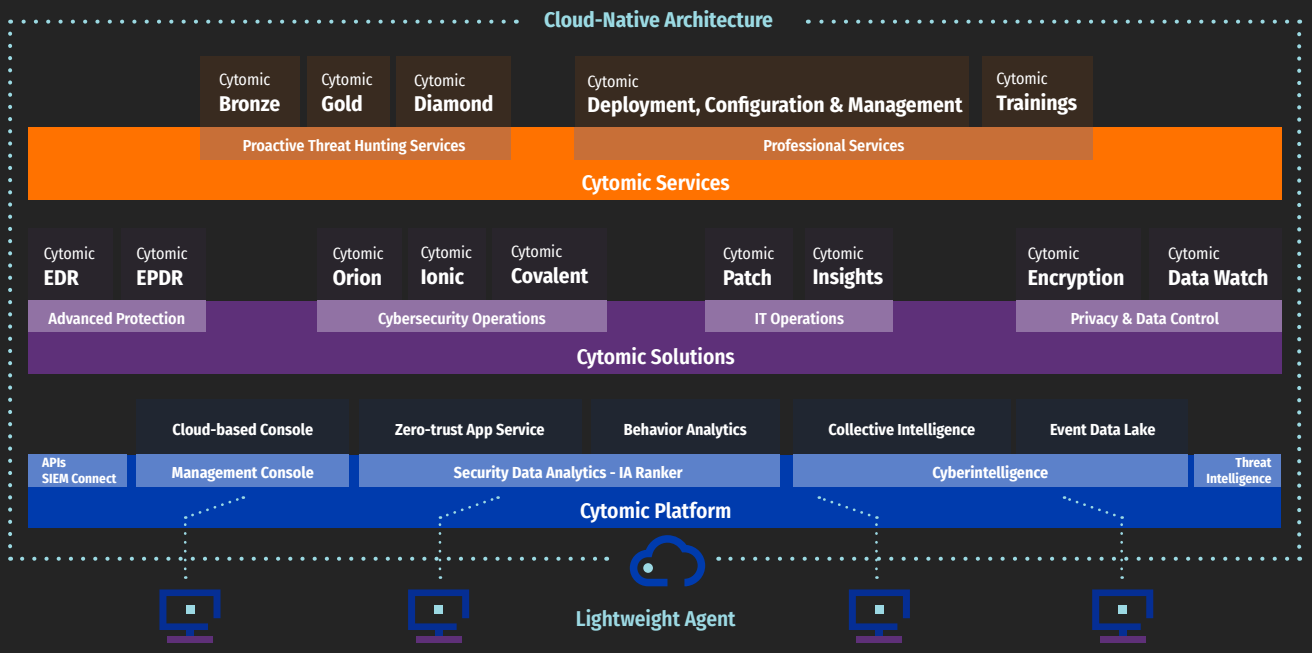
Su compromiso es el de apoyar a las organizaciones en su proceso de **maduración hacia un programa de seguridad avanzada,** con su propio equipo de seguridad y respuesta a incidentes o delegándolo en su proveedor de servicios de seguridad (MSSP, SOC, MDR y CSIRT).

Además, Cytomic acompaña activamente a estos proveedores especializados dotándolos de plataformas y herramientas EDR, únicas en el mercado, que les permita **expandir su portfolio a servicios de hunting, detección y respuesta a incidentes** en tiempo reducido.

Cytomic aprovecha el modelo de seguridad de Panda Security, que neutralizan proactivamente ciber ataques que instrumentalizan cualquier tipo de malware, exploits, o exhiban comportamientos anómalos en el endpoints. **Sobre ello,** ofrece un **framework** de soluciones y servicios focalizados en:

- **Descubrir atacantes utilizando técnicas living off the land y malwareless,** en su intento de evadir los control existente y comprometer a la organización.
- **Acelerar el proceso de investigación, mitigación y respuesta en el endpoint.** Acciones que, de otra forma, el SOC debe de acometer a ciegas y de forma manual, costosa e ineficiente, antes una situación de crisis.

Portfolio de Cytomic_



PROPUESTA DE VALOR_

Mayor eficiencia de SOC, menor MTTD y MTTR

- **Monitorización y visibilidad** en tiempo real.
  - **365 días** de visibilidad, telemetría enriquecida.
  - Cero compromisos con ataques malware gracias al **Zero-Trust Application Service.**
  - **Threat Hunting** Serivce incluido en los productos.
  - Detección de **comportamientos anómalos.**
  - Bloqueo de ataques con **exploits.**
  - **Búsqueda de IOCs** retrospectiva y en tiempo real.
  - **Alertas** avanzadas priorizadas y mapeada al **framework de MITRE ATT&CK.**
  - Herramientas de **hunting, detección** de anomalías, **triaje** e **investigación** con **analítica de datos a escala pre-creados.**
  - **Contención y remediación** masiva y remota.

Cooperación del stack tecnológico del SOC

- **Arquitectura API-First** que habilita:
  - La **integración** en el stack del SOC
  - La **automatización** de casos de uso hasta la remediación en el endpoint
- **Investigación integral en el SIEM o delegada a la plataforma Cytomic,** especializada en analítica endpoint a escala.
- **Respuesta a Incidentes integral desde el SOC:** Endpoints accionables desde la plataforma Cytomic o desde cualquier elemento del stack.

Menor TCO en ciberseguridad

- **Plataforma única** en la nube. **Agente único ligero.**
- Sin servidores, ni personal de mantenimiento.
- Despliegue en segundos. Coste mínimo de implantación.
- Menor coste del cibercrimen, al incrementar la eficiencia en prevención, detección, contención y recuperación de incidentes.
- Facilita el análisis de la causa raíz, y la mejora continua de la postura de seguridad.

Detección proactiva. Hunting de amenazas

- **Servicios incluidos por defecto en los productos:**
  - **Zero-Trust Application Service.**
  - **Threat Hunting Service.**
- Adicionalmente, **servicios gestionados Threat Hunting.**
- Servicio de **Telemetría en el SIEM** corporativo.