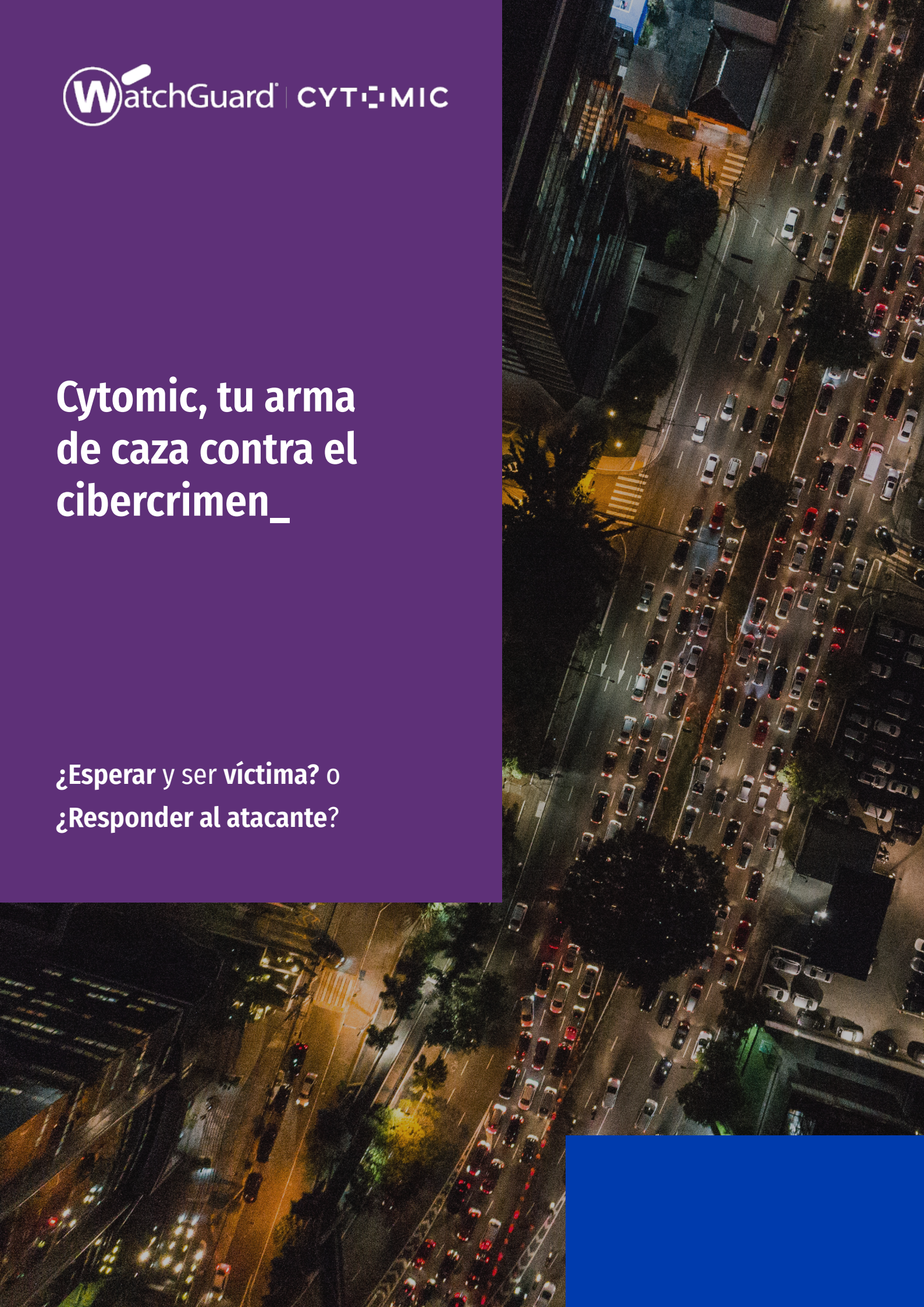
WatchGuard | CYTOMIC

Cytomic, tu arma de caza contra el cibercrimen_

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



WatchGuard Cytomic

No hay duda, la situación del cibercrimen actual es extremadamente grave. Los datos revelan un **aumento en número (+11% anual) y sofisticación de ataques y costes empresariales ocasionados (€550 mil millones).** Aunque el incremento de la inversión en ciberseguridad **(+9,8%, €+100 mil millones)**, se ha traducido en un mayor nivel de prevención, la seguridad total no existe: **ya no es suficiente con "sentarse y esperar" al atacante.**

Cibercrimen más sofisticado y numeroso_

↑11 %
Incidentes de Seguridad en 2019[1]

39s
Segundos entre un Ciberataque y otro a nivel mundial[2]

2.244
Ciberataques diarios [3]

Mayor coste del Cibercrimen_

550 € Mil Millones
Coste global del Cibercrimen en 2019[4]

71%
De los ataques fueron por motivo económico[5]

25%
De los ataques fueron con intenciones de espionaje[5]

Mayor presupuesto para combatir el Cibercrimen_

↑100 € Mil Millones
Gasto global en ciberseguridad 2019[6]

981€
Gasto medio en ciberseguridad por empleado[7]

50%
Del presupuesto en 2020 se destinará a servicios gestionados[7]

Esta realidad impulsa a las empresas a adoptar un **modelo de búsqueda activa y caza de amenazas,** y evolucionar sus **programas de seguridad avanzadas** combinando:

- **Estrictas medidas preventivas** con una exhaustiva reducción de la superficie de ataque, y un estricto gobierno de ejecución de aplicaciones.
- **Robustas capacidades proactivas de detección y respuesta** ante incidentes ocasionados por atacantes que han conseguido superar los controles existentes.

Cytomic y su portfolio de soluciones y servicios gestionados ayudan a estas organizaciones y a sus proveedores de servicio, en el desarrollo y automatización de sus programas de seguridad avanzada:

- **Evolucionando su equipo de seguridad, con experiencia, tecnologías y procesos, que les permita detectar contener y responder eficientemente, al atacante en la red.**

  En este proceso, el equipo de seguridad de la organización puede ser ya altamente especializado y maduro, mientras que en otras, la organización delega en su proveedor de servicios MDR (Managed Detection and Response), totalmente o parcialmente.

- **Adoptando servicios de Threat Hunting gestionado**

  Los servicios gestionados de threat hunting están diseñados para llenar el vacío en organizaciones sin los perfiles adecuados. En este escenario, el proveedor externo con experiencia, recursos, tecnologías y procesos es responsable de descubrir proactivamente indicios de actividad del atacante en la red.

WatchGuard | CYTOMIC

Retos en la evolución del programa de seguridad_

Varios son los retos a los que se enfrentan las organizaciones y sus **equipos de Seguridad (SOC) y respuesta a incidentes (CSIRT)** a la hora de implantar o robustecer su programa de seguridad:

Falta de expertos en ciberseguridad

En el 2021 habrá 3,5 millones de empleos de ciberseguridad sin cubrir a nivel mundial[8]. Como consecuencia, muchas organizaciones, que no dispondrán de estos equipos especializados, serán altamente susceptibles de ser atacados. afectando directamente a sus estrategias de transformación y a sus resultados empresariales.

El efecto “Fatiga” genera ineficiencias

Los SOCs se sienten abrumados con numerosas soluciones de seguridad que gestionar (Platform Fatigue), teniendo que dividir su tiempo y atención entre diferentes programas, sensores, fuentes de datos, logs y alertas sin filtrar o priorizar (Alert Fatigue). Hay demasiados lugares y elementos que analizar cuidadosamente para detectar amenazas, una situación que dificulta la eficiencia operacional e incrementa el riesgo.

Tiempo de detección y respuesta insuficientes

A medida que los ataques continúan aumentando en frecuencia y sofisticación, las organizaciones pasan innumerables horas identificando amenazas maliciosas manualmente. En el mejor de los casos, esto es un proceso largo, dando tiempo a los ataques a extenderse por toda la organización y causar daños.

Por todo ello, es crítico fortalecer los equipos de seguridad con **servicios gestionados o plataformas de seguridad** que automaticen la detección y la respuesta y orquesten el proceso de Incident Response entre los sistemas, minimizando el impacto en la organización.

47 %

De las alertas de seguridad se ignoran[9]

197 días

Es el tiempo que se tarda en identificar a un atacante en la red (MTTD Global) [10]

266 días

Es lo que se tarda en tomar medidas de contención al atacante (MTTR Global) [10]

En lugar de esperar para remediar los incidentes, los equipos de seguridad **deben hacer uso de la telemetría de los EDRs** para, proactivamente, buscar amenazas identificando **comportamientos sospechosos** y fuera de la política de seguridad

WatchGuard | CYTOMIC

¿Qué es WatchGuard Cytomic?

WatchGuard Cytomic es una nueva unidad de WatchGuard. 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 ciberataques que instrumentalizan cualquier tipo de malware, exploits, o exhiban comportamientos anómalos en el endpoint. **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.

Analítica de datos a escala_

La plataforma, está optimizada para prevenir ataques, detectar, investigar y responder a incidentes. Procesa en tiempo real, con diversos algoritmos y técnicas de IA, grandes volúmenes de eventos y atributos de la monitorización exhaustiva de actividad en los endpoints.

El equipo Experto en ciberseguridad de Cytomic supervisa la plataforma y sus resultado.

+70.000 — **Millones de eventos a la semana**

+10.000 — **Millones de eventos al día**

3 Billones — **De eventos en el Data Lake**

2 Millones — **De nuevos binarios clasificados a la semana**

300 Mil — **Nuevos binarios clasificados al día**

365 — **Retenciones de eventos al día**

La plataforma Cytomic_

La propuesta de valor de Cytomic se fundamenta en las capacidades de procesamiento a escala de su plataforma nativa en la nube y extensible mediante su API.

WatchGuard | 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

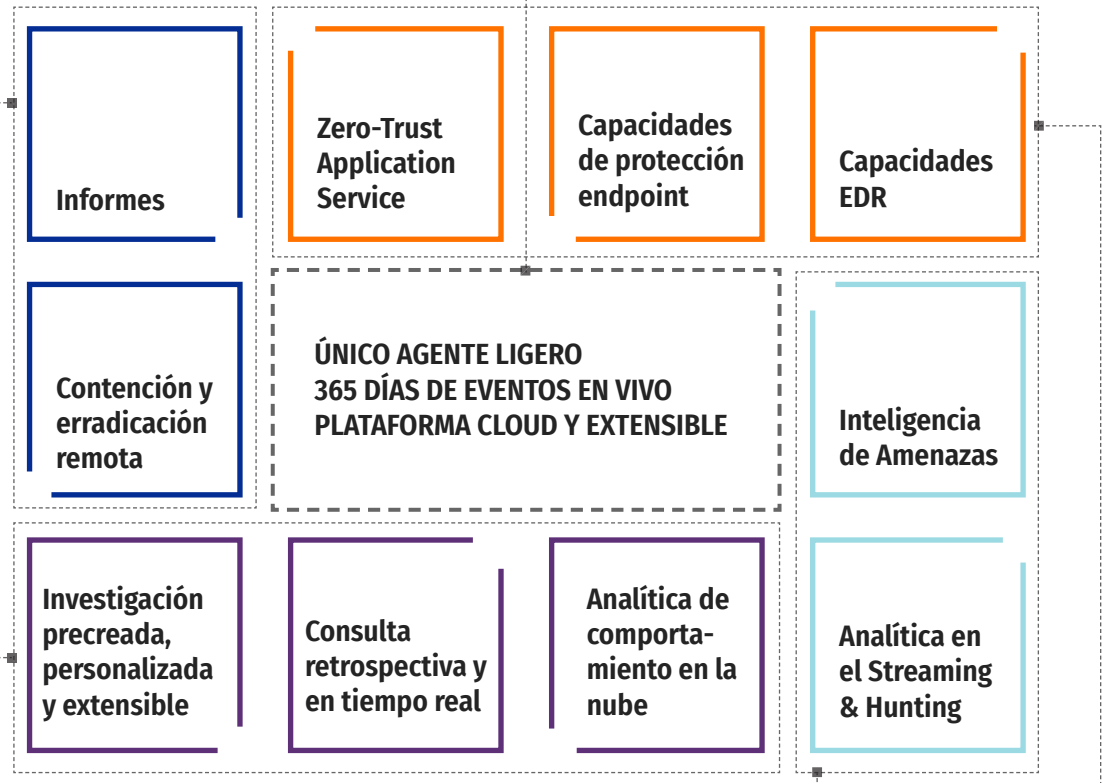
- **Servicios incluidos por defecto en los productos:**
  - **Zero-Trust Application Service.**
  - **Threat Hunting Service.**
- Adicionalmente, **servicios gestionados Threat Hunting.**
- Servicio de **Telemetría en el SIEM** corporativo.

Capacidades de la Plataforma Cytomic_

- **•Herramientas de triaje, de investigaciones automatizadas o guiadas**
- **• Jupyter Notebooks: Investigaciones preconstruidas y extensibles**
- **• Librería propietaria de threat hunting y analítica**

- **• Contención y respuestas en el endpoint** desde la nube
- **• Jupyter Notebooks: plantillas de informes reutilizables y auto-explicativos**

- **• Único agente ligero**
- **• Telemetría** filtrada, normalizada y contextualizada
- **• Telemetría** disponible 365 días. Hunting e investigaciones **en tiempo real y retrospectivo**
- **• Plataforma Cloud:** Menor coste, mayor rendimiento con entrega cloud 24/7
- **• Arquitectura API-First** que fomenta el intercambio de datos y acciones en el stack del SOC

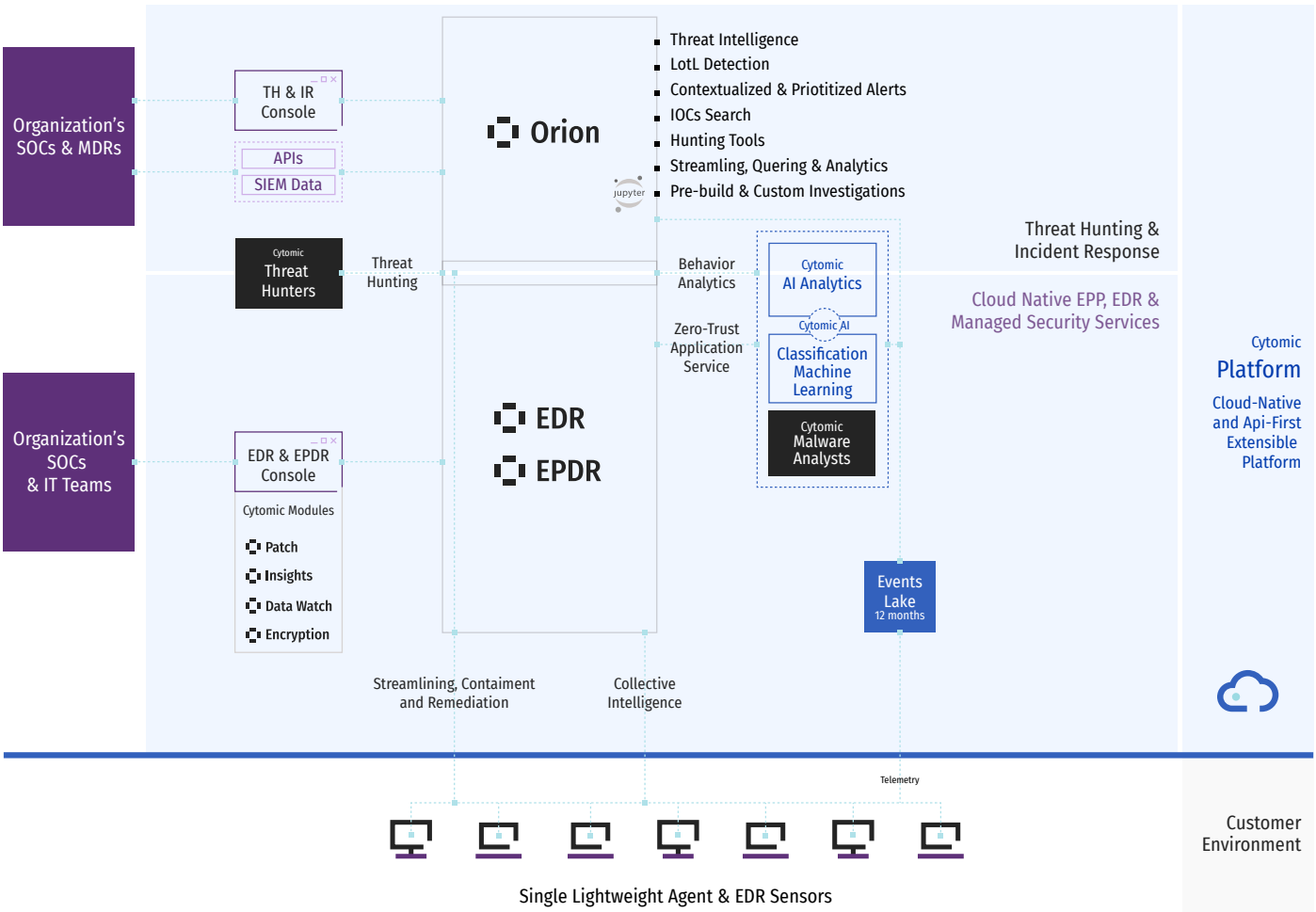


- **• Inteligencia de amenazas Cytomic** y **fuentes públicas** y otros organismos (CERTs, CTA, etc)
- **• Detección de TTPs** basado en conocimiento propio y de terceros (MITRE, etc)
- **• Alertas contextualizadas** y **priorizadas**
- **• Herramientas de Threat Hunting** que acelera el descubrimiento otras actividades anómalas

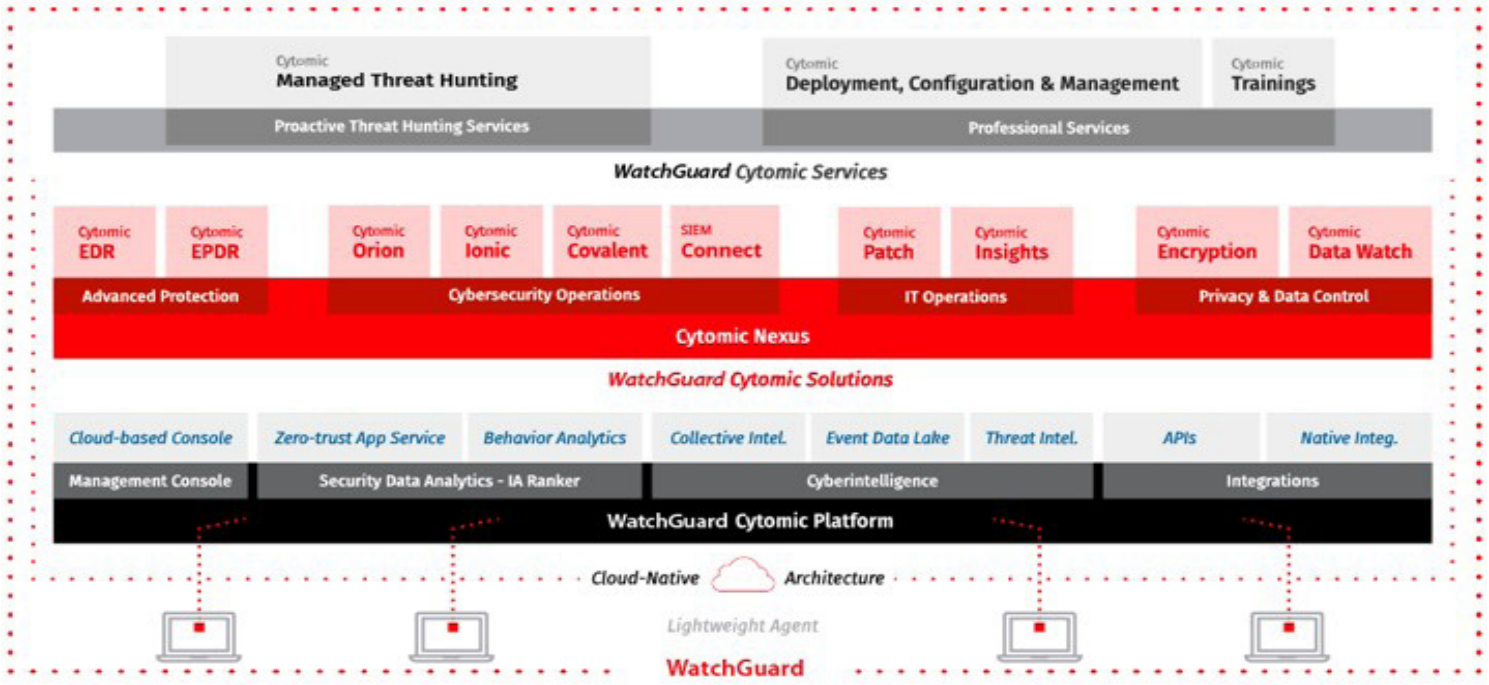
- **• Detección y prevención en el agente**
- **• Análisis de comportamiento anómalo determinista en el endpoint**
- **• Zero-Trust Application Service** deniega la ejecución de cualquier malware
- **• Reducción de la superficie de ataque:** Políticas avanzadas
- **• Búsquedas** retrospectivas y en tiempo real de **IOC y reglas Yara**

WatchGuard | CYTOMIC

Plataforma de Cytomic_



Portfolio de WatchGuard Cytomic_



WatchGuard | CYTOMIC

El Servicio Zero-Trust Application_

El servicio **Zero-Trust Application,** habilita un modelo de seguridad **"deny-all"** desatendido, sin alertas, ni delegación y sin penalizar la operativa de la organización.

En este modelo **las aplicaciones maliciosas, no son ya un vector de ataque exitoso para los adversarios.**

En las soluciones de seguridad avanzada en el endpoint de Cytomic, se deniegan la ejecución de toda aplicación que no haya sido anteriormente verificada y certificada por el servicio, e incluso si lo estuviera, su actividad es estrechamente vigilada para identificar comportamientos maliciosos

De esta forma, el servicio **rompe definitivamente la cadena del ataque,** sin importar la naturaleza del malware. Se erradican troyanos, gusanos, virus, etc y por supuesto los devastadores ransomware.

El servicio **Zero-Trust Application** combina diferentes tecnologías a escala en la plataforma, alojada en la nube de Cytomic.

Estas abarcan desde la **Inteligencia Colectiva,** un repositorio de conocimiento de aplicaciones legítimas y maliciosas, que es continuamente alimentada con nuevo conocimiento externo e interno, procedente de los millones de endpoints protegidos; hasta un **sistema basado en Inteligencia Artificial en la nube a escala,** donde se ejecutan diversos algoritmos de clasificación, desde los más sencillos, como algoritmos de similaridad y árboles de decisión, hasta los más complejos, como redes neuronales y modelos de deep learning.

El sistema procesa en tiempo real cientos de atributos estáticos, de comportamientos y contextuales de cada binario.

Todo ello bajo la supervisión de un **equipo humano expertos en malware y con años de experiencia en entornos heterogéneos.**

Las **aplicaciones maliciosas**, no son ya un vector de ataque exitoso para los adversarios, tras ser inspeccionadas y clasificadas por el Servicio Zero-Trust Application

Los equipos de seguridad de las organizaciones se benefician de este servicio, al filtrar automáticamente ataques con malware y poder centralizar sus esfuerzos en atacantes sin malware, y el análisis a escala de comportamientos anómalos en la red.

300.000 **Aplicaciones nuevas al día**

4 horas **Clasificación en menos de 4 horas**

8x5 **Ventana de servicio 8x5 CET**

WatchGuard | CYTOMIC

Las claves de las técnicas de ataque **Living off the land_**

Los ataques con técnica living off the Land (LotL) hacen uso de lo que ya existe en los dispositivos y servidores de la organización, no necesitan descargar o instalar ningún artefacto propio, lo que las hace extremadamente sigilosas.

Cinco son, los tipos principales de LotL:

- Herramientas de doble uso, como PowerShell o PsExec.
- Amenazas que se ejecutan en la memoria.
- Ataques sin archivos, como el código VBS en el registro.
- Ataques en archivos no ejecutables, como documentos de Office con macros y comandos.
- Ataques que usan binarios de Windows (como WMI) para ejecutar actividad maliciosa, los denominados LoLBins.

¿Qué ventajas ofrecen a los atacantes?

- Entran libremente a través de puntos de entrada seguros.
- No despiertan sospechas en ninguna de las fases del ataque: entrada, movimiento laterales, etc.
- Son difíciles de identificar, ya que se confunden con usos legítimos.
- Requieren muy pocos recursos y hay pocas barreras para ejecutarse.
- No requieren crear, comprar y desplegar nuevas aplicaciones maliciosos.

Las **soluciones avanzadas de seguridad y los servicios gestionado de Cytomic** monitorizan, vigilan y procesan a escala la actividad en los endpoints en busca de patrones anómalos fuera de los perfiles.

Junto con las **tecnologías,** el elemento humano de los **hunters y los analistas expertos de Cytomic,** es crítico para poder adaptarse a la evolución de los adversarios y las nuevas técnicas tanto en aplicaciones maliciosas como el técnicas LotL.

¿Cómo evitar los ataques de LotL?

- Limitar el uso de lenguajes de script. Si no es posible prescindir de ellos, reforzar las alertas.
- Monitorizar constantemente y detalladamente. De esta manera, se pueden descubrir actividades anómalas, antes de que ponga en peligro a la organización.
- Disponer de equipos de Operaciones de Seguridad (SOC/CSIRT) que ejecuten el programa de Incident Response de la organización. El SOC filtra las alertas de actividad anómala, investiga rápidamente las críticas y responde al atacante antes de que genere el daño. Además, una vez recuperado de la crisis, analizar el atacante para desarrollar nuevas medida de reducción de superficie de ataque, produce una mejora de la postura de seguridad de la organización.
- Disponer, además, de Threat Hunters que, liberados de los procesos cotidianos de Operaciones de Seguridad, puedan enfocarse en detectar evidencia de intrusos que hayan podido evadir todos los controles preventivos o de detección, en la organización. Los Hunter incluyen estos comportamiento maliciosos en el proceso de SOC para su detección en el futuro.

Evitar lenguajes de scripting

Monitorización y seguimiento

Servicios de Threat Hunting

Ciberresiliencia

WatchGuard | CYTOMIC

El Servicio Threat Hunting_

El servicio **de Threat Hunting incluido por defecto en todas las soluciones endpoint de Cytomic,** detecta atacantes que utilicen técnicas 'Living off the Land' en cualquiera de sus fases de la cyber kill chain.

El equipo de **Expertos en Ciberseguridad de Cytomic** gestiona y supervisa el servicio con las tecnologías y capacidades que ofrece **Cytomic Orion.**

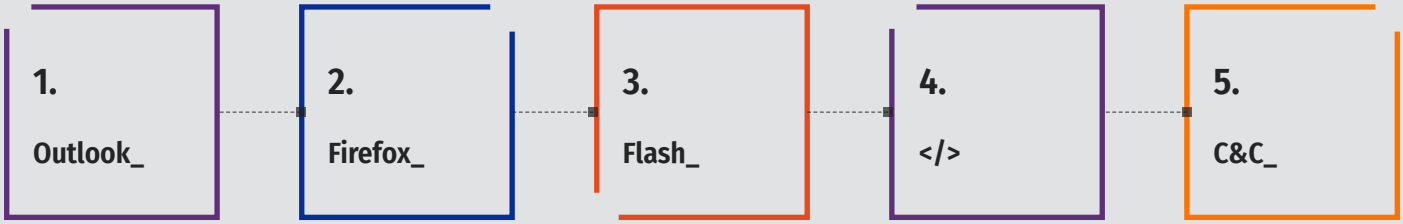
El **Cytomic Cybersecurity Team** (CCST) investiga los Indicios de ataque generadas en la plataforma al encontrar, en el streaming de eventos, patrones de **técnicas de evasión y compromiso (TTPs).**

Por otro lado, y **"asumiendo siempre el compromiso",** los Hunters de este equipo buscan proactivamente patrones de **comportamientos anómalos** no identificados anteriormente en la red. Para ello, crean reglas avanzadas de hunting, como **hipótesis** de trabajo, que son evaluadas contra la telemetría recogida en **tiempo real** e **histórico de 365 días**.

En el caso de encontrarse una situación anómala, **el cliente es proactivamente contactado** por el equipo, aportando un **análisis forense** de los sistemas afectados, el origen del ataque y las técnicas utilizadas, así como **recomendaciones** de como mitigar el ataque y reducir la superficie de ataque para evitar ser víctima de futuros ataques.

Las empresas deberían asumir que ya están comprometidas, **no existe una protección que cubra el 100% de las técnicas de ataque** y comportamientos anómalos presentes y futuros

Cientos de TTPs y reglas avanzadas de Hunting son evaluadas continuamente sobre el streaming de eventos de los endpoints



1. Un usuario visita una web usando Firefox desde un email de phishing
2. En esta web hay cargada una versión vulnerable de flash
3. Flash llama a PowerShell e introduce líneas de comando, operando desde la memoria
4. PowerShell se conecta a un servidor de comando y control sigiloso donde descarga un script de PowerShell malicioso que busca información sensible y se lo envía al atacante
5. Este ataque no descarga ningún malware en ningún momento, pero compromete la organización usando técnicas Living-off-the-land

Nuestro CyberSecurity Team_

Unidad de Security Data Science_

La unidad es responsable del servicio Zero-Trust Application, donde el sistema de Machine Learning a escala en la nube, asegura la clasificación del 100% de los binarios descubiertos.

Además, maximizan los resultados del proceso de Threat Hunting, aplicando técnicas de Machine Learning &Deep Learning, a los más de 10K millones de eventos diarios que procesa la plataforma, automatizando el análisis a partir de las anomalías identificadas, en forma de Jupyter Notebooks pre-creados, flexibles y reutilizables.

Unidad de especialistas en amenazas_

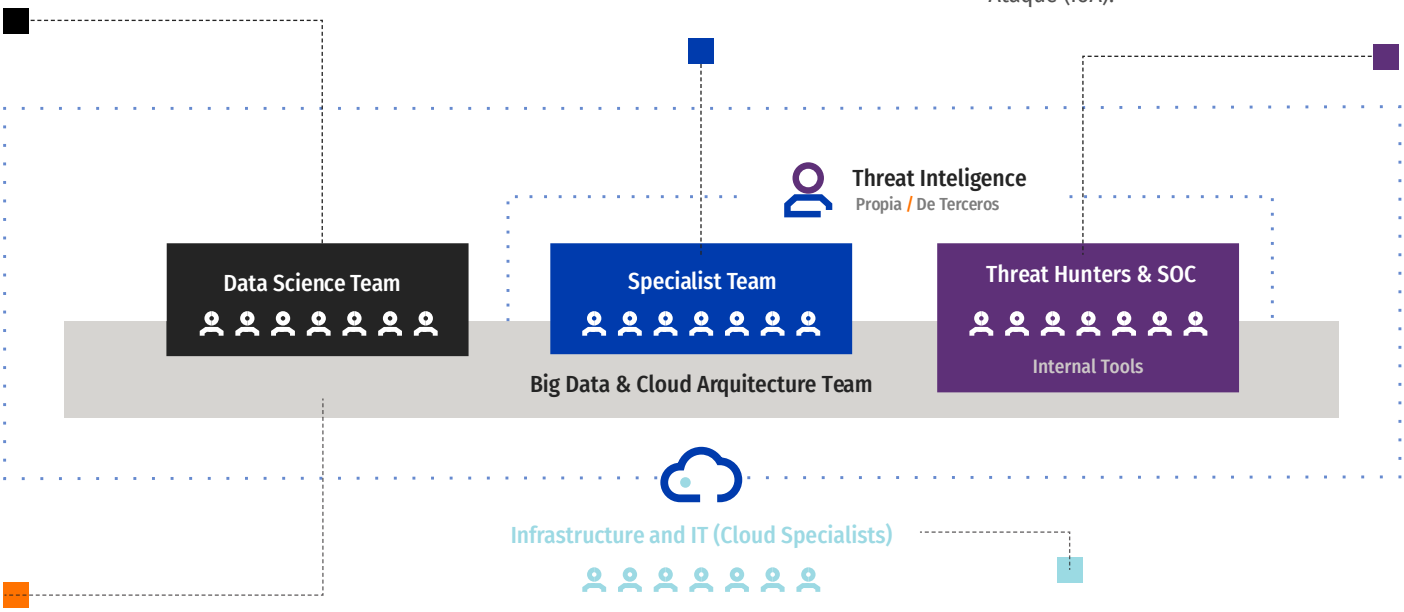
Los especialistas son miembros claves que apoyan al resto de unidades con su profundo conocimiento de amenazas y técnicas específicas de ataque. El equipo cuenta con expertos en:

- **Reverse engineering.**
- **Análisis avanzados sobre artefactos y TTPs.**
- **Análisis de fuentes de Threat Intelligence.**
- **Especialistas en explotación de vulnerabilidades.**

Hunters y equipo de operaciones_

Buscan proactivamente comportamientos anómalos, investigan y notifican a los clientes de cualquiera de los servicios de Threat Hunting de Cytomic.

Los Threat Hunters, son analistas de seguridad expertos que detectan nuevos ataques o principios de ataque en los clientes de Cytomic, operando Cytomic Orion, lo que les permite investigar en data lake de eventos de 365 días con un gran nivel de profundidad y detalle.
El equipo de operaciones de seguridad, gestiona las anomalías de comportamiento (TTPs) e Indicadores de Ataque (IoA).



Unidad de aplicaciones y Notebooks específicas para otras unidades_

Esta unidad sirve al resto de unidades y especialmente al SOC y los threat hunters cuando, por ejemplo: se requiere de un nuevo sensor en los endpoints, o una nueva regla de detección, o un método nuevo en la librearía de threat hunting que habilite la detección una nuevas técnica de evasión.

Unidad de especialistas en Big Data & Cloud_

La plataforma Cytomic se caracteriza por soportar inmensos volúmenes de eventos (70.000 millones a la semana) que deben ser procesados en tiempo real por complejos algoritmos de Machine Learning, además de ser almacenados en caliente durante 365 días para su procesamiento masivo y acceso puntual en las investigaciones. La unidad utiliza las últimas tecnologías de big data en la nube para que los servicios cumplan con los niveles preestablecidos.

WatchGuard | CYTOMIC

Orion_

Anticiparse a los adversarios, con analítica y visibilidad en tiempo real, es posible

Conseguir la eficiencia en la detección de amenazadas avanzadas, está directamente relacionada con la cantidad y la calidad de eventos monitorizados en los endpoints, y a la capacidad de enriquecerlos con inteligencia y analizarlos a escala.

Cazar ciber atacantes requiere tomar estos datos estructurados de forma masiva y aplicar analítica de comportamiento, incluidos AI, y que su resultado guíe a los analistas en una investigación completa y en una actuación inmediata en los endpoints. **Esta capacidad está prácticamente fuera del alcance de muchas organizaciones.**

Cytomic Orion, **acelera la respuesta a incidentes** y búsqueda de amenazas malwareless en base a analítica de comportamiento a escala desde la nube.

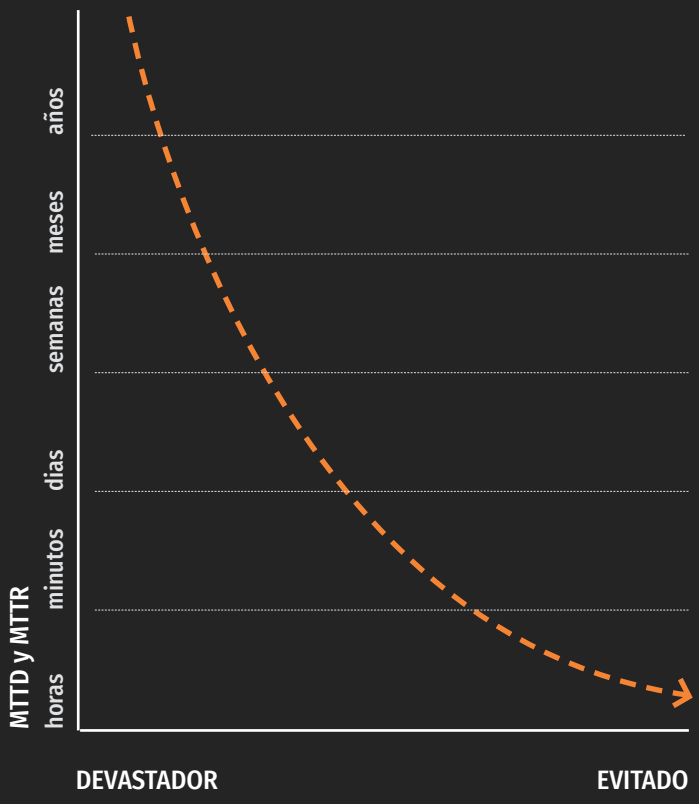
Es el componente analítico de la plataforma Cytomic, donde se automatiza la recopilación, enriquecimiento y filtrado de millones de eventos monitorizados de la actividad de los endpoints y su contexto. Sobre los que se aplican, junto con inteligencia de amenazas, cientos de algoritmos y reglas analíticas, en busca de comportamientos sospechosos o maliciosos en tiempo real y retrospectivo en 365 días.

Sus herramientas, consolas de trabajo y analítica preconstruida, como la librería de Threat Hunting y los Jupyter notebooks, permiten la búsqueda efectiva de amenazas, la investigación acelerada y la actuación sobre el endpoint inmediata, desde el primer día.

Las investigaciones preconstruidas, los Jupyter Notebooks, favorecen además una corta curva de aprendizaje de los analistas y hunters al ser auto explicativas, extensibles y repetibles.

Sus APIs y conectores permiten la integración bidireccional con el stack tecnológico del SOC, acelerando, todavía más, las capacidades de descubrimiento, investigación y actuación ante amenazas en la red corporativa.

El impacto de un incidentes es directamente proporcional al MTTD y MTTR



Cytomic Orion, ayuda a las organizaciones a cambiar su postura de **seguridad de defensiva a ofensiva y reducir el tiempo de investigación**, permitiendo a los analistas correlacionar rápidamente eventos y probar hipótesis.

Tiempo medio de detección (MTTD) *El tiempo medio que se necesita para detectar un atacante y que requiere esfuerzos adicionales de investigación y respuesta*

Tiempo medio de respuesta (MTTR) *El tiempo medio que se tarda en responder y en última instancia a resolver el incidente*

¿Qué capacidades del SOC se amplifican con Cytomic Orion?_

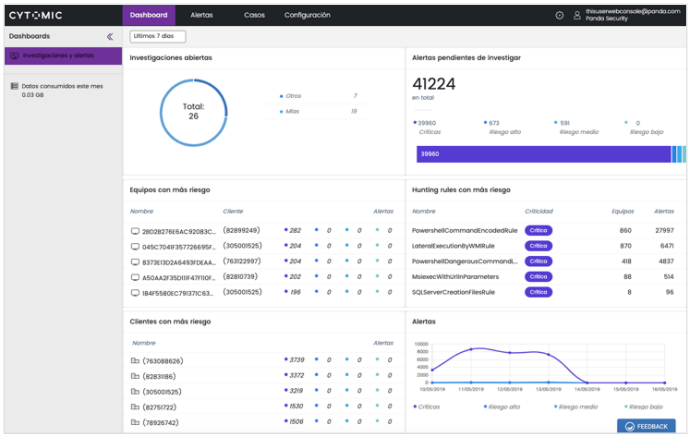
- Estar preparado ante un ataque y ejecutar el programa de Incident Response.
- Proceso ágil y continuo de caza, investigación, respuesta y mejora de la postura de seguridad.
- Caza de amenazas/Threat Hunting, con consulta avanzadas en el data lake de 365 días.
- Atribución y mapeo con cientos de TTPs del Framework ATTA&CK de MITRE.
- Búsqueda de IOCs en tiempo real y retrospectivo.
- Inteligencia de amenazas de la plataforma Cytomic y de fuentes externas.
- Maestría en investigaciones profundas y guiadas por las herramientas de la consola de Investigación.
- Automatización con las investigaciones pre-creadas con los Jupyter Notebooks.
- Contención y Remediación remota, a escala.
- APIs de integración con el stack tecnológico para el intercambio de información y procesos.
- Interoperatividad y automatización de los procesos en el stack tecnológico. Las APIs y conectores de la plataforma, fomentan el intercambio de información y procesos con el SOAR, SIEM, MISP, etc.

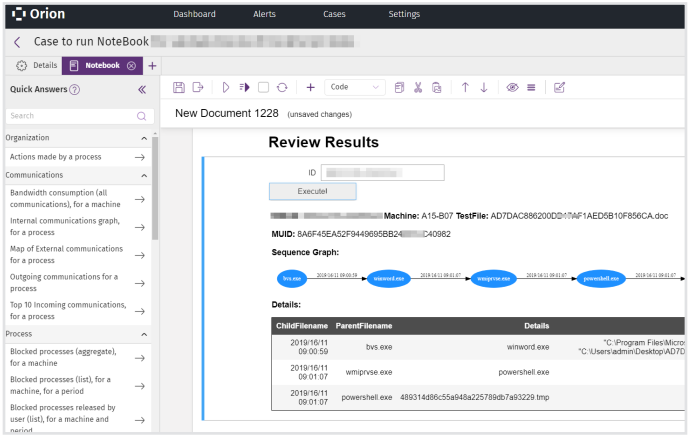
"Dado que la complejidad de los ataques, los proveedores de seguridad han desarrollado soluciones más flexibles con una mentalidad de "asumir el ataque".

Centrándose en las etapas de post-compromiso de la Cyber Kill Chain, con capacidades para detectar y responder a amenazas avanzadas de manera oportuna y efectiva."

Estas soluciones distinguen entre la actividad esperada y acciones anómalas que pueden indicar la presencia de una amenaza, un dispositivo comprometido o atacantes utilizando técnicas para ocultar su actividad bajo la apariencia de actividad "regular".

Paul Webber, Patreek Bhajanka, Mark Harris, Brad LaPorte
Analistas de Gartner (11)





La **consola de investigación** permite a los analistas analizar profundamente las evidencias. Los eventos enriquecidos con inteligencia de amenazas e información de seguridad patentada, las herramientas de correlación de eventos visuales y los árboles de procesos detallados incluyen otras capacidades, permiten a los analistas asignar rápidamente eventos a las secuencias de ataque.

Nuestros **Jupyter Notebooks** pre-creados, la librería de Threat Hunting y la consola de investigación, proporcionan visualizaciones de datos que aceleran las investigaciones.

Las ejecuciones, las conexiones de red, la correlación entre procesos, archivos y otros eventos permiten al analista del SOC investigar y reproducir un ataque, determinando en segundos el impacto y la causa raíz.

(11) Market Guide for Endpoint Detection and Response Solutions, 23 de diciembre de 2019. Paul Webber, Patreek Bhajanka, Mark Harris, Brad LaPorte.

WatchGuard | CYTOMIC

Integración de la plataforma Cytomic en el Stack tecnológico del SOC_

La integración en el stack tecnológico del SOC, donde este ya implementa su programa de respuesta a incidentes, acelera y habilita la automatización del proceso al permitir que las plataformas accedan a las capacidades de otras especializadas e independientes.

La integración de la plataforma Cytomic se realiza a través del conector SIEM y las APIs de integración.

365 días | Por defecto **"En caliente"**

Los IOCs y las Investigaciones se realizan en petabytes de eventos históricos de hasta 365 días

Beneficios de la integración del stack tecnológico del SOC:

Visibilidad unificada y cooperación

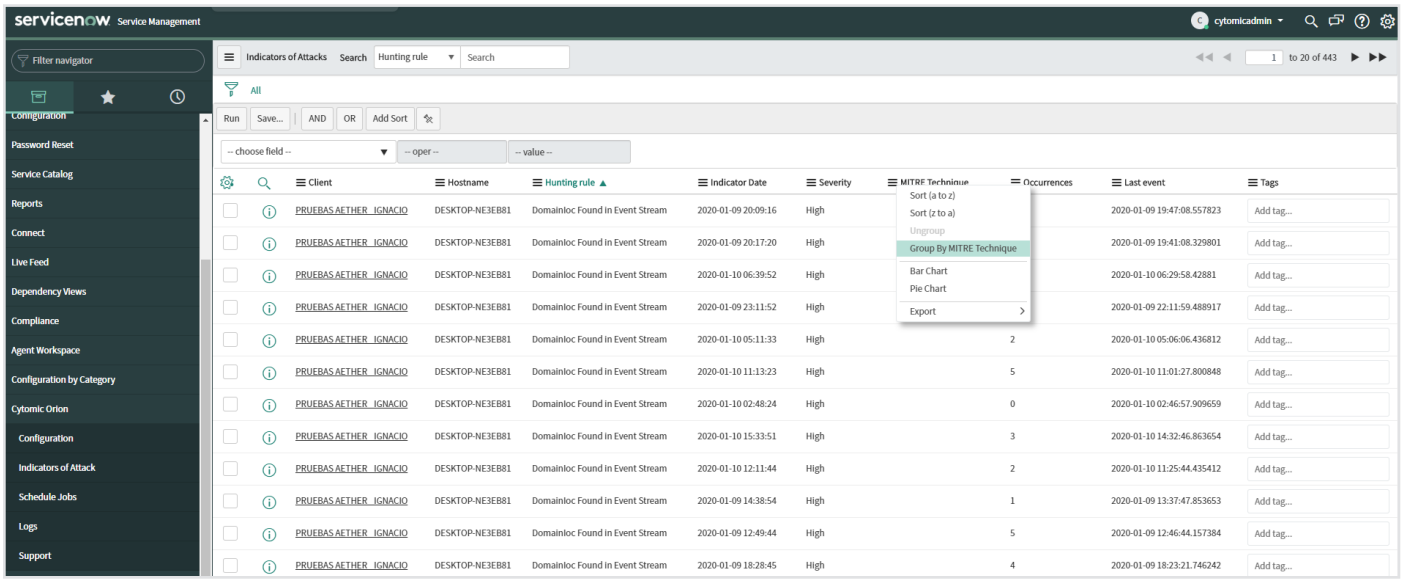
Permite correlacionar y coordinar fácilmente entre múltiples productos y extraer más valor de lo invertido en seguridad por las organizaciones. Enriquece la información de contexto del incidentes y permite descargar en la plataforma Cytomic los petabytes de datos necesarios para una investigación, que de otra forma se duplicación en otras soluciones, como el SIEM.

Rápida respuesta a incidentes

Proporciona a los analistas herramientas de actuación sincronizadas en toda la infraestructura, desde el perímetro, hasta la red y en particular los endpoints, que son los activos más afectados en un ciber ataque.

Coordinación entre los equipos de seguridad y de operaciones de IT

Los analistas de seguridad y los miembros de IT deben coordinarse para evitar y mitigar los incidentes, reduciendo la superficie de ataque y conteniendo y remediando cuando estos se producen. La integración de herramientas permite una respuesta coordinada y automátizada al generar alertar en las herramientas de ambas áreas.



Integración de los Indicios de Ataque de Cytomic Orion en la consola de Service Now mediante Integración con la API de Cytomic

WatchGuard | CYTOMIC

Cytomic **EDR_**

Cytomic EDR detecta y responde eficazmente a cualquier tipo de malware desconocido, y ataques sin archivos y sin malware, que las soluciones tradicionales no pueden detectar.

Se basa en el Servicio **Zero-Trust Application** que deniega la ejecución de cualquier binario hasta que se clasifiquen como de confianza.

Además, ofrece a los equipos de seguridad:

- Visibilidad total de las acciones de los adversarios.
- Sin impacto en los dispositivos y servidores ya que el agente es ligero y su arquitectura basada en la nube
- Detección de comportamientos anómalos en el endpoint (IOAs) bloqueando al atacante.
- Contención remotas desde la consola a los endpoints de forma masiva, como aislar o reiniciar equipos.

Cytomic EDR coexiste y complementa las soluciones de seguridad tradicionales.

Cytomic **EPDR_**

Integra en una única solución un stack completo de tecnologías preventivas en el endpoint, con capacidades EDR y el Servicio **Zero-Trust Application**.

Cytomic EPDR previene, detecta y responde a cualquier tipo de malware conocido y desconocido, ataques sin archivos y sin malware.

El Servicio Zero-Trust Application evita la ejecución de malware en los ordenadores, servidores, entornos virtuales y dispositivos móviles.

Extiende Cytomic EDR con una gama completa de capacidades de Protección Endpoint que siguen siendo necesarias para evitar que las amenazas lleguen a los dispositivos y servidores y reducir la superficie de ataque de estos.

	Cytomic EDR	Cytomic EPDR
Real-time endpoint monitoring	■	■
Lightweight cloud-based agent (Windows, Linux, Android, Mac, iOS)	■	■
Cloud-based big data Analytics	■	■
Zero-Trust App Service: Pre-execution, execution and post-execution	■	■
In-memory behavior anti-exploits	■	■
SaaS applications, such as Microsoft Office 365	■	■
Protection of systems when files are created		■
IDS, Firewall and Device Control		■
Web browsing and Email protection		■
Category-based URL filtering		■
Exchange server protection, antispam and content filtering		■

WatchGuard | CYTOMIC

Cytomic **Ionic_**

Coexiste y complementa las soluciones de seguridad tradicionales en el endpoint, con un conjunto completo de capacidades de EDR, y con Cytomic Orion, que permite a los equipos de seguridad (SOC) identificar, investigar y contener los actores maliciosos haciendo uso de técnicas living off the land, en la organización.

Además, Cytomic Ionic incrementa la efectividad del SOC e incrementa su escalabilidad, al beneficiarse del Zero-Trust application service que bloquea automáticamente cualquier ataque en el que se despliega un binario malicioso.

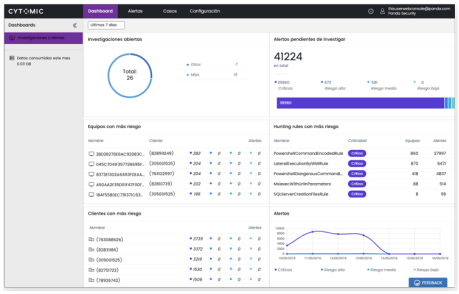
Esto hace que con Cytomic Ionic, la cantidad de incidentes a gestionar por el SOC es significativamente menor que cuando se utilizan otras soluciones EDR que no filtran todas las aplicaciones desconocidas que exhiben actividad maliciosa.

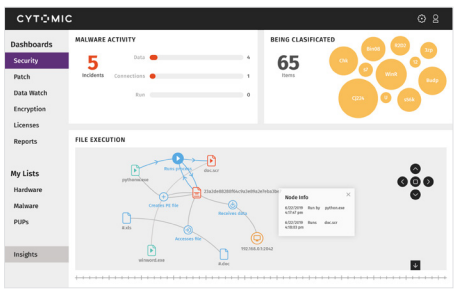
Cytomic **Covalent_**

Amplifica y extiende las capacidades preventivas y de detección de Cytomic Ionic con una gama completa de tecnologías de protección en el endpoint. Las capacidades de las soluciones EPP siguen siendo necesarias para evitar que las amenazas lleguen hasta o se ejecuten en los endpoints, así como para reducir su superficie de ataque.

Con Cytomic Covalent, incrementa por tanto la eficiencia y la escalabilidad del SOC al beneficiarse de una arquitectura integrada EPP y EDR junto con el Zero-Trust Application Service, que filtrar ataques basados en binarios maliciosos, incluso si son desconocidos y de las herramientas y servicios de Cytomic Orion, para acelerar la búsqueda, investigación y contención de actores maliciosos haciendo uso de técnicas living off the land.

La cantidad de alertas e incidentes a gestionar es significativamente menor que cuando se usa cualquier otra solución EPP o EDR que deja pasar al atacante cuando despliega y usa sus herramientas y aplicaciones maliciosas.





	Cytomic Orion	Cytomic Ionic	Cytomic Covalent
Threat Hunting Solution	■	■	■
Lightweight cloud-based agent (Windows, Linux, Android, Mac, iOS)		■	■
Real-time endpoint monitoring		■	■
Collective Intelligence lookups in real-time		■	■
Cloud-based big data Analytics		■	■
Zero-Trust App Service: Pre-execution, execution and post-execution		■	■
In-memory behavior anti-exploits		■	■
SaaS applications, such as Microsoft Office 365		■	■
Protection of systems when files are created			■
IDS, Firewall and Device Control			■
Web browsing and Email protection			■
Category-based URL filtering			■
Exchange server protection, antispam and content filtering			■

WatchGuard | CYTOMIC

Servicios gestionados de Threat Hunting_

Adicionalmente a las soluciones de protección endpoint, los servicios gestionados de Threat Hunting de Cytomic amplifican las capacidades de seguridad proactiva de las organizaciones que no dispongan de estos roles en sus equipos.

Estos servicios gestionados se especializan en descubrir comportamientos sospechosos típicos de técnicas de ataque malwareless y de buscar proactivamente comportamientos fuera de los habituales que pudieran ser Indicadores de Ataque.

Cuando estos indicios son destapados por los Threat Hunters de Cytomic, el cliente es notificado con información de contexto y recomendaciones de actuación. A partir de ese momento el cliente verifica y toma acciones en consecuencia, tanto para contener el ataque, como para realizar los cambios necesarios que reduzcan la superficie de ataque a futuros intentos de compromiso.

Los servicios de Threat Hunting gestionados extienden las capacidades propias de las organizaciones:

- Detectando de ciberataques en fase de reconocimiento, movimientos laterales, etc antes del despliegue de sus aplicaciones maliciosas.
- Sacando a la luz, aplicando analítica de datos, comportamientos anómalos de usuarios y equipos.
- Descubriendo los equipos que han sido comprometidos y las técnicas utilizadas.
- Relevando malas prácticas o configuraciones inseguras que pueden ser vectores de ataque.

	Cytomic Bronze
8/5 Offensive driven threat hunting	■
Cyber threats and living-off-the-land techniques email alerts	■
Monthly hunting reports	■

WatchGuard | CYTOMIC

Premios e Investigaciones_

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 gestionado de Hunting y con Cytomic Orion

Panda Adaptive Defense 360 — AV-Comparatives Single Product test — Panda Adaptive Defense 360

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

Tus datos te pertenecen_

Tus datos residen en la Unión Europea

El compromiso de Cytomic es mantener tus datos seguros.

Innovamos para proteger tus dispositivos, tus usuarios, tu información y tu privacidad. Y utilizamos los servidores más seguros para gestionar los datos de tu compañía.

Nuestros servidores están ubicados en Europa, bajo sus normativas y los estándares más estrictos de seguridad.

GDPR COMPLIANT

Más información en_
cytomic.ai

Contactanos en_
sales@cytomic.ai