DATASHEET

# Servicio Detección y Respuesta Gestionada (MDR) con **Palo Alto Networks® Cortex XDR™**

El Servicio de Detección y Respuesta Gestionada (MDR) de Entel Ocean, Cybersecurity Services, busca reducir los tiempos de detección de amenazas y respuesta ante incidentes. Nuestro servicio MDR fusiona la experiencia y experticia de nuestro equipo técnico con la tecnología de punta Cortex XDR de Palo Alto Networks, para ir más allá de las alertas de monitoreo.

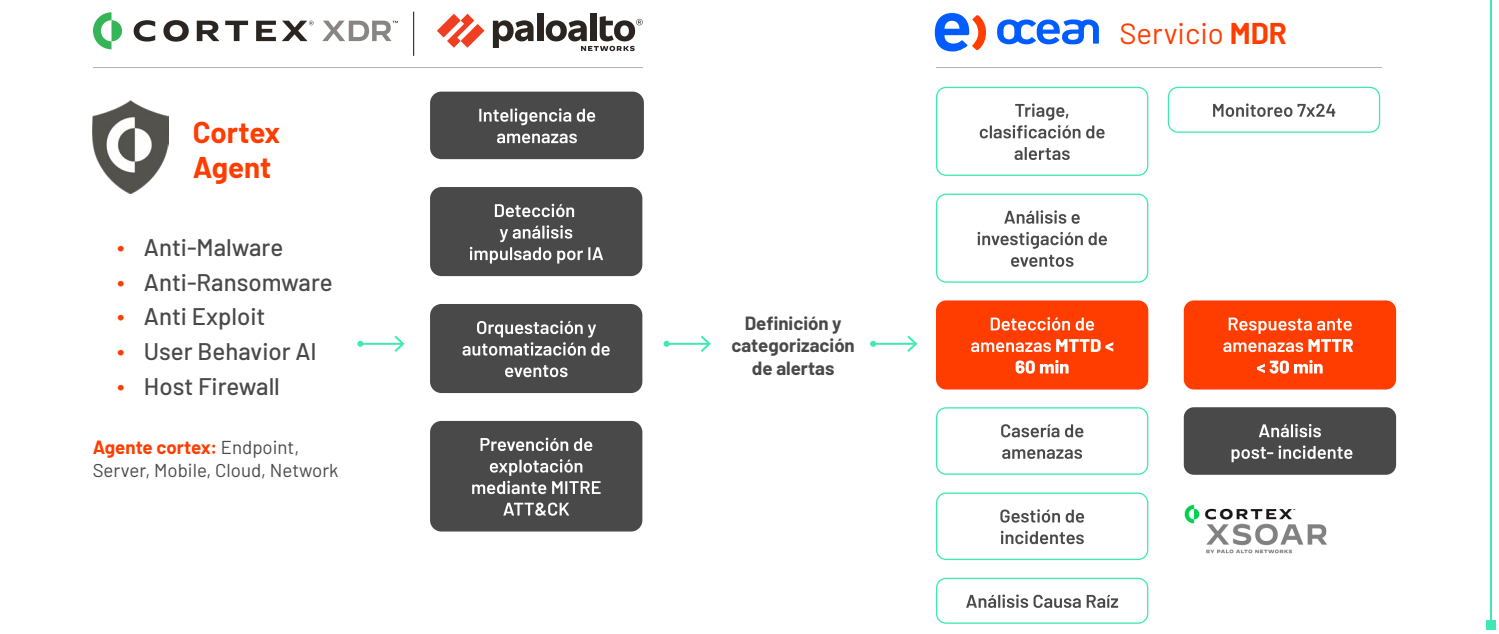
Damos visibilidad a nuestros clientes sobre los distintos tipos de ataques que se pudiesen materializar en su red, ya sea estaciones de trabajo, granjas de servidores, la nube, redes on-premise y dispositivos móviles, y así generar planes para contener ataques sofisticados, disminuir la exposición al riesgo, reducir la fatiga de las alertas y optimizar la eficiencia de los equipos SOC.

## Detección de amenazas y casería continua

La casería de amenazas forma parte fundamental del servicio, ya que permite profundizar en aquellas alertas no identificadas por Cortex XDR, las cuales son analizadas por nuestro equipo especialista, permitiendo actualizar los playbooks de remediación automática y apoyar a nuestros clientes a tomar una decisión más acertada a la hora de responder ante una amenaza.

## Beneficios Clave

- Equipo humano altamente especializado en análisis e investigación de amenazas.
- Categorización e Investigación de cada incidente 7x24.
- SLA garantizado: 60 minutos de detección y 30 minutos de respuesta.
- Creación y Optimización continua de Playbooks.
- Casería de amenazas proactiva en todo el ciclo del servicio.
- Reducción de fatiga de alertas del equipo SOC.
- Respuesta ante incidentes con soporte local presencial.
- Mejorar la postura de seguridad de la organización.



# ¿Cómo entregamos nuestro **servicio MDR?**

## Monitoreo Continuo

- **Visibilidad transversal:** Cobertura de todos los puntos finales de la red y la nube con monitoreo y análisis 24/7.
- **Gestión triage de incidentes:** revisión automatizada y manual para analizar detalles de alertas, incidentes y generar indicadores que permitan comprender el contexto y acciones de seguimiento.
- **Escalamiento de eventos y notificación:** escalamiento sobre incidentes que requieren mayor atención, empleando la metodología del framework MITRE ATT&CK.

## Casería de Amenazas Proactiva

- **Búsqueda de amenazas en todo el ciclo del servicio:** búsqueda basada en el análisis de comportamientos sospechosos, análisis Cortex XDR, reglas de detección personalizadas e investigación del Centro de Ciber Inteligencia (CCI) de Entel Ocean.
- **Inteligencia de amenazas:** integración de inteligencia de nuestro Centro de Ciber Inteligencia (CCI), basada en telemetría de nuestros clientes y diversas alianzas, así como detecciones de productos de Palo Alto Networks que permiten enriquecer las investigaciones.
- **Informes prácticos:** informes de amenazas que detallan el alcance, el origen y las herramientas de ataque de las amenazas detectadas, junto con las acciones recomendadas.
- **Asistencia directa:** Acceso al equipo de casería de amenazas para hacer preguntas y obtener orientación sobre las amenazas.

## Investigación y Respuesta Gestionada

- **Contención rápida de amenazas:** al detectarse una amenaza activa, los analistas realizaran rápidamente acciones de contención, aislando los puntos finales comprometidos y eliminando los archivos o procesos maliciosos mediante Cortex XDR.
- **Investigación y análisis:** realizamos nvestigación de endpoints, análisis artefactos de sistema y telemetría de la red y nube para identificar causa raíz y el alcance del incidente.
- **Rápida recuperación:** uso de Cortex XDR para eliminar archivos maliciosos, claves de registro y restaurar archivos dañados.

## Optimización y Mejora de la Postura de Seguridad

- **Estado de salud:** identificamos brechas sobre requisitos de hardening establecidos por la organización, mediante la definición de perfiles de seguridad en los endpoint, control de dispositivos, firewall de host y cifrado de disco.
- **Análisis de vulnerabilidades:** identificamos y cuantificamos las vulnerabilidades (CVE) de las aplicaciones que se encuentran instaladas en sus endpoint.
- **Inventario de hosts:** revisamos el inventario de hosts para identificar rápidamente cualquier problema de TI o de seguridad.

---

**Para más información:**
Visita nuestro sitio web

¿Quieres saber más sobre nuestro servicio de respuesta rápida y gestionada **MDR?**

Hablemos