CORTEX XDR

Detecte y detenga los ataques ocultos mediante la unificación de los datos de redes, endpoints y nubes.

Beneficios para la Empresa

- **Ataques ocultos descubiertos automáticamente:** Detectar continuamente amenazas con aprendizaje automático, analítica de comportamiento y reglas de detección personalizadas.
- **Fin de la fatiga y el desgaste por alertas:** Validar las alertas de seguridad en segundos mejora la productividad y el ánimo al reducir la sobrecarga laboral.
- **Mean Time To Identify (Tiempo Medio de Identificación – MTTI) reducido:** Combinar la detección precisa de ataques con la rápida evaluación de prioridades de alertas para reducir drásticamente el tiempo de espera.
- **Mean Time To Contain (Tiempo Medio de Contención – MTTC) reducido:** Investigar y responder a ataques externos y amenazas internas con precisión, sin años de experiencia.
- **Mayor Return of Investment (Retorno de la Inversión – ROI) de inversiones actuales con Cortex:** Resolver todas sus necesidades de seguridad a través de un ecosistema de aplicaciones confiables mientras se aprovecha la infraestructura existente como sensores y puntos de aplicación.

Derribe Silos para Simplificar Sus Investigaciones

Los equipos de seguridad suelen carecer de la visibilidad y la automatización requeridas para detener ataques. Las herramientas en silos como las de Endpoint Detection and Response (Detección y Respuesta de Endpoints – EDR) y Network Traffic Analysis (Análisis de Tráfico de Redes – NTA) recopilan grandes cantidades de datos, pero también obligan a los analistas a pasar de consola en consola para verificar amenazas mientras suman complejidad y demoran las investigaciones. Los equipos, que enfrentan la escasez de profesionales en seguridad cibernética, deben simplificar sus operaciones o lucharán por investigar y detener ataques.

Detecte, Investigue y Responda Rápidamente a las Amenazas

La solución de detección y respuesta de Cortex XDR integra de forma nativa los datos de redes, endpoints y nubes para detener ataques sofisticados. Aprovechar la analítica de comportamiento para identificar amenazas desconocidas y altamente evasivas dirigidas a sus redes. Los modelos de Machine Learning (Aprendizaje Automático – ML) y Artificial Intelligence (Inteligencia artificial – AI) descubren amenazas de cualquier origen, incluidos dispositivos administrados y no administrados.

Cortex XDR acelera la evaluación de prioridades de alertas y la respuesta ante incidentes al proveer un panorama completo de cada amenaza y revelar automáticamente la causa raíz. Al sincronizar los distintos tipos de datos y simplificar las investigaciones, Cortex XDR reduce el tiempo y la experiencia requeridos para cada etapa de las operaciones de seguridad, desde el análisis de prioridades hasta la caza de amenazas. La perfecta integración con los puntos de aplicación le permite responder rápidamente a las amenazas, así como aplicar el conocimiento obtenido de las investigaciones para detectar ataques similares en el futuro.

Protéjase Contra Amenazas Conocidas y Desconocidas con Traps

La verdadera seguridad comienza con una prevención blindada. La protección y respuesta de endpoints de Traps™, incluido con la solución Cortex XDR, utiliza múltiples métodos de prevención para proteger los endpoints contra malware, ransomware y exploits. Juntos, Traps y Cortex XDR ofrecen prevención, detección y respuesta consistentes a través de todos sus activos digitales. Su integración nativa con inteligencia de amenazas basada en la nube garantiza que la prevención sea coordinada a través de sus productos de seguridad de redes, endpoints y nubes.

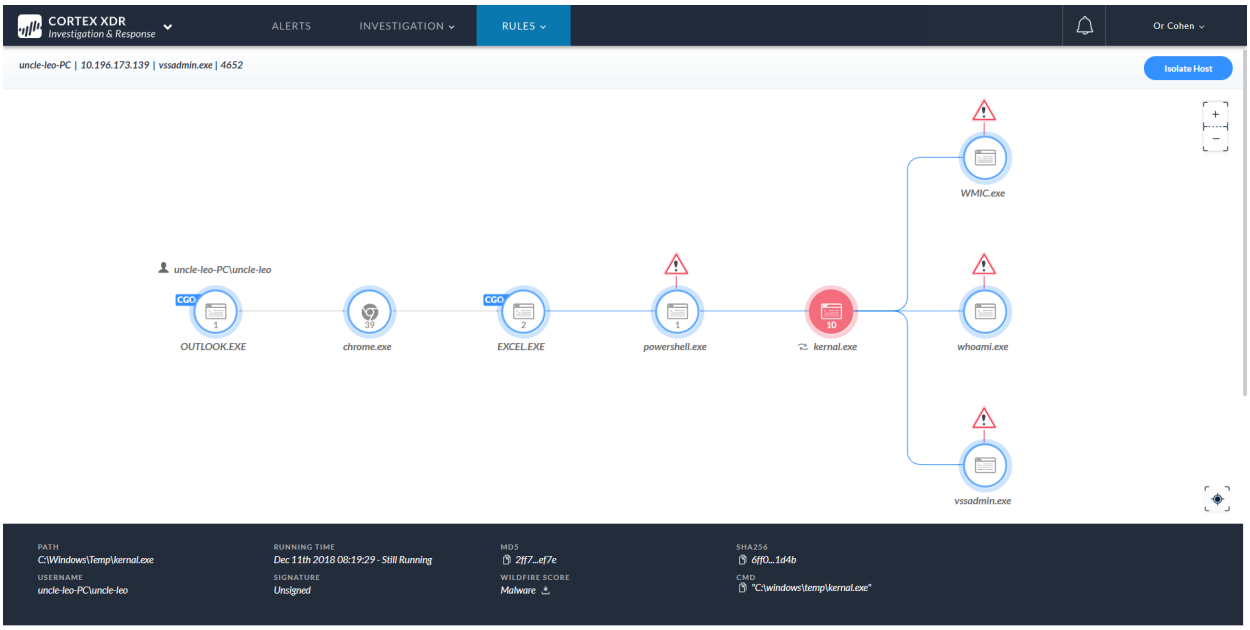

Figura 1: Panel de Gestión de Cortex XDR

Capacidades Clave

Obtener Completa Visibilidad

Correlacione datos de redes, endpoints y nubes para agilizar la detección y la respuesta. Cortex XDR permite ahorrar horas de análisis manual al correlacionar automáticamente los datos recopilados desde sus redes, endpoints y activos de nube. Sincroniza los distintos tipos de datos dentro de Cortex Data Lake, un almacenamiento de datos escalable y eficiente basado en la nube, para detectar los ataques con precisión y simplificar las investigaciones.

Automatizar la Detección de Ataques con AI

Busque amenazas ocultas con analítica de comportamiento. Cortex XDR señala automáticamente los ataques activos, permitiendo que su equipo evalúe las prioridades y contenga las amenazas antes de que se ocasione algún daño. Mediante el uso de aprendizaje automático, Cortex XDR perfila continuamente el comportamiento de usuarios y dispositivos para detectar actividades anómalas que indiquen ataques. A través de la evaluación de abundantes datos diseñados expresamente para analítica, Cortex XDR puede detectar ataques como robo de credenciales y amenazas en túneles DNS, que son prácticamente imposibles de identificar desde logs de amenazas estándar o datos de flujos de redes de alto nivel. Dado que la detección automática funciona todo el día, todos los días, puede quedarse tranquilo.

Detectar Amenazas con Poderosas Herramientas de Búsqueda

Descubra malware oculto, ataques dirigidos y amenazas internas. Su equipo de seguridad puede buscar, programar y guardar consultas para identificar amenazas difíciles de encontrar. Las capacidades de búsqueda flexible permiten a sus analistas detectar amenazas y buscar Indicators of Compromise (Indicadores de Compromiso – IoCs) sin necesidad de aprender un nuevo lenguaje de consulta. Al incorporar inteligencia de amenazas desde Palo Alto Networks con un completo conjunto de datos de redes, endpoints y nubes, su equipo puede detectar malware, amenazas externas y ataques internos, ya sea que los incidentes estén en curso o se hayan producido en el pasado.

Investigar Eventos Inmediatamente

Revele automáticamente la causa raíz de cada alerta. Con Cortex XDR, sus analistas pueden analizar alertas de cualquier origen con un simple clic, agilizando las investigaciones. Cortex XDR revela automáticamente la causa raíz, la reputación y la secuencia de eventos asociados con cada alerta, lo que disminuye la experiencia necesaria para lograr una validación precisa. Una detallada línea de tiempo de toda la actividad de los ataques proporciona detalles accionables para las investigaciones de incidentes, lo que les permite a los analistas determinar el alcance, el daño y los próximos pasos en segundos.

Coordinar la Respuesta A través de los Puntos de Aplicación

Detenga amenazas con una rápida y precisa reparación. Cortex XDR permite a su equipo de seguridad contener inmediatamente las amenazas de redes, endpoints y nubes desde una consola. Sus analistas pueden detener rápidamente la propagación de malware, restringir la actividad de redes hacia y desde los dispositivos y actualizar las listas de prevención de amenazas, como dominios incorrectos, a través de una perfecta integración con los puntos de aplicación. Con Cortex XDR, puede bloquear rápidamente ataques avanzados y, a la vez, obtener más valor de sus inversiones existentes.

Adaptar Sus Defensas para Detener Futuros Ataques

Detecte las tácticas, las técnicas y los procedimientos de los atacantes con reglas de comportamiento. Con Cortex XDR, su equipo puede aplicar el conocimiento de cada investigación para reducir su superficie de ataque y agilizar las investigaciones futuras; así cambiar su postura de seguridad de reactiva a proactiva. Sus analistas también pueden crear reglas de comportamiento detalladas que detectan actividades maliciosas exclusivas en sus redes. Las alertas informativas flexibles mejoran el análisis de la línea de tiempo al identificar comportamientos sospechosos y permitir que los eventos complejos sean fáciles de comprender.

Obtener Protección de Endpoints Líder en la Industria

Utilice un agente único para la prevención de amenazas de endpoints y para la recopilación de datos. Su suscripción a Cortex XDR incluye agentes Traps ilimitados que ofrecen la mejor protección de endpoints disponible. Traps le permite detener malware, exploits y ransomware conocido y desconocido mediante el bloqueo de comportamientos y técnicas maliciosos. El análisis de malware integrado y basado en la nube, junto con el servicio de prevención de malware WildFire® de Palo Alto Networks, mejora la precisión y la cobertura. Los agentes de Traps registran toda la actividad de los endpoints y la reenvía a Cortex Data Lake para su análisis y coordinación de una respuesta.

Fácil Implementación desde la Nube

Comience en tan solo minutos. Al ser una aplicación basada en la nube, Cortex XDR ofrece una simple implementación directa, que elimina la necesidad de implementar nuevos sensores o recopiladores de logs locales. Utiliza sus productos existentes de Palo Alto Networks como sensores y puntos de aplicación, reduciendo la cantidad de productos que deben gestionar. Si usted es un cliente nuevo, solo necesita implementar un tipo de sensor, como un firewall de nueva generación o Traps, para detectar y detener amenazas con Cortex XDR. Cortex XDR está creado en Cortex, la única plataforma SOC continua y abierta basada en AI. Ofrece nuevos niveles de simplicidad en operaciones de seguridad y mejora significativamente los resultados de seguridad a través de la automatización y de una precisión sin precedentes.

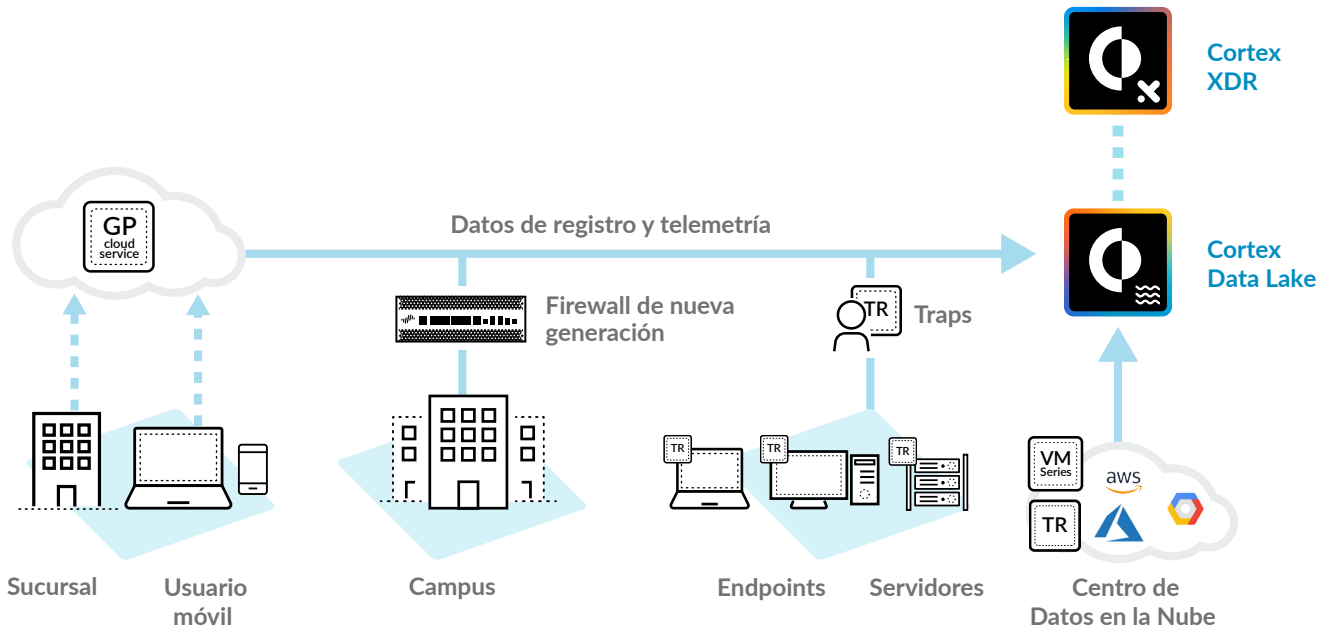

Figura 2: Análisis de datos provenientes de cualquier origen para su detección y respuesta

Beneficios Operativos

Lograr visibilidad de los datos en redes, endpoints y nubes: Recopile y correlacione datos de redes, endpoints y nubes a escala para su uso en la detección, la evaluación de prioridades, la investigación, la respuesta y la eliminación.

Detectar automáticamente ataques sofisticados las 24 horas, los 7 días de la semana: Aproveche el aprendizaje automático always-on (siempre activo) y reglas personalizadas para detectar amenazas avanzadas persistentes y otros ataques sofisticados.

Eliminar la sobrecarga de alertas: Simplifique las investigaciones con el análisis automático de la causa raíz y las vistas de la línea de tiempo, lo que reduce las capacidades requeridas para evaluar y analizar alertas.

Reducir drásticamente las alertas falsas positivas: Aplique los datos de cada investigación para refinar las reglas de detección de comportamiento y acelerar el análisis futuro, disminuir el ruido y el riesgo.

Incrementar la productividad del SOC: Agilice los procesos operativos en una única consola para consolidar la evaluación de prioridades de alertas, la investigación y la respuesta a través de las redes, los endpoints y los entornos de nube.

Reparar sin afectar el negocio: Interrumpa los ataques con precisión absoluta y evite tiempos de inactividad de usuarios o del sistema.

Eliminar amenazas avanzadas: Proteja su red contra señales maliciosas, violaciones a políticas, amenazas externas, ransomware, ataques sin archivos y de solo memoria y malware de día cero avanzado.

Optimizar el equipo de seguridad: Interrumpa cada etapa de un ataque al detectar IoCs, comportamientos anómalos y patrones maliciosos en la actividad.

Funcionalidades de Cortex XDR	
Investigación automática de alertas	Detección personalizada basada en el comportamiento
Análisis de causa raíz	Aprendizaje automático supervisado y no supervisado
Respuesta ante incidentes	Detección de ataques de malware y sin archivo
Contención de incidentes y recuperación	Detección de ataques dirigidos
Análisis de impacto posterior al incidente	Detección de amenazas internas
Detección de amenazas	Análisis de comportamiento riesgoso de usuarios
Búsquedas de IoCs e inteligencia de amenazas	Prevención de malware, ransomware y exploits con Traps

Especificaciones Técnicas	
Modelo de entrega	Aplicación entregada desde la nube
Retención de datos	Almacenamiento de datos de 30 días a tiempo ilimitado

Soporte de Sistema Operativo

Traps trabaja con múltiples endpoints de los sistemas operativos Windows®, macOS® y Linux. Para acceder a la lista completa de requisitos de sistema y de los sistemas operativos compatibles, por favor visite la Matriz de Compatibilidad de Traps.

Requisitos Mínimos de Pathfinder de Cortex XDR: 2 núcleos de CPU, 8 GB de RAM, 128 GB de almacenamiento con aprovisionamiento fino, VMware ESXi™ versión 5.1 o superior o hipervisor Microsoft Hyper-V® 6.3.96 o superior.

La licencia de Cortex XDR incluye:

- Aplicación Cortex XDR – Analytics
- Aplicación Cortex XDR – Investigation and Response
- Protección y respuesta de endpoints Traps
- Servicio de análisis de endpoints Cortex XDR – Pathfinder (alternativa sin agente para Traps)

3000 Tannery Way
Santa Clara, CA 95054

Línea principal: +1.408.753.4000
Ventas: +1.866.320.4788
Soporte técnico: +1.866.898.9087

www.paloaltonetworks.com

cortex-xdr-ds-022219