APRENDIZAJE SENCILLO

Edición especial de Palo Alto Networks

XDR

para dummies®

- Descubre qué es y qué no es el XDR
- Rompe la cadena del ataque con el XDR
- Analiza los casos de uso del XDR

Presentado por

CORTEX XDR BY PALO ALTO NETWORKS

Lawrence Miller

Acerca de Palo Alto Networks

Palo Alto Networks, líder mundial de la ciberseguridad, está dando forma al futuro centrado en la nube con una tecnología que transforma el modo en que trabajan las personas y las organizaciones. Nuestra misión es ser el socio preferido en materia de ciberseguridad, protegiendo nuestro estilo de vida digital. Ayudamos a abordar los mayores desafíos de seguridad del mundo con una innovación continua que hace uso de los últimos avances en inteligencia artificial, analíticas, automatización y organización. Al ofrecer una plataforma integrada y facilitar un ecosistema creciente de socios, estamos a la vanguardia de la protección de decenas de miles de organizaciones a través de nubes, redes y dispositivos móviles. Nuestra visión es crear un mundo en el que la seguridad y la protección mejoren día tras día. Para obtener más información, visita www.paloaltonetworks.com.

XDR

Edición especial de Palo Alto Networks

por Lawrence Miller

para dummies®

XDR Para Dummies®, edición especial de Palo Alto Networks

Una publicación de
John Wiley & Sons, Inc.
111 River St., Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-87975-6 (pbk); ISBN 978-1-119-87976-3 (ebk)

Agradecimientos del editor

Entre algunas de las personas que han ayudado a comercializar este libro figuran las siguientes:

Editora del proyecto: Elizabeth Kuball

Editora de adquisiciones: Ashley Coffey

Director editorial: Rev Mengle

Representante de expansión comercial: Cynthia Tweed

Editor de producción: Mohammed Zafar

Introducción

Mantener la seguridad de los datos críticos es cada vez más difícil debido a la rápida y creciente adopción de tendencias como la informática en la nube, el internet de las cosas (IoT) y la transformación digital, que aumentan el riesgo que corren los datos sensibles de las empresas. Al mismo tiempo, los responsables de las amenazas se aprovechan de muchas de estas mismas tendencias tecnológicas para aumentar la potencia y escala de sus ataques, que son cada vez más sofisticados.

Los equipos de seguridad han implementado herramientas, procesos puesto en práctica y contratado a personal para responder a las nuevas amenazas a medida que van surgiendo, pero se ven sobrepasados en número y en armas. Además, el hecho de añadir nuevas capacidades a sistemas existentes crea rápidamente un desorden de herramientas que se han integrado deficientemente, algo que exige mucho tiempo, energía y habilidad, cosas que a menudo escasean. Los procesos estáticos que no se adaptan a las tendencias y entornos en pleno cambio –como la nube y el trabajo remoto– se convierten rápidamente en algo anticuado e ineficaz. Así, los analistas de seguridad se encuentran en la tesitura de tener que llevar a cabo la tarea casi imposible de evaluar un diluvio interminable de alertas de seguridad, a pesar de haber recibido a menudo formación limitada y contar con herramientas también limitadas. La combinación de demasiadas alertas y la escasez de contexto hace que los equipos de seguridad pierdan visibilidad y control. Al final, la empresa corre cada vez más peligro.

El XDR (detección y respuesta extendidas) ha surgido para responder a esta complejidad. XDR está formado por soluciones de detección, investigación y respuesta ante amenazas que funcionan conjuntamente en todos los vectores de amenazas de la infraestructura de una empresa, incluidas la red, los *endpoints*, la nube y la identidad, en lugar de tener en cuenta un solo aspecto de la infraestructura. Al integrarse directamente en la arquitectura, las herramientas de XDR permiten, por diseño, recibir información y recomendaciones que optimizan el trabajo de los equipos de seguridad.

Acerca de este libro

XDR Para Dummies te ayuda a ponerte al día sobre la categoría de soluciones de seguridad de XDR y sobre qué pueden aportar a tu empresa. Este libro consta de cinco capítulos en los que se tratan los siguientes temas:

- El estado actual de la detección y respuesta, incluidas amenazas, limitaciones y retos (Capítulo 1).
- Qué es y qué no es el XDR (Capítulo 2).
- Cómo el XDR acaba con el ciclo de vida del ataque para detenerlo (Capítulo 3).
- Distintos casos de uso del XDR (Capítulo 4).
- Capacidades y características imprescindibles del XDR (Capítulo 5).

Cada capítulo se ha redactado de manera independiente, por lo que si ves un tema que despierta tu interés, puedes pasar libremente a ese capítulo. Este libro puede leerse en el orden que más te convenga (aunque no te recomiendo que lo leas boca abajo ni del revés).

Algunas suposiciones obvias

Se ha dicho que la mayoría de las suposiciones ha sobrevivido a su inutilidad, pero incluso así doy por supuestas algunas cosas.

Principalmente, doy por supuesto que trabajas para una organización que está buscando una manera mejor de aumentar la eficacia de su estrategia de seguridad, en concreto, sus capacidades de detección y respuesta. Quizá ocupas un cargo de responsabilidad en el departamento de TI; por ejemplo, eres el director de seguridad de la información, el director de información, el director de tecnología, o un vicepresidente o director de seguridad. O tal vez seas un arquitecto o ingeniero de redes o seguridad. Como tal, este libro se ha redactado para lectores técnicos con conocimientos generales sobre las operaciones, conceptos y tecnologías de seguridad modernos.

Si alguno de estos supuestos describe tu situación, no cabe ninguna duda de que este libro es para ti. Pero si tu situación es distinta, puedes seguir leyendo de todas formas. XDR es una tecnología que debes conocer y tu equipo te agradecerá que te conviertas en un eXperto en XRD.

Iconos utilizados en este libro

En todo este libro, a veces utilizo unos iconos especiales para llamar la atención sobre información importante. Aquí te los muestro:

RECUERDA

Este icono recordatorio indica información que debes almacenar en tu memoria no volátil, tu materia gris o tu cabeza junto a las fechas de aniversarios y cumpleaños.

CUESTIONES TÉCNICAS

Si quieres alcanzar el Olimpo de los expertos, ¡espabila! El icono de cuestiones técnicas explica la jerga que se esconde tras la jerga, y es de lo que están hechos los frikis.

CONSEJO

Los consejos se agradecen, nunca se esperan... y de verdad espero que agradezcas estos útiles datos.

ADVERTENCIA

Te avisamos de cosas de las que ya te advirtió tu madre. Bueno, quizá no, pero sí que te ofrecemos consejos prácticos para que no cometas errores que pueden resultar caros y frustrantes.

Más allá del libro

No puedo abarcar todo lo que me gustaría con un libro tan breve, así que si terminas el libro pensando: «¡Qué libro tan bueno! ¿Dónde puedo seguir aprendiendo?», visita `www.paloaltonetworks.com/cortex/cortex-xdr`.

EN ESTE CAPÍTULO

- Ver la necesidad urgente de mejorar el enfoque ante la seguridad
- Comprender las limitaciones de las herramientas tradicionales de detección y respuesta
- Abordar la fatiga que provocan las alertas y la falta de competencia en seguridad

Capítulo 1
Análisis del estado actual de la detección y respuesta a amenazas

En este capítulo, explico cómo han evolucionado las amenazas modernas hasta llegar a ser potencialmente más destructivas, por qué los métodos tradicionales para la prevención, detección y respuesta no son suficientes y cómo la fatiga que provocan las alertas y la falta de competencia en ciberseguridad aumentan los riesgos para tu organización.

Análisis del panorama de amenazas actual

Últimamente, las filtraciones de datos y los ataques de secuestro de archivos han pasado a ser tan frecuentes que prácticamente acaparan un segmento de noticias propio, como el tiempo, los deportes y el tráfico. Pero el hecho de que estos incidentes de seguridad sean tan habituales no los hace menos peligrosos. Cada minuto que un perpetrador de amenazas activo pasa operando en tu entorno, se produce un daño enorme.


ADVERTENCIA

Según el Instituto Ponemon, entre 2020 y 2021, el coste medio resultante de la filtración de datos aumentó un 10 % hasta llegar a los 4,24 millones de USD. Este ha sido el mayor aumento de costes en un solo año de los últimos siete años.

Sin duda conoces y vives esta realidad, y trabajas duro para detectar las amenazas y responder a ellas lo más rápido y eficazmente posible, antes de que se produzca una pérdida de datos. Sin embargo, esta es una batalla ardua frente a las tácticas, técnicas y procedimientos (TTP) cada vez más avanzados que usan los perpetradores de amenazas. Los atacantes pueden ahora poner en peligro un entorno casi cuando les plazca, sin usar métodos tradicionales como el *malware* basado en archivos. En lugar de ello, usarán métodos que ponen en peligro los archivos del sistema autorizados, atacarán el registro de un dispositivo o usarán de forma malintencionada utilidades como PowerShell. El aumento de los métodos de ataque novedosos y más evasivos ha generado la necesidad de contar con nuevas estrategias y tácticas para detectar amenazas, responder a ellas y prevenirlas.

RECUERDA

Para que una organización pueda estar al corriente del panorama de amenazas actual, necesita herramientas eficaces y un equipo formado por analistas de seguridad capacitados. Lamentablemente, lograr el equilibrio perfecto entre expertos en tecnología y expertos capacitados suele ser la excepción y no la regla en la mayoría de las organizaciones.

Reconocer las limitaciones de las tecnologías y los métodos tradicionales

Aunque tus equipos de seguridad hacen todo lo posible por evitar que ataques contra tu organización tengan éxito, hay que estar preparados para la inevitable realidad de que ningún entorno es completamente seguro. Algún día, una amenaza conseguirá colarse en tu entorno.

Para ayudar a los equipos de seguridad a combatir las amenazas, han salido al mercado muchas herramientas diferentes de registro, detección y respuesta. Cada una de estas herramientas tiene fortalezas y debilidades y puede ser útil frente a los ataques, como los incidentes conocidos de *malware* basado en archivos o los ataques que se han diseñado para acabar con solo una parte de la infraestructura. Pero la mayoría de estas herramientas sirven para un único fin y ninguna es especialmente adecuada para manejar de forma independiente amenazas sofisticadas.

ADVERTENCIA

Según ESG Research, el 66 % de las organizaciones cree que su eficacia de detección y respuesta a amenazas se ve limitada porque se basa en muchas herramientas de puntos independientes.

En los apartados siguientes, analizo en mayor profundidad algunas de las herramientas más utilizadas para el registro, detección y respuesta que utilizan los equipos de seguridad, y expongo cuáles son sus retos y limitaciones.

Detección y respuesta de puntos de conexión

La *detección y respuesta de puntos de conexión* (EDR) es una categoría de herramientas utilizada para detectar e investigar amenazas en los dispositivos de puntos de conexión. Las herramientas de EDR ofrecen por lo general capacidades de detección, análisis, investigación y respuesta.

La EDR surgió por primera vez en 2013 para ayudar en las investigaciones forenses que requerían una telemetría de punto de conexión muy detallada con el fin de llevar a cabo una ingeniería inversa del *malware* y comprender exactamente qué había hecho el perpetrador de la amenaza en un dispositivo afectado.

Las herramientas de EDR controlan los incidentes generados por los agentes del punto de conexión en busca de actividades sospechosas. Las alertas que generan las herramientas de EDR ayudan a los analistas de las operaciones de seguridad a identificar, investigar y remediar los incidentes. Las herramientas de EDR también recogen datos de telemetría sobre actividades sospechosas y pueden aportar a los datos existentes información contextual de incidentes relacionados. Con estas funciones, la EDR es fundamental para que los equipos de respuesta ante incidentes acorten los tiempos de respuesta.

Sin embargo, la EDR no puede por sí sola detectar las amenazas que sufre la empresa porque solo se centra en el punto de conexión. No ofrece visibilidad del tráfico de red de los dispositivos sin que se instalen agentes en la red y en los dispositivos en red —como enrutadores, conmutadores, servidores, dispositivos del internet de las cosas (IoT), uso del dispositivo propio (BYOD) y sistema de control industrial (ICS)— y recursos en la nube, como ofertas de cargas de trabajo, redes de nubes y plataforma como servicio (PaaS).

Plataforma de protección del punto de conexión

Una *plataforma de protección del punto de conexión* (EPP) es un agente de *software* instalado en los dispositivos de punto de conexión para evitar ataques de *malware* basado en archivos y detectar actividades maliciosas. La EPP es la evolución de las soluciones tradicionales antivirus y *antimalware* basadas en *host* y se considera por lo general la primera línea de defensa en un punto de conexión.

Las capacidades de detección en las distintas soluciones de EPP varían, pero la mayoría usan algún tipo de combinación de técnicas de detección y prevención, incluidas las siguientes:

- Indicadores estáticos de riesgo (IOC, es decir, detección basada en firmas).
- Aplicaciones de listas blancas (permisos) o listas negras (bloqueos), localizadores uniformes de recursos (URL), puertos y direcciones.
- Análisis de comportamiento y aprendizaje automático.
- Espacios seguros para expandir (o probar) amenazas sospechosas, como ejecutables.

Una solución de EPP debe gestionarse en la nube para que pueda llevarse a cabo un control continuo y la recogida de los datos de las actividades, además de poder ejecutar acciones de corrección remotas si el punto de conexión se está usando en la red corporativa o de manera remota. Asimismo, las soluciones de EPP cuentan con la ayuda de los datos en la nube. Dicho de otro modo, el agente del punto de conexión no tiene que mantener una base de datos local de todos los IOC conocidos; en lugar de ello, el agente del punto de conexión puede comprobar un recurso en la nube para encontrar los últimos veredictos sobre objetos que no puede clasificar y aprovechar la información sobre las amenazas en tiempo real.

La EPP se ha diseñado principalmente para evitar o controlar y, por lo tanto, no se centra en la detección ni en la recogida de información para la defensa ante los ataques modernos. La mayoría de las plataformas de EPP carecen también de las capacidades de respuesta necesarias para investigar los incidentes. Por ello, la EPP por sí misma no puede ofrecer las funciones esenciales para detener los ataques modernos.

Administración de eventos e información de seguridad

Las herramientas de *software de administración de eventos e información de seguridad* (SIEM) ofrecen recogida, correlación y análisis de los eventos de seguridad casi en tiempo real, además de notificación de alertas de seguridad generadas por varios dispositivos y aplicaciones en red.

Muchas organizaciones asignan gran parte de sus presupuestos de seguridad a las herramientas de SIEM para recopilar los registros de diferentes dispositivos de seguridad y entornos de servidores. Las SIEM se diseñaron inicialmente y principalmente como recopiladores de registros para crear informes de cumplimiento. Con el tiempo, su uso se extendió a la detección de amenazas, y las SIEM son ahora un repositorio de alertas central para muchos centros de operaciones de seguridad (SOC).

La SIEM centraliza las alertas y añade datos de registro mediante análisis y normalización. Los equipos de seguridad pueden así ver los datos

de registro en un solo lugar, pero normalmente no se han generado de manera eficaz y los analistas de primera línea encargados de analizarlos no pueden usar muchas veces las herramientas que contienen los datos fuente enriquecidos para validar las alertas. En general, las SIEM carecen de profundidad de análisis para las fuentes de datos clave, como los datos de punto de conexión y los datos de red, y pueden ser difíciles de implementar, configurar y mantener, en parte porque carecen de este conocimiento directo.

Detección y respuesta de red y análisis de comportamiento de usuarios y entidades

Las herramientas de *detección y respuesta de red* (NDR) y de *análisis de comportamiento de usuarios y entidades* (UEBA) representan una clase aún más nueva de herramientas de análisis de la seguridad que ha surgido para abordar las dificultades de la SIEM a la hora de detectar ataques desconocidos. Estas herramientas usan el aprendizaje automático para elaborar una línea base de actividad de la telemetría recogida y buscar después acciones atípicas que puedan ser indicativas de un comportamiento malicioso. Estas tecnologías permiten a las organizaciones identificar ataques que antes eran desconocidos al reconocer patrones de tráfico inusuales.

Sin embargo, estas herramientas también tienen sus limitaciones. Los productos basados en red están limitados a la red y no pueden controlar ni hacer un seguimiento de los eventos locales, como procesar información reunida en los puntos de conexión. La NDR también tiene una profundidad limitada; si la EDR es profunda y estrecha, la NDR es superficial y ancha.

RECUERDA

La complejidad de los ataques modernos exige el análisis de varias fuentes de datos para identificar y confirmar la actividad maliciosa. Añadir capas de herramientas unidimensionales genera gastos importantes a los equipos de seguridad, crea posibles puntos ciegos y exige mucho esfuerzo manual por parte de los analistas de seguridad para cambiar de consolas y comprender un ataque.

Demasiadas alertas para tan poco tiempo y personal

Las herramientas de detección y prevención generan miles de alertas cada día, muchas más de las que los miembros de los equipos de seguridad pueden gestionar de manera eficaz. Estas alertas llegan de muchas fuentes desconectadas, lo que hace que sean los analistas de seguridad quienes tienen que montar el puzle (consulta la figura 1-1).

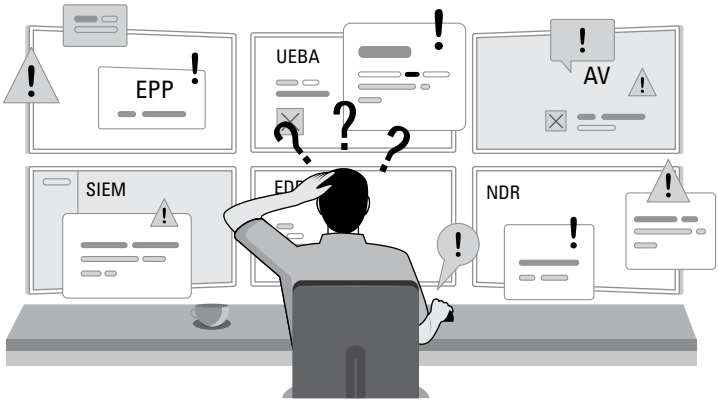

FIGURA 1-1: las herramientas en silos ralentizan la investigación y la respuesta.

Para analizar una posible amenaza son necesarios, por lo general, una serie de pasos:

1. Revisar los datos de registro disponibles para comenzar a atar los cabos de lo que ha ocurrido.
2. Comparar manualmente los datos con las fuentes de inteligencia de amenazas para determinar si los indicadores son maliciosos o no.
3. Buscar eventos relacionados usando IOC para determinar si la alerta forma parte de un ataque mayor.
4. Recopilar contexto en torno al incidente, incluidos los sistemas, *hosts*, activos, recursos, direcciones IP y archivos asociados a cada alerta.
5. Crear una escala temporal e identificar la causa raíz de una alerta.
6. Comprobar si otros miembros del equipo están gestionando los nuevos enlaces de información a las alertas para coordinar los esfuerzos.
7. Evaluar si la alerta necesita remitirse a una instancia superior, descartarse o solucionarse rápidamente y cerrarse.

Llevar a cabo todos estos pasos en un SOC tradicional lleva mucho tiempo y requiere muchas herramientas, y esto es solo la parte de la evaluación. El resultado final es que los analistas solo tienen tiempo para gestionar las alertas de «mayor prioridad» que se encuentran cada día, con el inconveniente de que se pasa por alto un preocupante número de alertas de «baja prioridad». Y si no se tiene el contexto adecuado para clasificar una alerta como de prioridad «alta» o «baja», el SOC puede no darse cuenta de lo que es realmente importante ni ocuparse de problemas que no son realmente críticos.

¿QUÉ HACEN LOS EQUIPOS DEL SOC?

Los equipos de operaciones de seguridad, sean grandes o pequeños, tienen ciertas funciones clave. El modelo tradicional para muchos equipos de operaciones de seguridad y del SOC divide estas funciones en una estructura de analistas en niveles, según el grado de experiencia. Estas son las responsabilidades principales de esos niveles:

- **Nivel 1 – Evaluación:** a esto es a lo que dedican la mayor parte del tiempo los analistas de seguridad. Los analistas de nivel 1 son por lo general los que menos experiencia tienen y su función principal es controlar los registros de eventos en busca de actividad sospechosa. Cuando creen que algo debe investigarse más, reúnen el mayor contexto posible del mayor número de fuentes que puedan para crear un informe en forma de incidente que incluye al usuario, *host*, dirección IP y cualquier indicador estático de riesgo relacionado, y remiten el incidente al nivel 2.
- **Nivel 2 – Investigación:** los analistas del nivel 2 investigan más a fondo la actividad sospechosa para determinar la naturaleza de la amenaza y hasta qué punto se ha infiltrado en el entorno, lo que incluye la elaboración de una escala de tiempo para comprender la secuenciación y para relacionar los eventos con el fin de determinar su causa raíz. Deben investigar más a fondo para comprender hasta dónde ha llegado el ataque. Estos analistas coordinan después una respuesta para remediar el problema. Esta es una actividad de mayor impacto para la que a menudo se necesitan analistas con más experiencia.
- **Nivel 3+ – En busca de amenazas:** aquí se encuentran los analistas con más experiencia, dedicados a responder a incidentes complejos y pasar el resto del tiempo buscando en datos forenses y de telemetría amenazas que pueden no haber sido marcadas como sospechosas por el *software* de detección. La empresa media dedica la menor cantidad de tiempo a las actividades de búsqueda de amenazas porque las actividades de los niveles 1 y 2 consumen muchos recursos de analistas.

Aunque este modelo puede ser el más frecuente, no es necesariamente el ideal. La mayoría de las personas no pueden dedicarse a controlar registros todo el día. La fatiga ante las alertas es real y las amenazas se cuelan a través de todo el ruido generado por la cantidad de sensores que hay en un SOC. Puede resultar difícil retener a los analistas que llevan a cabo esta tarea, ya que prefieren participar en las investigaciones (y pueden tener métodos nuevos e innovadores que nunca se conocerán porque no tienen las habilidades técnicas necesarias para los procesos de investigación existentes). Se dedica muy poco tiempo a la búsqueda de amenazas y a la mejora de procesos, porque la mayoría de las horas de los recursos se dedican a descubrir y mitigar amenazas.

Además, los analistas de seguridad que se encargan de las evaluaciones de alertas no tienen muchas veces el contexto suficiente para determinar el riesgo real que presenta un ataque para la organización. Así, la alerta se remite a un grupo de mayor nivel para una validación más exhaustiva, lo que exige más tiempo, trabajo y recursos y genera a la vez ineficiencias en todos los niveles.

RECUERDA

La mayoría de las empresas reciben miles de alertas procedentes de multitud de soluciones de control, pero tanto ruido es contraproducente. La detección avanzada no quiere decir que haya *más* alertas; se trata de que haya más y *mejores* alertas que requieren algún tipo de acción. Conseguir este tipo de detección avanzada exige la integración de todas las tecnologías de detección en uso, además de análisis sofisticados que analicen los datos en los puntos de conexión, en la red y en la nube para hallar y validar la actividad del adversario en tu entorno.

Incluso con herramientas mejores y más exhaustivas para detectar amenazas, la gestión de las alertas, y de posibles incidentes, exige una validación y evaluación posteriores por parte de responsables de respuestas que estén capacitados. Lamentablemente, no hay suficientes personas que tengan estos conocimientos, y esta importante falta de competencia afecta a la capacidad de las organizaciones para estar al día con los métodos de los atacantes (consulta la figura 1-2).

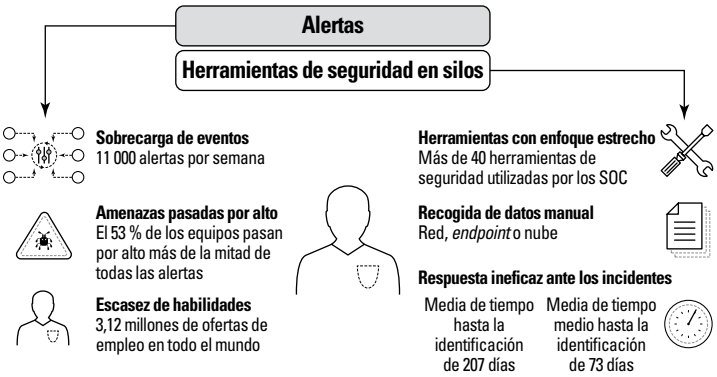

FIGURA 1-2: los muchos retos de un analista de seguridad.

Estos perpetradores utilizan herramientas y técnicas sumamente automatizadas para encontrar vulnerabilidades y conseguir un acceso inicial a tu entorno. Esto agrava la falta de competencia porque a los atacantes les resulta más rápido y económico ampliar sus herramientas

automáticas que a las organizaciones añadir más personal de seguridad capacitado. Así que tienes que buscar herramientas que puedan:

Hacer que tu personal con menos experiencia sea más eficaz y eficiente.

Automatizar la detección de amenazas complejas.

Simplificar las investigaciones.

Ayudar a los analistas a mejorar sus habilidades.

CONSEJO

En su estudio *Cybersecurity Workforce Study* de 2020, el Consorcio Internacional de Certificación de Seguridad de Sistemas de Información (ISC)[2] indicó que existía una carencia de 3,12 millones de profesionales de ciberseguridad capacitados a nivel global. Según Cyberseek, actualmente en Estados Unidos hay más de 300 000 puestos de trabajo en ciberseguridad sin cubrir, una cifra que se espera que crezca considerablemente durante los próximos años.

Muchas empresas eligen subcontratar las funciones de detección y respuesta, bien en su totalidad o en parte, a proveedores de servicios de seguridad gestionados (MSSP) o proveedores de detección y respuesta gestionadas (MDR). Subcontratar esta función es algo frecuente (y se considera la práctica recomendada en muchos casos), sobre todo para equipos con presupuestos de seguridad reducidos u organizaciones que no desean o no tienen recursos para gestionar su propia seguridad. Sin embargo, las organizaciones que quieren una visibilidad y control completos no deben estancarse subcontratando la seguridad simplemente porque sus herramientas no son adecuadas. También es importante tener en cuenta que la pila de tecnología es igual de importante para un equipo de seguridad subcontratado; los proveedores que usan herramientas existentes se encontrarán con las mismas ineficiencias que afectan a los equipos de seguridad internos.

Lo que realmente se necesita es un conjunto de tecnologías que reduzca el número total de alertas y permita al mismo tiempo a los analistas con menos experiencia evaluar por sí mismos las amenazas con eficiencia y confianza, asegurándose de que solo las alertas de alta fidelidad se deriven a los analistas con más experiencia.

EN ESTE CAPÍTULO

- **Comenzar con una prevención de amenazas férrea para atenuar el ruido.**
- **Asegurar una visibilidad de extremo a extremo en tu entorno.**
- **Reducir las investigaciones manuales para acelerar y mejorar la respuesta a incidentes.**
- **Maximizar el valor de tus inversiones en seguridad.**

Capítulo 2
Definición de XDR

El XDR, detección y respuesta extendidas, es un nuevo enfoque ante la detección y respuesta a amenazas. El término XDR lo acuñó Nir Zuk, el director de tecnología y cofundador de Palo Alto Networks, en 2018. El motivo fundamental para crear el XDR fue detener los ataques de manera más eficiente, detectar las técnicas y tácticas de los atacantes que no se pueden evitar y ayudar a los equipos del centro de operaciones de seguridad (SOC) a responder mejor a las amenazas que requieren investigación.

Según Forrester Research, el XDR «optimiza la detección, investigación, respuesta y búsqueda de amenazas en tiempo real. El XDR unifica las detecciones en endpoints relevantes para la seguridad con la telemetría de las herramientas empresariales y de seguridad, como el análisis y la visibilidad de la red (NAV), la seguridad del correo electrónico, la administración de identidades y accesos, y la seguridad en la nube, entre otras».

La *X* en XDR significa *extendidas*, pero, en realidad, representa cualquier fuente de datos, ya que no resulta eficiente ni eficaz analizar los componentes individuales de un entorno de forma aislada. El XDR aporta un enfoque proactivo ante la detección y respuesta a las amenazas, brindando visibilidad a través de redes, nubes y *endpoints* mientras hace uso del análisis y la automatización para hacer frente a las amenazas cada vez más sofisticadas de hoy en día.

En este capítulo, aprenderás qué es el XDR y los requisitos clave de una solución XDR.

Cómo garantizar la solidez de la prevención de amenazas

La base del XDR es una férrea prevención de las amenazas. Una solución XDR debe bloquear con precisión más del 99 % de las amenazas que se pueden bloquear automáticamente en tiempo real o casi real, sin verificación manual. Gracias a la mejor prevención de amenazas de su clase, tu equipo puede concentrarse en identificar y detener ataques más sofisticados e imperceptibles en lugar de perder el tiempo investigando todas las posibles amenazas que traspasan tus defensas.

Para vencer las amenazas en *endpoints*, necesitas una solución sólida con un antivirus integrado de próxima generación (NGAV) que pueda detectar y bloquear cada etapa de un ataque, desde el *exploit* inicial y la instalación de *malware* hasta las acciones ilícitas que lleva a cabo un actor de amenazas mediante la ejecución del *malware*. Cada capa de la defensa debe ser lo suficientemente inteligente como para acabar con las técnicas de evasión del actor de amenazas y adaptarse continuamente para detener las últimas amenazas.

CONSEJO

Busca las siguientes capacidades NGAV en una solución XDR:

- Análisis local y prevención de amenazas basados en aprendizaje automático.
- Prevención de amenazas basada en el comportamiento para el análisis dinámico de los procesos en ejecución.
- Prevención de *exploits* según sus técnicas.
- Prevención de amenazas conocidas basada en información sobre amenazas, como *hashes* de archivos.
- Integración automatizada en un servicio de prevención de *malware* en la nube, con informes de análisis y soporte para archivos con un tamaño mínimo de 100 MB.
- Firmas sin demora para ofrecer protección rápidamente y compartir información sobre las amenazas.
- Capacidad de protección de *shell* inversa.
- Actualizaciones transparentes del motor de detección de amenazas.
- Perfiles y excepciones de seguridad.

- Exploración puntual y programada de *endpoints*.
- Protección contra *malware*, *ransomware* y ataques sin archivos.
- Agente ligero único para protección, detección y respuesta en *endpoints*.

Tu solución XDR también debe reducir tu superficie de ataque y proteger los datos confidenciales con funciones de protección de *endpoints*, incluidas las siguientes:

- Cortafuegos de *host*
- Cifrado de disco
- Controlador de dispositivo de bus serie universal (USB)
- Reglas de prevención personalizables

Por último, tu solución XDR debe ser compatible con un cliente de seguridad de red para *endpoints* a fin de proporcionar acceso remoto seguro, prevención de amenazas y filtrado del localizador uniforme de recursos (URL).

Visibilidad y detección completas

La visibilidad y la detección son fundamentales para reducir las amenazas. Si no puedes *ver* una amenaza, no puedes identificarla ni investigarla y, desde luego, no puedes detenerla. Los actores de amenazas aprovechan la nube y el aprendizaje automático para llevar a cabo ataques masivos y multifacéticos que les permiten establecer puntos persistentes y exfiltrar datos valiosos y propiedad intelectual. Esto significa que el XDR debe tener capacidades sólidas de detección y visibilidad, incluidas las siguientes:

- **Amplia visibilidad y comprensión contextual:** los productos puntuales en silos generan datos en silos, algo que no es eficaz. No puedes esperar para defenderte bien de los ataques si no eres al menos tan ágil en tu propio entorno como lo son los actores de amenazas. El XDR debe tener capacidades de visibilidad y detección en todo tu entorno, integrando la telemetría desde tus *endpoints*, red y entornos en la nube. Además, debe poder correlacionar estas fuentes de datos para comprender cómo se vinculan varios eventos y cuándo un determinado comportamiento es (o no) sospechoso según el contexto (consulta la figura 2-1).

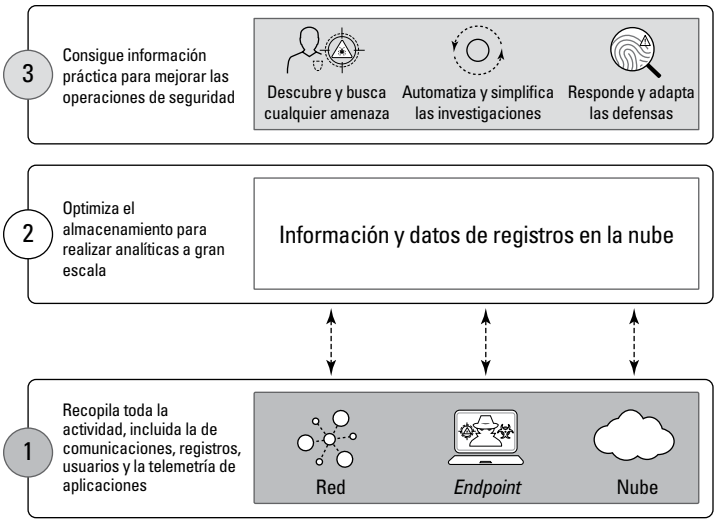

FIGURA 2-1: el XDR pone fin a los silos tradicionales de detección y respuesta.

- **Retención de datos:** los atacantes son pacientes y persistentes. Saben que es más difícil detectarlos si operan lentamente, esperando a los periodos de retención de registros de las tecnologías de detección a las que se enfrentan. El XDR no debe ponérselo fácil. Tus sistemas de detección deben recopilar, correlacionar y analizar datos de la red, el *endpoint* y la nube en un único repositorio, con 30 días o más de retención histórica.
- **Análisis de tráfico interno y externo:** las técnicas de detección tradicionales se centran principalmente en los atacantes externos, lo que no proporciona una visión completa de los posibles actores de amenazas. La detección no puede buscar únicamente ataques que procedan de más allá del perímetro. También tiene que trazar el perfil y analizar las amenazas internas para buscar comportamientos anómalos y potencialmente maliciosos e identificar el uso indebido de credenciales.
- **Información sobre amenazas integrada:** debes estar equipado para hacer frente a los ataques desconocidos. Un método para equilibrar la balanza es aprovechar los ataques conocidos que han visto primero otras organizaciones. La detección debe basarse en la información sobre amenazas recopilada a través de una red global de empresas. Cuando una organización de la red extendida identifica un ataque, puedes utilizar el conocimiento obtenido de ese ataque inicial para identificar ataques posteriores en tu propio entorno.

- **Detección personalizable:** la protección de tu organización presenta desafíos únicos asociados a sistemas específicos, grupos de usuarios diferentes y distintos actores de amenazas. Los sistemas de detección deben ser también sumamente personalizables en función de las necesidades específicas de tu entorno. Estos desafíos requieren una solución XDR que admita detecciones personalizadas y predefinidas.
- **Detección basada en aprendizaje automático:** al haber ataques que no se parecen al *malware* tradicional, como los que ponen en peligro los archivos autorizados del sistema, utilizan entornos de *scripts* y atacan al registro, la tecnología de detección debe utilizar técnicas analíticas avanzadas para analizar toda la telemetría recopilada. Estos enfoques incluyen el aprendizaje automático supervisado y semisupervisado.

CONSEJO

Busca una solución XDR que aborde los siguientes requisitos clave de visibilidad y detección:

- Análisis de comportamientos para trazar el perfil del comportamiento y detectar anomalías indicativas de un ataque mediante el análisis del tráfico de red, eventos de *endpoints* y eventos de usuarios a lo largo del tiempo.
- Capacidades de aprendizaje automático supervisadas y no supervisadas.
- Reglas de detección predefinidas y personalizables basadas en el comportamiento.
- Reglas personalizadas que pueden detectar ataques de forma retroactiva.
- Exclusiones de alertas granulares para el ajuste opcional de alertas de *endpoints*, redes, nubes o terceros.
- Información sobre amenazas compartida para distribuir la inteligencia de amenazas colectiva desde un servicio de análisis de *malware* en la nube a cortafuegos, agentes de *endpoints* y servicios de detección y respuesta.
- Capacidad para consumir fuentes de información sobre amenazas de fuentes de terceros en formatos de notación de objetos JavaScript (JSON) y valores separados por comas (CSV).
- Detección de técnicas de ataque a lo largo del ciclo de vida del ataque, que incluya descubrimiento, movimiento lateral, comando y control y exfiltración.

- Capacidad demostrada para detectar las tácticas y técnicas de los atacantes a través de evaluaciones de las tácticas, técnicas y conocimiento común de adversarios (ATT&CK) de MITRE.
- Etiquetado de las tácticas y técnicas de ATT&CK de MITRE en las alertas y reglas de detección.
- Gestión de activos con descubrimiento de dispositivos no autorizados.
- Evaluación de vulnerabilidades.
- Inventario de *host* con información detallada de usuarios, sistemas y aplicaciones.

Automatización de las investigaciones y respuestas

Cuando recibes una alerta sobre posibles amenazas en tu entorno, debes poder clasificar e investigar rápidamente esas amenazas. Hacer esto de manera efectiva, especialmente durante un ataque que afecta a múltiples partes de tu entorno, es donde fallan los sistemas tradicionales de detección y respuesta. Las soluciones XDR pueden mejorar este proceso drásticamente gracias a sus capacidades de investigación y respuesta que incluyen lo siguiente:

- **Correlación y agrupación de alertas y datos de telemetría relacionados:** cuando se trata de ataques contra tu organización, el tiempo es esencial. En el momento en que recibes una alerta de amenaza, el atacante ya está trabajando duro para llevar a cabo su misión y lograr sus objetivos en tu entorno. Debes poder comprender rápidamente el ataque y su cadena de causalidad completa. Esto significa que tu herramienta XDR debe primero reducir el ruido agrupando automáticamente las alertas relacionadas y priorizando de manera efectiva los eventos que requieren tu atención con mayor urgencia. A continuación, tu herramienta XDR debe poder construir una línea de tiempo del ataque, uniendo registros de actividad de tus entornos de red, *endpoint* y nube. Al visualizar la actividad y secuenciar los eventos, se puede determinar la causa raíz de la amenaza y se puede evaluar el daño potencial y el alcance (consulta la figura 2-2).

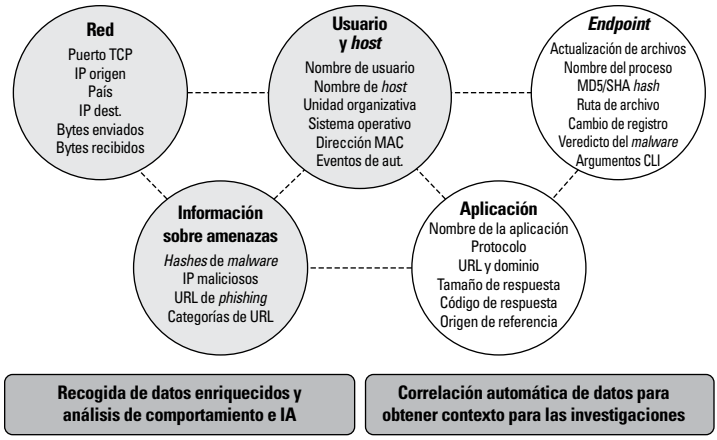

FIGURA 2-2: el XDR correlaciona y une datos enriquecidos.

- **Investigación rápida de incidentes con acceso instantáneo a todos los artefactos forenses, eventos e información sobre amenazas en un solo lugar:** identifica rápidamente la actividad de los atacantes mediante la revisión de artefactos clave, como registros de eventos, claves de registro, historial del navegador y mucho más. Las herramientas de código abierto actuales obligan a los equipos a recopilar pruebas de una variedad heterogénea de agentes y *scripts*. Los agentes de un solo propósito para el análisis forense, la protección de *endpoints* y la detección y respuesta pueden obstaculizar el rendimiento y añadir complejidad. Para resolver un incidente, debes encontrar el punto de entrada y rastrear los remanentes, aunque tus adversarios hayan intentado cubrir sus huellas.
- **Interfaces de usuario consolidadas con capacidad dinámica rápida:** tus analistas de seguridad, cuando comienzan a profundizar en las alertas, necesitan un entorno de trabajo optimizado que les permita moverse dinámicamente entre los datos de cualquier fuente con un solo clic. Los analistas no deberían tener que perder el tiempo pasando de una herramienta a otra.
- **Búsqueda de amenazas manual y automatizada:** cada vez son más las organizaciones que buscan de forma proactiva adversarios activos, lo que permite a sus analistas elaborar hipótesis de ataque y buscar actividades relevantes en el entorno. Apoyar la búsqueda de amenazas requiere potentes capacidades de búsqueda que encuentren evidencias que puedan probar las hipótesis, además de información sobre amenazas integrada para buscar actividades que ya se han observado en la red extendida. Esta información sobre

amenazas debe integrarse y automatizarse de manera que quede claro si una amenaza se ha observado antes sin que se necesite una cantidad considerable de trabajo manual por parte de los analistas (por ejemplo, abrir 30 pestañas de navegador diferentes para buscar numerosas fuentes de información sobre amenazas de una dirección IP maliciosa conocida).

- **Orquestación de la respuesta:** una vez que se ha detectado e investigado la actividad de la amenaza, el siguiente paso es la remediación y aplicación de políticas eficientes y efectivas. Tu sistema debe poder orquestar una respuesta coordinada a las amenazas activas y prevenir futuros ataques en tus entornos de red, *endpoint* y nube. Esto incluye la comunicación entre las tecnologías de prevención (es decir, un ataque bloqueado en la red actualiza automáticamente las políticas en los *endpoints*), ya sea de forma nativa o construida a través de interfaces de programación de aplicaciones (API). También incluye la capacidad de un analista para tomar acciones de respuesta directamente a través de la interfaz XDR.

CONSEJO

Busca las siguientes capacidades de investigación y respuesta en una solución XDR:

- Análisis automatizado de la causa raíz de cualquier alerta, incluidas las alertas de red, si hay datos de *endpoint* disponibles.
- Visualización de las cadenas de ejecución que conducen a una alerta.
- Visión de análisis temporal para ver todas las acciones y alertas en una línea de tiempo.
- Consulta de indicadores de compromiso (IOC) y comportamientos de *endpoints*, *hosts* conectados y desconectados, registros del tráfico de red de los cortafuegos y registros de autenticación de proveedores de administración de identidad.
- Lenguaje de consulta avanzado compatible con el uso de comodines, expresiones regulares, JSON, agregación de datos, manipulación de campos y valores, combinación de datos de fuentes dispares y visualización de datos.
- Capacidad de un analista para cambiar fácil y dinámicamente entre vistas con filtrado granular y clasificación de resultados de consultas.
- Agregación automática de información de protocolo de internet (IP) o *hash* relevante, incluida la información sobre amenazas, eventos e incidentes relacionados en una sola vista para simplificar las

investigaciones y bloquear el acceso a direcciones IP o dominios maliciosos.

- Identificación de si un evento fue bloqueado por un agente de *endpoint*, cortafuegos u otra tecnología de prevención y capacidad remota para ver, suspender o finalizar procesos en ejecución o descargar binarios.
- Unión automatizada de alertas de seguridad, como alertas de cortafuegos, a datos de *endpoint*.
- Cancelación de ruido y eliminación de binarios no significativos y bibliotecas de vínculos dinámicos (DLL) de la cadena.
- Contexto para el analista del SOC sobre tácticas, técnicas y procedimientos (TTP) que permite utilizar el conocimiento adquirido y facilitar futuras investigaciones.
- Integración con soluciones de orquestación de la seguridad, automatización y respuesta (SOAR) y administración de eventos e información de seguridad (SIEM).
- Puntuación de incidentes que permite clasificar y priorizar los incidentes de alto riesgo para concentrarse rápidamente en las amenazas más críticas; creación de puntuaciones de incidentes basadas en los atributos de las alertas, incluidos los usuarios o *hosts* en una alerta.
- Puesta en cuarentena de archivos maliciosos y eliminación de estos en sus directorios de trabajo.
- Encontrar y eliminar archivos rápidamente en toda tu organización con Search & Destroy, que indexa archivos de *endpoint*.
- Acceso directo a los *endpoints* con Live Terminal para ejecutar Python, PowerShell o comandos o *scripts* del sistema; revisar y gestionar procesos activos y ver, eliminar, mover o descargar archivos.

Mayor eficacia de la seguridad

El XDR debe acelerar considerablemente el rendimiento de la inversión (ROI) en seguridad. Esto significa aumentar la eficiencia y la eficacia de tu equipo de seguridad para poder prevenir o superar la escasez de personal, mejorar la integración entre tus herramientas existentes y fortalecer la eficacia de la prevención a lo largo del tiempo con una infraestructura escalable e inteligencia artificial (IA). Para cumplir estos criterios, el XDR debe tener las siguientes capacidades:

- **Orquestación de la seguridad:** los mismos atributos que hacen que la orquestación sea importante para simplificar las investigaciones, también permiten maximizar el ROI de tu pila de seguridad. Cada organización tiene una base instalada de soluciones de seguridad que pueden utilizarse para responder a las amenazas activas. Un aspecto clave de cualquier sistema de detección y respuesta es aprovechar las inversiones en estas soluciones existentes, de forma que cualquier respuesta pueda aplicarse de manera coherente en toda la empresa.
- **Ingestión de datos de terceros:** hoy en día, todas las organizaciones tienen una variedad de herramientas de seguridad diferentes y en silos. Cuanto mayor sea la visibilidad de una solución XDR sobre los datos de cada una de esas herramientas diferentes, más completa será la seguridad que pueda proporcionar. Las mejores soluciones XDR tendrán la flexibilidad de ingerir datos de otras herramientas en tu entorno para maximizar el valor y la eficacia.
- **Almacenamiento y procesamiento escalables:** dada la persistencia de los actores de amenazas actuales, no querrás descartar la telemetría que pueda proporcionar evidencia forense importante de la actividad del atacante en ataques «imperceptibles y lentos» que pueden durar meses o incluso años. También necesitas la potencia analítica para poder utilizar toda esta telemetría de manera eficaz. Las plataformas XDR en la nube brindan esta accesibilidad y escala prácticamente ilimitadas.
- **Mejora con el tiempo:** la detección de ataques cada vez más sofisticados requiere IA integrada y aprendizaje automático, así como automatización y orquestación para reducir los esfuerzos manuales y permitir que los analistas de seguridad sean más eficaces y eficientes. Las soluciones XDR deben aprender de la experiencia, reducir el riesgo futuro y fortalecer continuamente la prevención mediante la aplicación de los conocimientos adquiridos a través de la detección, la investigación y la respuesta.
- **Creación de informes y paneles de información:** los equipos de seguridad deben poder comprender y comunicar la postura de seguridad y las métricas operativas de la organización. Las soluciones XDR deben ser capaces de proporcionar mejores resultados de seguridad y resumir el estado de la seguridad a través de informes y paneles de información intuitivos y personalizables.

¿UN VERDADERO O FALSO AMIGO? DEFINICIÓN DEL VERDADERO XDR

El XDR está cobrando cada vez más fuerza y aceptación en la industria por parte de la comunidad de analistas, proveedores de seguridad y usuarios finales en general, pero al igual que otras categorías de soluciones de seguridad, viene acompañado de una serie de matices. Y debido a que algunos de los matices del XDR son simplemente un cambio de marca de la detección y respuesta de *endpoints* (EDR), los proveedores no comparten necesariamente las mismas capacidades. Merece la pena prestar atención.

Entonces, ¿cómo puedes distinguir entre las distintas opciones que tienes en el mercado? Según un analista líder de la industria, «son muy pocos los proveedores que pueden ofrecer de verdad un producto XDR». ¿Cómo puedes saber si una solución es un verdadero XDR y no un proveedor más que se ha subido al tren del XDR? Las especificaciones siguientes, aunque no son exhaustivas, pueden ayudarte a separar los ganadores de los aspirantes.

Una verdadera solución XDR:

- Debe poder tomar, normalizar y procesar datos de todas las fuentes de datos (incluidas las fuentes de datos de terceros).
- Debe proporcionar uniones de datos y no simplemente correlacionarlos.
- Es nativa de la nube y puede ampliarse de manera efectiva hasta un grado infinito.
- Combina de forma nativa la red, el *endpoint*, la identidad y la nube para llevar a cabo un análisis de datos cruzados.
- Aplica lógica inteligente y avanzada para mostrar la historia completa de un incidente en una sola vista.
- Asigna automáticamente evidencia y artefactos al marco de ATT&CK de MITRE.
- Proporciona una capacidad integrada para llevar a cabo análisis forenses profundos.
- Cuenta con el respaldo de equipos de servicios de seguridad e investigación de seguridad de primera clase.

¿Adopta la solución un enfoque que prioriza la prevención?

El XDR es «detección y respuesta extendidas» y su fortaleza radica en la capacidad de interoperar a un nivel profundo de integración con disposi-

(continuación)

(continuación)

tivos que pueden bloquear, interrumpir y contener amenazas y ataques antes de que se produzca ningún daño. Los más importantes dispositivos de este tipo son los cortafuegos y *endpoints* de red de próxima generación, porque la red representa el registro completo de las comunicaciones y *endpoints* y la forma en que los usuarios interactúan con todas las aplicaciones y datos.

¿La solución de detección se basa solamente en el endpoint?

¿Puede la solución detectar ataques basados en la identidad, la nube y los datos de red, o incluso entre dispositivos no administrados? Algunos proveedores de «XDR» dirán que ven los datos de la red cuando a lo que realmente se refieren es al tráfico de la red recopilado por los agentes de *endpoint*.

Un verdadero XDR permitirá que cualquier dato se correlacione con la actividad de amenazas y se etiquete con TTP de ATT&CK de MITRE para poder proporcionar una imagen más detallada del movimiento del adversario.

¿Tiene la solución capacidades nativas de investigación y respuesta?

Un verdadero XDR:

- Utiliza análisis de seguridad para automatizar las recomendaciones de respuesta.
- Permite llevar a cabo acciones de respuesta nativas en el *endpoint*.
- Puede integrarse con otras herramientas, como SOAR, para la respuesta (aunque no las necesita).
- Permite una respuesta a través de la red de *endpoints* y los puntos de aplicación en la nube en lugar de solo en los *endpoints*.
- Permite un soporte nativo de las búsquedas puntuales en todas las fuentes de datos de terceros utilizando métodos de búsqueda e investigación optimizados para los analistas.
- Optimiza la clasificación y las investigaciones al mostrar todos los artefactos maliciosos, alertas correlacionadas, *hosts* y usuarios relacionados, asignados a ATT&CK de MITRE.
- Puede proporcionar recomendaciones inteligentes para acciones de respuesta específicas basadas en ATT&CK de MITRE.

EN ESTE CAPÍTULO

- Conocer más de cerca el ciclo de vida del ataque.
- Analizar un ejemplo de ataque multifacético.

Capítulo 3
Fin del ciclo de vida del ataque gracias al XDR

Los actores de amenazas han evolucionado y han pasado de ejecutar ataques directos contra un servidor o activo de alto valor («conmoción y pavor») a llevar a cabo procesos pacientes de varios pasos que combinan *exploits*, *malware*, sigilo y evasión en un ataque de red coordinado («imperceptible y lento») .

En este capítulo, aprenderás en qué consiste el ciclo de vida del ataque y cómo la detección y respuesta extendidas (XDR) te ayudan a ponerle fin para detener los ataques contra tu entorno. En este capítulo te ofrecemos una representación general de las fases comunes de un ataque. Muchos equipos de seguridad se han acogido al marco de tácticas, técnicas y conocimiento común de adversarios (ATT&CK) de MITRE para poder rastrear las amenazas en las distintas fases de un ataque. Un verdadero XDR debe poder detectar cada paso que da un adversario y asignar cada paso a las tácticas y técnicas ATT&CK de MITRE para simplificar las investigaciones.

Comprender el ciclo de vida del ataque

El ciclo de vida del ataque ilustra la secuencia de eventos (o pasos) que da un atacante para infiltrarse en una red y exfiltrar (o robar) datos valiosos. Estos pasos incluyen el *exploit* de vulnerabilidades inicial, la instalación de *malware*, el comando y control, el movimiento lateral y la exfiltración (consulta la figura 3-1).

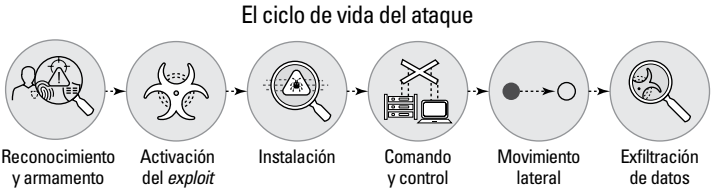

FIGURA 3-1: para que el ataque tenga éxito se necesitan varios pasos.

CONSEJO

Si puedes detectar los pasos al comienzo del ciclo de vida, puedes evitar que los atacantes ejecuten las fases posteriores de un ataque. En los apartados siguientes se analiza más de cerca el ciclo de vida del ataque y cómo el XDR te ayuda a romper ese ciclo de vida.

Reconocimiento

Los actores de amenazas planean meticulosamente sus ataques. Investigan, identifican y seleccionan objetivos, a menudo extrayendo información pública de los perfiles de las redes sociales de los empleados objetivo o de sitios web corporativos, que pueden ser útiles para la ingeniería social y las estafas de *phishing*. Los atacantes también utilizan varias herramientas para buscar vulnerabilidades de la red, servicios y aplicaciones que puedan aprovechar, como analizadores de red, escáneres de vulnerabilidades de red, descifradores de contraseñas, escáneres de puertos y escáneres de vulnerabilidades de aplicaciones web.

El XDR rompe el ciclo de vida durante el reconocimiento a través de una monitorización e inspección continuas de los flujos de tráfico de la red para detectar y prevenir la exploración no autorizada de puertos y vulnerabilidades, barridos de *host* y otras actividades sospechosas.

Armamento

A continuación, los atacantes determinan qué métodos utilizar para poner en peligro un *endpoint* objetivo. Pueden optar por incrustar código intruso en archivos aparentemente inofensivos, como un documento de Microsoft Word o un mensaje de correo electrónico. O, en el caso de ataques altamente dirigidos, los atacantes pueden personalizar los productos para que coincidan con los intereses específicos de un individuo dentro de la organización objetivo. Después, los atacantes intentan enviar su carga armada a un *endpoint* objetivo, por ejemplo, por correo electrónico, mensajería instantánea (IM), descarga automática (mediante la cual el navegador web de un usuario final es redirigido a una página web que descarga *malware* automáticamente en el *endpoint* en un segundo plano) o archivos compartidos infectados.

Romper el ciclo de vida en esta fase de un ataque es difícil porque el uso de estas armas generalmente tiene lugar en la red del atacante. Sin embargo, el análisis de artefactos (tanto el *malware* como las armas) puede proporcionar información importante sobre amenazas para permitir una protección efectiva desde el día cero cuando se intenta llevar a cabo la entrega. El XDR brinda visibilidad de todo el tráfico de la red para bloquear de manera efectiva sitios web, aplicaciones y direcciones de protocolo de internet (IP) maliciosos o que suponen un riesgo, y evitar el uso de *exploits* y *malware* conocidos y desconocidos.

Activación del exploit

Después de que una carga armada se entrega a un *endpoint* objetivo, debe activarse. Un usuario final puede desencadenar involuntariamente un *exploit*, por ejemplo, al hacer clic en un enlace malicioso o abrir un archivo adjunto infectado en un correo electrónico, o un atacante puede desencadenar de forma remota un *exploit* contra una vulnerabilidad conocida del servidor en la red de destino.

Romper el ciclo de vida en esta fase de un ataque requiere capacidades de XDR que incluyen las siguientes:

- Gestión de vulnerabilidades y parches
- Detección y prevención de *malware*
- Información sobre amenazas (incluidas amenazas conocidas y desconocidas)
- Bloqueo de aplicaciones y servicios de riesgo, no autorizados o innecesarios
- Registro y supervisión de toda la actividad de la red, *endpoints* y la nube

CUESTIONES TÉCNICAS

Un agente XDR eficaz previene vulnerabilidades conocidas, desde el día cero y sin parche al bloquear las técnicas de activación de *exploits* que los atacantes utilizan para manipular las aplicaciones. Aunque existen miles de *exploits*, normalmente se basan en un pequeño conjunto de técnicas de activación que no cambian a menudo. Al bloquear estas técnicas, el XDR evita los intentos de los *exploits* antes de que los *endpoints* puedan verse comprometidos (consulta la figura 3-2).

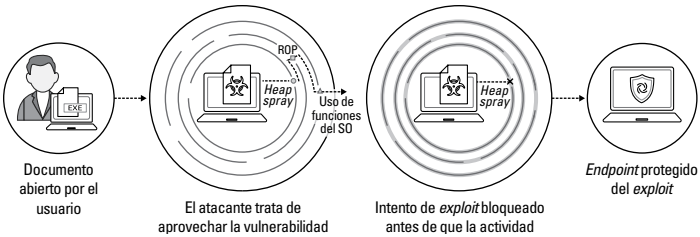

FIGURA 3-2: una solución XDR avanzada se centra en las técnicas y comportamientos de *exploits* en lugar de en los propios *exploits*.

Instalación

A continuación, un atacante aumentará los privilegios en el *endpoint* comprometido (por ejemplo, estableciendo un acceso a *shell* remoto e instalando *rootkits* u otro *malware*). Con el acceso a *shell* remoto, el atacante tiene el control del *endpoint* y puede ejecutar comandos en modo privilegiado desde una interfaz de línea de comandos (CLI), como si estuviera sentado físicamente delante del *endpoint*. Luego, el atacante se moverá lateralmente a través de la red del objetivo, ejecutando el código de ataque, identificando otros objetivos de oportunidad y comprometiendo los *endpoints* adicionales para generar persistencia.

La clave para romper el ciclo de vida en esta fase de un ataque es evitar la instalación en el *endpoint* y limitar o restringir el movimiento lateral del atacante dentro de la red. El XDR aprovecha las tecnologías de detección y respuesta de *endpoints* (EDR) y la plataforma de protección de *endpoints* (EPP) para evitar la instalación. El XDR también supervisa e inspecciona todo el tráfico entre zonas o segmentos en un modelo Zero Trust y proporciona un control granular de las aplicaciones que están permitidas en el entorno.

Comando y control

Los actores de amenazas establecen canales de comunicación cifrados a los servidores de comando y control a través de internet. Este planteamiento les permite modificar sus objetivos y métodos de ataque a medida que se identifican objetivos de oportunidad adicionales dentro de la red de la víctima, así como evadir cualquier nueva medida defensiva de seguridad que la organización pueda intentar implementar si se descubren artefactos de ataque. La comunicación es esencial para un ataque porque permite al atacante dirigir dicho ataque de forma remota y ejecutar sus objetivos. El tráfico de comando y control debe ser resistente y sigiloso para que un ataque tenga éxito.

Para romper el ciclo de vida en esta fase de un ataque se necesita lo siguiente:

- Inspeccionar todo el tráfico de la red (incluidas las comunicaciones cifradas)
- Bloquear las comunicaciones salientes de comando y control con firmas anti-comando y control (junto con cargas de patrones de datos y archivos)
- Bloquear todas las comunicaciones salientes a localizadores uniformes de recursos (URL) y direcciones IP maliciosos conocidos
- Bloquear las técnicas de ataque novedosas que emplean métodos de evasión de puertos
- Evitar el uso de anonimizadores y *proxies* en la red
- Supervisar el sistema de nombres de dominio (DNS) en busca de dominios maliciosos y contrarrestar los sumideros (*sinkholes*) o el envenenamiento del DNS
- Redirigir comunicaciones salientes maliciosas a señuelos (*honeypots*) para identificar o bloquear *endpoints* comprometidos y analizar el tráfico del ataque

Movimiento lateral y exfiltración

Los atacantes tienen a menudo varios objetivos de ataque diferentes, incluido el robo de datos, la destrucción o modificación de sistemas, redes y datos críticos, y la denegación de servicio (DoS). Esta última fase del ciclo de vida también puede ser utilizada por un atacante para avanzar en las primeras fases del ataque contra otro objetivo. Por ejemplo, un atacante puede poner en peligro la extranet de una empresa para infiltrarse en uno de sus socios comerciales, que es el objetivo principal. Estos tipos de ataques a la cadena de suministro llegaron a los titulares de noticias en 2020 con el ataque SolarWinds.

Para romper el ciclo de vida en esta fase se necesitan herramientas XDR que puedan detectar y prevenir automáticamente la exfiltración de datos y otras acciones maliciosas o no autorizadas.

Análisis de un ejemplo de ataque

Para ayudarte a visualizar todos los pasos del ciclo de vida del ataque y su función en un ataque, echemos un vistazo a un ataque hipotético. En la figura 3-3, un actor de amenazas ejecuta los pasos siguientes para atacar un objetivo:

1. Activación del *exploit*.

   El atacante aprovecha los errores del servidor web para tomar el control del servidor.

2. Instalación.

   El atacante usa el control del servidor para instalar Mimikatz y obtener acceso a las credenciales de administrador.

3. Comando y control.

   El atacante instala *malware* adicional y herramientas de acceso remoto para establecer comunicaciones de persistencia y de comando y control.

4. Movimiento lateral.

   El adversario se mueve lateralmente a través de la red, pone en peligro varios *endpoints* y accede a aplicaciones en la nube pública y privada.

5. Acceso y exfiltración.

   El atacante mira los archivos de configuración en el servidor, encuentra la ubicación de la base de datos de *back-end*, consulta la base de datos y guarda los resultados en un archivo local. Los datos recopilados se cargan en una ubicación de almacenamiento en la nube «autorizada». A continuación, el atacante elimina el archivo que contiene los datos de la base de datos, borra los registros locales y cierra la sesión.

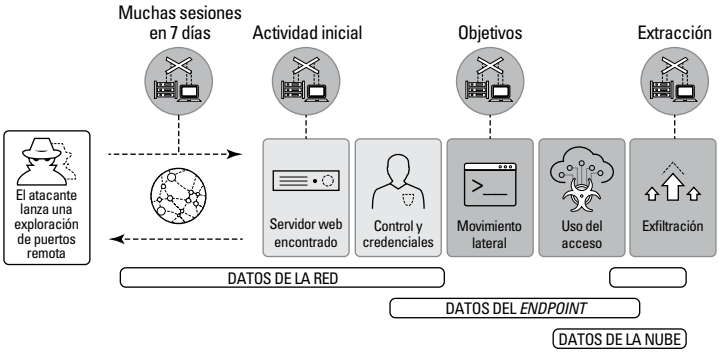

FIGURA 3-3: el XDR puede detener de forma exclusiva estos ataques avanzados que constan de varios pasos al recopilar datos de todas las fuentes y poder detectar y detener las tácticas de ataque que otras herramientas pasan por alto.

Una plataforma XDR recopila y analiza varios tipos de datos para detectar y detener las tácticas del adversario a lo largo del ciclo de vida del ataque.

EN ESTE CAPÍTULO

- Detectar la actividad de amenazas con XDR.
- Gestionar y validar las alertas.
- Agilizar las investigaciones y la respuesta.
- Facilitar la búsqueda proactiva de amenazas.

Capítulo 4
Análisis de casos de uso del XDR

En este capítulo, te presento los casos de uso más frecuentes para que tu organización pueda mejorar sus capacidades de detección y respuesta, incluida la detección, clasificación y validación de alertas, la automatización de las investigaciones y respuesta, y la búsqueda de amenazas.

Detección

Para evitar que un ciberataque logre su objetivo, debes centrarte en detectarlo en cada fase de su ciclo de vida. El XDR (detección y respuesta extendidas) utiliza el aprendizaje automático para descubrir las características únicas de tu organización, lo que le permite diferenciar entre la actividad de las amenazas y la actividad normal, más allá de lo que es posible con un análisis manual o con reglas de correlación estática. Este aprendizaje automático impulsa el análisis avanzado, la creación de perfiles y la detección de amenazas de comportamiento. A través de esta detección integral, una solución XDR mejora la capacidad de detectar actividad maliciosa, incluidos ataques dirigidos, personas internas malintencionadas y mucho más.

Ataques dirigidos

Los atacantes intentan que sus actividades se mezclen con el uso legítimo en cada fase del ciclo de vida del ataque. Con la capacidad del XDR de recopilar datos de cualquier fuente para detectar y unir automáticamente

datos de seguridad clave para los análisis avanzados de datos cruzados, puedes detectar los ataques más sigilosos. Con la analítica, puedes trazar el perfil del comportamiento del usuario y detectar comportamientos anómalos, como los intentos de un atacante para comprometer dispositivos y moverse lateralmente en la red, buscando y exfiltrando datos confidenciales.

Personas internas malintencionadas

Las personas internas malintencionadas utilizan sus credenciales de confianza y el acceso para robar datos corporativos sin ser detectados. El XDR aborda esta amenaza buscando anomalías en el comportamiento y la actividad del usuario (consulta la figura 4-1). Las soluciones XDR pueden agilizar el análisis al presentar una vista completa de cada usuario con una puntuación de riesgo clara.

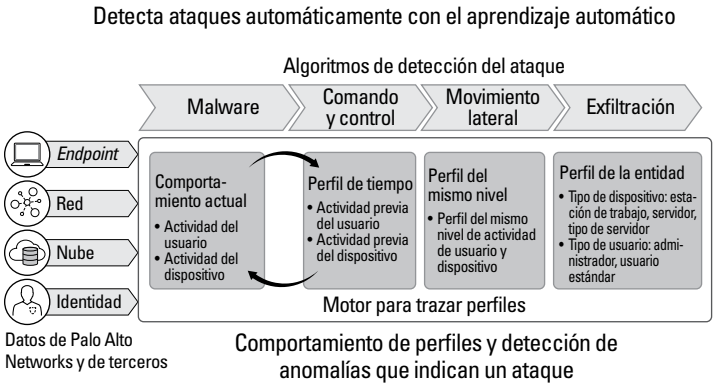

FIGURA 4-1: los análisis de comportamiento descubren anomalías a nivel de usuario, aplicación y dispositivo.

Riesgo inadvertido

Los empleados bien intencionados pueden exponer de manera inadvertida a las organizaciones a riesgos innecesarios mediante un abuso y uso indebido del acceso autorizado. Una solución XDR permite a las organizaciones seguir las mejores prácticas de seguridad al supervisar la actividad del usuario e identificar el comportamiento de riesgo para detectar cuándo un empleado infringe las políticas de seguridad, ya sea de forma inadvertida o no.

Endpoints comprometidos

Los atacantes a menudo usan el *malware* para infiltrarse en redes específicas comprometiendo un *endpoint* y moviéndose lateralmente a través de la red. El XDR reúne los datos de seguridad de las redes y *endpoints* para buscar tráfico anómalo generado por *malware* y otras actividades

maliciosas. Estos datos de seguridad también proporcionan los medios para investigar en todo el entorno y poder determinar el alcance del ataque.

Por ejemplo, si un actor de amenazas añade un nuevo valor a la clave de registro de ejecución automática, una solución XDR podría detectar el nuevo valor de ejecución automática y generar una alerta con una descripción clara de esta actividad sospechosa, incluido un contexto de investigación enriquecido con la táctica y la técnica ATT&CK de MITRE. La solución XDR podría incluso determinar qué proceso añadió el valor de ejecución automática y la secuencia de eventos que condujeron a la actualización para proporcionar la historia completa del ataque.

RECUERDA

El XDR detecta ataques activos con una precisión incomparable y aumenta la capacidad de los equipos de seguridad para:

- Detectar la actividad maliciosa de los recursos internos y externos mediante la búsqueda de patrones entre la actividad que tiene lugar en la red, los *endpoints* y la nube.
- Utilizar técnicas analíticas de vanguardia con cantidades significativas de datos de seguridad para identificar actividad anormal sin aumentar el nivel de falsos positivos.
- Aprovechar la respuesta interna y la información sobre amenazas externa para aprender de ataques pasados y hacer que esa experiencia sea accesible a analistas menos sofisticados, mejorando así el rendimiento de todo el equipo de seguridad.

Investigación y clasificación de alertas

Las soluciones XDR simplifican la clasificación y el análisis de las alertas al revelar la causa raíz de estas, lo que hace que puedan investigarse mucho más rápidamente. Si solo están disponibles los datos del endpoint, se presenta la causa raíz del *endpoint*. Si los datos de la red y del *endpoint* están disponibles, la plataforma XDR puede asociar automáticamente la actividad de la red con los eventos del *endpoint*. Por ejemplo, el XDR no solo determina qué ejecutable del *endpoint* ha sido el responsable de una alerta en la red, sino que también puede averiguar qué aplicación inició el ejecutable.

Dados los desafíos que presenta la falta de habilidades de seguridad de la que hablamos en el capítulo 1, el XDR mejora la capacidad de un analista con menos experiencia para detectar y validar un ataque potencial al agrupar las alertas en incidentes y, dentro de esos incidentes, resumir las actividades o acciones en etiquetas que añaden contexto. Esta flexibilidad garantiza la captura y aprovechamiento del conocimiento para todo el equipo.

El XDR crea una línea de tiempo de los eventos que conducen a la alerta y proporciona información integrada sobre las amenazas. Todo esto permite a los analistas comprender la causa raíz de una alerta, su naturaleza exacta y qué medida deben tomar.

Te explicamos a continuación cómo el XDR ayuda a simplificar el análisis y las investigaciones de incidentes:

1. Evaluación.

   El proceso comienza con la solución XDR que evalúa tanto las alertas externas (por ejemplo, herramientas de seguridad de terceros) como las alertas generadas internamente (basadas en reglas y otros indicadores) para determinar un comportamiento potencialmente sospechoso.

2. Priorización.

   A continuación, la herramienta XDR agrupa automáticamente esas alertas en incidentes, asignándoles un nivel de prioridad para dirigir a los analistas a los incidentes que representan la mayor amenaza. Los analistas pueden hacer clic en cada incidente y ver la lista completa de alertas, dispositivos, información sobre amenazas relacionada y otros contextos para poder comprender el alcance completo de la alerta.

3. Análisis.

   El XDR proporciona una cadena de ataque visual (consulta la figura 4-2), aprovechando las diversas fuentes de telemetría que permite recopilar todo lo que sea relevante para el incidente y proporcionar contexto adicional, causalidad y garantizar un análisis mejor y más rápido. La cadena de ataque muestra los pasos que dio un atacante al revelar la secuencia de procesos que condujeron al paso final del ataque. Además de mostrar las alertas relacionadas, incluida una alerta EPP para el agente XDR, también identifica la causa raíz.

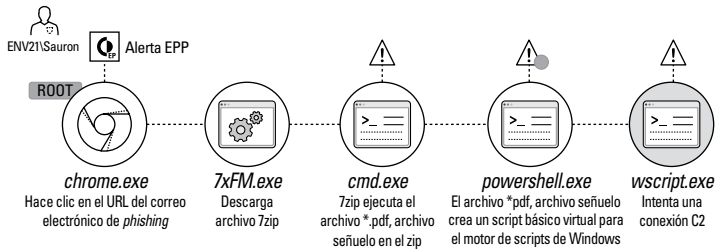

FIGURA 4-2: un ejemplo de cadena de ataque visualizada con XDR.

4. Enriquecimiento.

   Después, la cadena de ataque se enriquece con información contextual adicional, incluida una vista detallada de cómo se generó la alerta, su causa raíz, otros dispositivos de *endpoint*, red y nube afectados, y la reputación de todos los artefactos forenses.

Al contarse por miles las alertas que llegan cada día, automatizar el proceso de clasificación y ofrecer a los analistas información contextual enriquecida es la única forma de gestionar todo el volumen. Con el XDR, los equipos de seguridad pueden dedicar su tiempo y energía a lo que tendrá más efecto: remediar las alertas que pueden causar el mayor daño.

RECUERDA

Con el XDR, los analistas tienen una mayor capacidad para:

Reducir su acumulación de alertas con la gestión de incidentes, la agrupación inteligente de las alertas y el contexto de investigación.

Reducir drásticamente la posibilidad de pasar por alto un ataque.

Analizar las alertas para mejorar la detección y garantizar que la productividad y las defensas posteriores no se vean perjudicadas.

Aplicar nuevos desencadenantes de comportamiento para mejorar los tiempos de clasificación y, opcionalmente, transformar las reglas de detección en reglas de prevención para una prevención de ciclo cerrado.

Investigaciones y respuesta automatizadas y simplificadas

Una vez que se ha clasificado y priorizado una alerta, puede justificarse una investigación más profunda. La automatización del XDR acelera el proceso de investigación de cualquier alerta o campaña de búsqueda, eliminando las tareas manuales que requieren mucho tiempo al tener una imagen clara de la amenaza, analizar la causa raíz, verificar la reputación y resolver la atribución del ataque.

Las herramientas XDR comienzan añadiendo toda la telemetría a un repositorio de datos de seguridad, como un lago de datos en la nube (consulta la figura 4-3). Para reducir el tiempo de investigación, la solución XDR puede correlacionar y agrupar las alertas de todas las herramientas de detección en una pequeña cantidad de incidentes precisos sobre los que se puede actuar, incluida la información sobre el usuario, la aplicación y el dispositivo. El XDR también puede ayudar en las investigaciones forenses al interrogar a los *endpoints* para determinar qué proceso o ejecución inició un ataque.

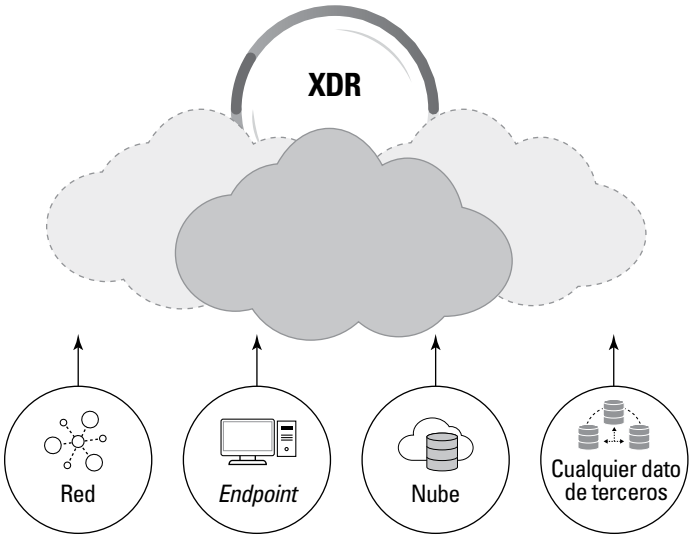

FIGURA 4-3: las herramientas XDR unen datos de diferentes sensores en un repositorio de datos en la nube.

Para profundizar en el incidente, una solución XDR determina después si el proceso del *endpoint* es malicioso. Para ello, se integra con fuentes y servicios de información sobre amenazas que permiten analizar el proceso. Una solución XDR facilita a los analistas de seguridad la verificación de los ataques al presentar toda la información que necesitan en una única interfaz.

Las herramientas XDR también pueden adaptar las defensas, aplicando el conocimiento de incidentes y campañas de búsqueda anteriores para prevenir automáticamente que cualquier amenaza encontrada anteriormente vuelva a producirse con éxito. Este «aprendizaje asistido» permite la detección temprana de ataques según lo que ya se haya visto en el entorno.

Una vez que se ha validado la amenaza, los encargados de la respuesta ante los incidentes pueden elegir entre docenas de técnicas de respuesta y reparación remotas para detener el ataque, prevenir ataques posteriores y restaurar archivos dañados o eliminados, entre otras cosas. Algunas opciones de respuesta consisten en aislar los *endpoints*, bloquear, eliminar o poner en cuarentena archivos, revertir archivos y el registro a un estado limpio, acceder directamente a los *endpoints* y ejecutar *scripts*. El equipo de seguridad se volverá sumamente eficiente, requerirá menos formación, reducirá la carga de los encargados de la respuesta ante los incidentes con más experiencia y minimizará los tiempos de resolución de incidentes.

RECUERDA

Con el XDR, los encargados de la respuesta ante los incidentes tienen una mayor capacidad para:

- Encontrar amenazas sigilosas más rápido aprovechando la información sobre amenazas y el análisis de comportamiento.
- Simplificar y acelerar la investigación y la respuesta al proporcionar búsquedas profundas y extensas de la telemetría recopilada de las redes, los *endpoints* y la nube.

Búsqueda de amenazas

Las soluciones XDR mejoran tus capacidades de búsqueda de amenazas a través de la identificación automática y puntual de la actividad maliciosa en tu entorno. Los buscadores de amenazas pueden llevar a cabo consultas avanzadas y obtener resultados al instante. Algunos ejemplos de cómo el XDR proporciona las capacidades necesarias para trabajar con distintos métodos de búsqueda de amenazas son:

- **Basado en información:** este es el tipo más frecuente de ejercicio de búsqueda de amenazas, donde el buscador ha recibido una pista sobre una amenaza potencial antes de buscarla. Bien se trate de una pista que proviene de la información sobre amenazas, de un nuevo indicador de compromiso (IOC), de un consejo de alguien de la organización o de una mera sospecha, la complejidad de la búsqueda de amenazas basada en la información dependerá del nivel de detalle que la información proporcione. A partir de una fuente de datos integrada que está vinculada a varios proveedores de información sobre amenazas, una solución XDR puede importar manualmente artefactos o indicadores de compromiso de diferentes normas para proporcionar resultados de búsqueda rápidos y sólidos.
- **Sin pistas:** en la búsqueda de amenazas sin pistas, otro método también muy frecuente, el buscador usa sus propios conocimientos o información existente sobre cómo se deben usar un ordenador, aplicación, usuario, datos o red y trata de identificar anomalías o usos anómalos. Este tipo de búsqueda avanzada de amenazas generalmente se deja a los miembros del equipo más experimentados, que utilizan técnicas como la talla de datos y la analítica para lograr resultados. Una solución XDR simplifica este proceso al incorporar estas técnicas avanzadas en su interfaz, lo que permite a los buscadores con cualquier nivel de experiencia aprovecharlas sin *scripts*, herramientas adicionales ni la necesidad de aprender un nuevo lenguaje de consulta.
- **Basado en resultados:** con este método, el buscador busca alertas pasadas en cuarentena, investigaciones completadas o cualquier

otra amenaza resuelta y las utiliza para identificar variantes de la amenaza, nuevas amenazas potenciales o vectores de ataque abiertos. Una solución XDR de calidad puede incorporar de forma automática y continua la búsqueda de amenazas basada en resultados directamente en el flujo de trabajo de las alertas de seguridad y manejo de incidentes. Las lecciones aprendidas con cada investigación se aplican para garantizar que no se vuelvan a producir los ataques.

- **Basado en el cumplimiento:** este método de búsqueda de amenazas se centra en garantizar el cumplimiento de los requisitos internos, de la industria y del gobierno mediante la puesta en práctica de búsquedas de rutina que indiquen incumplimiento, por ejemplo, datos confidenciales almacenados en sistemas no autorizados o aumento de privilegios por parte de usuarios administradores. Se puede configurar una solución XDR para alertar a los analistas de seguridad de este tipo de actividad y proporcionar un medio para investigar rápidamente la situación.
- **Basado en el aprendizaje automático:** los sistemas de aprendizaje automático establecen como referencia los comportamientos típicos de una organización para comprender lo que es normal y lo que no. Mediante análisis a gran escala, las soluciones XDR utilizan el aprendizaje automático para supervisar comportamientos e identificar anomalías que se desvían de estas referencias establecidas. Estos indicadores de compromiso del comportamiento (BIOC) detectan muchas amenazas sigilosas que es posible que un analista no pueda identificar manualmente y se optimizan continuamente con el tiempo para mejorar el modelo de aprendizaje automático. Esta forma de búsqueda de amenazas representa el mayor ahorro de tiempo para los analistas y es fundamental para optimizar los resultados de seguridad.

RECUERDA

Con el XDR, los buscadores de amenazas tienen una mayor capacidad para:

- Aprovechar los datos de la red, los *endpoints* y la nube para realizar búsquedas y análisis.
- Aprovechar la automatización para hacer búsquedas en toda la actividad de la red, los *endpoints* y la nube.
- Utilizar búsquedas y asistentes sumamente configurables para encontrar amenazas internas y externas que han identificado los IOC y BIOC tradicionales y que están almacenadas en tu biblioteca de amenazas.
- Remediar los ataques mediante la integración con controles de seguridad.

EN ESTE CAPÍTULO

- **Garantizar una prevención de amenazas sólida y una visibilidad completa.**
- **Simplificar las investigaciones con funciones de análisis, aprendizaje automático, respuesta coordinada y orquestación.**
- **Maximizar la flexibilidad con un paquete de protección completo.**
- **Observar la validación de terceros, las hojas de ruta innovadoras y el valor total.**

Capítulo 5
Diez funciones y características clave del XDR

El XDR (detección y respuesta extendidas) permite a las organizaciones evitar que los ciberataques logren su objetivo, además de simplificar y fortalecer los procesos de seguridad mediante un enfoque proactivo ante la detección y respuesta de amenazas. El XDR detiene los ataques modernos recopilando y analizando los datos de cualquier fuente. Unifica la prevención, detección, investigación y respuesta para brindar una seguridad y eficiencia operativa incomparables.

En este capítulo te presentamos diez elementos «imprescindibles» que debes buscar en una solución XDR para tu organización. También explicamos cómo Cortex XDR, la primera plataforma de detección y respuesta extendidas de la industria, ofrece estas características esenciales.

La mejor prevención de amenazas en endpoints de su clase

La protección de tu organización comienza con la mejor prevención de amenazas en *endpoints* de su clase, que bloquea *malware*, *ransomware*, ataques sin archivos y *exploits* conocidos y desconocidos.

RECUERDA

Cortex XDR proporciona todo lo que necesitas para la prevención, detección y respuesta de amenazas con un solo agente que se gestiona desde la nube. Protege tus *endpoints* con el mejor análisis local de la industria impulsado por inteligencia artificial (IA) y con protección basada en el comportamiento (consulta la figura 5-1).

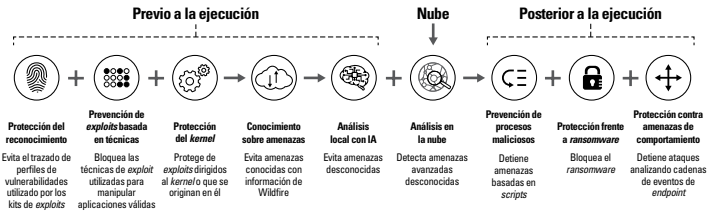

FIGURA 5-1: Cortex XDR proporciona una prevención completa de amenazas en *endpoints*.

Busca un antivirus de próxima generación que proporcione:

- Protección contra *malware*, *ransomware* y amenazas sin archivos
- Información global sobre amenazas en tiempo real basada en la nube
- Análisis local mediante aprendizaje automático
- Protección contra amenazas de comportamiento
- Protección granular de procesos secundarios
- Prevención de *exploits* basada en técnicas y antes de la instalación del *exploit*
- Prevención de *exploits* en el *kernel*
- Protección contra robo de credenciales

Conjunto flexible de funciones de protección de endpoints

Necesitas una forma sencilla de identificar y priorizar los riesgos de los *endpoints*, reducir tu superficie de ataque y detener la pérdida de datos. Busca características de protección de *endpoints*, incluidas las siguientes:

- **Evaluación de vulnerabilidades:** aprovecha la evaluación de vulnerabilidades y la visibilidad de las aplicaciones en los *endpoints* administrados y no administrados, entre otras cosas, para obtener una visión de los activos digitales en toda la empresa.
- **Cortafuegos de host:** administra de manera centralizada las comunicaciones entrantes y salientes en tus *endpoints* desde la consola de administración de Cortex XDR.
- **Cifrado de disco:** aplica políticas de cifrado o descifrado en tus *endpoints* y accede a las listas de todas las unidades cifradas.
- **Control de dispositivos:** supervisa y controla de forma granular el acceso al bus serie universal (USB) para proteger tus *endpoints*.

Visibilidad ampliada en todas las fuentes de datos

Para reducir el riesgo de que un ataque tenga éxito, necesitas un enfoque integral de detección y respuesta que elimine los puntos ciegos, aumente la precisión y agilice las investigaciones en todos los entornos, incluida la red, la nube y el *endpoint*.

CONSEJO

Cortex XDR es la primera plataforma de XDR de la industria que integra de forma nativa los datos del *endpoint*, la red y la nube para detener ataques sofisticados. Cortex XDR ofrece todas las capacidades de la detección y respuesta de red (NDR), detección y respuesta de *endpoints* (EDR), protección de *endpoints* (EPP), detección y respuesta en la nube (CDR) y análisis de comportamiento de usuarios y entidades (UEBA), como se muestra en la figura 5-2.

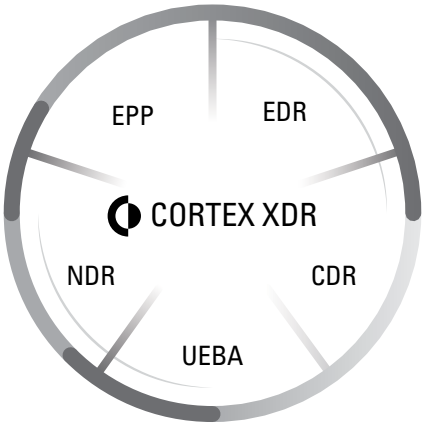

FIGURA 5-2: Cortex XDR recopila y analiza datos enriquecidos para ofrecer las capacidades que tradicionalmente proporcionaban las herramientas EPP, EDR, NDR, CDR y UEBA.

Investigaciones simplificadas

Las herramientas de seguridad en silos de hoy en día generan alertas infinitas con un contexto limitado. Según el informe *Cost of a Data Breach Report* (*El coste de una filtración de datos*) de 2020 del Ponemon Institute, la media de tiempo para identificar y contener una filtración es de 280 días. Para reducir los tiempos de respuesta, las herramientas de seguridad deben proporcionar una imagen completa de los incidentes, con detalles completos de la investigación.

CONSEJO

Cortex XDR simplifica las investigaciones al revelar automáticamente la causa raíz, la secuencia de eventos y los detalles de información sobre amenazas de las alertas. Reduce el tiempo de investigación en un 88 % al revelar la causa raíz y el contexto enriquecido de las alertas de red, *endpoint* y nube, y reduce las alertas en un 98 % con la agrupación de alertas inteligente y la desduplicación.

Analítica y aprendizaje automático

Los actores de amenazas aprovechan las tecnologías de aprendizaje automático y en la nube para aumentar la escala y la eficacia de sus ataques. Necesitas un conjunto completo de técnicas de análisis y aprendizaje automático para adelantarte a las amenazas que evolucionan rápidamente y combatir los ataques sofisticados.

RECUERDA

Cortex XDR proporciona:

- Un análisis local impulsado por IA para bloquear *malware*
- Un análisis de comportamiento para detectar intrusiones y ataques activos
- Un análisis global para mejorar la precisión y alcance de la detección

Respuesta coordinada

Después de identificar las amenazas en tu entorno, debes contenerlas rápidamente. Tu equipo necesita opciones de respuesta integradas y flexibles para detener los ataques rápida y eficazmente antes de que puedan causar más daños. Una solución XDR debe permitir a tu equipo detener de forma remota la propagación de *malware*, restringir la actividad de la red desde y hacia los dispositivos y actualizar las listas de prevención de amenazas, como los dominios perjudiciales, a través de una estrecha integración con los puntos de aplicación.

CONSEJO

Cortex XDR permite a tu equipo de seguridad eliminar al instante las amenazas en la red, el *endpoint* y la nube desde una sola consola.

Automatización de las tareas de seguridad

Las tareas y los procesos manuales ralentizan la respuesta ante incidentes y aumentan el coste de las operaciones de seguridad. Al ejecutar distintas acciones de respuesta de forma nativa en el *endpoint* y en otros puntos de cumplimiento clave, las soluciones XDR pueden contener amenazas rápidamente. Los centros de operaciones de seguridad avanzados pueden necesitar procesos que incluyan la lógica de decisiones y la orquestación de los flujos de trabajo controlados por cuadernos de estrategias e incluir distintas acciones en una amplia gama de herramientas de seguridad y TI de proveedores diferentes. Una solución de automatización y orquestación de seguridad con todas las funciones que proporcione lógica de orquestación y tenga integraciones de socios y contenido y cuadernos de estrategias predefinidos puede responder a estas necesidades. Por lo tanto, busca una solución XDR que se integre sólidamente en una plataforma SOAR líder en la industria.

RECUERDA

Cortex XDR se integra sólidamente con Cortex XSOAR para proporcionar una gestión completa de la información sobre amenazas y ofrece más de 750 integraciones de socios y 680 paquetes de contenido para que puedas llevar tus operaciones de seguridad a un nivel más avanzado.

Pruebas y validación independientes

Al elegir una solución XDR, siempre debes revisar las pruebas de terceros, la validación de los analistas y los testimonios de clientes para obtener un punto de vista independiente y objetivo.

CONSEJO

Cortex XDR ha logrado resultados excepcionales en las pruebas, incluida la mejor detección y protección combinadas en la evaluación de la tercera ronda de ATT&CK de MITRE, y una calificación de «Líder estratégico» en la prueba de prevención y respuesta de *endpoint* (EPR) de AV-Comparatives. Cortex XDR, que ha recibido el reconocimiento de clientes y evaluadores, es una herramienta de confianza para proteger tus *endpoints* y datos.

Ritmo de innovación rápido

Para dejar atrás a los ágiles adversarios, busca proveedores que fortalezcan o amplíen continuamente las capacidades de sus productos.

CONSEJO

Cortex XDR continúa redefiniendo la forma en que los equipos de operaciones de seguridad abordan las complejas amenazas modernas y consiguen mayor eficiencia. Al tratar el problema de integración del sistema de recopilar, integrar y analizar los datos y combinarlo con la capacidad de iniciar flujos de trabajo sumamente optimizados y automatizados, el XDR ayuda a resolver con firmeza los desafíos de la detección, investigación y respuesta a escala.

Un rendimiento de la inversión incomparable

Al seleccionar un elemento clave de tu infraestructura de seguridad, debes asegurarte de que proporcionará un valor real que puedas demostrar fácilmente a las partes interesadas.

RECUERDA

Cortex XDR reduce el coste total de propiedad (TCO) en un 44 %, como media, en comparación con las herramientas tradicionales, ya que:

- Aprovecha tus herramientas de seguridad existentes como sensores para la detección y respuesta
- Elimina los servidores de registros locales con implementación en la nube
- Simplifica las operaciones con la unión de datos, agrupación de alertas y análisis de la causa raíz

CORTEX® XDR™

Evaluado. Examinado. Comprobado.

Prueba en real contra el ataque SolarWind

Prevención de amenazas en un 100% y visibilidad en fase de detección al 97% en la ronda 3 de evaluación de MITRE ATT&CK

Líder en Forrester como "Endpoint Security Software As A Service" en el segundo trimestre de 2021

Aprenda más sobre la primera plataforma XDR de la industria

Cortex XDR:
http://go.paloaltonetworks.com/xdrpdpes

Guía esencial para la ronda 3 de MITRE:
http://go.paloaltonetworks.com/mitrewileyes

Forrester ESS Wave:
http://go.paloaltonetworks.com/esswileyes

Contacte con nosotros hoy:
+31 20 808 4600

paloalto® NETWORKS

Mejora la eficacia de tus operaciones de seguridad con el XDR (detección y respuesta extendidas)

Los equipos de seguridad se enfrentan a una enorme variedad de amenazas, desde *ransomware* hasta ataques sin archivos y violaciones de datos. Sin embargo, el mayor problema de muchos analistas de seguridad no es la cantidad interminable de ataques que copan los titulares de las noticias, sino las tareas repetitivas que deben llevar a cabo todos los días para clasificar los eventos e intentar reducir una interminable acumulación de alertas. El XDR (detección y respuesta extendidas) es un nuevo método para detectar, investigar y responder a las amenazas que integra y analiza los datos de cualquier fuente.

Dentro encontrarás...

- Cómo reconocer las limitaciones de los métodos actuales
- Abordar la escasez de personal de ciberseguridad
- Asegurar una prevención de amenazas sólida
- Conseguir una visibilidad completa
- Automatizar las investigaciones y la respuesta
- Mejorar la eficacia de la seguridad
- Proteger los recursos de la red, del endpoint y de la nube

paloalto NETWORKS

Lawrence Miller ha trabajado en distintas industrias de la tecnología de la información durante más de 25 años. Es coautor de *CISSP Para Dummies* y ha escrito más de 200 libros *Para Dummies* sobre numerosos temas de tecnología y seguridad.

Visita Dummies.com®
para ver vídeos, fotografías paso a paso, artículos con instrucciones o para comprar productos.

ISBN: 978-1-119-87975-6

para dummies®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.