XDR: guía esencial

Todo lo que hay que saber sobre la tecnología de detección y respuesta ampliadas (XDR) que está transformando las operaciones de seguridad

Una guía indispensable para el sector de Palo Alto Networks

paloalto NETWORKS | CORTEX XDR BY PALO ALTO NETWORKS

Contenido

CORTEX® XDR™ BY PALO ALTO NETWORKS

Introducción

Año tras año, el desafío de proteger los datos cruciales se intensifica. La evolución de las tendencias tecnológicas, incluido el auge de la adopción de la nube y del Internet de las cosas (IdC), aumenta la vulnerabilidad de los datos confidenciales ante unos atacantes cada vez más sofisticados. Al mismo tiempo, los adversarios utilizan esas mismas herramientas para ganar poder y presencia, lo que les permite perpetrar ataques con gran eficiencia en repetidas ocasiones.

Pese a haber implementado herramientas, procesos y modelos de dotación de personal que responden a las nuevas amenazas conforme surgen, los equipos de seguridad se ven superados, tanto en número como en potencia de fuego. Al final, el resultado de ir añadiendo nuevas funciones a sistemas existentes es una maraña de herramientas mal integradas que absorben mucho tiempo, energía y experiencia. Los analistas menos experimentados cargan con la tarea imposible de clasificar un flujo interminable de alertas de seguridad, pero tanto la formación que reciben como sus recursos son limitados. Por culpa de esta combinación de demasiadas alertas y contexto insuficiente, los equipos de seguridad pierden visibilidad y agilidad frente a sus adversarios. A la larga, la empresa es más vulnerable.

XDR se ha abierto paso como una categoría de mercado en respuesta a esta complejidad con una premisa básica muy sencilla: es una categoría de soluciones de detección, investigación y respuesta frente a amenazas que funciona en todos los vectores de amenazas de la infraestructura de una empresa (como la red, los endpoints y la nube), y no únicamente en uno de ellos. Las herramientas de XDR, que se caracterizan por estar mejor integradas, aumentan la visibilidad y el acceso a la información, tanto para los modelos de aprendizaje automático en los que se basan como para los analistas de seguridad que las utilizan.

«La ciberdelincuencia es la mayor amenaza a la que se enfrenta cualquier empresa en cualquier lugar del mundo».

Ginni Rometty, directora ejecutiva de IBM

CORTEX XDR BY PALO ALTO NETWORKS

Acerca de esta guía

¿Necesita informarse acerca de la categoría XDR y de las implicaciones para su empresa? Está en el sitio adecuado. Definiremos XDR, describiremos sus funciones clave, sus casos de uso aplicables y su impacto en las funciones de operaciones de seguridad más importantes. El objetivo es que, al final, comprenda:

- qué es y qué no es la tecnología XDR;
- sus ventajas con respecto a las herramientas de detección y respuesta tradicionales;
- en qué funciones debe fijarse al comparar distintas soluciones XDR;
- cómo le puede ayudar esta tecnología a simplificar y mejorar sus operaciones de seguridad.

El desafío

Nos hemos acostumbrado tanto a las noticias sobre brechas de datos y ataques informáticos perpetrados por adversarios sofisticados que la sociedad los ha naturalizado. En el mundo empresarial, tener adversarios en nuestro entorno, seamos o no conscientes de ello, se ha convertido en una realidad aceptada que se suele tomar a la ligera. Pero el hecho de que los adversarios sean habituales no los hace menos peligrosos. Lo cierto es que cada minuto que un adversario activo manipula su entorno, se produce un daño imposible de cuantificar. Como profesional de las operaciones de seguridad que es, sabe perfectamente lo difícil que es detectar los ataques y responder a ellos lo más rápida y eficazmente posible para evitar las temidas pérdidas de datos.

Esto es cada vez más difícil, dado que los ataques y las tácticas empleados por los adversarios son cada vez más avanzados. Ahora, los atacantes pueden poner en riesgo los dispositivos sin tan siquiera recurrir a archivos de malware. Los atacantes sofisticados se sirven de distintos métodos, como la manipulación de archivos del sistema autorizados, la inserción de ataques en el registro de un dispositivo o el uso de utilidades como PowerShell con intenciones malévolas. Esta oleada de ataques, cada vez más singulares y dañinos, hace necesario adoptar nuevas estrategias y tácticas de detección.

Cada día, las brechas sustraen cerca de 4 millones de registros digitales.

Cybersecurity Ventures

CORTEX XDR BY PALO ALTO NETWORKS

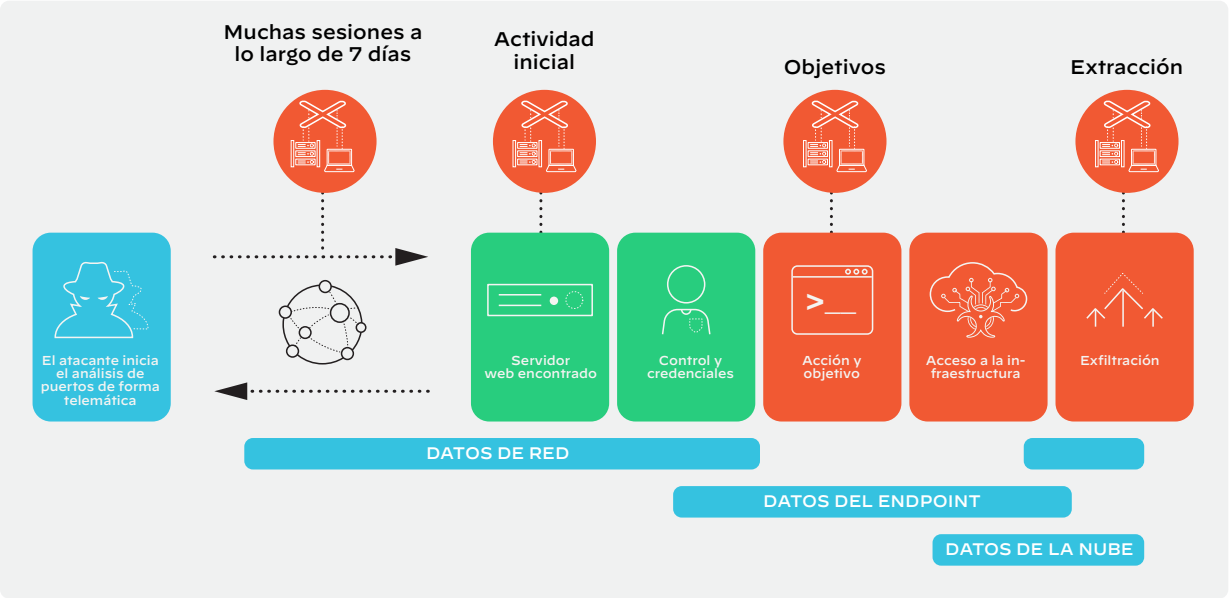

Figura 1: Ejemplo de ataque en varias fases

El atacante:

- se pasa una semana analizando cada cierto tiempo la zona desmilitarizada (DMZ, por sus siglas en inglés) de una empresa, valiéndose del puerto 80 para no ser detectado de inmediato, y acaba infiltrándose a través de un servidor web;
- analiza a fondo el servidor web para ver qué otros puertos y servicios hay disponibles;
- aprovecha los errores del servidor web para controlarlo;
- una vez que se ha hecho con el control del servidor, ejecuta mimikatz para obtener las credenciales de administración;
- examina los archivos de configuración del servidor y localiza la base de datos interna;
- consulta la base de datos y guarda los resultados en un archivo local;
- carga los datos recopilados a un espacio de almacenamiento en la nube autorizado o aprobado;
- elimina el archivo que contiene los datos de la base de datos y borra los logs locales;
- cierra la sesión, con los datos y las credenciales ya en su haber.

CORTEX XDR BY PALO ALTO NETWORKS

Un delicado equilibrio

Para que una organización se mantenga a la vanguardia de la seguridad, se necesitan sobre todo dos cosas: herramientas eficaces y un equipo de analistas de seguridad competentes. Lamentablemente, conseguir el equilibrio apropiado entre capital tecnológico y humano tiende a ser la excepción, más que la regla.

Las tecnologías de detección y prevención generan cientos o miles de alertas al día: mucho más de lo que los equipos de seguridad son capaces de gestionar. Estas alertas proceden de muchas fuentes inconexas, por lo que a los analistas no les queda más remedio que encajar las piezas del puzle por sí solos. El análisis de una amenaza potencial suele requerir seguir ciertos pasos:

1) Revisar los datos de los logs disponibles para empezar a atar cabos y saber qué ha podido ocurrir.
2) Comparar manualmente lo ocurrido con los datos de las distintas fuentes de inteligencia sobre amenazas para determinar si los indicadores son conocidos por ser maliciosos.
3) Encontrar vacíos de información y buscar datos disponibles que puedan arrojar luz sobre cuáles podrían ser los siguientes pasos del ataque.
4) Comprobar si la nueva información está conectada con otras alertas de las que ya se estén haciendo cargo otros miembros del equipo para coordinar esfuerzos.
5) Evaluar si la alerta se debe derivar, descartar o resolver y cerrar cuanto antes.

El 69 % de las organizaciones dudan de la capacidad de su software antivirus para bloquear las amenazas que se ciernen sobre sus entornos.

Ponemon Institute

CORTEX XDR BY PALO ALTO NETWORKS

Normalmente, concluir todo este proceso conlleva mucho tiempo y requiere el uso de varias herramientas; y eso que solo nos estamos refiriendo a la clasificación. En conclusión, los analistas solo tienen tiempo para responder a las alertas de máxima prioridad que reciben diariamente; mientras tanto, un preocupante número de alertas de menor prioridad quedan directamente desatendidas.

Y para rizar aún más el rizo, los analistas de seguridad a cargo de la clasificación y priorización de alertas no suelen disponer de la suficiente información contextual para valorar el riesgo real que un ataque dado representa para la organización. Así, la alerta se deriva a un grupo más sofisticado para que la valide, lo que requiere aún más tiempo, trabajo y recursos; las ineficiencias a todos los niveles están servidas.

Muchas organizaciones intentan utilizar API para integrar sus datos de detección y respuesta. Para ello, suelen usar un costoso sistema de información de seguridad y gestión de eventos (SIEM, por sus siglas en inglés) como piedra angular de sus operaciones de seguridad, que agrega datos de registro analizándolos y normalizándolos, lo que termina despojándolos de buena parte de su valioso contexto. Los equipos de seguridad pueden ver los datos de registro en un solo lugar, pero carentes de sentido, y los primeros analistas que se encargan de dárselo muchas veces no pueden utilizar las herramientas que contienen los datos de origen, que aportan más información.

Otras empresas prefieren externalizar sus funciones de detección y respuesta, parcial o completamente, ya sea a proveedores de servicios de seguridad gestionados (MSSP, por sus siglas en inglés) o a proveedores de detección y respuesta gestionadas (MDR, por sus siglas en inglés), aún más especializados en las amenazas. La externalización de esta función no tiene nada de malo, sobre todo en el caso de los equipos con presupuestos de seguridad más exiguos o que prefieran no contratar recursos para gestionar su propia seguridad. Sin embargo, las organizaciones que busquen tener una visibilidad y un control completos no deberían optar por externalizar su seguridad solo porque sus herramientas sean inadecuadas. También merece la pena recordar que la pila de tecnología sigue siendo importante cuando el equipo de seguridad está externalizado; los proveedores que utilizan herramientas anticuadas se toparán con las mismas ineficiencias que asedian a los equipos de seguridad internos.

Lo que de verdad se necesita es un conjunto de tecnologías que, además de reducir el número total de alertas, permitan a los analistas con menos experiencia valorar por sí mismos las amenazas con confianza y eficiencia, de modo que sus compañeros más experimentados solo reciban alertas fiables.

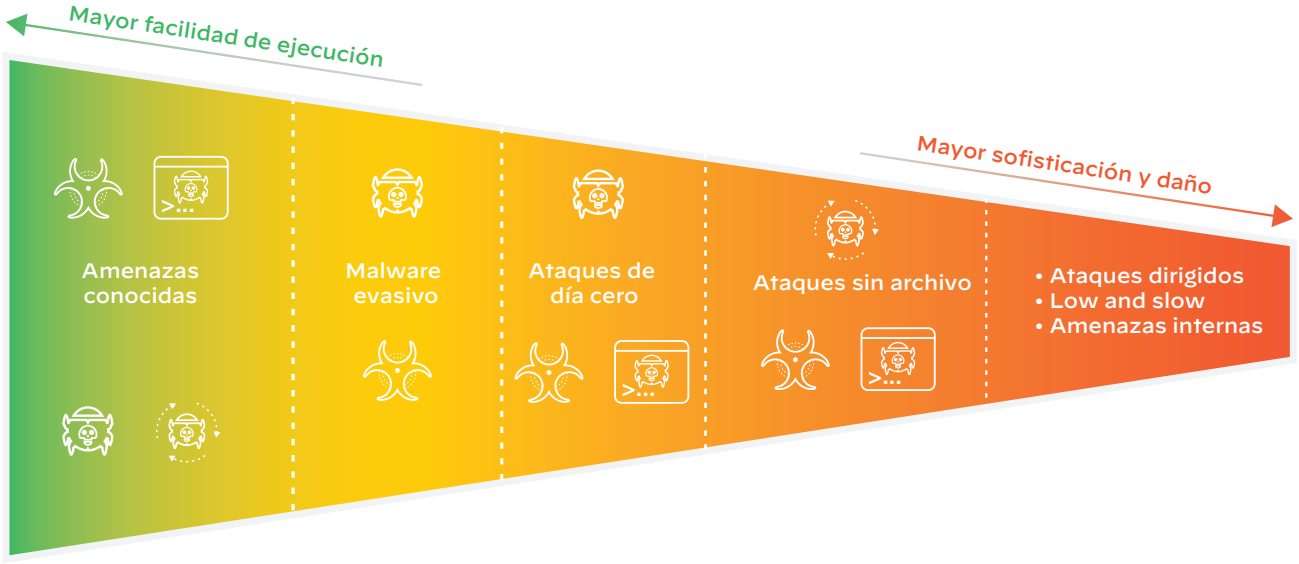

Figura 2: Las herramientas de detección y respuesta están diseñadas para detener ataques sofisticados

CORTEX XDR BY PALO ALTO NETWORKS

Tecnologías de protección, detección y respuesta

Aunque el objetivo primordial siga siendo prevenir los ataques, las organizaciones deben estar preparadas para la realidad de que un porcentaje de atacantes habilidosos encontrarán la manera de introducirse en su infraestructura y conseguir sus objetivos. El mercado pone a disposición de los equipos de seguridad diversas herramientas de creación de logs, detección y respuesta para ayudarlos a encontrar las amenazas que hayan conseguido burlar los mecanismos de prevención. Cada herramienta tiene sus ventajas e inconvenientes, y pueden ser útiles para combatir los ataques sencillos, tales como los de malware basado en archivos o los que amenazan solamente a una parte de la infraestructura. Sin embargo, la mayoría de ellas están diseñadas con un propósito único y ninguna es particularmente adecuada para gestionar campañas complejas por sí sola. Por eso, los equipos de seguridad recurren principalmente a las herramientas de detección y respuesta descritas en los siguientes apartados.

EDR y EPP

Definición de Gartner: *el mercado de soluciones de detección y respuesta en el endpoint (EDR, por sus siglas en inglés) abarca aquellas soluciones que registran y almacenan los comportamientos que se observan en el nivel del sistema del endpoint, utilizan distintas técnicas de análisis de datos para detectar comportamientos sospechosos en el sistema, proporcionan información contextual, bloquean actividad maliciosa y ofrecen sugerencias de corrección para restaurar los sistemas afectados. Las soluciones de EDR deben proporcionar, principalmente, las cuatro funciones siguientes:*

- *Detección de incidentes de seguridad*
- *Bloqueo de incidentes en el endpoint*
- *Investigación de incidentes de seguridad*
- *Orientación para la corrección*

Según IDC, de aquí a 2022 la tasa de crecimiento anual compuesto del gasto en seguridad será del 9,9 %.

Worldwide Security Spending Guide **(disponible en inglés), IDC**

Por sí sola, la solución de EDR no puede proporcionar detección de amenazas de gama empresarial debido a que está destinada al endpoint únicamente. No ofrece visibilidad del tráfico entre los dispositivos de la red sin instalar agentes en los dispositivos (IdC, BYOD, sistemas de control industrial o ICS, conmutadores, enrutadores, servidores, etc.) y recursos en la nube (p. ej., cargas de trabajo, redes de nube, plataformas como servicio o PaaS). Además, las empresas utilizan muchos dispositivos de endpoint no gestionados incompatibles con los agentes de EDR, lo que ofrece a los atacantes potenciales puntos de entrada sin supervisar.

EPP

Definición de Gartner: *una plataforma de protección del endpoint (EPP, por sus siglas en inglés) es una solución que se implementa en los endpoints para evitar ataques de malware basados en archivos, detectar actividad maliciosa y dotar a los dispositivos de funciones de investigación y corrección que permitan responder a alertas e incidentes de seguridad dinámicos.*

No todas las soluciones de este tipo tienen las mismas funciones de detección, pero las más avanzadas combinan varias técnicas, como los indicadores de riesgo (IOC, por sus siglas en inglés) estáticos y el análisis del comportamiento. La mejor opción son las soluciones EPP que se gestionan sobre todo en la nube y que permiten supervisar y recopilar constantemente los datos de actividad, así como hacer correcciones de forma remota, tanto si el endpoint está en la red corporativa como si se encuentra fuera de la oficina. Además, como estas soluciones se nutren de los datos de la nube, el agente del endpoint no tiene que mantener una base de datos local donde se guarden todos los IOC conocidos. Cuando no consiga clasificar ciertos objetos, bastará con que busque los veredictos más recientes en un recurso en la nube.

Sistemas SIEM

Definición de Gartner: *la tecnología de información de seguridad y gestión de eventos (SIEM, por sus siglas en inglés) ofrece herramientas de detección de amenazas, cumplimiento normativo y gestión de incidentes de seguridad que recopilan y analizan eventos de seguridad ocurridos en el pasado o en curso, así como una amplia variedad de otras fuentes de datos contextuales y de eventos. Las funciones centrales cubren un amplio espectro de tareas de recopilación y gestión de logs, la capacidad de analizar eventos de log y otros datos procedentes de diversas fuentes, y funciones operativas (como la gestión de incidentes, los paneles y la creación de informes).*

Las soluciones de detección y respuesta en el endpoint (EDR) surgieron en 2013 para facilitar las investigaciones forenses que requerían datos de telemetría del endpoint muy detallados para realizar operaciones de ingeniería inversa de malware y entender exactamente qué hizo el atacante en un dispositivo atacado.

Muchas organizaciones destinan una gran proporción de sus presupuestos de seguridad a sistemas SIEM para recopilar los logs de los dispositivos de seguridad y entornos de servidor. En principio, los SIEM se diseñaron con el fin de recopilar logs para emitir informes. Con el tiempo, su uso se fue extendiendo a la detección de amenazas y ahora los SIEM se han convertido en el repositorio de alertas centralizado de muchos centros de operaciones de seguridad.

Un sistema SIEM centraliza las alertas de muchos dispositivos de seguridad y de red e informa sobre ataques comunes. El problema es que, por sí solo, un SIEM dificulta la detección avanzada porque solo busca ataques concretos según las reglas que se hayan definido en el sistema. Si un atacante sofisticado utiliza un nuevo patrón, lo más probable es que el ataque pase desapercibido para el SIEM. De hecho, los logs que activan el análisis basado en SIEM rara vez proporcionan el contexto necesario para validar las alertas.

NDR y UEBA

Definiciones de Gartner:

Las soluciones de detección y respuesta en la red (NDR, por sus siglas en inglés) *detectan el tráfico sospechoso que circula por las redes empresariales con técnicas que, en su mayoría, no se sirven de firmas, como el aprendizaje automático y otros métodos de análisis. Las herramientas de NDR analizan constantemente el tráfico sin procesar y los registros de flujo para crear modelos que reflejen comportamientos de red normales.*

Las soluciones de análisis del comportamiento de entidades y usuarios (UEBA, por sus siglas en inglés)*, por su parte, ofrecen herramientas de creación de perfiles y detección de anomalías basadas en diversas metodologías de análisis básico (p. ej., reglas que se sirven de firmas, comparación de patrones y estadísticas sencillas) y de análisis avanzado. Los proveedores utilizan paquetes de análisis para evaluar la actividad de los usuarios y otras entidades (como hosts, aplicaciones, tráfico de red y repositorios de datos) y así descubrir posibles incidentes.*

Los datos de Gartner indican que la seguridad es uno de los principales factores de gasto en TI, y la detección y respuesta es la primera categoría de gasto en seguridad.

Por fin surge una nueva clase de herramientas de análisis de seguridad —entre ellas, las soluciones de detección y respuesta en la red (NDR) y de análisis del comportamiento de entidades y usuarios (UEBA)— para complementar a los sistemas SIEM, que no son tan eficaces a la hora de detectar ataques desconocidos. Estas herramientas utilizan el aprendizaje automático para desarrollar una base de referencia a partir de la telemetría recopilada que después puedan utilizar para buscar acciones atípicas sospechosas de tener un comportamiento malicioso. Estas tecnologías permiten a las organizaciones identificar ataques desconocidos previamente mediante el reconocimiento de patrones de tráfico inusuales.

Pero estas herramientas también tienen sus limitaciones. Los productos basados en red están limitados a la red y no pueden ni supervisar ni controlar eventos locales, como la información sobre procesos recopilada en los endpoints. La tecnología NDR tiene también una profundidad limitada; si los sistemas de EDR son profundos y estrechos, las soluciones de NDR son anchas y superficiales. Las herramientas de UEBA, por su parte, dependen en gran medida de los logs de terceros para supervisar y detectar las amenazas, analizarlas y asignar calificaciones de riesgo a los usuarios. Sin embargo, si las herramientas de terceros dejan de detectar alguna amenaza o prescinden de algún componente de la infraestructura, las soluciones de UEBA se vuelven ineficaces.

Figura 3: Las herramientas aisladas ralentizan la investigación y la respuesta

CORTEX XDR BY PALO ALTO NETWORKS

Conclusión

Los ataques modernos son tan complejos que, para identificar y confirmar la actividad maliciosa, es preciso analizar varias fuentes de datos. Combinar distintas herramientas unidimensionales añade un gasto nada desdeñable para los equipos de seguridad, crea ángulos muertos y requiere mucho trabajo manual por parte de los analistas de seguridad porque los obliga a cambiar de una consola a otra y a entender los ataques por sí solos.

Según 451 Research, el 76 % de los equipos de seguridad identifican al menos un cuarto de los ataques a través de la búsqueda de amenazas manual, lo que indica que las tecnologías y procesos de detección de ataques que tienen implementados para este fin no están cumpliendo su objetivo. A menos que cuente con herramientas de visibilidad completa y análisis de todos los componentes de su entorno, antes o después se le escapará alguna amenaza.

Poner solución al déficit de formación en ciberseguridad

Aunque tuviera a su disposición las mejores y más completas herramientas para la detección de amenazas, gestionar las alertas —y los posibles incidentes— requiere personal muy especializado capaz de validarlas, clasificarlas y asignarles prioridades. Desgraciadamente, estos especialistas escasean, y este déficit de formación repercute en la capacidad de las organizaciones para seguirle el ritmo a los atacantes.

ESG Research concluyó que el 66 % de las organizaciones sienten que la eficacia de su sistema de detección y respuesta frente a amenazas se ve limitada porque se basa en varias herramientas independientes.

ESG

Hoy en día, los adversarios utilizan ataques muy automatizados para encontrar vulnerabilidades e introducirse en los entornos, lo que exacerba aún más si cabe este déficit de formación especializada, ya que pueden adaptar sus herramientas automatizadas de forma más económica y antes de que a las organizaciones les dé tiempo a incorporar personal de seguridad cualificado en sus equipos. De ahí la necesidad de buscar herramientas que vengan a subsanar las carencias de su personal menos experimentado, mediante la automatización de tareas repetitivas, la simplificación de las investigaciones y la adquisición de habilidades.

La mayoría de las empresas recibe miles de alertas de multitud de soluciones de supervisión, pero tanta sobreinformación es contraproducente. La detección no es más avanzada cuantas más alertas reciba el equipo de seguridad, sino cuanto mejores —y más útiles y aprovechables— sean esas alertas. Para llegar a este punto, no solo es necesario integrar la totalidad de las tecnologías de detección en uso, sino también herramientas de análisis sofisticado que analicen los datos de los endpoints, la red y la nube para encontrar y validar la actividad de los adversarios en un entorno dado.

Solo en Estados Unidos, hay más de 300 000 vacantes en el sector de la ciberseguridad, un número que se prevé que siga aumentando en los próximos años.

Cyberseek

Definición de «XDR»

XDR (siglas en inglés de «detección y respuesta ampliadas») es una nueva categoría que ha emergido para satisfacer la necesidad de las empresas de contar con una herramienta de detección y respuesta más completa y sofisticada. La «X» viene de «extended» (ampliadas), pero en realidad representa cualquier fuente de datos, puesto que considerar cada componente de la infraestructura por separado no es ni eficiente ni efectivo. XDR emplea técnicas de aprendizaje automático y análisis dinámico para combinar funciones y resultados asociados a los sistemas SIEM, UEBA, NDR y EDR.

Si XDR es el futuro de la detección y la respuesta, esta herramienta tiene que ser capaz de solucionar los problemas más importantes a los que nos enfrentamos día tras día. Teniendo esto en cuenta, vamos a definir los requisitos que debe cumplir una solución XDR para resolver los problemas identificados anteriormente.

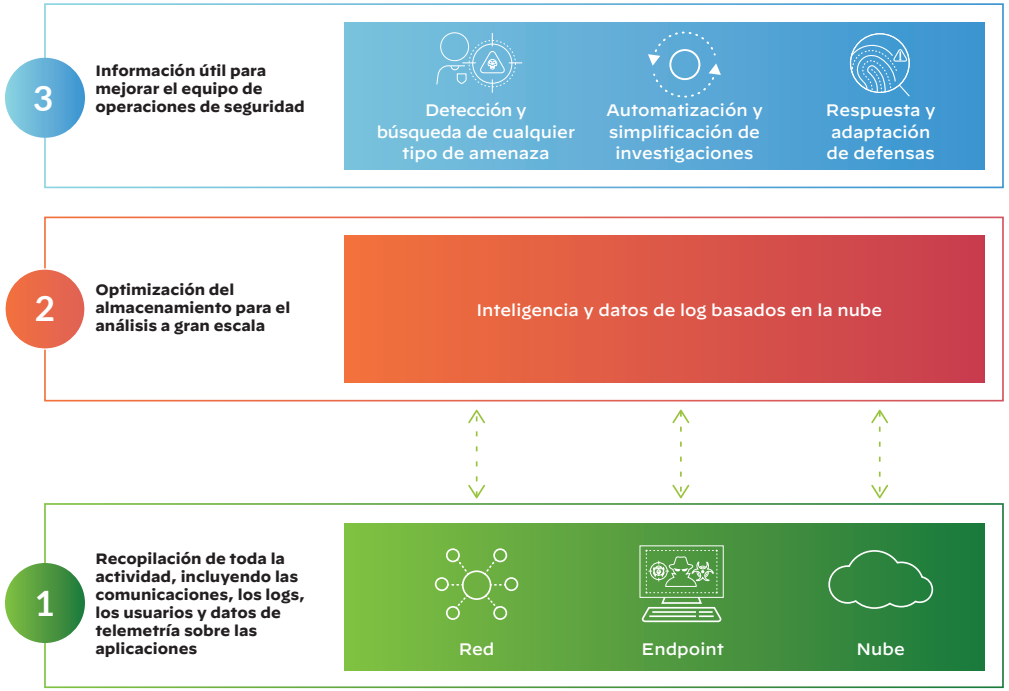

Figura 4: XDR rompe los silos tradicionales de detección y respuesta

CORTEX XDR BY PALO ALTO NETWORKS

Requisito 1: Bloqueo de ataques mediante la prevención de amenazas

La tecnología XDR ofrece una prevención de amenazas sin rival. Concretamente, una solución XDR debería detener más del 99 % de los ataques que pueden bloquearse automáticamente. Esto daría a su equipo la ventaja necesaria para centrarse en localizar y frenar las amenazas más sigilosas, en lugar de perder tiempo investigando todos los ataques que inevitablemente se sufren cuando la protección es insuficiente.

Para contener las amenazas en el endpoint hace falta una solución robusta que incorpore un antivirus de nueva generación (NGAV, por sus siglas en inglés). Esa es la clave para detectar y bloquear todas las fases de un ataque: el exploit inicial, la instalación del malware y la ejecución de este con fines maliciosos. Todas las capas de defensa deben ser lo bastante inteligentes como para resistir a las técnicas de evasión y contar con la adaptabilidad necesaria para que ni las amenazas más recientes logren sortearlas. También es aconsejable que las soluciones XDR elegidas reduzcan la superficie de ataque y protejan los datos confidenciales con funciones de protección del endpoint (p. ej., cortafuegos de host, control de dispositivos y cifrado de disco).

Requisito 2: Localización de amenazas sigilosas más rápida gracias al análisis de la red, los endpoints y la nube

La visibilidad es fundamental para contener las amenazas. Si no puede ver una amenaza, no puede investigarla ni, por descontado, detenerla. Los atacantes se aprovechan de las propiedades de la nube y el aprendizaje automático para perpetrar campañas polifacéticas que les permitan consolidarse en los entornos de las organizaciones y exfiltrar datos cruciales y de propiedad intelectual. Esto significa que una solución XDR debe reunir todas las funciones siguientes.

El 88 % de los hackers creen que pueden infiltrarse en un sistema objetivo en menos de 12 horas.

Nuix (a través de NBC)

CORTEX XDR BY PALO ALTO NETWORKS

Amplia visibilidad y comprensión contextual

Los productos independientes aislados conducen inevitablemente a una sola cosa: silos de datos. Y esto hace ya tiempo que dejó de ser una opción. Para combatir a los atacantes de forma eficaz tiene que ser, como mínimo, tan hábil en su propio entorno como ellos. XDR debe tener funciones de visibilidad y detección en todo su entorno, e integrar la telemetría de sus endpoints, redes y entornos en la nube. Además, debe establecer correlaciones entre esas fuentes de datos para entender cómo están relacionados los distintos eventos y si, por contexto, un comportamiento es o no sospechoso.

Conservación de datos

Los atacantes pueden ser muy pacientes. Son perfectamente conscientes de que la detección es más improbable si se mueven despacio, de modo que no tienen ningún problema en esperar a que expiren los periodos de conservación de logs de las tecnologías de detección de su empresa. XDR no debería ponérselo fácil. Sus sistemas de detección tienen que recopilar, correlacionar y analizar los datos de la red, los endpoints y la nube en un único repositorio, y ofrecer un periodo de conservación de 30 días como mínimo.

Análisis del tráfico tanto interno como externo

Las técnicas de detección convencionales se centran, primordialmente, en los atacantes externos, lo que proporciona una visión incompleta de los posibles adversarios. La detección no puede buscar únicamente ataques procedentes de fuera del perímetro. También debe crear perfiles y analizar circunscripciones internas para buscar comportamientos anómalos y potencialmente maliciosos en aras de identificar un uso indebido de las credenciales.

Solo el 38 % de las organizaciones consideran que están preparadas para gestionar un ciberataque sofisticado.

Cybint

CORTEX XDR BY PALO ALTO NETWORKS

Inteligencia sobre amenazas integrada

Debe contar con las herramientas necesarias para gestionar los ataques desconocidos. Un método de gran ayuda es la posibilidad de aprovechar los ataques conocidos que ya hayan visto otras organizaciones con anterioridad mediante el empleo de la inteligencia sobre amenazas recopilada por una red internacional de empresas. Cuando otra organización de la red identifica un ataque, puede aprovechar el conocimiento adquirido con el ataque inicial para identificar ataques sucesivos.

Detección personalizable

La protección de cada organización deriva en otros problemas, pues sus sistemas, usuarios y adversarios son únicos. Lo ideal sería que los sistemas de detección pudieran configurarse según las necesidades concretas de su entorno y ofrecer detecciones tanto predefinidas como a medida.

Detección basada en el aprendizaje automático

Con ataques que no parecen malware tradicional —como los que se dirigen a los archivos del sistema autorizados, utilizan entornos de scripts y atacan al registro— es preciso que la tecnología de detección emplee técnicas analíticas avanzadas que examinen toda la telemetría recopilada. Estas metodologías incluyen aprendizaje automático supervisado y parcialmente supervisado.

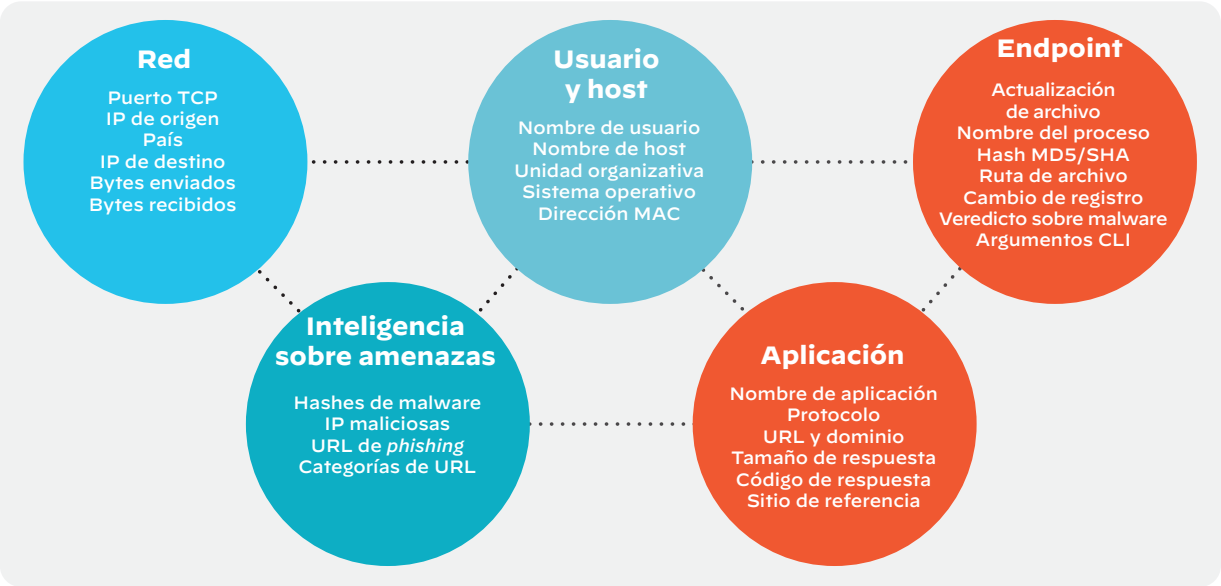

Figura 5: XDR establece correlaciones entre datos enriquecidos y les da sentido

CORTEX XDR BY PALO ALTO NETWORKS

Requisito 3: Simplificación de la investigación y respuesta a amenazas conocidas y desconocidas

Una vez alertado por la presencia de posibles amenazas en su entorno, es el momento de clasificarlas, priorizarlas e investigarlas sin tiempo que perder. El problema de los sistemas tradicionales de detección y respuesta es que no aciertan a realizar este proceso de forma rápida y efectiva, sobre todo cuando el ataque afecta a distintos componentes de la infraestructura. Pero las soluciones XDR pueden mejorar drásticamente el proceso de investigación y dedicaremos los próximos apartados a explicar cómo.

Correlación y agrupación de alertas relacionadas y de datos de telemetría

Para cuando se recibe una alerta, el atacante ya se ha puesto a trabajar en su objetivo. Por eso, el tiempo es esencial. Tiene que ser capaz de entender rápidamente el ataque y toda su cadena de causalidades. Esto significa, en primer lugar, que su herramienta de XDR debe reducir la cantidad de información innecesaria agrupando automáticamente las alertas relacionadas y priorizando de forma efectiva los eventos que requieran su atención con la mayor urgencia. Después, su herramienta de XDR deberá describir una cronología del ataque y reunir los logs de actividad de la red, los endpoints y la nube. Visualizar la actividad y secuenciar los eventos permite determinar la causa original del ataque, así como valorar el daño potencial y las posibilidades de proliferación.

Interfaces de usuario consolidadas con capacidad de desplazar los datos

Ya metidos en harina con las alertas, los analistas necesitan un entorno de trabajo optimizado que les permita desplazar los datos desde cualquier fuente con un solo clic. Si dos herramientas ya pueden hacer perder un tiempo precioso a los analistas, imagínese lo que ocurre cuando hay muchas más.

Búsqueda de amenazas manual y automatizada

Cada vez son más las organizaciones que buscan adversarios activos de forma preventiva para que sus analistas puedan formular hipótesis de ataque y discernir entre la actividad que es relevante de la que no lo es. La búsqueda de amenazas requiere funciones de búsqueda avanzadas para encontrar las pruebas que demuestren las hipótesis, así como inteligencia sobre amenazas integrada que permita buscar actividad vista por otros miembros de la red ampliada. Esta inteligencia sobre amenazas debería integrarse y automatizarse de manera que quede bien claro si una amenaza se ha visto con anterioridad sin necesidad de realizar un enorme trabajo de análisis manual, por ejemplo, abriendo 30 ventanas del navegador distintas para buscar una dirección IP «mala» en distintos canales de inteligencia sobre amenazas.

Funciones de orquestación

Una vez detectada e investigada la actividad de un atacante, el siguiente paso es aplicar las políticas de forma eficiente y eficaz. Su sistema debe ser capaz de orquestar una respuesta coordinada a las amenazas activas y prevenir futuros ataques en la red, los endpoints y la nube. Esto incluye la comunicación entre las tecnologías de prevención (p. ej., un ataque bloqueado en la red que actualice automáticamente las políticas que se aplican a los endpoints), ya sea de forma nativa o a través de API, y la capacidad de que el analista responda directamente a través de la interfaz de XDR.

Requisito 4: Mejora de la rentabilidad de las inversiones en seguridad actuales y futuras

XDR debería disparar la rentabilidad de sus inversiones en seguridad. Esto supone aumentar la eficiencia de su equipo para evitar la escasez de personal o, si no es posible, sobreponerse a ella; mejorar la integración entre sus herramientas, y reforzar la eficacia de sus medidas de prevención a lo largo del tiempo con una infraestructura redimensionable e inteligencia artificial. Para ello, XDR debe estar equipado con las siguientes funciones.

Orquestación de la seguridad

Los atributos que hacen que la orquestación sea tan importante a la hora de simplificar las investigaciones son los mismos que permiten maximizar la rentabilidad de las inversiones en su solución de seguridad. Cada organización cuenta con su propia base instalada de controles de seguridad a los que puede recurrir para responder a las amenazas activas. Un aspecto clave de todo sistema de detección y respuesta es el aprovechamiento de lo invertido en los controles existentes para garantizar una respuesta homogénea en toda la empresa.

Procesamiento de datos de terceros

Todas las empresas tienen kits de herramientas de seguridad heterogéneos. Cuanta mayor visibilidad de los datos de cada una de esas herramientas ofrezca la solución XDR, más completa será la seguridad que proporcione. Las mejores soluciones XDR tendrán la flexibilidad de procesar datos de otras herramientas de su entorno, lo que maximiza su valor a la vez que su eficacia.

Almacenamiento y computación escalables

Dada la impredecibilidad de los adversarios de hoy en día, no es cuestión de despreciar la telemetría que puede dar pistas sobre la actividad de un atacante en ataques persistentes más lentos. Esto requiere suficiente capacidad para almacenar pruebas forenses durante meses (o incluso años), así como una gran potencia de análisis que permita dar uso a toda esa telemetría de manera eficaz. Las plataformas basadas en la nube ofrecen este nivel de accesibilidad y capacidad sin restricciones.

Mejora a lo largo del tiempo

Detectar ataques cada vez más sofisticados requiere integrar herramientas de inteligencia artificial, aprendizaje automático y automatización para reducir el esfuerzo manual y aprovechar así al máximo una plantilla de analistas de seguridad escasa. Las soluciones XDR deberían aprender de la experiencia para así reducir el riesgo en el futuro y reforzar continuamente la prevención mediante la aplicación del conocimiento adquirido a través de la detección, la investigación y la respuesta.

Informes y paneles

Sus equipos de seguridad tienen que ser capaces de entender y comunicar su estrategia de seguridad y parámetros operativos. Las soluciones XDR no solo tienen que poder arrojar unos resultados de seguridad más valiosos, sino que también deben resumir el estado de la seguridad a través de informes y paneles.

El uso de técnicas de análisis avanzado e inteligencia sobre amenazas integrada garantiza que tanto los profesionales encargados de responder a las alertas como los responsables de buscar las amenazas cuentan con toda la información que necesitan para localizar y responder adecuadamente a la actividad de los atacantes.

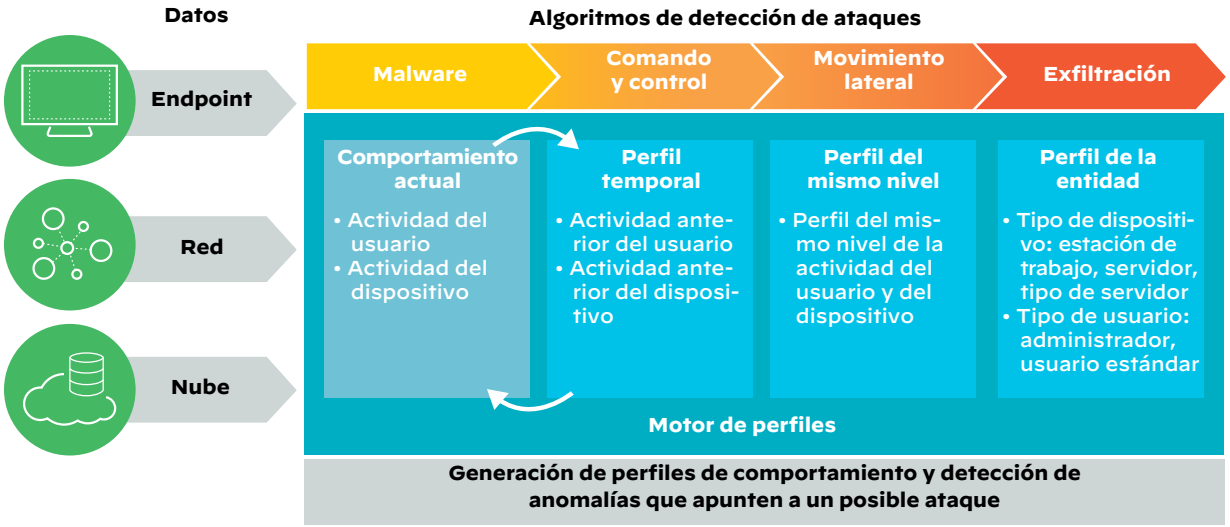

Figura 6: Localice amenazas que solo afectan a su entorno mediante la IA

CORTEX XDR BY PALO ALTO NETWORKS

Figura 7: XDR se adapta a lo largo del tiempo para reforzar las defensas de forma continuada

CORTEX XDR BY PALO ALTO NETWORKS

Casos de uso de las soluciones XDR

Todos los equipos de operaciones de seguridad, grandes y pequeños, tienen en común una serie de funciones clave. El modelo tradicional que siguen muchos equipos de operaciones de seguridad divide estas funciones en una estructura de analistas por niveles basada en la experiencia de sus integrantes. Estas son las principales responsabilidades de cada nivel:

Nivel 1: Clasificación y priorización

Este es el nivel al que se dedica la mayor parte del tiempo de los analistas. Los analistas de nivel 1 suelen ser los que menos experiencia tienen acumulada y su función principal consiste en supervisar los logs de los eventos en busca de actividad sospechosa. Cuando consideran que hay algo que requiere una investigación más pormenorizada, recopilan el máximo de información posible y derivan el incidente al nivel 2.

Nivel 2: Investigación

Los analistas de nivel 2 estudian la actividad sospechosa más a fondo para clarificar la naturaleza de la amenaza y a qué parte de la infraestructura afecta. A continuación, estos analistas coordinan una respuesta que subsane el problema. Esta es una actividad de mayor impacto que, a menudo, requiere el trabajo de analistas más experimentados.

Nivel 3: Búsqueda de amenazas

Estos son los analistas con más experiencia y se encargan de responder a incidentes complejos. El resto del tiempo lo dedican a analizar informes forenses y datos de telemetría relativos a amenazas que el software de detección podría no haber identificado como sospechoso. Por lo general, las empresas destinan un tiempo mínimo a las actividades de búsqueda de amenazas, pues las actividades de los niveles 1 y 2 consumen una gran cantidad de recursos de análisis.

Pero el hecho de que este modelo sea el más común no significa que sea el ideal. Para empezar, casi nadie está capacitado para estar todo el día supervisando logs. No podemos negar el «mal de alertas» y la cantidad de información innecesaria generada por el sinfín de sensores que hay en un SOC es tal que siempre habrá alguna amenaza que consiga colarse en el sistema. Por otra parte, no es fácil retener analistas dedicados en exclusiva a esta tarea, ya que en general prefieren hacer algo que contribuya de forma más significativa a las investigaciones (y pueden conocer enfoques nuevos e innovadores que terminan desaprovechándose si carecen de las habilidades técnicas necesarias para trabajar con procesos de investigaciones más obsoletos). En segundo lugar, se dedica mucho menos tiempo a la búsqueda de amenazas y a la mejora de los procesos, pues la mayor parte del tiempo se destina a descubrir y mitigar amenazas.

Ahora que hemos definido XDR, vamos a explorar cómo repercute en las operaciones de seguridad a todos estos niveles y cómo mejorar este modelo. Lo haremos dividiéndolo en funciones clave: detección, clasificación y priorización de alertas, investigación y respuesta, y búsqueda de amenazas.

Detección

La capacidad de prevenir la pérdida de datos tiene mucho que ver con la capacidad para detectar adversarios que intentan llevar a cabo actividad maliciosa en su entorno. XDR utiliza el aprendizaje automático para absorber las características únicas de su organización y le permite diferenciar entre ataques y actividad inofensiva más allá de las posibilidades del análisis manual o las reglas de correlación estáticas. Este aprendizaje automático aporta información al análisis avanzado, a la generación de perfiles y a la detección de amenazas basada en el comportamiento. Gracias a esta tecnología de detección tan exhaustiva, una solución XDR mejora la capacidad de detectar actividad nefaria, incluidos los ataques dirigidos, el personal interno malintencionado, etc.

Ataques dirigidos

Los atacantes intentan pasar desapercibidos mezclándose con usuarios legítimos al desarrollar tareas de reconocimiento y lanzar ataques de exploit en las redes objetivo. Las soluciones XDR ejecutan análisis sofisticados de los datos de seguridad relativos a su red, endpoints y nube para ayudarle a detectar comportamientos anómalos de adversarios que intentan atacar sus dispositivos y desplazarse lateralmente por la red con el objetivo de localizar y exfiltrar los datos sobre sus clientes y su propiedad intelectual.

Personal interno malintencionado

El personal interno malintencionado utiliza sus credenciales y privilegios de acceso, que son de confianza, para robar cantidades nada desdeñables de datos corporativos sin que nadie lo note. Para responder a esta amenaza, XDR busca cambios anómalos en el comportamiento de los usuarios y la actividad resultante en la infraestructura que delaten técnicas de reconocimiento interno y movimiento lateral.

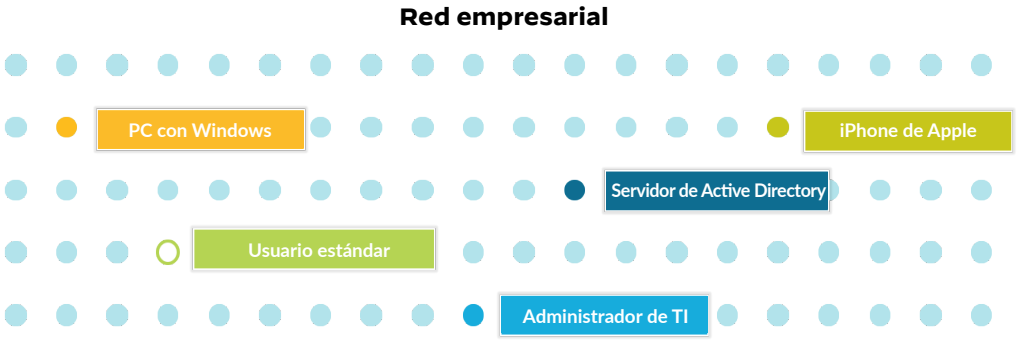

Figura 9: El análisis de comportamiento detecta anomalías a nivel de usuario, aplicación y dispositivo

Riesgo accidental

A veces, empleados bienintencionados exponen a sus organizaciones a riesgos innecesarios por descuido. Una solución XDR permite a las organizaciones seguir prácticas de seguridad recomendadas para vigilar la actividad de los usuarios e identificar comportamientos peligrosos que puedan apuntar a casos de incumplimiento de las políticas de seguridad por parte de un empleado, sea o no de forma intencionada.

CORTEX XDR BY PALO ALTO NETWORKS

Endpoints en riesgo

Los atacantes suelen utilizar malware para infiltrarse en sus redes objetivo atacando a los endpoints y desplazándose lateralmente por la red. XDR reúne los datos de seguridad de todas las redes y endpoints para detectar tráfico anómalo generado por el malware y otra actividad maliciosa. Estos datos de seguridad también proporcionan recursos para investigar la infraestructura y valorar el grado de proliferación de la campaña de ataques.

Dadas las complicaciones presentadas por el déficit de formación especializada al que nos referíamos anteriormente, XDR equipa a los analistas menos experimentados con recursos que les permiten detectar y validar un posible ataque. Para ello, agrupa las alertas por incidentes y, dentro de esos incidentes, sintetiza las actividades o acciones en etiquetas que aportan contexto. Esta flexibilidad garantiza que todo el equipo recibe y aprovecha el conocimiento adquirido.

Por ejemplo, si un adversario añadiera un valor nuevo a la clave del registro de Autorun, una solución XDR podría generar automáticamente una etiqueta que crease una acción para el analista llamada «Archivo ejecutable configurado para iniciarse tras arrancar»; el tipo de ataque, clasificado como «Persistencia», y una descripción detallada tal como «El proceso ha añadido una clave nueva a la carpeta de Autorun del registro de Windows para garantizar que un archivo ejecutable o de script se ejecuta al arrancar. Repase qué archivo y por qué».

Una solución XDR identifica ataques activos con una exactitud milimétrica gracias a tres funciones: integra algoritmos de detección de ataques con datos recopilados en la red, los endpoints y la nube; aplica un marco de detección estructurado, y aprende tanto de las respuestas internas como de la inteligencia sobre amenazas externa.

RESUMEN

Ventajas de XDR en la detección de amenazas

XDR ofrece a los equipos de seguridad mayor capacidad para:

- detectar actividad maliciosa procedente de recursos tanto internos como externos buscando patrones entre la actividad que se desarrolla en la red, los endpoints y la nube;
- aplicar técnicas de análisis punteras a cantidades de datos de seguridad significativas para identificar actividad anormal sin que aumente el nivel de falsos positivos;
- aprovechar la inteligencia sobre amenazas externas y las respuestas internas para aprender de los ataques del pasado y poner toda esa experiencia a disposición de analistas menos experimentados con el fin de mejorar el rendimiento de todo el equipo de seguridad.

Clasificación y validación de alertas

Gracias a que XDR agrupa los datos de la red, los endpoints y la nube, puede determinar automáticamente la causa original de los ataques, lo que agiliza considerablemente su validación e investigación. Por ejemplo, XDR no solo identifica qué ejecutable del endpoint ha sido el responsable de un ataque a la red determinado, sino que también es capaz de averiguar qué aplicación cargó el ejecutable.

XDR establece una cronología de los eventos que condujeron al ataque y proporciona inteligencia sobre amenazas integrada. Todo esto permite a los analistas entender la causa original de un ataque, las características exactas de la amenaza y qué medidas tomar.

Así funciona la clasificación y validación de alertas con XDR:

1) **Evaluación**: el proceso comienza con una evaluación tanto de las alertas externas (del SIEM y otros controles) como de las generadas de forma interna (basándose en reglas y otros indicadores) para determinar si existe comportamiento sospechoso.
2) **Priorización**: a continuación, la herramienta de XDR agrupa automáticamente esas alertas por incidentes y asigna un nivel de prioridad a cada uno de ellos para concentrar el análisis en aquellos incidentes que representen la mayor amenaza. Los analistas pueden hacer clic en cada incidente y ver la lista completa de alertas, dispositivos, inteligencia sobre amenazas asociada e información contextual para entender mejor el alcance real del ataque.
3) **Análisis**: en cada incidente, los analistas pueden ir ampliando la información de las alertas para acceder a una cadena de ataque visual y utilizar las distintas fuentes de telemetría para recopilar toda la información que pueda arrojar luz sobre el posible ataque, y mejorar y agilizar el análisis.

Los datos de uso de los productos de Palo Alto Networks muestran una media de 50 alertas generadas por cada incidente de seguridad. Al identificar estos eventos relacionados y agruparlos por incidentes, XDR puede reducir en un 98 % el número de alertas que ve un analista.

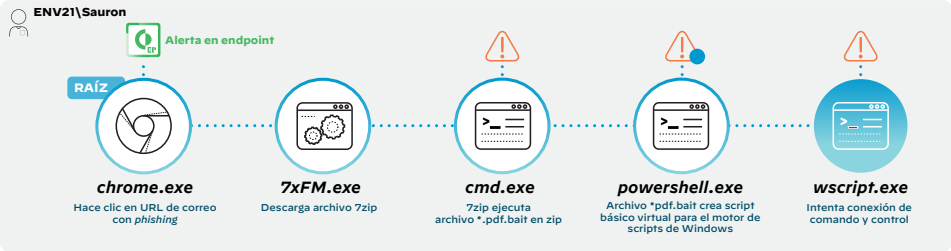

Figura 10: Visualización de una cadena de ataque mediante XDR

4) **Información enriquecida**: la cadena de ataque recibe información contextual adicional que incluye una vista detallada de cómo se generó la alerta, su causa original, otros dispositivos de endpoint, red y nube involucrados, y la reputación de todos los artefactos forenses.
5) **Validación**: los procesos de información enriquecida, análisis, evaluación y priorización se producen automáticamente antes de enviar la alerta a la persona responsable de responder para que realice una investigación más formal. XDR utiliza el historial de todas las alertas investigadas hasta el momento para añadir contexto a la cronología de las alertas activas con el fin de mejorar la priorización y la velocidad a la que se valida la alerta.

Teniendo en cuenta que los equipos de seguridad reciben miles —y, a veces, millones— de alertas al día, automatizar el proceso de clasificación y facilitar a los analistas información contextualizada es la única forma de gestionar el volumen. Con XDR, los equipos de seguridad pueden dedicar su tiempo y energía a las tareas más importantes: detener los ataques con el potencial de perpetrar el mayor daño.

RESUMEN

Ventajas de XDR en la clasificación y validación de alertas

Los analistas gozan de mayor capacidad para:

- procesar más eventos al día, no solo los priorizados por las herramientas de alerta de seguridad o los sistemas SIEM;
- reducir drásticamente la posibilidad de que se les escape alguna alerta;
- analizar alertas de falsos positivos para mejorar la detección, por una parte, y garantizar que ni la actividad ni las defensas que se desarrollan en etapas posteriores se vean afectadas, por otra;
- aplicar nuevos activadores de comportamiento para mejorar los tiempos de clasificación y reforzar las defensas de manera constante.

CORTEX XDR BY PALO ALTO NETWORKS

Automatización y simplificación de las investigaciones y la respuesta

Una vez clasificada y priorizada una alerta, es preciso realizar una investigación en profundidad. La automatización de XDR acelera el proceso de investigación de cualquier alerta o campaña de búsqueda preventiva de amenazas gracias a que elimina las lentas tareas manuales proporcionando una imagen transparente de la amenaza, analiza la causa original, verifica la reputación y resuelve la atribución del ataque.

Las herramientas de XDR empiezan por agregar toda la telemetría de los endpoints, la red y la nube a un repositorio de datos de seguridad, como puede ser un lago de datos. Con el fin de agilizar la investigación, la solución XDR puede correlacionar y agrupar las alertas de las distintas herramientas de detección en un número reducido de incidentes precisos y útiles, así como información acerca del usuario, de la aplicación y del dispositivo. XDR también agiliza las investigaciones forenses interrogando a los endpoints para determinar qué proceso o ejecutable inició el ataque.

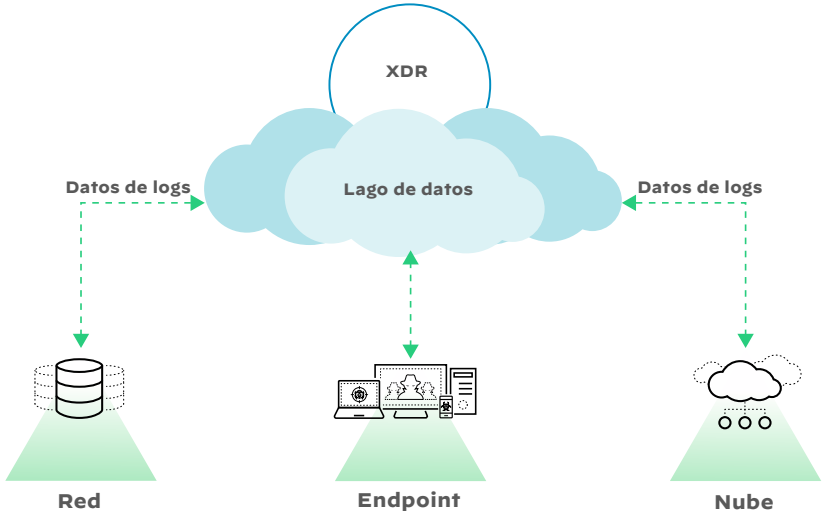

Figura 11: Las herramientas de XDR agrupan los datos de distintos sensores en un lago de datos basado en la nube

CORTEX XDR BY PALO ALTO NETWORKS

Las soluciones XDR integran las fuentes de inteligencia sobre amenazas y los servicios de análisis para determinar si el proceso que se está desarrollando en el endpoint es malicioso o no. Asimismo, facilitan a los analistas la verificación de los ataques y les presentan toda la información que necesitan en una única interfaz.

Las herramientas de XDR también pueden adaptar las defensas aplicando el conocimiento adquirido a partir de los incidentes y campañas de búsqueda de amenazas anteriores para evitar, sin intervención humana alguna, que se vuelva a producir ninguna de las amenazas encontradas en el pasado. Este «aprendizaje asistido» permite detectar los ataques en una etapa temprana basándose en lo que ya se ha visto.

Los responsables de responder a los incidentes pueden, por tanto, elegir entre decenas de técnicas telemáticas de respuesta y corrección para limpiar quirúrgicamente los sistemas infectados sin interrumpir la actividad empresarial. El equipo de seguridad ganará en eficiencia, requerirá menos formación, aliviará la carga de trabajo de los analistas más experimentados y reducirá al mínimo los tiempos de resolución de incidentes.

RESUMEN

Ventajas de XDR en la investigación de amenazas

Los responsables de responder a los incidentes gozan de mayor capacidad para:

- agilizar la localización de amenazas sigilosas aprovechando la inteligencia sobre amenazas y el análisis de comportamiento;
- simplificar y acelerar los procesos de investigación y respuesta proporcionando una amplia gama de herramientas de búsqueda de telemetría recopilada en redes, endpoints y la nube.

Búsqueda de amenazas

Las soluciones XDR refuerzan visiblemente las funciones de búsqueda de amenazas gracias a la identificación, automatizada y ad hoc, de actividad maliciosa en la infraestructura. Quienes se dedican a buscar amenazas pueden enviar consultas avanzadas para conseguir resultados instantáneos con un grado de precisión superior. A continuación le presentamos varios ejemplos de cómo XDR proporciona las funciones necesarias para poder trabajar con los distintos métodos de búsqueda de amenazas.

Búsqueda de amenazas basada en la inteligencia

Este es el tipo de ejercicio de búsqueda de amenazas más común, en el que la persona encargada de buscar las amenazas recibe una pista sobre una posible amenaza antes de empezar a buscarla. Ya sea por un indicio de la inteligencia sobre amenazas, un indicador de riesgo (IOC, por sus siglas en inglés) recién descubierto, un aviso de un empleado de la organización o una mera sospecha, la complejidad de la búsqueda de amenazas basada en información puntual y oportuna dependerá del nivel de detalle ofrecido por dicha información. A partir de una fuente de datos integrada que esté vinculada con varios proveedores de inteligencia sobre amenazas, una solución XDR puede importar de forma manual artefactos o indicadores de compromiso de distintas normas para ofrecer resultados de búsqueda rápidos y robustos.

Búsqueda de amenazas sin indicios

Este enfoque, que le sigue los talones al primero, se refiere a aquel en el que la persona encargada de buscar las amenazas utiliza su propio conocimiento de cómo se supone que hay que utilizar un ordenador, aplicación, usuario, dato o red para identificar usos anómalos o anormales. Este tipo de enfoque se suele considerar avanzado, pues normalmente se deja en manos del miembro del equipo más experimentado, quien para realizar su trabajo utilizará técnicas como el data carving y el análisis de datos. Una solución XDR simplifica este proceso integrando estas técnicas avanzadas en su propia IU, lo que permite a los especialistas dedicados a la búsqueda de amenazas de todos los niveles de experiencia utilizar estas técnicas sin scripts, herramientas adicionales ni la necesidad de aprender un nuevo lenguaje de consultas.

Búsqueda de amenazas basada en resultados

En este enfoque, el especialista en búsqueda de amenazas busca entre las alertas puestas en cuarentena, las conclusiones de las investigaciones o cualquier otra amenaza sin resolver del pasado, y utiliza esta información para identificar variantes de la amenaza, posibles amenazas nuevas o vectores de ataque abiertos. Una buena solución XDR puede incorporar técnicas de búsqueda de amenazas basadas en resultados directamente en el flujo de trabajo de las alertas de seguridad y gestión de incidentes, y hacerlo de forma automática e ininterrumpida. Se aplican las lecciones aprendidas con cada investigación para garantizar que los ataques no vuelvan a repetirse.

Búsqueda de amenazas basada en el cumplimiento normativo

Este enfoque está orientado a asegurar el cumplimiento de las políticas internas, sectoriales y gubernamentales realizando búsquedas rutinarias que señalen los casos de incumplimiento, como datos confidenciales almacenados en sistemas no autorizados o un aumento de privilegios por parte de los usuarios administradores. Una solución XDR puede configurarse para alertar a los analistas de seguridad de este tipo de actividad y proporcionar un medio para investigar la situación rápidamente.

Búsqueda de amenazas basada en el aprendizaje automático

Los sistemas de aprendizaje automático funcionan como base de referencia de los comportamientos típicos de una organización para diferenciar lo que es normal de lo que no lo es. Las soluciones XDR, gracias al uso de herramientas de análisis a gran escala, emplean el aprendizaje automático para vigilar comportamientos e identificar anomalías que se desvíen de estas bases de referencia. Estos indicadores de comportamiento peligroso (BIOC, por sus siglas en inglés) detectan muchas amenazas sigilosas que podría no haber identificado un analista de forma manual y se optimizan continuamente con el paso del tiempo para mejorar el modelo de aprendizaje automático. Esta forma de buscar amenazas es la que más tiempo ahorra a los analistas y es crucial para optimizar los resultados de seguridad.

RESUMEN

Ventajas de XDR en la búsqueda de amenazas

Los especialistas en búsqueda de amenazas gozan de mayor capacidad para:

- beneficiarse de los datos de la red, los endpoints y la nube para realizar labores de búsqueda y análisis;
- aprovechar la automatización para buscar amenazas en toda la actividad de la red, los endpoints y la nube;
- utilizar tanto búsquedas como asistentes con gran capacidad de personalización para encontrar amenazas internas y externas identificadas por indicadores IOC y BIOC almacenados en la biblioteca de amenazas;
- corregir los ataques gracias a la integración con controles de seguridad.

Conclusión

Las empresas se están viendo impelidas a instaurar una serie de cambios fundacionales en sus tecnologías y procesos de detección y análisis. Las tecnologías heredadas son demasiado rígidas y limitadas, y no aciertan a proporcionar la flexibilidad ni la capacidad necesarias para enfrentarse a los adversarios de hoy en día. Por otra parte, las empresas necesitan trabajar de una forma más efectiva y eficiente para sobreponerse a la escasez de analistas de seguridad cualificados.

Por su valor como herramienta de respuesta a incidentes y la excelente protección que ofrece (que, además, apenas afecta a los endpoints), la tecnología XDR va camino de convertirse en el método de detección y respuesta del futuro. Para reforzar la seguridad de los endpoints, no basta con utilizar agentes con funciones de prevención integradas; se necesita una estrategia de seguridad exhaustiva que ofrezca protección extra. XDR abre un nuevo camino, con una mayor visibilidad de los endpoints, las redes y la nube, así como una solución de análisis basada en el aprendizaje automático más efectiva con tecnologías de corrección integradas que cambian de raíz el modo de buscar, detectar, investigar y responder a las amenazas.

Lista de comprobación para la solicitud de propuestas de soluciones XDR

Nuestra lista de comprobación recoge una serie de requisitos agrupados en nueve categorías que le servirán de guía a la hora de evaluar las distintas plataformas que está considerando. Utilícela como punto de partida y adáptela a las necesidades de su empresa para no equivocarse a la hora de elegir a los proveedores más adecuados para su organización.

Descargue ahora la lista de comprobación.

Ni los mejores sistemas de prevención de amenazas están a salvo de los atacantes sofisticados, quienes ponen en riesgo datos cruciales y, además, suelen hacerlo de la forma más notoria y dañina posible. La mayoría de las empresas cuentan con herramientas de detección y respuesta a amenazas para lidiar con ataques que esquivan sus defensas iniciales, pero estas herramientas solo ven la punta del iceberg de la infraestructura de TI. Como no son lo suficientemente inteligentes o carecen de la integración necesaria para correlacionar los distintos eventos que se producen durante un ataque, simplemente envían alertas cada vez que algo parece remotamente sospechoso, por lo que se reciben alertas cientos —¡o miles!— de veces al día. Los analistas de seguridad se pasan la mayoría del tiempo filtrando estas alertas para encontrar las importantes. Muchas amenazas reales acaban colándose en el entorno y no llegan a descubrirse hasta pasados varios meses.

Claramente, el sistema no funciona.

Una nueva categoría de herramientas de detección y respuesta empresariales

Las soluciones XDR agrupan los datos del endpoint, la red y la nube en un robusto lago de datos. A continuación, aplican algoritmos inteligentes de aprendizaje automático y técnicas de análisis avanzado para determinar con precisión qué riesgos constituyen una amenaza y cuáles son inofensivos. Toda esta información contextualizada se pone a disposición de los analistas y ayuda a simplificar y acelerar las investigaciones. Lea este libro electrónico para familiarizarse con esta nueva categoría de herramientas y descubrir:

- las carencias de las tecnologías de detección y respuesta a amenazas actuales;
- qué es la tecnología XDR y qué requisitos debe cumplir;
- cómo mejorar las operaciones de seguridad con XDR.

Taller práctico de investigación y búsqueda de amenazas

¿Quiere aprender a usar las prácticas recomendadas en materia de investigación y búsqueda de amenazas? Asista a un taller virtual.

En solo tres horas, mejorará sus competencias con ejercicios prácticos. Le enseñaremos a descubrir quién podría estar poniendo en riesgo su entorno —actúe donde actúe— y a frustrar los ataques dirigidos a su empresa, por sofisticados que sean.

Dé el primer paso hoy mismo. Inscríbase aquí.

Oval Tower,De Entrée 99 - 197
1101HE Ámsterdam
Países Bajos

Tel.: +31 20 888 1883

www.paloaltonetworks.es

cortex_eb_the-essential-guide-to-xdr-042221-es