McAfee MVISION XDR

La primera solución de detección y respuesta ampliadas proactiva, basada en datos y abierta, diseñada para ayudar a las empresas a detener los ataques sofisticados.

Realidades de las operaciones de seguridad

El centro de operaciones de seguridad (SOC) es una función esencial del organigrama de ciberseguridad de una empresa, con atención especial a la detección y corrección rápida de amenazas para evitar daños a los activos y datos. Si el SOC tiene dificultades, es muy probable que los resultados de la seguridad sean cuestionables y las empresas se expongan a riesgos. Los desafíos de los SOC siguen aumentando en número y escala a pesar del aumento de la inversión. Tres cuartos de los profesionales de seguridad afirman que la detección y respuesta a amenazas es más difícil hoy que hace dos años, según un estudio de la empresa ESG[1]. Entonces, ¿significa esto que los adversarios están ganando la batalla?

Se puede decir que las funciones del SOC están todavía en proceso de maduración. Un reciente estudio del instituto SANS[2] descubrió que solo el 29 % de las empresas se consideran maduras o muy maduras en lo relativo a caza de amenazas y que solo el 40 % incluyen la respuesta a incidentes dentro de las funciones del SOC.

El 59 % de las empresas han sufrido un ciberincidente serio y, sin embargo, solo el 26 % afirma que su SOC fue capaz de identificar el ataque más importante.

(Ernst & Young, 2020)

Síganos

Cargas de trabajo intensas y complejidad de administración en el SOC

En la mayoría de los casos, el SOC cuenta con recursos insuficientes debido a la inmensa escasez de profesionales de ciberseguridad, y de las dificultades de retención del personal. Además, el SOC se ha visto inundado de una enorme cantidad de herramientas aisladas, lo que ha añadido un nivel de complejidad que obstaculiza su capacidad para detectar y responder de manera rápida y apropiada. Según ESG[3], el 66 % de las empresas afirman que la eficacia de la detección y respuesta a amenazas es limitada ya que depende de múltiples herramientas individuales.

La implicación para el SOC es que el tiempo para detectar y responder a las amenazas es de meses, lo que genera tiempos de permanencia más largos permitiendo a los ciberdelincuentes generar más daño. Lo que se necesita es visibilidad y control sencillos de todos los ciberactivos, con inteligencia procesable para pasar rápidamente a la resolución de las amenazas. El enfoque de herramientas fragmentadas necesita integrarse y optimizarse en los endpoints, la red, la nube y las aplicaciones para eliminar complejidad. Es necesario aliviar la sobrecarga de alertas con detección y análisis automatizados que prioricen y filtren las amenazas. Es preciso dotar a los SOC con funciones de detección, investigación y respuesta inteligentes y eficaces para adelantarse a los ataques o resolverlos antes de que se produzcan daños importantes.

Mejore la eficacia y productividad del SOC

McAfee® MVISION XDR es la respuesta a los problemas de seguridad e ineficacia operativa de los SOC. Añade de manera exclusiva las funciones de detección y respuesta a amenazas ampliadas (XDR) como administración de amenazas avanzadas basada en la nube en toda la infraestructura de TI, gracias a que incluye cobertura específica frente a todo el ciclo de vida del ataque, con prioridad a la protección de lo que importa y medidas sencillas para organizar una respuesta eficaz. MVISION XDR reduce los riesgos desde los dispositivos hasta la nube, mejorando rápidamente la eficacia del SOC mediante la disminución de los ciclos reactivos, al tiempo que ahorra hasta el 95 % en costos de evaluación de campañas de amenazas [4] con la primera solución XDR abierta, proactiva y basada en datos.

Los ataques remotos por ciberdelincuentes externos contra servicios en la nube aumentaron un 630 % en 2020.

(McAfee, 2020)

Principales ventajas

Los SOC pueden hacer más con MVISION XDR, gracias a una vista unificada de todos los endpoints, la red y la nube. MVISION XDR ayuda a:

- Reducir el error humano como resultado del cambio manual entre herramientas y datos.
- Priorizar y proteger lo que importa con conocimiento de los datos desde una vista unificada que equilibra importancia y confidencialidad.
- Minimizar el riesgo antes y después de los ataques con inteligencia proactiva y procesable, investigaciones guiadas y automatizadas y contramedidas prescriptivas.
- Mejorar la visibilidad y el control, y eliminar las tediosas tareas manuales organizando sin esfuerzo las soluciones de seguridad para que trabajen conjuntamente.
- Ofrecer gestión de ciberamenazas procesable sin necesidad de aumentar la plantilla, dotando adecuadamente al personal actual.

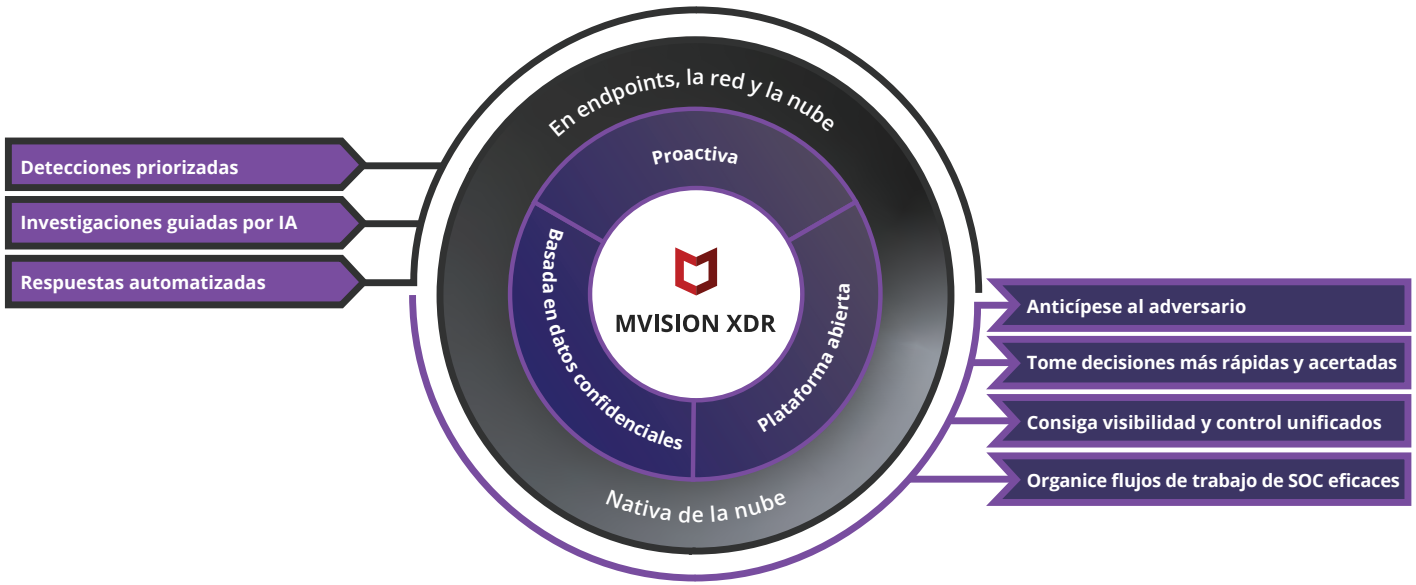

Figura 1. Las ventajas principales y resultados de MVISION XDR.

Consiga información procesable y proactiva para adelantarse a los ciberdelincuentes

La mayoría de las soluciones XDR solo ofrecen opciones después de que un ataque haya conseguido infiltrarse en el entorno de la empresa, lo que crea un SOC muy reactivo y en constante modo "apagafuegos". MVISION XDR, con tecnología de McAfee MVISION Insights, es la única solución XDR que aborda el ciclo de vida completo de un ataque con flujos de trabajo reactivos robustos después del ataque, y nuevas funciones proactivas antes del ataque. Los SOC pueden actuar sobre las amenazas externas que importan antes de que se produzca el ataque. Las empresas pueden dar prioridad a las amenazas, predecir si van a funcionar las contramedidas y recomendar medidas correctivas. El resultado es una detección y respuesta más rápidas, que se producen en minutos en lugar de en semanas.

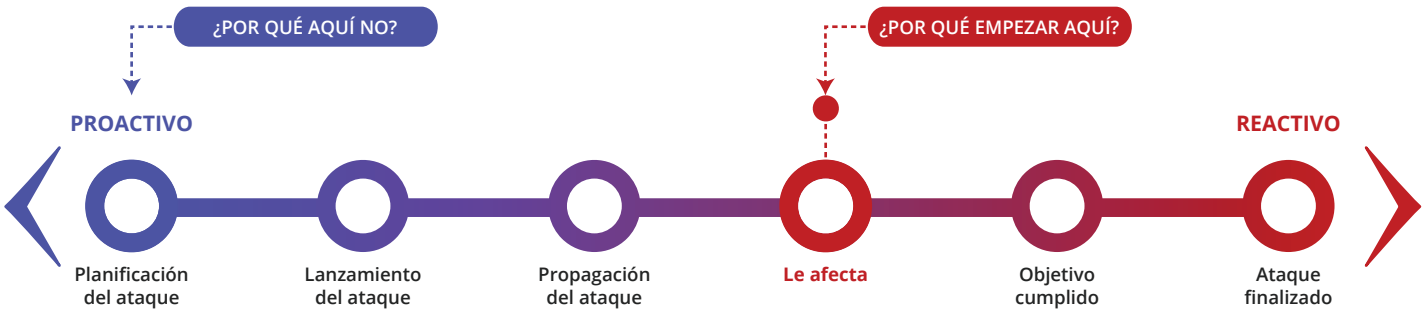

Figura 2. MVISION XDR aborda todo el ciclo de vida del ataque con funciones proactivas y reactivas.

Consiga visibilidad y control unificadas de múltiples vectores de ataque

La capacidad para ver y dar sentido a la actividad del adversario en varios vectores es fundamental, sobre todo teniendo en cuenta lo imprevisibles que pueden ser los movimientos de los ciberdelincuentes. Y lo que es más importante, una vez que la situación de la amenaza es evidente, los analistas pueden actuar en todos los vectores para resolverla.

MVISION XDR combina telemetría de redes de sensores locales y en la nube para proporcionar sin problemas una vista completa de los datos de la empresa, junto con el comportamiento de los ciberdelincuentes. Mediante la conversión de un flujo grande de alertas de toda la empresa en un número de incidentes más pequeño, MVISION XDR reduce el ruido y sitúa a los analistas más cerca de la solución.

Desde un panel intuitivo, los analistas del SOC reciben los principales hallazgos relacionados con su entorno, campañas principales y prioridades recomendadas en base a trabajo y análisis de investigación automático.

Desde esta vista, los analistas pueden profundizar e investigar y evaluar fácilmente las medidas necesarias. Las opciones de respuesta pueden afectar a múltiples vectores en toda la empresa.

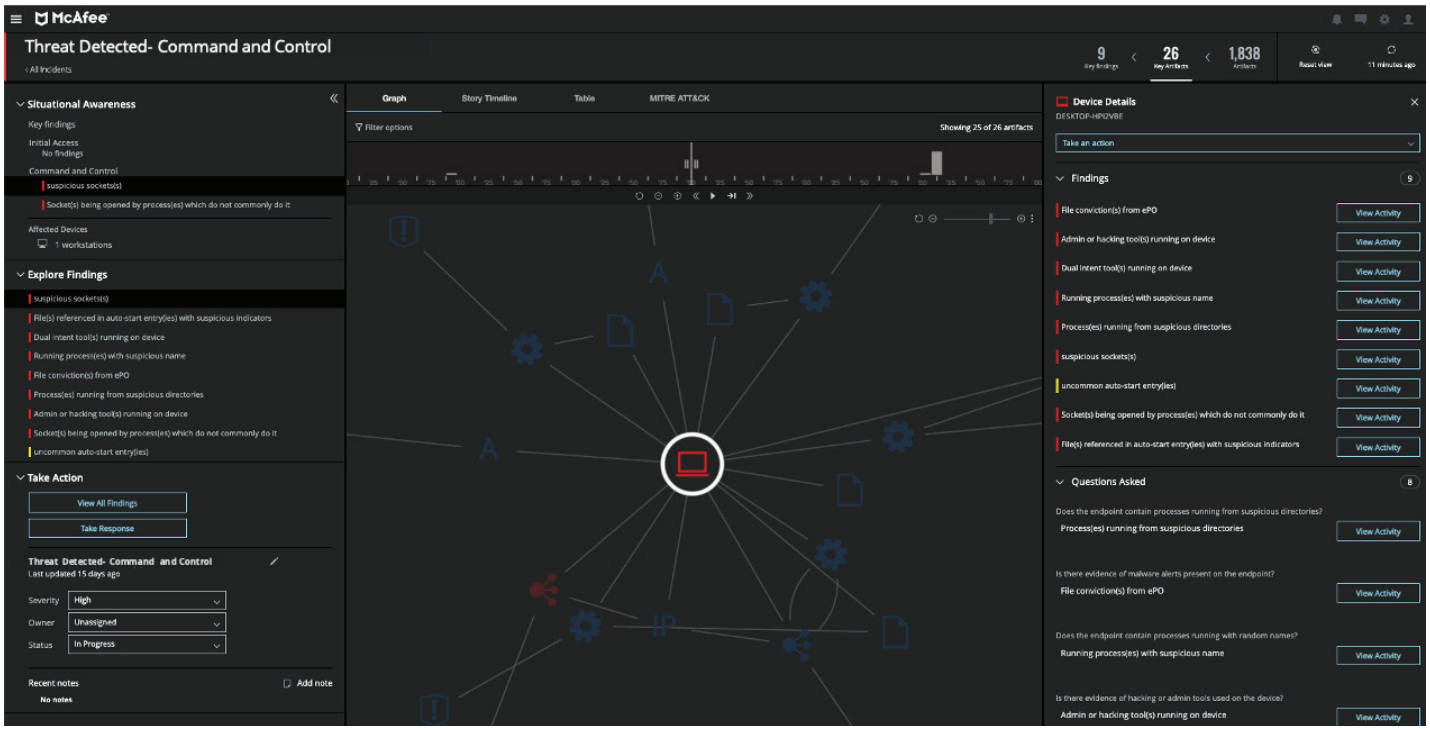

Figura 3. Gracias a la priorización de incidentes con investigación guiada y en profundidad, y de flujos de trabajo de respuestas, se consigue reducir la sobrecarga de alertas y acelerar la respuesta.

Tome decisiones más rápidas y acertadas

Los SOC deben adoptar decisiones rápidamente para resolver las amenazas y minimizar el daño. Los pasos para la toma más rápida de decisiones incluyen acelerar los trabajos de investigación y dar prioridad a lo fundamental. MVISION XDR acelera las investigaciones con investigaciones automáticas y guiadas por inteligencia artificial. Las investigaciones guiadas por inteligencia artificial ayudan a los analistas del SOC: plantea y contesta preguntas, mientras recopila, resume y muestra pruebas de distintas fuentes. Esto ayuda a los analistas del SOC a aprender continuamente mientras optimizan sus competencias de investigación y respuesta. Además, pueden llevarse a cabo en cualquier momento investigaciones automáticas procedentes de una lógica de filtrado de eficacia probada. Ambas opciones eliminan la necesidad de recopilar y analizar las pruebas. También eliminan el ruido de alertas y dotan a los analistas de las herramientas necesarias para tomar una decisión de forma rápida.

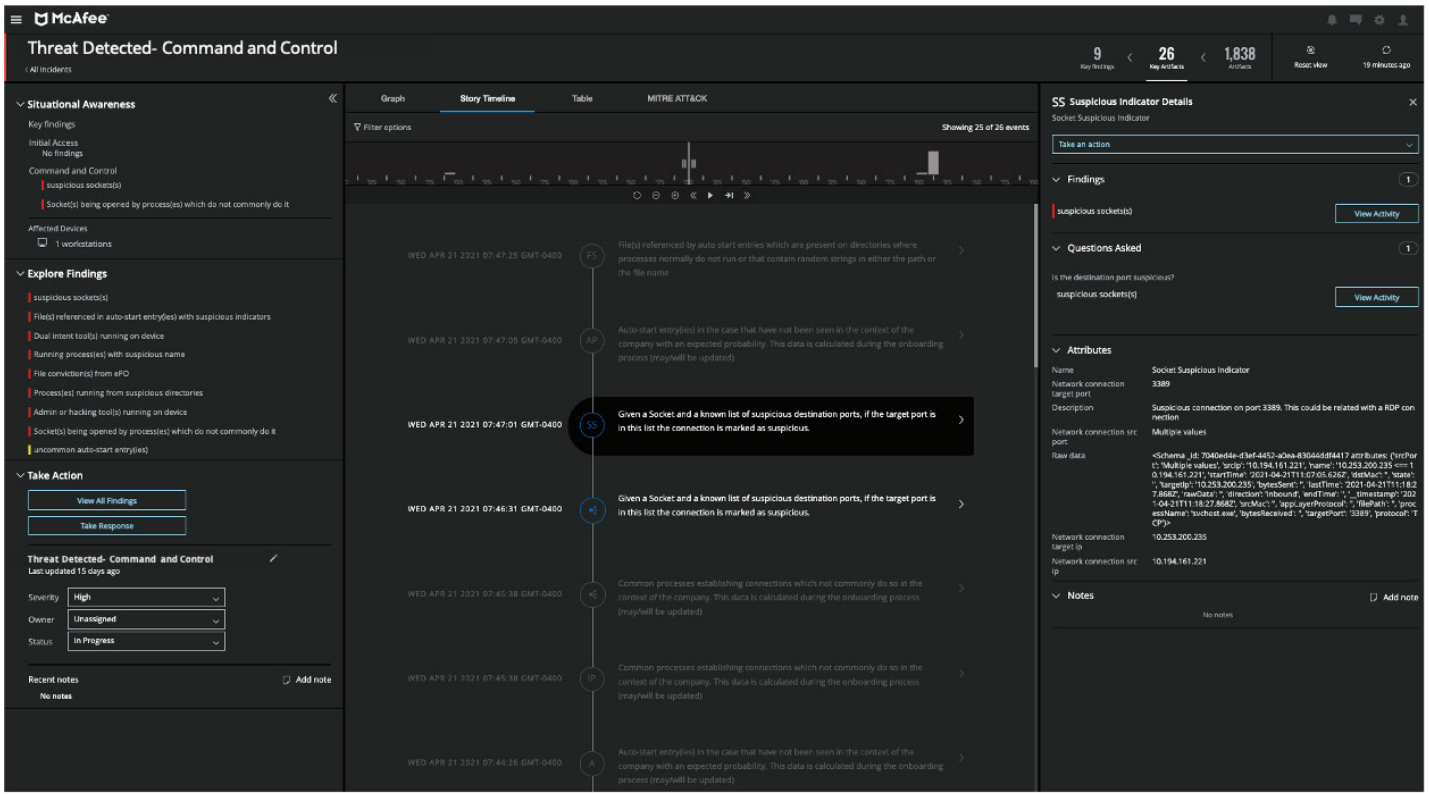

Figura 4. La cronología de la historia procesable proporciona una vista detallada de los eventos que componen la totalidad de un ataque.

MVISION XDR recopila inteligencia sobre amenazas de una amplia variedad de fuentes, como soluciones de información y eventos de seguridad (SIEM), y ofrece una búsqueda fácil del autor y la procedencia del incidente o amenaza. La historia del adversario se muestra de manera sencilla en una cronología con incidentes y datos y comportamientos relacionados. Los analistas pueden profundizar en los hallazgos y pruebas para evaluar mejor el evento utilizando su conocimiento e intuición. Las acciones recomendadas se ofrecen en base a trabajos anteriores realizados por la empresa e información sobre la respuesta que otras empresas del sector dieron al problema.

MVISION XDR ofrece una variedad de opciones de priorización para adoptar rápidamente una decisión crítica. Las amenazas e incidentes pueden organizarse por prioridad en función del impacto en la empresa, como la pérdida de datos o el daño. A una amenaza que cumple determinados criterios en función de las categorías de protección de datos, identidad y tipo de dispositivo se le puede asignar una prioridad mayor. Por ejemplo, tendrá prioridad el dispositivo de un ejecutivo financiero que almacene datos muy sensibles y que esté en peligro.

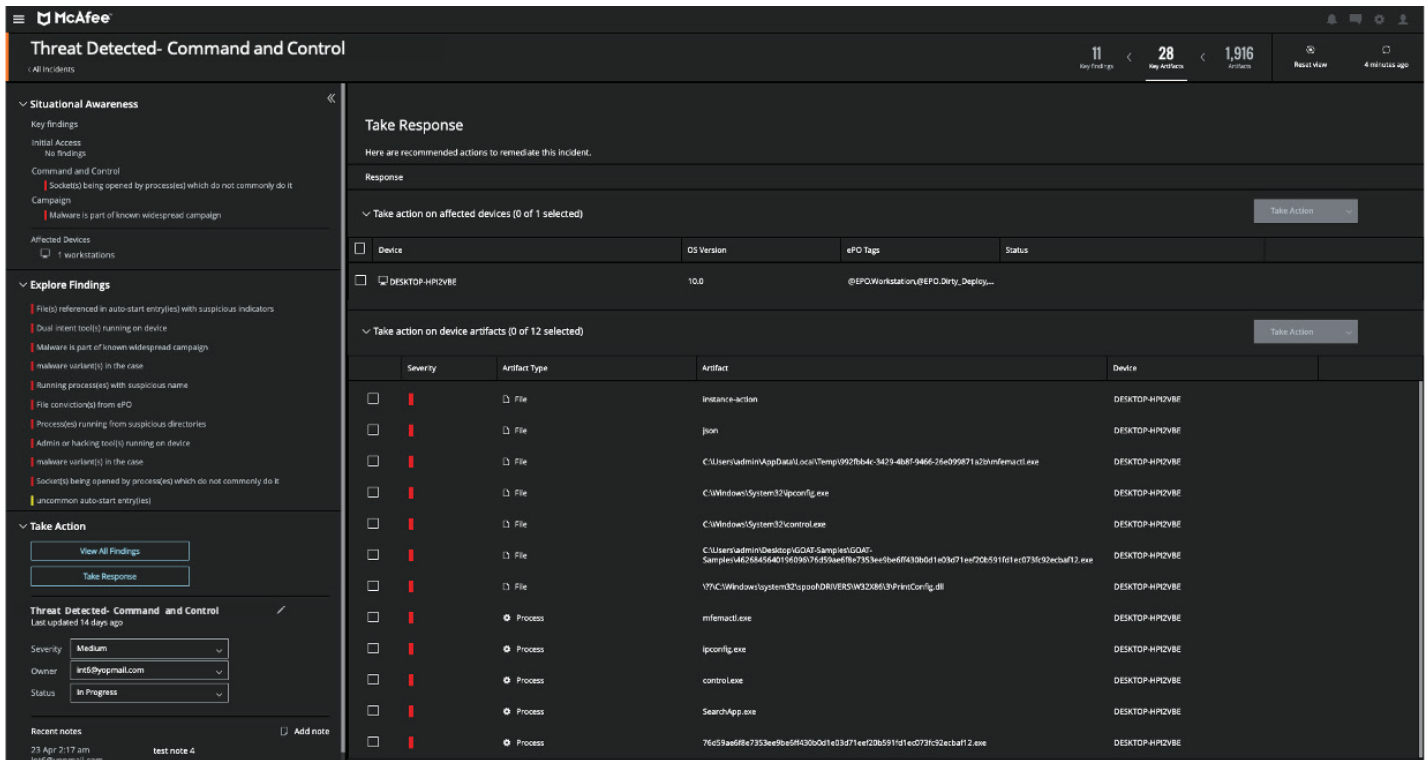

Figura 5. Las acciones recomendadas le ayudarán a moverse rápidamente para corregir los incidentes y contener las amenazas.

Organice flujos de trabajo eficaces y automatizados

MVISION XDR es una plataforma abierta e integrada que se amplía con múltiples vectores y conecta otras funciones de seguridad. Esto permite a la herramienta de seguridad trabajar de una forma unificada para neutralizar al adversario. No hay necesidad de pasar manualmente de una herramienta a otra ni de copiar/pegar datos, lo que ahorra tiempo y reduce el error humano. También permite la correlación de detecciones entre herramientas de seguridad para obtener una alerta y decisión con un nivel de confianza alto. La interfaz de programación de aplicaciones (API) abierta permite a las empresas crear de forma simple flujos de trabajo (cazar, investigar, responder, mitigar) con McAfee y/o terceros desde una plataforma (marketplace) fácil de utilizar, lo que se traduce en una gestión de ciberamenazas simplificada.

Otras soluciones de terceros pueden incluir la gestión de incidencias de TI, respuesta, automatización y orquestación de la seguridad (SOAR), SIEM e inteligencia sobre amenazas. MVISION XDR le permite aprovechar las inversiones existentes, sean o no de McAfee. No hay necesidad de sustituir sus ciberdefensas actuales.

El trayecto a MVISION XDR le permite pasar de una fase a otra en las funciones y flujos de trabajo a su ritmo. El compromiso de McAfee con la seguridad integrada y abierta, que facilita el intercambio de información y la coordinación de la protección, queda reflejado en nuestro papel como cofundador de la Open Cybersecurity Alliance (OCA), una iniciativa de seguridad en todo el sector y la contribución a la ontología OpenDXL, un mecanismo de transporte común y protocolo de intercambio de información.

En resumen

MVISION XDR es la primera solución XDR proactiva, basada en datos y abierta del sector que capacita a los equipos de los SOC para:

- Dar sentido a alertas independientes para ver el ciclo de vida completo del ataque, dar prioridad a las amenazas que importan y adelantarse a los ciberdelincuentes.
- Automatizar los procesos de investigación y respuesta para eliminar las tareas manuales y ahorrar tiempo para centrarse en otras tareas que aprovechen mejor sus conocimientos.
- Cazar de forma proactiva las amenazas y la actividad de los adversarios contra su empresa y mitigar los riesgos en activos y datos desprotegidos.

Más información

Para obtener más información, visite mcafee.com/xdr.

1. Encuesta sobre el panorama de detección y respuesta a amenazas, ESG, 2019
2. "Is Your Threat Hunting Working?" (¿Funciona su actividad de caza de amenazas?), SANS, 2020
3. Encuesta sobre el panorama de detección y respuesta a amenazas, ESG, 2019
4. Investigación interna entre clientes de McAfee.

Av. Paseo de la Reforma No.342 Piso 25
Colonia Juárez, México DF
C.P. 06600
+52-55-50890250
www.mcafee.com/mx