McAfee MVISION Insights

La primera solución de seguridad para endpoints con función XDR para ayudarle a adelantarse a los ciberdelincuentes.

Las ciberamenazas evolucionan tanto y tan rápido que suponen un peligro constante y un punto de tensión para las empresas. La reacción de estas ha sido aumentar el presupuesto dedicado a la seguridad en un panorama de escasez de expertos en seguridad, pero ni aun así pueden mantenerse a la par de los adversarios que continuamente renuevan su arsenal de herramientas, tácticas y técnicas. Las opciones actuales solo aportan inteligencia compartimentada que requiere intervención humana y manual. Es posible que sirvan para amenazas inmediatas, pero los crecientes números y matices de los ciberataques vienen arrinconando a los equipos de seguridad en una situación de reactividad aparentemente constante. Una plataforma de inteligencia sobre amenazas puede ofrecer multitud de datos de amenazas, pero requiere integración manual y ciclos de análisis, lo que limita la capacidad de acción y corrección. La gestión de vulnerabilidades ofrece información sobre vulnerabilidades existentes y sobre su gravedad, sin embargo, no permite saber si su seguridad actual puede defenderle frente a las amenazas actuales del mundo real.

La solución es McAfee® MVISION Insights, con información en tiempo real que le permite tomar medidas proactivas. Una información completa, que ha sido sintetizada y analizada por inteligencia artificial y por personas, puede proporcionar priorización en cuanto a las amenazas y campañas con mayor probabilidad de dirigirse contra su empresa. MVISION Insights predice exactamente el impacto que una amenaza tendría sobre su seguridad en general, además de determinar las medidas que debe tomar para optimizar su nivel de seguridad.

Principales ventajas

- **Información de riesgos reunida por mil millones de sensores:** identifique de forma proactiva las posibles amenazas procedentes de un origen de confianza en el exterior de su perímetro. Clasifique por prioridades los proyectos de amenazas en función del sector, los ciberdelincuentes, la ubicación geográfica y el estado o postura de seguridad de la empresa.
- **Identificación de campañas de amenazas antes de que haya ataques y asignación de una prioridad a su nivel de riesgo desde una sola consola:** consiga inteligencia procesable sobre una amenaza y sepa cómo responderá la seguridad de sus endpoints, incluso con recomendaciones para su corrección.
- **Reducción del tiempo medio hasta la detección y la resolución:** simplifique los flujos de trabajo para agilizar la aplicación de otras medidas de protección. Evalúe su postura de seguridad actual en endpoints y la nube con los cambios necesarios, y acelere el tiempo de respuesta de meses a horas.

Síganos

Transforme su seguridad para ser más proactivo

MVISION Insights incorpora a la plataforma de administración de McAfee® funciones que se adaptan perfectamente y dinamizan las operaciones de gestión de riesgos y amenazas, para mejorar proactivamente las medidas de defensa y reducir los tiempos de respuesta, todo ello usando menos recursos. La inteligencia sobre riesgos recopilada y mejorada procedente de 1000 millones de sensores evaluada por reconocidos investigadores de amenazas avanzadas proporciona a su empresa la información que necesita para priorizar las defensas. Una sola consola ofrece detección, corrección, un menor tiempo de respuesta y una importante disminución de los riesgos.

Las estrategias reactivas tienen su cometido como componente crítico de la ciberdefensa, pero se limitan a jugar a la contra y apagar fuegos. Los ciberdelincuentes emplean herramientas de próxima generación para ingeniar campañas con el fin de atacar las defensas tradicionales, poniendo a prueba los productos de seguridad reactivos para comprobar qué técnicas penetrarán sus escudos. Las empresas necesitan hacer frente a todo el ciclo de vida del ataque, antes y después de resultar afectadas.

Consiga cobertura del ciclo de vida completo de los ataques

Figura 1. Ciclo de vida de un ataque típico.

A fin de cuentas, la inteligencia y la información procesable le ofrecen la mejor medida de ciberseguridad posible frente a las amenazas más probables y aumentan su confianza en las defensas dispuestas. Así es cómo McAfee MVISION Insights lo consigue:

- **Identificación automática de las amenazas globales que antes no eran visibles:** MVISION Insights aprovecha una inmensa reserva de inteligencia de seguridad obtenida mediante más de mil millones de sensores, con análisis optimizado de amenazas a través de la asociación hombre-máquina. El aprendizaje automático detecta amenazas inéditas que los analistas humanos sería improbable que descubrieran debido a la falta de visualización y de procesamiento. La interfaz humana iguala y supera la inteligencia y la creatividad de los atacantes que están al otro lado de esos códigos mediante intuición y experiencia.
- **Mejora del conocimiento de la situación y atención a lo que importa:** sabrá con precisión las posibilidades de sus defensas antes de que se materialicen las amenazas. MVISION Insights supervisa y prioriza proactivamente las amenazas locales y globales que se prevé que afectarán a su empresa.
- **Análisis mediante aprendizaje automático:** esta función le permite averiguar cómo reaccionaría su postura de seguridad global específica en puntos estratégicos de los endpoints y la nube y, a continuación, indica las medidas preventivas de protección que se prescriben y que puede implementar con rapidez y facilidad para bloquear esos ataques.

MVISION Insights ofrece respuestas a preguntas relacionadas con riesgos en endpoints y otros sistemas

- ¿Corre algún riesgo? ¿Cuál es el grado de exposición?
- ¿Cómo prioriza los ataques que podrían afectar a su organización? ¿Cómo aprende sobre ellos? ¿Qué proceso de investigación sigue?
- ¿Cómo conoce las amenazas que aún no han afectado a su organización, pero es probable que lo hagan?
- Incluso si tuviera una plataforma de inteligencia sobre amenazas, ¿cómo priorizaría los ataques dentro de la base de datos de la plataforma?
- ¿Cómo se entera de las amenazas que han afectado a empresas similares?
- ¿Qué prevalencia tiene en su sector y su zona?
- ¿Es mi empresa objetivo de un ciberdelincuente específico?
- ¿Cómo resiste esta amenaza con su estado de seguridad actual?
- ¿Qué confianza tiene en el panorama de amenazas completo y por qué?

El panel de MVISION Insights impulsa la seguridad proactiva

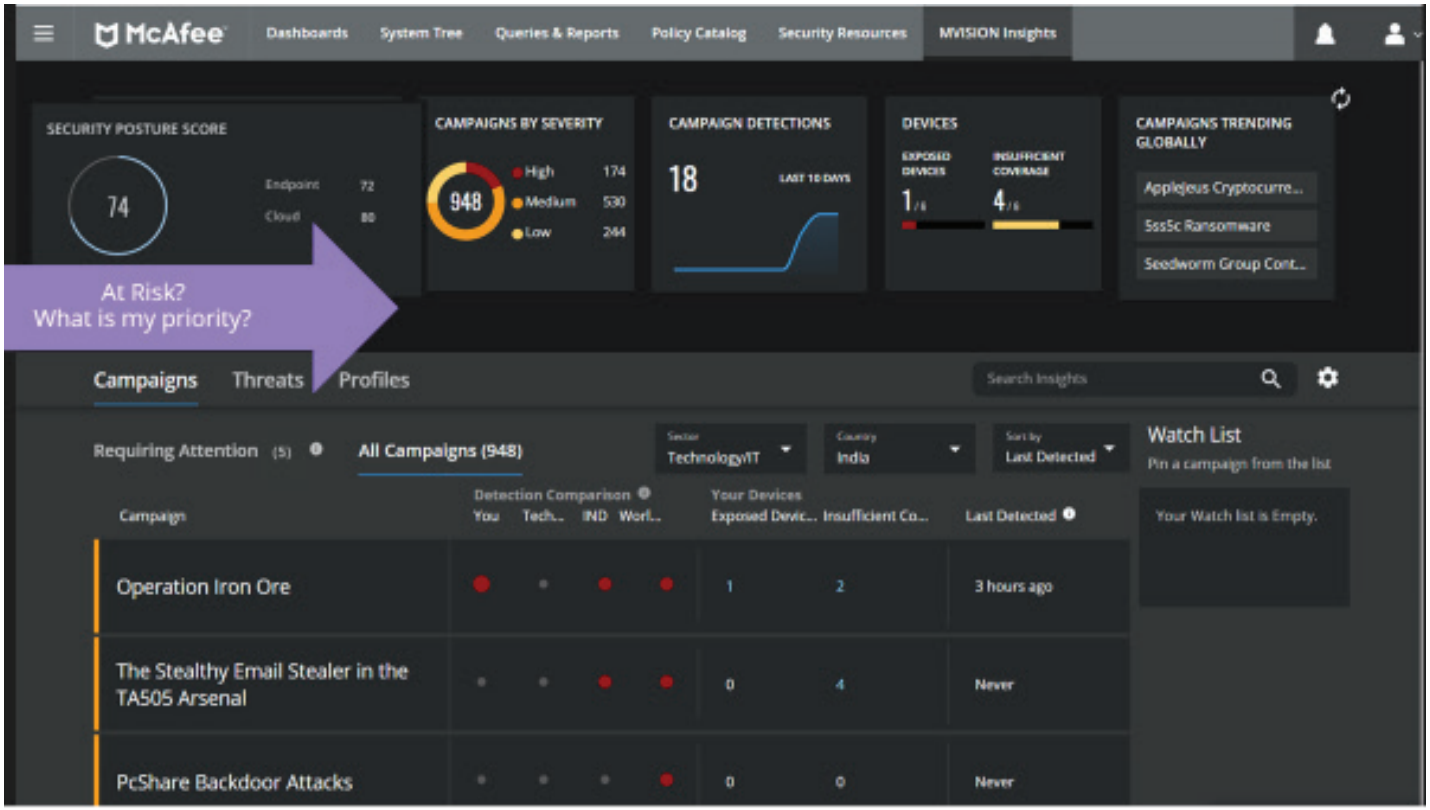

Figura 2. Panel de MVISION Insights.

Avance con una postura de seguridad completa

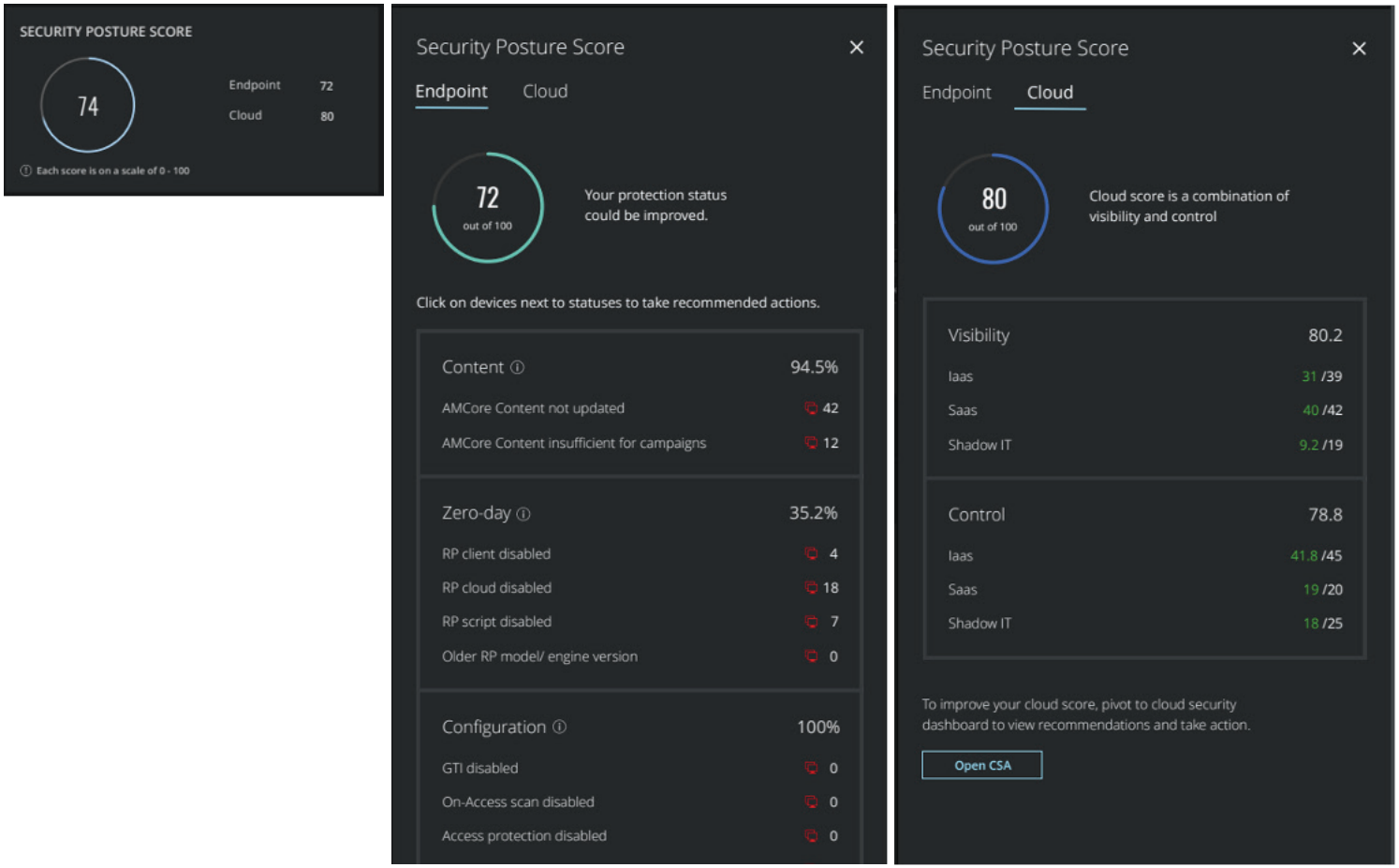

Figura 3. Puntuación de la postura de seguridad unificada y procesable de un vistazo.

Consiga evaluaciones de riesgos procesables

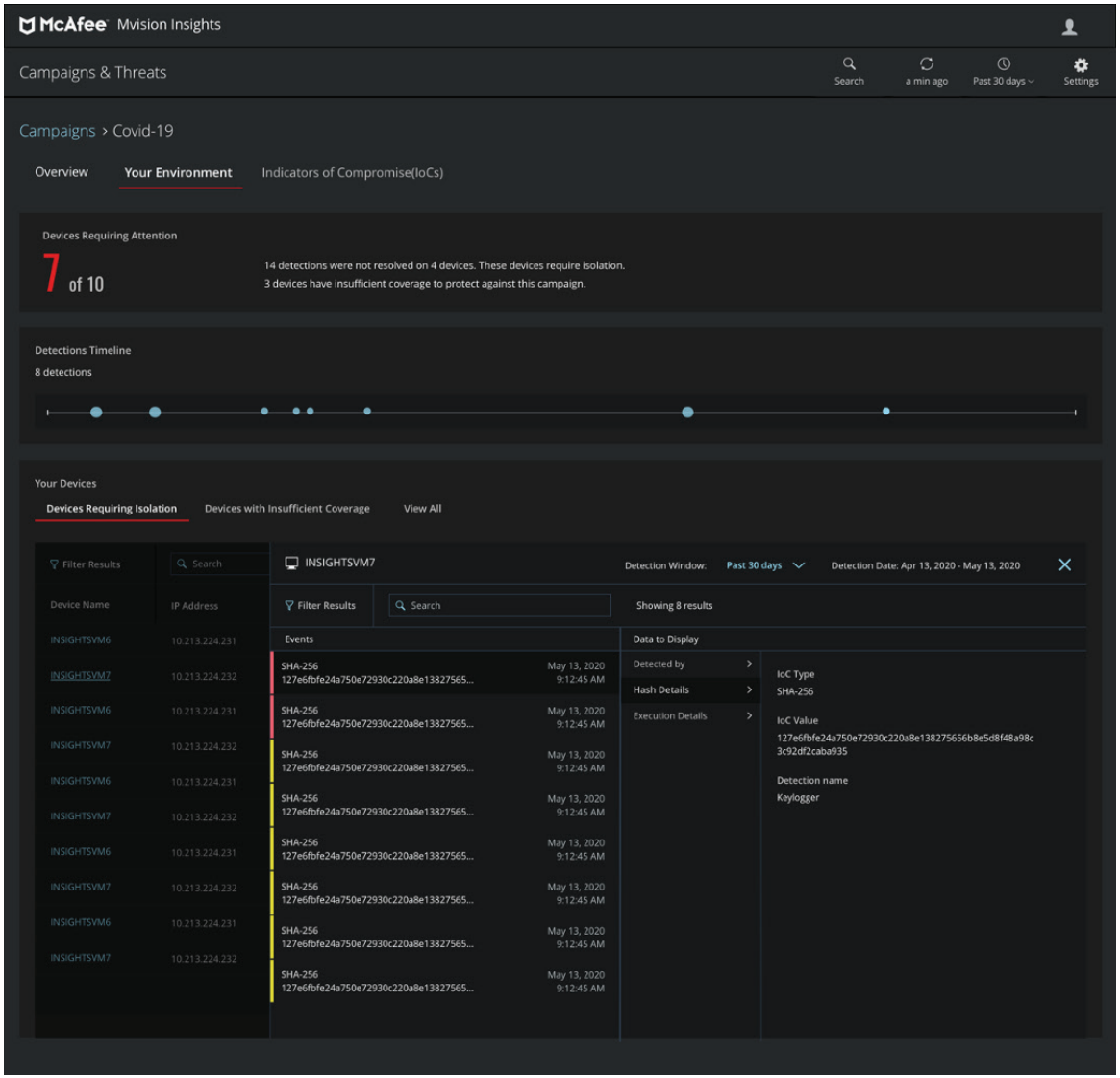

Figura 4. Sepa lo que requiere atención en su entorno para repeler las amenazas de forma proactiva.

Importante reducción del tiempo de detección y respuesta

MVISION Insights ayuda a su empresa a dar el siguiente paso crítico proactivamente, para cambiar y corregir su entorno específico con instrucciones establecidas y acciones automatizadas. La automatización aumenta la eficacia frente a ataques externos, gracias a que las amenazas externas se analizan y comparan sin necesidad de intervención humana y a que se establecen mecanismos proactivos de defensa antes de que se produzcan ataques.

- **El tiempo medio hasta la detección y la resolución se reduce de meses a minutos:** la colaboración entre el hombre y la máquina (aprendizaje profundo y aprendizaje automático), junto a las funciones de análisis avanzado se amplían para cribar enormes cantidades de datos y presentar inteligencia práctica. La mayor capacidad de detección disminuye preventivamente los tiempos de respuesta y los riesgos.
- **Se mejora la relación señal-ruido en los indicadores de amenazas:** los análisis avanzados amplían la detección y le ayudan a dar mayor sentido a las alertas. El análisis de amenazas de MVISION Insights puede recurrir fácilmente a McAfee® EDR para buscar contexto adicional, como indicadores de peligro (IoC), y reducir los ciclos de investigación. Se comparte importante información contextual sobre los ciberdelincuentes/organizaciones criminales detrás de la campaña: las herramientas que utilizan, las vulnerabilidades y exposiciones comunes (CVE) a las que han estado asociadas, las tácticas/subtécnicas estándar y los indicadores de peligro asociados, así como fuentes confiables sobre la organización.
- **Las amenazas se indican de una forma que es comprensible, clasificadas por prioridad y con capacidad de acción:** una postura de seguridad completa y unificada incluye tanto evaluaciones de endpoints como de la nube, y le permite centrarse en lo que importa en todo el entorno. Incluso los analistas noveles ganarán en confianza, gracias a que cuentan con una respuesta guiada por inteligencia y datos analizados y priorizados. Desde la consola integrada, es posible responder con facilidad y rapidez modificando las configuraciones, aislando los dispositivos infectados, actualizando las directivas o recurriendo a la detección y respuesta para endpoints (EDR).

Capacitación de los recursos de los SOC

Los departamentos de seguridad se ven sobrepasados por el inmenso volumen de información que deben examinar para proteger sus entornos. Las limitaciones de recursos y tiempo impiden el análisis de las amenazas y las defensas. La asociación hombre-máquina mejora la capacidad de análisis, sea cual sea el nivel de los analistas, y permite explorar enormes cantidades de datos y presentarlos como información procesable. MVISION Insights permite que su empresa subsane la falta de profesionales y aumente las capacidades del personal de los centros de operaciones de seguridad. Los equipos de seguridad están mejor informados para tomar mejores decisiones.

- Es el conocimiento humano que se adquiere a partir de la información procesada lo que permite a los equipos de seguridad personalizar y maximizar la defensa de la empresa con el fin de optimizar su protección, sin necesidad de incrementar el tamaño

de la plantilla ni depender de que los miembros tengan más experiencia. MVISION Insights ofrece información más práctica a MVISION EDR a fin de reducir la duración del ciclo de investigación, aportando los conocimientos y recursos necesarios para llevar a cabo las investigaciones. Los analistas pueden verificar el riesgo del incidente y su causa principal con mayor velocidad y eficacia.

- La solución ayuda a los directores de seguridad (CSO) a obtener el máximo rendimiento de su plantilla y de sus productos, a liberar a los analistas de seguridad de las tareas rutinarias y a mejorar la eficacia incluso de los miembros más inexpertos del equipo. Las empresas pueden lograr una reducción de las horas dedicadas a la gestión de la seguridad. Además, se simplifican los flujos de trabajo para agilizar la aplicación de otras medidas de protección.
- La detección, respuesta y defensa ante las amenazas prioritarias se llevan a cabo automáticamente desde una sola consola, y se reduce la necesidad de que los analistas cambien de una tarea a otra. MVISION Insights acumula y analiza los datos relevantes con medidas prácticas en un solo lugar, poniéndolos al alcance de los analistas de seguridad cuando los necesiten.

Información más detallada

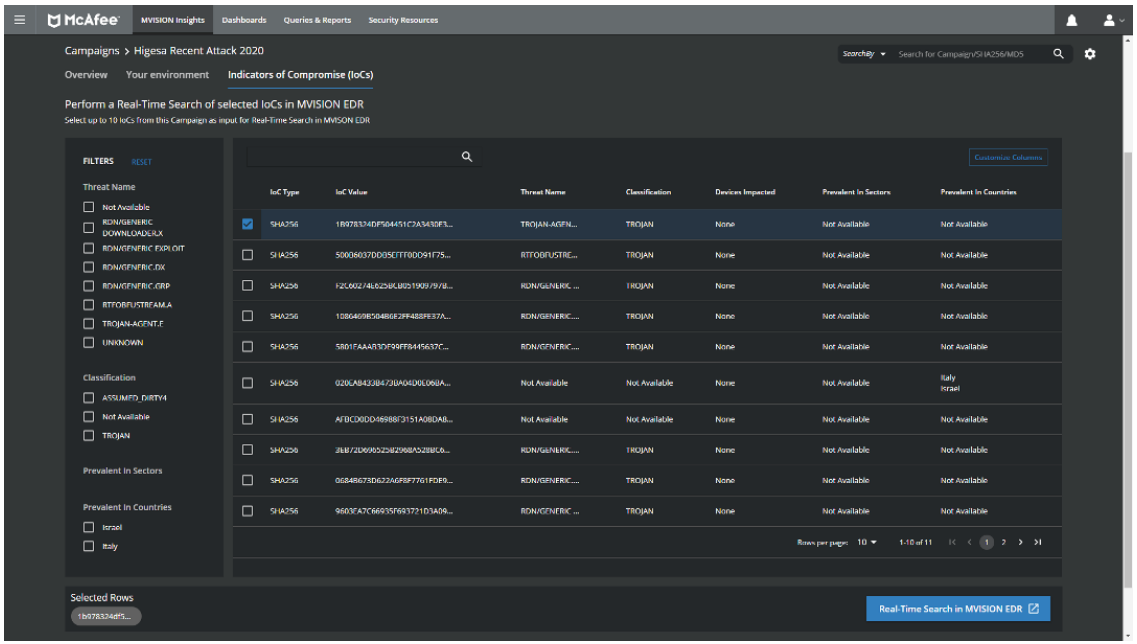

Figura 5. Indague más para comprender los eventos de amenazas y determinar su capacidad para proteger su organización con la opción de cambiar a la función EDR.

Requisitos de MVISION Insights

MVISION Insights se gestiona mediante el software McAfee® ePolicy Orchestrator® (McAfee® ePO™) 5.10 (in situ e IaaS) y McAfee® MVISION ePO™ (SaaS). Está optimizado para su uso con nuestra última tecnología de protección de endpoints: McAfee® Endpoint Security y McAfee® Agent. MVISION Insights requiere telemetría de McAfee Endpoint Security (con autorización del usuario) para funcionar correctamente.

Ejemplo de casos de uso

Problema	Solución	Resultado
¿Soy objetivo de posibles ataques? **¿Es una nueva variante de una campaña?**	▪ Evaluación de amenazas conocidas. ▪ Evaluación de grupo o autor de amenazas graves. ▪ Análisis retrospectivo de ciertos ataques. ▪ Generación de informes comparativos sobre la eficacia de la protección. ▪ Análisis retrospectivo de ataques con indicador de peligro de usuarios.	Responda a la pregunta: ¿Corro peligro? ¿Soy objetivo de un ciberdelincuente específico? ¿Hay una campaña que es probable que me afecte?
¿Cuál es mi postura de seguridad global?	▪ Postura de seguridad unificada desde el endpoint hasta la nube.	Evaluación y actuación en función de mi higiene de seguridad global.
¿Me protege mi configuración de protección actual?	▪ Comprobación local del estado de la protección.	Evaluación del estado actual de mi seguridad.
¿Qué tengo que hacer en concreto para estar protegido?	▪ Comprobación local del estado de la protección.	Medidas de orientación sobre lo que hay que hacer.
¿Pueden mis otras funciones de seguridad aislar la amenaza?	▪ Publicación para aislar o contener en otras funciones de seguridad.	Envío de acciones de contención a otras funciones de seguridad para mitigar todavía más el riesgo (a través de Data Exchange Layer [DXL]).

Más información

Para obtener más información, visite www.mcafee.com.

Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas, Madrid, España
+34 91 347 85 00
www.mcafee.com/es