McAfee Investigator

Transforme a los analistas en expertos investigadores

McAfee® Investigator ayuda a los analistas a cerrar más casos en menos tiempo y con mayor confianza de haber determinado el origen del problema. Las alertas clasificadas activan el análisis especializado de los sistemas SIEM y datos de endpoints en tiempo real pertinentes. Los centros de operaciones de seguridad pueden investigar de manera eficaz el malware, las amenazas a través de la red y los indicadores de peligro mediante la automatización, la experiencia y la inteligencia artificial.

Desafíos de los centros de operaciones de seguridad

Los problemas que generan los enormes volúmenes de datos y su tiempo de conservación complican la tarea de evaluar con precisión la importancia y alcance de una alerta. Los analistas a menudo ignoran las alertas porque carecen del contexto o del conocimiento para decidir si deberían tratarse como incidentes formales.

En consecuencia, las investigaciones de los incidentes seleccionados pueden prolongarse en el tiempo y requerir un amplio conocimiento de los vectores de amenazas para llegar hasta el fondo del problema. Estas tendencias implican que aumenta la necesidad de disponer de analistas de centros de operaciones de datos experimentados, y sin embargo la reserva de expertos es escasa.

Nuevos análisis investigativos

Los centros de operaciones de seguridad maduros están haciendo frente a este problema con automatización y análisis sofisticados para agilizar el cierre de los mismos mientras se identifica el origen del problema, según una investigación de McAfee[1].

McAfee Investigator pone la automatización y los análisis avanzados al alcance de todos los centros de operaciones de seguridad. Como oferta de seguridad como servicio (SaaS), los sistemas especializados y las herramientas de captura para endpoints se integran con las fuentes de datos y sistemas de administración de la seguridad existentes para ofrecer una rápida rentabilización con un mínimo esfuerzo.

Estos análisis interactivos proporcionan automatización, conocimiento y orientación actualizada permanentemente para capacitar a los responsables de la respuesta

Principales ventajas

- **Reduzca el tiempo de permanencia:** la exploración de los datos del caso aumenta las posibilidades de detectar el origen del problema en lugar de corregir un síntoma.
- **Pase de alertas a casos:** reduzca el tiempo dedicado a las investigaciones manuales y de prioridad baja.
- **Preste atención a lo desconocido:** céntrese en los artefactos y datos únicos que requieren interpretación y decisiones humanas.
- **Mejore la clasificación:** procese más casos en menos tiempo y con mayor calidad.
- **Reduzca la fatiga de los analistas:** aproveche al máximo el tiempo limitado, la energía y la capacidad cognitiva.
- **Desarrolle las aptitudes de los analistas:** los analistas reciben formación a través de manuales e información relevante sobre las cuestiones e hipótesis adecuadas dentro del flujo de trabajo.

a incidentes para investigar a fondo el malware, las amenazas a través de la red y los indicadores de peligro en menos tiempo y con mayor precisión.

Clasifique de forma rápida y precisa

McAfee Investigator mejora la clasificación de manera inmediata permitiendo que las operaciones de seguridad automaticen la asignación de prioridades a determinadas situaciones para gestionarlas de manera inmediata. Para estas y otras alertas que desea explorar un analista, McAfee Investigator recopila, organiza, resume y muestra las alertas, la actividad, las pruebas y la inteligencia reunida sobre un ataque potencial.

Se recopilan datos en segundo plano y se incluyen solo los que son importantes para llevar a cabo una investigación sobre amenazas específica que permitirá tomar una decisión. Los datos de las soluciones de administración de eventos e información de seguridad (SIEM) pueden complementarse con datos de los endpoints, sin necesidad de agentes de detección y respuesta para endpoints (EDR) en cada nodo. Este modelo sustituye la información aislada por visibilidad contextual de los indicadores de peligro, tácticas, técnicas, procedimientos y relaciones.

Un motor de análisis de datos y aprendizaje automático compara las pruebas con referencias conocidas y fuentes de inteligencia sobre amenazas. Procesa los artefactos y aumenta la información sospechosa fundamental.

Gracias a la recopilación y priorización automáticas de los datos adecuados, McAfee Investigator reduce el esfuerzo y aumenta la velocidad con la que los analistas pueden determinar el riesgo y urgencia del incidente.

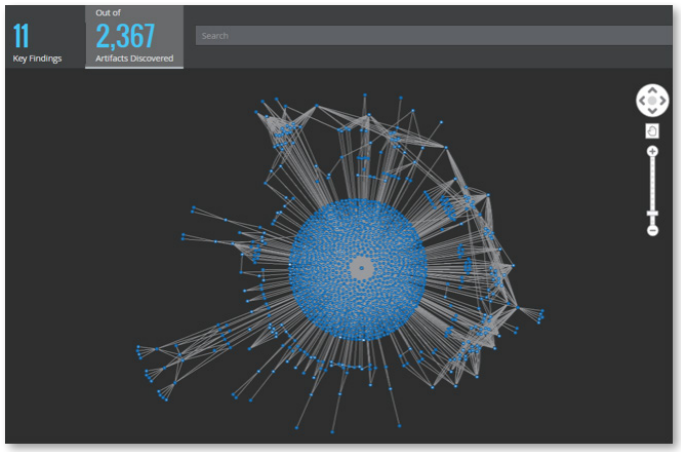

Figura 1. McAfee Investigator recopila miles de elementos de prueba.

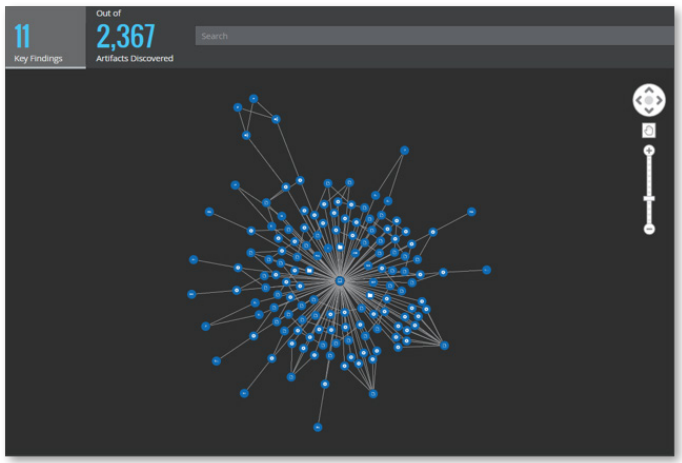

Figura 2. McAfee Investigator aplica entonces análisis y asesoramiento especializado para presentar las conclusiones que importan.

Principales ventajas (continuación)

- **Aumente el valor de los sistemas actuales:** se mejoran las fuentes de datos y análisis existentes para centrar objetivos y aumentar la precisión.

Características principales

- Recopilación precisa de datos bajo demanda
- Agente de recopilación de datos en los endpoints diferenciado
- Interpretación de los datos recopilados con asesoramiento especializado e inteligencia artificial
- Visualizaciones interactivas
- Hipótesis multivector para explorar datos factibles
- Referencias para inteligencia institucional
- Gestión de casos específicamente para las investigaciones

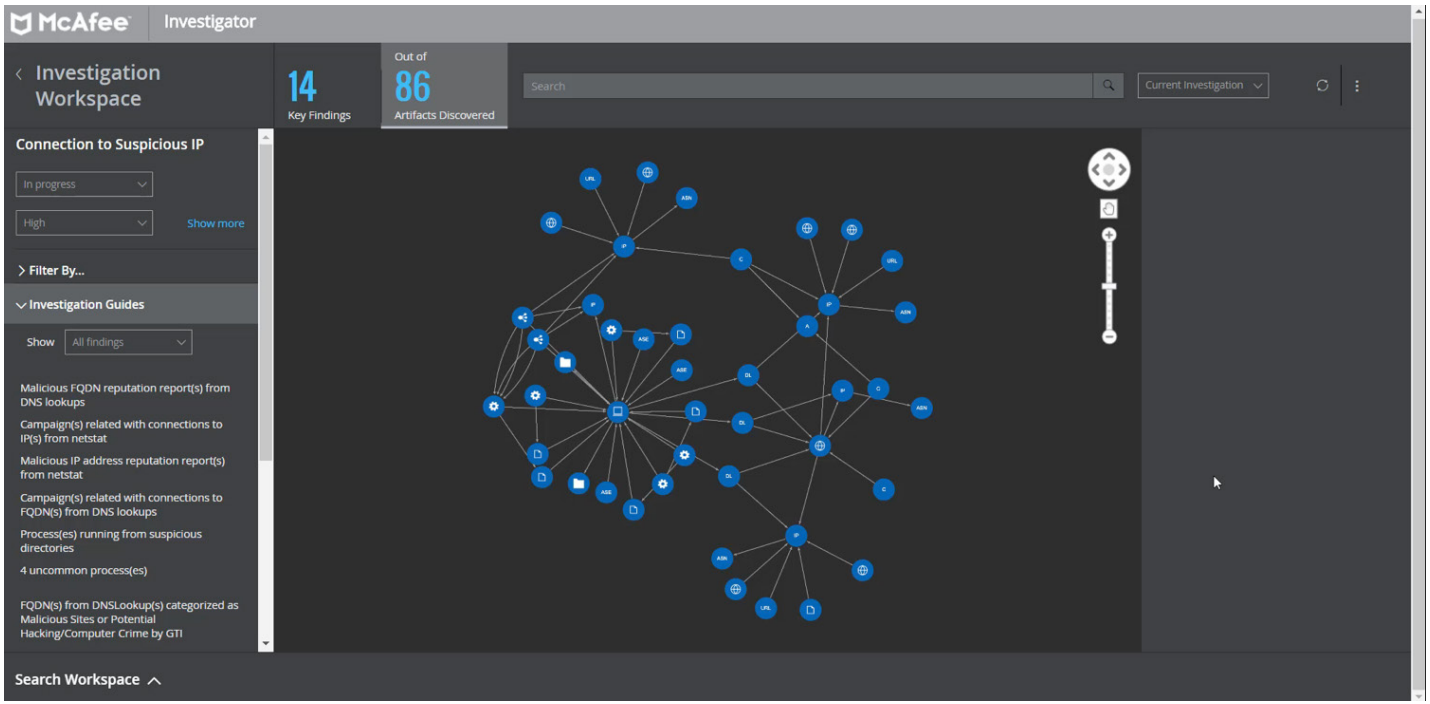

Figura 3. El espacio de trabajo convierte en obvias y fáciles de analizar las conclusiones principales.

Los analistas pueden adoptar decisiones de clasificación precisas de forma más rápida y poner el foco en las amenazas más importantes.

A nivel organizativo, los beneficios son muchos. Al elevar la clasificación de meras revisiones de alertas a casos contextuales, todos los analistas aumentan su eficacia, se gestionan un mayor número de casos por parte de analistas de Nivel 1, y los analistas dedican el tiempo a las actividades de mayor valor.

Cuando se elige un incidente para llevar a cabo una investigación detallada, los analistas aprovechan los manuales interactivos que les dirigen a lo que es importante a medida que se determina su alcance y se evalúa. Los manuales de investigación no se basan en scripts ni en código estático. El sistema simula el cerebro humano, explorando muchas hipótesis en paralelo para conseguir la máxima velocidad y exactitud.

Los manuales en lenguaje natural se han realizado con una combinación de experiencia de los investigadores de Foundstone® e inteligencia artificial. Esta es una de las formas mediante las que McAfee Investigator incorpora la asociación hombre-máquina.

El espacio de trabajo estructura la información y los hallazgos sobre los casos para que los analistas planteen las cuestiones adecuadas. Esta exploración focalizada y multivector se traduce en el cierre de casos eficaz y preciso con un alto grado de confianza de que los analistas han identificado la causa fundamental.

Mejore la experiencia y la colaboración

El espacio de trabajo de McAfee Investigator continúa con las innovaciones de McAfee en lo que a interfaz de usuario se refiere. Impulsa los flujos de trabajo y la navegación a través de datos de un único entorno cognitivo. Este modelo reduce la sobrecarga de información generada a partir de la gran multitud de tipos de alertas y elimina la necesidad de revisar varias pantallas.

El espacio de trabajo enseña a los analistas inexpertos y de nivel intermedio a implementar los procesos de pensamiento de analistas avanzados, generando experiencia sin formación adicional. Además, activa flujos de trabajo de casos para simplificar el acceso, el registro, el intercambio y la actualización de casos entre equipos. El intercambio sistemático de datos es especialmente importante si tenemos en cuenta los niveles y equipos distribuidos que caracterizan a los centros de operaciones de seguridad.

Aproveche las herramientas y datos existentes

McAfee Investigator trabaja con un sistema SIEM y el software McAfee® ePolicy Orchestrator® para añadir análisis avanzados a las fuentes de datos, referencias, correlaciones y alertas existentes. Un agente diferenciado recopila nuevos datos de endpoints que resultan fundamentales para realizar una interpretación precisa de pruebas discretas. Los servicios profesionales facilitan la incorporación y la activación correctas.

Más información

Con McAfee Investigator, cuando tiene una sospecha, no necesita dedicar horas a recopilar datos e incluso más tiempo a interpretarlos. El motor de análisis avanzado que utiliza McAfee Investigator inspecciona y clasifica las alertas de amenazas dentro de una interfaz basada en el contexto para escalar las operaciones de seguridad. McAfee Investigator automatiza el uso de conocimientos especializados en investigaciones de centros de operaciones de seguridad, lo que permite a los analistas trabajar de forma más inteligente, rápida y con un mayor grado de precisión.

Esta es la verdadera asociación hombre-máquina.

Para obtener más información, visite **www.mcafee.com/mx/products/investigator.aspx**.

1. https://www.mcafee.com/mx/resources/reports/rp-disrupting-disruptors.pdf

McAfee Together is power.

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

3644_1017
Octubre de 2017