FIREEYE SECURITY ORCHESTRATOR

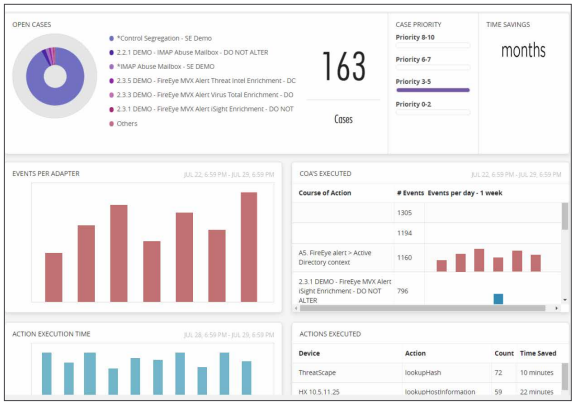
INTEGRE Y AUTOMATICE LAS TECNOLOGÍAS Y LOS PROCESOS DE ADMINISTRACIÓN DE INCIDENTES EN TODA SU INFRAESTRUCTURA DE TI

DESCRIPCIÓN GENERAL

El volumen de ciberataques ha llegado a niveles nunca vistos, y si sus defensas no están a la altura, aumentará enormemente el riesgo de convertirse en víctima. Los agresores cuentan con los recursos intelectuales, la capacidad computacional y la infraestructura de las redes de transferencia digital más rápidas. Modifican la firma de su ataque, se adaptan para emplear nuevos métodos de infección y cambian constantemente su estrategia para conseguir infiltrarse en su red y, de esta forma, ponen a prueba sus defensas en cualquier momento. Durante todo el día, todos los días. Si a eso añadimos el volumen de alertas que soportan la mayoría de los centros de operaciones de seguridad a diario y la dificultad para encontrar los recursos necesarios para gestionar esos centros de operaciones, con un programa tradicional basado en la intervención y la contención manuales la lucha sería desigual.

FireEye Security Orchestrator acelera y simplifica la detección y la respuesta a amenazas mediante la centralización de tecnologías y procesos de administración de incidentes diferentes en una única consola que proporciona respuestas en tiempo real para mejorar los tiempos de respuesta, reducir la exposición a riesgos y garantizar la coherencia entre los procesos de un programa de seguridad. Los años de experiencia de FireEye en la lucha contra los ataques más devastadores del mundo han ayudado a perfeccionar procesos eficaces que permiten detectar, investigar y responder a las amenazas. FireEye Security Orchestrator permite combinar estas mejores prácticas en los datos del despliegue de FireEye, SIEM y otras tecnologías empresariales.

FireEye Security Orchestrator puede adoptar cambios a nivel de red, host y aplicaciones, e incluso en sistemas de control de acceso físico. Su capacidad para responder de manera eficaz en solo segundos detiene en seco al intruso y blinda el entorno, lo que reduce los daños y riesgos para la empresa.



VENTAJAS

- Mejore la capacidad de su equipo de seguridad con asistencia para el despliegue y el diseño, y tácticas predefinidas, proporcionada por un equipo que cuenta con una década de experiencia en la primera línea de las investigaciones de los ciberataques más importantes.
- Elimine errores a través de un proceso estandarizado y automatización, mientras reduce las exigencias de tiempo en equipos de centros de operaciones de seguridad de por sí muy sobrecargados.
- Permita a los equipos del centro de operaciones de seguridad reducir el riesgo con tiempos de respuesta más rápidos y deje que se centren en las tareas de mayor prioridad, que pueden mejorar todavía más su estado de seguridad, como la persecución.
- Paneles centralizados y administración de casos para afianzar su proceso de operaciones de seguridad.

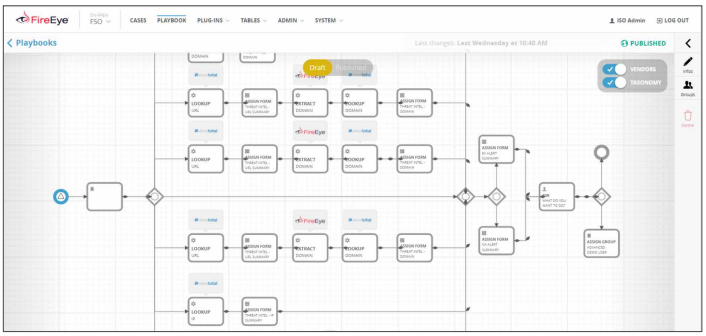
Con FireEye Security Orchestrator, ahorra tiempo y recursos mediante la unificación de los datos relacionados con incidentes y sus tecnologías de seguridad en una única plataforma de operaciones de seguridad.

Nuestros clientes reducen de manera importante los tiempos de respuesta y eliminan errores de proceso, lo que a la larga reduce la exposición general a riesgos.

CARACTERÍSTICAS FUNDAMENTALES

Tácticas de respuesta a incidentes

Las tácticas de respuesta a incidentes, también conocidas como planes de acción (CoA), organizan las operaciones de seguridad en flujos de trabajo dirigidos por personas y en tareas automatizadas. Una vez que los procesos de su centro de operaciones de seguridad están documentados, automatizados y optimizados gracias a la experiencia de FireEye en la lucha contra los ataques más avanzados del mundo, sus tiempos de respuesta disminuirán y, al mismo tiempo, garantizará la coherencia entre los procesos de todo el programa de seguridad.



Utilice el nuevo Creador de planes de acción para crear flujos de trabajo inteligentes y diversificados que se ajusten a sus directivas de seguridad y a la infraestructura de soporte de su empresa. Incluye una cartera completa de complementos y flujos de trabajo preconfigurados en todas las herramientas de sus operaciones de seguridad, como SIEM, firewall, inteligencia sobre amenazas, sistemas de prevención de intrusiones (IPS) y de administración de incidencias (o ticketing). Permite la creación de flujos de trabajo personalizados para las directivas de seguridad y la infraestructura de soporte de su empresa. Gracias a las tácticas, puede deconstruir los flujos de trabajo de los analistas de seguridad en una secuencia automatizada completa o parcial de tareas, con la posibilidad de solicitar a los analistas sugerencias que permiten informar a la dirección sobre un flujo de trabajo concreto. El resultado final será un entorno en perfecta sincronía con los flujos de trabajo de seguridad desarrollados y aprobados por su empresa. Estos cambios se convertirán en flujos de trabajo de automatización que pueden iniciarse automáticamente, activados por eventos de su infraestructura o ejecutados cuando sea necesario por el personal de su centro de operaciones de seguridad.

Acceso basado en funciones

Cree grupos basados en funciones y asigne permisos concretos a cada táctica o a etapas específicas dentro de una táctica. De esta forma, cada equipo dispone de acceso y privilegios de ejecución para leer los resultados solamente de los flujos de trabajo que necesita. Puede utilizar grupos y usuarios locales, o integrar su directorio de Active Directory u Open LDAP, y asignarlo a funciones en Security Orchestrator.

Complementos

Integre, unifique y controle su arquitectura de TI desde un único panel, a través de los complementos. Los complementos son el hilo conductor que une sus dispositivos, aplicaciones, servicios y datos en FireEye Security Orchestrator. Están diseñados para admitir algunas de las tecnologías de seguridad e infraestructura más populares.

Esta arquitectura conectable permite a las empresas cambiar o incorporar tecnología con un mínimo de formación sobre respuesta e integración. Los complementos ofrecen comando y control bidireccional para recibir datos y ejecutar acciones.

Paneles centralizados y persecución avanzada

FireEye Security Orchestrator ofrece un panel de investigación que permite buscar en las distintas herramientas de seguridad y facilita la persecución de los agresores que han atacado su empresa. También puede administrar los casos y pasar rápidamente de las tácticas al contexto adicional en toda la infraestructura de seguridad existente.

Además, sus analistas pueden consultar un panel centralizado y mapas mundiales de amenazas para crear una vista integral de los datos y ataques detectados por los dispositivos de FireEye dentro de su empresa. Esta vista puede ofrecerle tanto datos históricos como información en tiempo real

para agilizar la detección y la respuesta. También puede llevar a cabo investigaciones en profundidad a través de búsquedas ultrarrápidas, escalonadas y muy flexibles en los datos de notificaciones de alertas de FireEye. Esto le permite acceder rápidamente desde una alerta a un contexto más amplio sobre el ataque. Todos los paneles de búsqueda pueden guardarse y enviarse por correo electrónico.

Informes

Puede crear informes únicos o recurrentes que detallan, correlacionan y muestran alertas relacionadas. Los equipos de seguridad pueden determinar con rapidez las fuentes, metodología y objetivos de un ataque, así como evitar que vuelva a producirse en el futuro. Los informes pueden personalizarse con:

- Miles de parámetros de alerta
- Filtros minuciosos
- Varios formatos de archivos
- Representaciones con gráficos específicos para la empresa
- Servicios profesionales: plataforma de orquestación

Hay disponibles servicios de despliegue personalizados para diseñar y desplegar FireEye Security Orchestrator en su programa y arquitectura de seguridad. Estos servicios aprovechan la experiencia de FireEye para diseñar las tácticas adecuadas según las soluciones de tecnología de su entorno y las amenazas a las que se enfrenta su empresa a diario.

Para más información sobre FireEye, visite:
www.FireEye.com

ACERCA DE FIREEYE, INC.

FireEye es el líder en seguridad como servicio basado en la inteligencia. FireEye, que funciona como una extensión escalable y flexible de las operaciones de seguridad del cliente, ofrece una sola plataforma que combina innovadoras tecnologías de seguridad, inteligencia sobre amenazas a nivel de nación-estado y los servicios de consultoría de Mandiant® de fama mundial. Gracias a este enfoque, FireEye elimina la complejidad y la carga de la ciberseguridad para las organizaciones que desean estar preparadas, prevenir y responder a los ciberataques. FireEye tiene más de 5000 clientes en más de 67 países, incluidas más de 940 empresas de la lista Forbes Global 2000.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
+1 408.321.6300 / 877.FIREEYE (347.3393) / LATAM@FireEye.com

www.FireEye.com