CROWDSTRIKE

CROWDSTRIKE **FALCON INSIGHT™** DETECCIÓN Y RESPUESTA PARA ENDPOINTS

TRANSMISIÓN DEL CICLO VITAL DE DETECCIÓN Y RESPUESTA ANTE AMENAZAS CON RAPIDEZ, AUTOMATIZACIÓN Y VISIBILIDAD SIN PARANGÓN

FALCON INSIGHT — DETECCIÓN Y RESPUESTA PARA ENDPOINTS (EDR) SIMPLIFICADA

Las herramientas de seguridad de endpoints tradicionales presentan puntos ciegos que no les permiten ver y detener las amenazas avanzadas. Falcon Insight soluciona este problema proporcionando una visibilidad integral de los endpoints en toda la empresa. Insight supervisa permanentemente la actividad de los endpoints y analiza los datos en tiempo real para identificar de forma automática la actividad de amenazas, lo que le permite detectar y prevenir amenazas avanzadas cuando se producen. La actividad de los endpoints también se transmite a la plataforma CrowdStrike Falcon®, de manera que los equipos de seguridad puedan investigar rápidamente los incidentes, responder a las alertas y cazar de forma proactiva nuevas amenazas.

FALCON INSIGHT ES EL LÍDER DEL SECTOR EN EDR

"Mejor análisis de comportamiento/detección de amenazas corporativas" Security Magazine Award 2017

"Máxima puntuación en detección" (5/5) y "Máxima puntuación en coste" (relación calidad-precio) en 2017 Forrester Endpoint Security Wave

Calificación de "Strong" (valoración más alta posible) en todos los casos de uso evaluados en el informe 2017 Comparison of Endpoint Detection and Response Technologies and Solutions de Gartner

VENTAJAS CLAVE

» Detección automática de amenazas avanzadas

» Agilización de las investigaciones con análisis forense en tiempo real

» Remediación segura

» Búsquedas corporativas en cinco segundos

» Habilitación del servicio de cacería de amenazas Falcon OverWatch™

CAPACIDADES CLAVE DEL PRODUCTO

DETECCIÓN Y RESOLUCIÓN SIMPLIFICADAS

- **Detecte automáticamente las actividades de los atacantes** — Insight utiliza indicadores de ataque (IOA) para identificar de forma automática el comportamiento de los atacantes y envía alertas por orden de prioridad a la IU de Falcon, eliminando así las investigaciones exhaustivas y las búsquedas manuales.
- **Descifre ataques completos en una sola pantalla** — Un árbol de procesos de fácil lectura proporciona detalles de la totalidad del ataque en contexto para acelerar y simplificar las investigaciones.
- **Agilice el proceso de investigación** — La IU intuitiva le permite estructurar y realizar búsquedas en toda la empresa en cuestión de segundos.
- **Obtenga contexto e inteligencia** — La inteligencia de amenazas integrada proporciona el contexto completo de un ataque, incluida la atribución.
- **Contenga los sistemas bajo sospecha con tan solo un clic** — Pone fin de inmediato a la actividad de los adversarios conteniendo los sistemas comprometidos.

OBTENGA MÁXIMA VISIBILIDAD EN TIEMPO REAL

- **Observe cada movimiento en tiempo real** — La visibilidad inmediata le permite ver las actividades como si estuviera "mirando por encima del hombro" a los adversarios.
- **Capture detalles críticos para investigaciones forense** — El controlador de modo kernel de Falcon Insight captura más de 200 eventos e información relacionada necesaria para realizar un seguimiento de los incidentes.
- **Obtenga respuestas en cuestión de segundos** — La base de datos CrowdStrike Threat Graph™ almacena datos de los eventos y responde a las consultas en cinco segundos o menos, incluso en relación con miles de millones de eventos.
- **Registros de hasta 90 días** — Falcon Insight ofrece un registro completo de la actividad de los endpoints con el tiempo, independientemente de que su entorno este compuesto por menos de 100 endpoints o más de 500.000.

TIEMPO DE CREACIÓN DE VALOR INMEDIATO

- **Ahorre tiempo, esfuerzo y dinero** — Falcon Insight, basado en la nube, se proporciona a través de la plataforma CrowdStrike Falcon™ y no requiere infraestructura de gestión in situ.
- **Implementación en minutos** — Los clientes de CrowdStrike pueden implementar el agente Falcon entregado a través de la nube en hasta 70.000 endpoints en menos de un día.
- **Operatividad inmediata** — Con detección y visibilidad sin parangón desde el primer día, Falcon Insight ofrece supervisión y registro inmediatos tras la instalación sin necesidad de reinicios, ajustes ni configuraciones de base o complejas.
- **Impacto cero en los endpoints** — Con un agente liviano que tan solo necesita 20 MB de espacio en el endpoint, las búsquedas se realizan en la base de datos Falcon Threat Graph™ sin repercutir en el rendimiento de los endpoints o la red.

LA FACULTAD DE EVITAR FALLOS SILENCIOSOS Y DETENER VULNERACIONES

Las tecnologías de prevención no son perfectas. Si los atacantes consiguen eludir la protección de su empresa, pueden pasar desapercibidos durante semanas o meses, porque los equipos de seguridad no disponen de la visibilidad ni de las herramientas de detección necesarias para identificar actividades posteriores a una vulneración. Este periodo de "fallo silencioso" se traduce en éxito para el atacante y en una posible catástrofe para la empresa. Falcon Insight detecta, identifica y permite responder rápidamente a los incidentes que pasan desapercibidos para la protección existente.

CROWDSTRIKE

CrowdStrike es el líder en protección de endpoints de próxima generación entregada desde la nube. CrowdStrike ha revolucionado la protección de endpoints al ser la primera y única empresa en unificar antivirus de próxima generación, detección y respuesta para endpoints (EDR), y un servicio gestionado de cacería 24/7, todo ello de la mano de un único agente liviano.

Más información en **crowdstrike.com**