

# CROWDSTRIKE FALCON INTELLIGENCE

Falcon Intelligence de CrowdStrike integra la inteligencia de amenazas a la protección de endpoints, automatizando las investigaciones de incidentes y acelerando la respuesta frente a las brechas

## CROWDSTRIKE FALCON INTELLIGENCE

### HACER DE LA SEGURIDAD PREDICTIVA UNA REALIDAD

Para los equipos de ciber protección que se esfuerzan por responder a las alertas de ciberseguridad y no tienen el tiempo o la experiencia para adelantarse a las amenazas emergentes, la solución Falcon Intelligence™ de CrowdStrike ofrece la inteligencia que usted necesita, al mismo tiempo que elimina la complejidad de investigaciones de incidentes que consumen una gran cantidad de recursos. Falcon Intelligence es la única solución que integra realmente la inteligencia de amenazas a la protección de endpoints, realizando investigaciones automáticamente, acelerando las respuestas y permitiéndoles a los equipos de seguridad pasar de un estado reactivo a uno predictivo y proactivo.

Utilizando como base la plataforma única y nativa de la nube Falcon® de CrowdStrike, los equipos de ciber protección ahora pueden analizar automáticamente el malware identificado en los endpoints, encontrar muestras relacionadas con el buscador de malware más grande del sector y enriquecer los resultados con una inteligencia de amenazas personalizada. Este sistema de circuito cerrado les proporciona a los equipos de seguridad indicadores de compromiso (IOCs) personalizados que pueden ser compartidos con sus otras herramientas de seguridad, así como informes de inteligencia que muestran la historia completa de un ataque. Con una comprensión completa del ataque, su equipo está capacitado para responder más rápido y organizar contramedidas proactivas en toda su organización.

Falcon Intelligence y la inteligencia integrada de amenazas son el siguiente paso de la protección de endpoints. Falcon Intelligence lleva el antivirus y las alertas de detección y respuesta de endpoints a un siguiente nivel, no solo evidenciando lo que ha ocurrido en éstos, sino, también, revelando el "quién, por qué y cómo" detrás de un ataque. Comprender la amenaza a este nivel de detalle es la clave para adelantarse a futuros ataques y aumentar el costo para el adversario.

Falcon Intelligence les permite a los clientes de todos los tamaños comprender mejor las amenazas a las que se están enfrentando, al mismo tiempo que mejora la eficacia de sus otras inversiones en seguridad con inteligencia práctica y personalizada para defenderse de futuros ataques, haciendo de la seguridad proactiva una realidad.

## PRINCIPALES BENEFICIOS

Automatiza las investigaciones de todas las amenazas que llegan a sus endpoints

Brinda IOCs (Indicadores de Compromiso) personalizados para protegerse proactivamente de amenazas evasivas

Provee información completa sobre los ataques para permitir una mejor y más rápida toma de decisiones

Fortalece su equipo con análisis de los expertos de CrowdStrike® Intelligence

Simplifica las operaciones mediante una integración perfecta con la plataforma Falcon de CrowdStrike



# PRINCIPALES CAPACIDADES DEL PRODUCTO

## AUTOMATIZA Y SIMPLIFICA LAS INVESTIGACIONES DE INCIDENTES

### Integración perfecta de endpoints:

Analice las amenazas de gran impacto tomadas directamente de sus endpoints que están siendo protegidos por la plataforma Falcon de CrowdStrike. Los análisis del Falcon Intelligence son presentados como parte de los detalles de detección de una alerta de protección de endpoints de la plataforma Falcon. Independientemente de su tamaño o nivel de capacidades, los equipos de seguridad nunca perderán la oportunidad de aprender de un ataque a sus entornos.

### Ahorre tiempo, esfuerzo y dinero:

Automatice cada paso de una investigación sobre ciber amenazas y reduzca el tiempo de análisis de días a minutos. Falcon Intelligence combina la inteligencia de amenazas y el análisis y búsqueda de malware en una solución perfecta.

### Detenga a los actores maliciosos en su camino:

La inteligencia de amenazas de CrowdStrike provee la atribución del actor para exponer los motivos, las herramientas y la estrategia del atacante. Se indican orientaciones y pasos prácticos para que su equipo pueda implementar contramedidas proactivas y adelantarse a futuros ataques.

## COMPARTA IOC'S PERSONALIZADOS PARA UNA ORGANIZACIÓN DE LA SEGURIDAD

### Defiéndase de las amenazas más significativas

Mantenga a su equipo enfocado en las amenazas con las que usted realmente se ha encontrado. Falcon Intelligence ofrece IOC's personalizados que resultan del análisis automatizado de amenazas tomadas directamente de sus endpoints. Los IOC personalizados incluyen una protección contra la amenaza con la que usted se ha encontrado recientemente, así como de las amenazas relacionadas dentro de la misma campaña o familia del malware. Esta capacidad exclusiva conlleva una comprensión más profunda de las amenazas y un conjunto personalizado de IOC's para defenderse de futuros ataques.

### Obtenga acceso a los IOC's de CrowdStrike Falcon

Intelligence le permite ampliar sus defensas con un acceso en tiempo real a los IOC's globales ofrecidos por CrowdStrike.

### Integre contramedidas fácilmente

Protégase de futuros ataques con IOC's que son fácilmente utilizables por su infraestructura de seguridad. Un amplio conjunto de APIs y herramientas prediseñadas permiten una fácil armonización con las soluciones de seguridad existentes.

## EMPODERE A SU EQUIPO CON LA INTELIGENCIA DE AMENAZAS DE CROWDSTRIKE

<b>Informes de Inteligencia</b>	Reciba informes de inteligencia de amenazas confiables y detallados por parte del equipo global de CrowdStrike Intelligence. Éstos incluyen alertas de amenazas en tiempo real, informes técnicos con análisis de expertos e informes estratégicos que describen las amenazas a industrias, regiones e infraestructuras.
<b>Monitoreo de Amenazas</b>	Monitoree la web para detectar actividad adversaria dirigida contra su organización con el fin de priorizar los recursos y responder eficazmente a ciberataques inminentes.
<b>Análisis de Malware por Expertos</b>	Escale muestras particulares de malware a un experto de CrowdStrike para una investigación más detallada o una segunda opinión.
<b>Soporte de Inteligencia</b>	El equipo de CrowdStrike trabaja para asegurarse de que tiene una comprensión clara de sus requisitos de inteligencia y de que usted haya sido integrado exitosamente.
<b>Reglas de YARA/SNORT</b>	El equipo también realiza revisiones trimestrales. Adelántese a las últimas amenazas de adversarios y organice sus defensas con las reglas de YARA y SNORT, creadas y validadas por los expertos de CrowdStrike.

Comience a usar la versión de prueba gratuita del AV de última generación

## FALCON INTELLIGENCE — PROPUESTAS DEL PRODUCTO

Hay dos niveles de Falcon Intelligence, permitiéndole a su organización elegir la opción que mejor se adapta a sus necesidades y requisitos misionales.

Característica	Falcon Intelligence	Falcon Intelligence Premium
Integración de Endpoints	X	X
Inteligencia Automatizada	X	X
Inteligencia Personalizada	X	X
IOC's Globales y Personalizados	X	X
Informes de Inteligencia		X
Monitoreo de Amenazas		X
Soporte de Inteligencia		X
Análisis de Malware por Expertos		X
Reglas de YARA/SNORT		X
Reuniones Informativas Trimestrales		X

## SOBRE CROWDSTRIKE

CrowdStrike® Inc (Nasdaq: CRWD), un líder mundial en ciberseguridad, está redefiniendo la seguridad en la era de la nube con una plataforma de protección de endpoints construida desde cero para detener las brechas. La arquitectura de un agente único y liviano de la plataforma CrowdStrike Falcon® aprovecha la inteligencia artificial (IA) a escala de nube y ofrece protección y visibilidad en tiempo real en toda la empresa, previniendo ataques en endpoints, dentro o fuera de la red. Alimentada por la tecnología patentada de la CrowdStrike Threat Graph®, CrowdStrike Falcon correlaciona más de 2.5 billones de eventos por semana, y en tiempo real, relativos a endpoints de todo el mundo, alimentando una de las plataformas de datos más avanzadas del mundo en seguridad.