CROWDSTRIKE

FALCON COMPLETE: DETECCIÓN Y RESPUESTA GESTIONADA, DEMOSTRADA Y PROFESIONAL

PROTECCIÓN OPTIMIZADA PARA TODOS SUS SISTEMAS, EN TODO MOMENTO

INTRODUCCIÓN

La escasez de recursos y experiencia en ciberseguridad puede impedir a las empresas sacar el máximo provecho de la tecnología de seguridad que adquieren, lo que aumenta su nivel de riesgo y vulnerabilidad. Esto puede generar daños y requerir trabajo de corrección, lo que podría haberse evitado si las tecnologías de seguridad hubieran estado adecuadamente configuradas y actualizadas, o si se hubieran advertido, investigado y corregido con rapidez las alertas de seguridad que preceden a un incidente.

CrowdStrike® Falcon Complete™ es un servicio gestionado de detección y respuesta (MDR) que soluciona estos problemas para los clientes de CrowdStrike Falcon®, ya que aumenta la eficacia de la plataforma Falcon con la incorporación de un equipo dedicado de profesionales de seguridad. El principal y único objetivo de Falcon Complete es la administración y supervisión de la seguridad de sus endpoints, así como responder a las amenazas con rapidez y precisión, para que no tenga que hacerlo usted.

Falcon Complete es una solución integral para empresas que no disponen de grandes presupuestos de seguridad. La protección frente a las amenazas actuales requiere vigilancia permanente por parte de personal cualificado, y no son muchas las empresas que pueden hacer frente al coste asociado a la creación de un programa de seguridad completo que cuente permanentemente con expertos en seguridad. Pero incluso para las empresas que disponen de los recursos financieros para crear dichos programas internamente, el equipo de Falcon Complete es la forma más rápida y sencilla de disponer de un programa de seguridad de endpoints completo y maduro.

En CrowdStrike estamos tan firmemente convencidos de la calidad de nuestras funciones de protección contra violaciones de la seguridad que Falcon Complete viene con una garantía de prevención de violaciones de seguridad de hasta 1 millón de dólares[1], si se produce un incidente dentro del entorno protegido.

Falcon Complete complementa sus inversiones en tecnología Falcon con los profesionales dedicados y los procesos maduros que se necesitan para detener las violaciones de seguridad, donde y cuando se produzcan.

Este documento técnico explora los desafíos que implica obtener el máximo provecho de su solución de seguridad de endpoints y cómo el equipo de Falcon Complete se encuentra en una posición privilegiada para resolverlos.

> **El principal y único objetivo de Falcon Complete es la administración y supervisión de la seguridad de sus endpoints, así como responder a las amenazas con rapidez y precisión, para que no tenga que hacerlo usted.**

1 Se aplican restricciones. Para obtener más información, consulte las preguntas más frecuentes sobre la garantía de prevención de violaciones de seguridad de Falcon Complete .

DESAFÍOS COMUNES A LA HORA DE MAXIMIZAR EL ESTADO DE SEGURIDAD

Las empresas se enfrentan a problemas habituales a la hora de implementar un programa de seguridad de endpoints, lo que impulsa la demanda de servicios MDR, como Falcon Complete:

- **Dificultad para administrar la tecnología.** Para garantizar los niveles adecuados de protección, cualquier solución de seguridad requiere administración periódica proactiva. Esto garantiza el adecuado despliegue de cada endpoint de la organización y la configuración apropiada para proteger contra las amenazas modernas. Los equipos de TI no suelen disponer de las herramientas ni del ancho de banda necesario para administrar continuamente su protección de endpoints. Además, es posible que no dispongan del tiempo ni la experiencia necesarios para saber la mejor forma de configurar las directivas de seguridad en función de sus necesidades y para mantener sus endpoints protegidos. Esta situación puede dar lugar a un despliegue parcial y una configuración inadecuada de la solución para endpoints, lo que dejaría lagunas de seguridad que podrían exponer a la empresa a intrusiones.
- **Incapacidad para actuar de manera fiable contra las amenazas a tiempo de impedir una violación de la seguridad.** Las alertas de seguridad ofrecen información crítica sobre las amenazas emergentes, lo que permite a los responsables de la seguridad responder en las fases iniciales que son cruciales, antes de que se produzca una violación de la seguridad. Sin embargo, su valor depende de que los analistas puedan revisarlas y actuar a tiempo. La gestión de las alertas requiere tiempo, energía y experiencia. Muchas empresas padecen una falta estos importantes recursos de ciberseguridad. Incluso para las empresas que cuentan con un equipo de seguridad dedicado o un centro de operaciones de seguridad (SOC), la gestión de las alertas generadas por un producto de seguridad para endpoints puede ser una tarea abrumadora. Si se crea un exceso de alertas, es posible que se dejen algunas sin comprobar, lo que abriría la puerta a los ciberdelincuentes.
- **Dificultad en la corrección adecuada tras un incidente.** Se requiere formación y experiencia para determinar la mejor forma de corregir un incidente. Desafortunadamente, muchas empresas carecen del tiempo y la experiencia necesarios para comprender la naturaleza y el alcance de un incidente cuando se produce. Esto puede provocar que los equipos de seguridad se afanen durante semanas en remediar una situación, a menudo mediante acciones innecesarias y complicadas, como la recreación de imágenes, o peor aún, creer que se ha limpiado un entorno cuando no es así.

"Para 2024, el 25 % de las empresas utilizarán servicios MDR, frente al 5 % que lo hacen en la actualidad. Para 2024, el 40 % de las medianas empresas utilizarán MDR como único servicio gestionado de seguridad".

Gartner Research
Market Guide for Managed Detection and Response Services (Guía de mercado de servicios de detección y respuesta gestionados), 15 de julio de 2019[2]

2 Craig Lawson, Toby Bussa, Sid Deshpande, Pete Shoard, Kelly Kavanagh, "Market Guide for Managed Detection and Response Services" (Guía de mercado de servicios de detección y respuesta gestionados), 15 de julio de 2019

EL EQUIPO DE FALCON COMPLETE: EXPERTOS EN ADMINISTRACIÓN, SUPERVISIÓN Y RESPUESTA PERMANENTES

Falcon Complete refuerza acreditadas tecnologías de protección de CrowdStrike con las personas, experiencia y procesos necesarios para proporcionar un enfoque práctico a la seguridad de endpoints.

Basada en la plataforma CrowdStrike Falcon, Falcon Complete es la solución de protección de endpoints más completa de CrowdStrike. Proporciona una seguridad incomparable, gracias a que refuerza el antivirus de nueva generación Falcon Prevent™, la detección y respuesta a incidentes de endpoints de Falcon Insight™ y la caza de amenazas gestionada de Falcon OverWatch™, junto con la experiencia y el compromiso permanente del equipo de Falcon Complete. El equipo administra y supervisa de manera activa la plataforma Falcon para los clientes, y corrige los incidentes de forma remota cuando es necesario. En definitiva, soluciona el problema de la implementación y ejecución de un programa de seguridad de endpoints eficaz y maduro sin la dificultad, responsabilidad y costes que acarrearía su gestión interna.

UN EQUIPO ALTAMENTE CUALIFICADO Y MOTIVADO

El equipo de Falcon Complete se encarga de administrar y supervisar la plataforma Falcon, así como de responder a las amenazas que detecta. Está compuesto por curtidos profesionales de la seguridad que tienen a sus espaldas una amplia experiencia en la gestión y respuesta a incidentes, la investigación forense, el análisis de centros de operaciones de seguridad y la administración de TI. El equipo tiene presencia internacional, con miembros repartidos por Estados Unidos, Reino Unido y Australia, lo que permite ofrecer una cobertura real ininterrumpida ("siguiendo al sol").

Tras años prestando servicios de respuesta a incidentes, estos expertos han perfeccionado sus habilidades hasta extremar su nivel de competencia y eficacia. Gracias a su dedicación permanente a la administración de la plataforma Falcon, han desarrollado la "memoria muscular" necesaria para clasificar y responder rápidamente a las amenazas. Este es un factor que los diferencia de otros profesionales de la seguridad que posiblemente desempeñen varias funciones y a los que se asigna una gran variedad de responsabilidades de TI y tecnologías de seguridad, lo que a menudo les impide dominar plenamente un área concreta.

De hecho, muchos de los miembros del equipo decidieron unirse a Falcon Complete porque les permite aplicar y mejorar sus conocimientos a diario, algo que no siempre ocurre cuando se trabaja para una única empresa. Los miembros del equipo de Falcon Complete pueden dedicarse enteramente al trabajo que más les gusta, como la gestión de incidentes, el análisis de malware o la corrección. Este entorno hace de CrowdStrike una empresa que atrae y retiene a los mejores talentos del planeta.

Todo el equipo cuenta con las certificaciones CCFA y CCFR, que garantizan que están extremadamente cualificados para el uso de la plataforma Falcon y que conocen perfectamente sus herramientas y su estructura de datos. Por lo tanto, el equipo sabe cómo realizar una rápida clasificación de una forma que muchos clientes son incapaces de conseguir porque no cuentan con la experiencia e intuición necesarias.

El equipo de Falcon Complete tiene, además, una estrecha relación con el resto de expertos en seguridad de CrowdStrike. La colaboración con el equipo de CrowdStrike Intelligence les permite acceder a una ingente cantidad

EL EQUIPO DE FALCON COMPLETE

Expertos en la plataforma CrowdStrike Falcon: con certificaciones CrowdStrike Certified Falcon Responder (CCFR) y CrowdStrike Certified Falcon Administrator (CCFA)

Expertos en respuesta a incidentes: muchos años de experiencia en investigación forense digital y respuesta a incidentes (DFIR)

Siempre vigilando — 24/7/365

de información sobre ciberamenazas. Este acceso a inteligencia en tiempo real se traduce en detecciones más rápidas, más precisas y oportunas, la capacidad de anticiparse a los atacantes, recomendaciones más detalladas y completas, y una extraordinaria gestión, resolución y corrección de incidentes.

ADMINISTRACIÓN, SUPERVISIÓN Y RESPUESTA A AMENAZAS

Las tres primeras áreas en las que trabaja el equipo de Falcon Complete (administración y supervisión de la plataforma Falcon, y respuesta a incidentes) se combinan para ofrecer una seguridad integral que empieza desde el primer día.

Incorporación: una verdadera asociación con su empresa

Convertirse en cliente de Falcon Complete es un proceso rápido y eficaz que la gran mayoría de las empresas tardaría tan solo unos días en completar. El proceso de incorporación se inicia con el trabajo conjunto entre su empresa y el equipo de Falcon Complete para seleccionar el estado de seguridad adecuado para su entorno y documentarlo en un "modelo operativo". Este modelo operativo determina la manera en la que hay que configurar Falcon y también cómo desea el cliente que el equipo responda a las amenazas. Define el flujo con el que el equipo clasificará las detecciones y cómo, en determinadas circunstancias, responderá a esas detecciones o escalará los problemas a su empresa para su aprobación. Esto garantiza la absoluta sintonía entre su empresa y el equipo de Falcon Complete, de manera que todos saben lo que esperar de los otros.

Para definir su estado de seguridad, rellenará una breve lista de comprobación que proporciona una visión general de su estrategia de seguridad deseada y de lo que es más importante para usted. El equipo de Falcon Complete traduce esa información en el adecuado estado de seguridad, incluida cuál es la configuración apropiada de la plataforma Falcon.

Para agilizar y facilitar el proceso, el equipo de Falcon Complete ofrece recomendaciones básicas. Estas recomendaciones pueden resumirse como distintos niveles del estado de seguridad: activo, moderado o prudente.

- **Activo** significa que las directivas de prevención de la plataforma Falcon están definidas para ser bastantes restrictivas, en base a las recomendaciones y contramedidas predefinidas de CrowdStrike que el cliente ha autorizado a adoptar al equipo de Falcon Complete cuando se detectan amenazas en su entorno. Un estado activo significa que se ha activado la prevención proactiva y, en caso de detección, el equipo es capaz de responder de manera inmediata y remota.
- Un estado **moderado** significa que no están activadas algunas de las directivas de prevención, pero que el equipo puede tomar algunas medidas predefinidas, con la excepción de aquellas que pueden afectar a las actividades de TI, como el aislamiento (de la red) de un dispositivo.
- Con un estado **prudente**, el equipo solo supervisa las detecciones. Únicamente están activadas las prevenciones de máxima confianza, y el equipo no lleva a cabo ninguna medida correctiva en respuesta a un incidente. Esta es una opción para zonas de la red en las que el cliente no quiere que intervenga el equipo de Falcon Complete.

Estas sencillas opciones permiten al equipo crear una estrategia de seguridad para endpoints personalizada para un cliente y aplicar distintos niveles de estado a sectores diferentes del entorno. Por ejemplo, una empresa podría necesitar un estado agresivo para proteger sus estaciones de trabajo, ya que de ahí proceden la mayoría de las alertas y es donde se inician la mayoría de las intrusiones. Sin embargo, el cliente podría desear una postura más prudente para determinados sistemas, debido a necesidades de gestión de cambios internas u otras consideraciones. Para implementar ese modelo personalizado, el equipo de Falcon Complete, en colaboración con el cliente, puede dividir el entorno en grupos lógicos.

Convertirse en cliente de Falcon Complete es un proceso rápido y eficaz que la gran mayoría de las empresas tardaría tan solo unos días en completar.

Todas estas aportaciones se recopilan durante el proceso de incorporación, y al finalizar el proceso, el equipo prepara un modelo operativo con un estado de seguridad definido que se adapta perfectamente a su empresa. A partir de ahí, el equipo adopta las medidas necesarias para implementar el modelo, como la configuración de directivas o la activación de las contramedidas que aplicará el equipo cuando se enfrente a situaciones diferentes. En la mayoría de los casos, el proceso de incorporación puede completarse en cuestión de días.

Administración permanente

El proceso descrito anteriormente no es algo totalmente fijo. Con el tiempo, su empresa evoluciona, sus necesidades pueden cambiar, o bien puede hacerlo el propio producto. El equipo se reúne con usted periódicamente, lo que garantiza que el modelo operativo y su implementación están siempre actualizados a lo largo del tiempo. El equipo también le ayuda a estar atento a los cambios en su entorno. Por ejemplo, si se despliega el agente de Falcon en nuevos endpoints, el equipo de Falcon Complete comprobará que existen los grupos lógicos adecuados para administrar esos endpoints, y que los endpoints se añaden a los grupos correspondientes. Esto garantiza que los nuevos agentes que entren en funcionamiento se incorporan a los grupos adecuados y reciben las directivas de prevención convenientes.

El equipo también busca dispositivos no gestionados y riesgos relacionados, utilizando para ello la tecnología Falcon Discover™ incluida en Falcon Complete. Asimismo, se supervisan los cambios en el número de endpoints desplegados, como un número considerable de nuevas instalaciones. La verificación periódica del estado de actualización de los agentes y de que tienen las directivas de prevención adecuadas garantiza una población de agentes sana y un nivel de protección óptimo en todo momento.

> **Verificar periódicamente que todos los agentes están actualizados y tienen las directivas de prevención adecuadas garantiza una población de agentes sana y un nivel de protección óptimo en todo momento.**

Administración de la plataforma Falcon antes y después de Falcon Complete

Antes de Falcon Complete	Con administración de los expertos de Falcon Complete
• Problemas de visibilidad y control de los sistemas no gestionados • Sistemas desprotegidos y expuestos pasan desapercibidos en los márgenes	• Control completo de los sistemas no gestionados • Falcon Complete ayuda a los clientes a asegurarse de que todos los recursos estén adecuadamente agrupados, clasificados y protegidos
• Retrasos en la actualización del agente de Falcon • Máquinas con agentes de Falcon obsoletos que pueden carecer de las últimas técnicas de protección	• Control estricto del agente de Falcon • Falcon Complete garantiza que el agente de Falcon actual está instalado, ofreciendo el mejor nivel de protección disponible
• Un gran número de directivas, aplicadas de manera incoherente • Con el tiempo, se desarrolla una amalgama de directivas que genera confusión, complica las investigaciones de amenazas y puede generar lagunas de protección	• Administración rigurosa de la configuración • Se aplican sistemáticamente directivas de mejores prácticas de eficacia demostrada a todos los sistemas
RESULTADO: protección optimizada para todos sus sistemas, en todo momento	

Supervisión de la plataforma Falcon

El equipo de Falcon Complete supervisa la plataforma Falcon 24 horas del día, siete días a la semana, para localizar nuevas alertas de seguridad. Además investiga cada detección, con independencia de su gravedad. La clasificación comienza por conocer la fuente original de la detección. Por ejemplo, si el motor de aprendizaje automático de Falcon determina que un archivo es malicioso, el equipo investigará cuándo se introdujo el archivo por primera vez en el endpoint y qué proceso lo escribió en el sistema. A partir de ahí realizará un rastreo retrospectivo del árbol de procesos para averiguar cómo se originó esa cadena de eventos, qué cuenta de usuario estaba asociada a esos procesos y cómo se conectó el usuario. A continuación, investiga si el archivo malicioso se ha observado en otro sistema, para poder determinar si el ataque alcanzó a varios endpoints o solo a uno. El equipo responde a esas preguntas en los primeros minutos de una detección.

Esto le ofrece una enorme ventaja respecto a la mayoría de profesionales de la respuesta a incidentes, gracias a su acceso directo a los equipos de CrowdStrike. Por ejemplo, el equipo de Falcon Complete trabaja estrechamente con Falcon OverWatch, el equipo que se encarga de la caza proactiva de amenazas. También aprovecha sus relaciones internas con CrowdStrike Services, CrowdStrike Intelligence y con el equipo de soporte de CrowdStrike. De esta forma puede someter cada detección a un proceso de clasificación, contención, erradicación y recuperación que es increíblemente rápido, exhaustivo y eficaz.

Este proceso eficaz y completo permite al equipo tramitar cada detección y en el proceso determinar con certeza si la detección es un falso positivo, si es un caso aislado en un único endpoint, o si se trata de un incidente generalizado. Esta información determina la forma de responder del equipo.

> **“El equipo de Falcon Complete supervisa la plataforma Falcon 24 horas del día, siete días a la semana, para localizar nuevas alertas de seguridad. Además, investiga cada detección, con independencia de su gravedad.**

Supervisión antes y después de Falcon Complete

Antes de Falcon Complete	Con supervisión de los expertos de Falcon Complete
• 8 horas diarias de supervisión activa • Los ciberdelincuentes no respetan el horario de trabajo ni las vacaciones, y puede ocurrir que las amenazas que surjan fuera del horario laboral pasen desapercibidas hasta el siguiente día laborable	• 24 horas diarias de supervisión activa • Falcon Complete siempre está vigilando, lo que garantiza que las amenazas emergentes se gestionan en tiempo real, a medida que ocurren
• La mayoría de las detecciones pasan desapercibidas • Las detecciones de menor gravedad, como el malware bloqueado, se suelen ignorar aunque representan una prueba clara de una posible actividad futura del agresor	• Investigación humana de todas las detecciones • Falcon Complete investiga las detecciones de gravedad crítica, alta, media y baja sin demora, lo que garantiza la identificación de las intrusiones en la fase más temprana posible
• 6 horas: tiempo medio para comenzar la respuesta[3] • La respuesta se retrasa porque los equipos suelen carecer del conocimiento, la inteligencia sobre amenazas y la experiencia necesarias	• 10 minutos: tiempo medio para comenzar la respuesta[4] • Falcon Complete crea y ajusta continuamente un manual reproducible para garantizar que se investigan todas las amenazas de manera rápida y eficaz
RESULTADO: supervisión de amenazas, 24/7/365, para responder a los ataques en minutos, a medida que ocurren	

3 Vanson Bourne, "The 2019 Global Security Attitude Survey" (Encuesta sobre actitudes respecto a la seguridad a nivel mundial), noviembre de 2019

4 Tiempo medio que necesita Falcon Complete para investigar y responder a incidentes de seguridad, medido durante la primera mitad de 2020. Los tiempos de investigación y respuesta individuales pueden variar.

Respuesta a alertas

La tercera responsabilidad del equipo de Falcon Complete es la respuesta a las alertas. Cuando se produce una detección de gravedad crítica, alta o media, el equipo inicia el proceso para corroborar que se trata de una amenaza legítima.

Si determina que la alerta es un falso positivo, sigue el manual desarrollado junto al cliente y responde en función de las necesidades. Eso puede incluir acciones de contención, como el bloqueo de un hash o de una red que contiene un dispositivo afectado. El agente de Falcon permite que esas acciones se lleven a cabo inmediatamente.

A continuación, y si es necesario, el equipo pasa a la fase de corrección. Esto puede incluir el acceso remoto a un endpoint para impedir el avance de un ataque, la limpieza de un endpoint comprometido o la eliminación de artefactos de malware. Las ventajas para el cliente son enormes, ya que el equipo de Falcon Complete no se conforma con alertar de la existencia de un problema, sino que lo resuelve completamente para que el cliente no tenga que hacerlo. Todo ello sin necesidad de recurrir a complicadas y costosas estrategias, como la recreación de imágenes de los sistemas.

En caso de que se determine que la alerta es un falso positivo, el equipo reacciona para que no se desencadenen acciones innecesarias. A continuación selecciona la mejor estrategia para cada cliente y situación. Por ejemplo, el equipo de Falcon Complete determinará si la mejor solución es la inclusión en una lista blanca, la creación de exclusiones o trabajar con los equipos de respuesta a incidentes y soporte de CrowdStrike para crear nuevos patrones y eliminar falsos positivos en el futuro.

> **El equipo de Falcon Complete resuelve plenamente el problema para que el cliente no tenga que hacerlo, sin complicadas y costosas estrategias, como la recreación de imágenes de los sistemas.**

Respuesta antes y después de Falcon Complete

Antes de Falcon Complete	Con la respuesta quirúrgica de Falcon Complete
• 6-8 horas: tiempo que necesita el departamento de TI para recrear la imagen del sistema • El restablecimiento de la imagen inicial es la técnica de corrección más común; es fiable pero laboriosa	• 45 minutos: tiempo para realizar una corrección quirúrgica[4] • Falcon Complete ejecuta una corrección quirúrgica de forma remota, a menudo sin necesidad de recrear la imagen
• 6-8 horas: tiempo de inactividad de los usuarios finales durante la recreación de la imagen del sistema • La recreación de la imagen no solo es cara, sino que tiene un fuerte impacto en la productividad de los usuarios y puede eliminar importantes pruebas forenses	• 0 minutos: normalmente, la corrección quirúrgica no genera tiempo de inactividad en los usuarios finales • Falcon Complete puede llevar a cabo la corrección sin que el usuario llegue a saber que está ocurriendo
• Incertidumbre • Una vez finalizada la respuesta inicial, los responsables de la respuesta pueden apresurarse para abordar el siguiente caso, dejando quizás las puertas abiertas para que la amenaza reaparezca en el futuro	• Confianza • Falcon Complete lleva a cabo análisis completos sobre cada intrusión, lo que permite la corrección plena y completa, con el respaldo de la garantía de prevención de violaciones de seguridad de CrowdStrike
RESULTADO: la corrección quirúrgica erradica las amenazas con rapidez y precisión	

Cómo trabaja Falcon Complete con un MSSP

Muchas empresas se preguntan, "¿Necesito Falcon Complete si tengo un proveedor de servicios de seguridad gestionados (MSSP)?" Las ofertas de los MSSP pueden variar enormemente pero, en general, se centran en la supervisión y administración generalizadas de las herramientas de seguridad dentro de una empresa. Esto incluye por lo general una clasificación básica de las alertas de seguridad, junto con otros servicios, como administración y actualizaciones de tecnología, cumplimiento de normativas y administración de vulnerabilidades.

El enfoque de Falcon Complete es completamente distinto, ya que ofrece integración rápida e integral, con una experiencia incomparable en la plataforma CrowdStrike Falcon. Los servicios de Falcon Complete están especialmente centrados en la labor de administrar, supervisar y responder a las amenazas con la máxima efectividad y en el menor tiempo posible. Gracias a este enfoque, Falcon Complete puede ofrecer valor inmediato, a un bajo coste en un plazo muy breve, y respaldar el trabajo con la garantía de prevención de violaciones de seguridad más completa del sector.

> **Los servicios de Falcon Complete están especialmente centrados en la labor de administrar, supervisar y responder a las amenazas con la máxima efectividad y en el menor tiempo posible.**

Comparación de Falcon Complete con los MSSP

Fase	Actividad	Falcon Complete	MSSP
Administración	Dotada de expertos en la plataforma Falcon e investigación forense digital y respuesta a incidentes	x	
	Ayuda a identificar y eliminar los sistemas no gestionados	x	
	Mantiene la versión actual de los sensores de Falcon en los endpoints protegidos	x	
	Configura y optimiza permanentemente las directivas de Falcon	x	
	Asegura que todos los sistemas están debidamente agrupados y adecuadamente protegidos por la plataforma Falcon	x	
	Incluye comprobaciones proactivas y generación de informes	x	x
Supervisión	Ofrece supervisión 24/7/365 de la plataforma Falcon	x	x
	Investiga las detecciones de gravedad crítica y alta	x	x
	Investiga las detecciones de gravedad media y baja	x	?
	Incluye caza proactiva de amenazas por parte de personas	x	?
	Disfruta de acceso profundo a inteligencia sobre CrowdStrike y a especialistas de OverWatch	x	
Respuesta	Determina la estrategia de respuesta	x	x
	Ofrece consejos sobre la respuesta	x	x
	Aísla de forma proactiva los sistemas comprometidos	x	
	Realiza correcciones quirúrgicas	x	
	Proporciona un resumen posintrusión con recomendaciones para reforzar la protección	x	
	Proporciona acuerdos de nivel de servicio (SLA) de investigación y respuesta	x	x
	Incluye garantía de prevención de violaciones de seguridad	x	

AYUDA PRÁCTICA INMEDIATA PARA LOS CLIENTES

INMEDIATAMENTE OPERATIVO

La primera ventaja, y también la más obvia, de utilizar CrowdStrike para administrar todos los aspectos de la seguridad de endpoints es su inmediata efectividad. Las empresas que intentan crear un SOC eficiente que sea capaz de responder a amenazas y corregirlas de manera eficaz descubren que se trata de un proceso largo, complejo y caro. Desde buscar y contratar el talento adecuado y adquirir la tecnología apropiada, a definir directivas y crear un proceso de respuesta a incidentes, la tarea completa puede llevar meses, o incluso años.

Un factor que influye en este retraso es que dichos programas a menudo quedan relegados frente a otros proyectos de TI urgentes, dando lugar a unos tiempos de implementación largos que dejan vulnerables a las empresas. El coste también puede ser un problema. La creación de un modelo que cuente con personal permanente requiere al menos cuatro empleados a tiempo completo, lo que puede poner fuera del alcance de muchas empresas la obtención del nivel necesario de madurez en seguridad. La tarea es igualmente complicada para las empresas que sí disponen del presupuesto necesario, ya que no resulta fácil encontrar y retener la experiencia necesaria. La contratación, formación y retención de personal cualificado suficiente para enfrentarse a adversarios tan avanzados y sofisticados puede ser una tarea abrumadora para las empresas. Esto plantea un problema importante para un sector que, en general, sufre escasez de expertos en seguridad cualificados.

Sin embargo, el equipo de Falcon Complete ofrece rentabilidad inmediata, aporta al momento expertos en seguridad que trabajan junto con el personal del cliente, y asume la administración de la plataforma Falcon. Además, ofrece recomendaciones y un modelo operativo a cada cliente, que incluye un manual personalizado y un equipo completamente operativo de manera permanente, capaz de iniciar la supervisión tan pronto como se produzca la incorporación del cliente.

RESULTADOS GARANTIZADOS, SIN MÁS ESFUERZO

Otra ventaja importante que ofrece el equipo de Falcon Complete es la corrección de forma remota. En situaciones en las que hay endpoints comprometidos, el equipo de Falcon Complete aporta una ayuda adicional, no solo más alertas, actuando para corregir los sistemas para que no tengan que hacerlo los clientes. Las aptitudes exclusivas del equipo le permiten responder a los incidentes de manera eficaz, rápida y fiable. Esta experiencia es tan difícil de alcanzar que la mayoría de las empresas recurren a recrear completamente una imagen del sistema como procedimiento de corrección cuando se considera que está infectado o comprometido.

Este método puede ser una solución eficaz, pero es también muy costosa. Además, a menudo se convierte en un problema tanto para los departamentos de TI como para los usuarios finales, cuya productividad se ve afectada al tener que entregar sus portátiles a soporte técnico. A su vez, el equipo de soporte técnico se ve obligado a dedicar una importante cantidad de tiempo a la tarea de recreación de la imagen para garantizar la fiabilidad de las estaciones de trabajo de los usuarios finales.

Lo que realmente diferencia al equipo de Falcon Complete es su capacidad de analizar y conocer plena y rápidamente el alcance y los detalles de un incidente, lo que le permite aplicar las medidas correctivas con confianza sin recurrir por defecto a la recreación de imágenes.

El equipo llevará a cabo el análisis necesario para conocer en profundidad el incidente. Por ejemplo, ¿se trata de una infección de malware comercial o de un ciberdelincuente que ha dejado una puerta trasera en el entorno? El equipo pondrá en práctica entonces las mismas capacidades que emplearía en una investigación a fondo, pero las aplica de una forma rápida y táctica en un único sistema para saber el avance del ataque, los métodos de persistencia empleados y la naturaleza de la puerta trasera o malware utilizado por el agresor para acceder al sistema. Una vez que el equipo obtiene un conocimiento exhaustivo del ataque, puede eliminar con total confianza y de forma remota las puertas traseras, limpiar el malware, desactivar los métodos de persistencia y detener los procesos maliciosos que se ejecutan en memoria. El equipo puede hacer esto de una forma más integral que si utilizara solamente soluciones antivirus o procesos automatizados.

Los clientes se quitan un enorme peso de encima ya que recurrían a la recreación de imágenes de endpoints que no precisaban medidas tan extremas. Con el equipo de Falcon Complete a su lado, gracias al análisis adecuado y adoptando las medidas precisas, en la mayoría de los casos será absolutamente innecesario recurrir a la recreación de la imagen de los sistemas. Esto supone una manera mucho menos perturbadora de corregir incidentes: abordando el verdadero problema y corrigiendo el problema real en un enfoque asequible y mucho más eficaz que la recreación de imágenes.

CONCLUSIÓN

Falcon Complete proporciona a su empresa un programa de seguridad de endpoints maduro y eficaz, a una velocidad, coste y nivel de efectividad que muy pocas empresas pueden conseguir por sí solas, o incluso con la ayuda de otras terceras partes.

Trasladar la responsabilidad de la administración de la seguridad de endpoints a CrowdStrike ahorra a las empresas innumerables meses de esfuerzo dedicado a crear un programa de seguridad de endpoints, implementarlo, administrarlo, gestionar las alertas y responder a los incidentes.

Mediante la incorporación de un equipo específicamente dedicado y altamente cualificado para el uso y la administración de la plataforma CrowdStrike Falcon, empresas de todos los tamaños pueden alcanzar inmediatamente los mayores niveles de madurez en su estrategia de seguridad para endpoints, llevar a un nivel superior el programa de ciberseguridad general y mejorar inmediatamente su estado de seguridad.

La ventaja más obvia que ofrece el equipo de Falcon Complete es la tranquilidad.

Los clientes se sienten tranquilos al saber que el mejor equipo de expertos en seguridad en sus respectivos campos se encarga de vigilar los endpoints de la empresa las 24 horas al día, incluidos los fines de semana, durante la noche, cuando se encuentran en una reunión u ocupados de cualquier otra forma. Los clientes de Falcon Complete pueden estar seguros de que el equipo de Falcon Complete tomará las medidas necesarias para corregir los incidentes, para que no tengan que hacerlo ellos.

ACERCA DE CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), líder mundial en ciberseguridad, redefine la seguridad en la era de la nube mediante una plataforma de protección de endpoints que ha sido construida desde la base con el objetivo de detener las violaciones de la seguridad. La arquitectura de un solo agente ligero de CrowdStrike Falcon® aprovecha la inteligencia artificial a escala de la nube y ofrece protección en tiempo real y visibilidad en toda la empresa, evitando los ataques a los endpoints, estén o no conectados a la red. Gracias a CrowdStrike Threat Graph®, CrowdStrike Falcon correlaciona a la semana, en tiempo real , más de 3 billones de eventos relativos a los endpoints en todo el planeta, alimentando una de las plataformas de datos para seguridad más avanzadas del mundo.

Con CrowdStrike, los clientes disfrutan de la mejor protección, el mejor rendimiento y la rentabilidad inmediata que aporta la plataforma Falcon nativa de la nube.

Cuando hablamos de CrowdStrike, solo hay que recordar una cosa:
impedimos las violaciones de la seguridad.

Más información sobre Falcon Complete