CROWDSTRIKE

SERVICIOS DE RESPUESTA A INCIDENTES DE CROWDSTRIKE

Prepárese, reaccione y solucione los incidentes con rapidez y eficacia

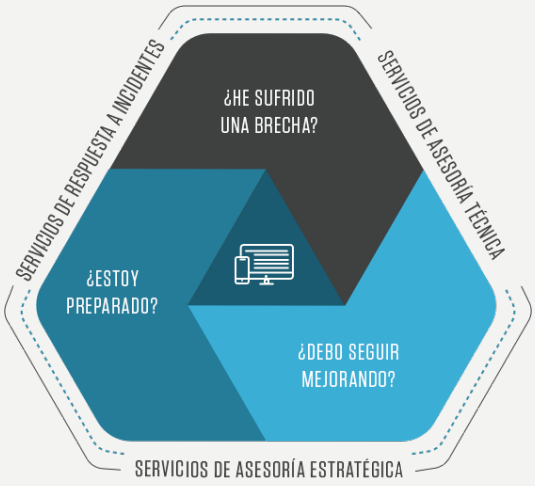
SERVICIOS DE RESPUESTA A INCIDENTES DE CROWDSTRIKE

SERVICIOS ADECUADOS PARA CADA CLIENTE

Los servicios de CrowdStrike® incluyen respuesta a incidentes y ofertas que desempeñan un papel crucial para que su empresa sea mas eficiente en la gestión de los incidentes de ciberseguridad. Estos servicios están diseñados para permitir que las empresas aprendan, se preparen y reaccionen de forma rápida ante los incidentes.

Para ello, los servicios de CrowdStrike reúnen un equipo formado por profesionales de la seguridad del ámbito de la inteligencia, las fuerzas de seguridad y la industria; arquitectos e ingenieros de las mejores empresas tecnológicas del mundo; y consultores de seguridad que lideran las investigaciones sobre intrusiones más exigentes del mundo.

Este equipo utiliza la plataforma CrowdStrike Falcon®, que proporciona una protección sin precedentes y facilita en tiempo real la respuesta a incidentes, un análisis forense detallado e inteligencia sobre amenazas para garantizar que ninguna amenaza quede sin detectar. Los servicios de CrowdStrike ofrecen a las empresas una excelente ayuda para prepararse, responder y prevenir los daños que provocan una amplia variedad de incidentes de seguridad y ciberataques avanzados, y lo que es más importante les permite defenderse frente a ataques futuros.



Los servicios de respuesta a incidentes (IR) y de CrowdStrike se puede utilizar por separado o bien combinados, y pueden estar cubiertos por un contrato de servicios. Este contrato es flexible: si considera que no tiene necesidad de los servicios IR de CrowdStrike, puede utilizar las horas del contrato disponibles para los servicios proactivos, que se centran en ayudarle a mejorar su estado de seguridad general.

SERVICIOS DE INCIDENTE RESPUESTA DE CROWDSTRIKE

Los servicios de CrowdStrike ayudan a las empresas a reforzar y madurar su estado de seguridad dando respuesta a tres preguntas fundamentales:

¿HE SUFRIDO UNA BRECHA?

- Servicios de respuesta a incidentes
- Servicios de recuperación de endpoints
- Evaluación de compromisos
- Supervisión de la seguridad de la red

¿DEBO SEGUIR MEJORANDO?

- Evaluación del nivel de madurez en ciberseguridad
- Evaluación de la seguridad de Active Directory
- Evaluación de seguridad de la nube
- Evaluación del centro de operaciones de seguridad (SOC)
- Evaluación de higiene de las tecnologías de información (TI)
- Programa de mejora de la ciberseguridad
- Programa de seguridad en profundidad
- Desarrollo del programa de inteligencia de amenazas

¿ESTOY PREPARADO?

- Ejercicio de simulación teórica
- Ejercicio de práctica real
- Ejercicio de emulación del adversario
- Ejercicio equipo rojo/equipo azul
- Servicios de pruebas de penetración

SERVICIOS GESTIONADOS, SOPORTE Y FORMACIÓN

- Falcon Complete™
- Soporte operativo para Falcon
- Formación sobre Falcon (CrowdStrike University)

SERVICIOS DE RESPUESTA A INCIDENTES DE CROWDSTRIKE

¿HE SUFRIDO UN INCIDENTE?

SERVICIOS DE RESPUESTA A INCIDENTES

- Acelere el proceso de corrección cuando se produce una brecha gracias a una visión integral del atacante que permite reanudar la actividad empresarial de forma inmediata. Los servicios de respuesta a incidentes (IR) de CrowdStrike gestionan en colaboración con su empresa los incidentes de seguridad críticos y llevan a cabo análisis forenses para resolver los ciberataques inmediatamente e implementar una solución duradera que evite que se repitan.
- El equipo de respuesta a incidentes de CrowdStrike adopta para la respuesta un enfoque basado en la inteligencia, que combina respuesta a incidentes reales, investigaciones forenses y experiencia en corrección con tecnología de vanguardia, empleando la exclusiva plataforma Falcon en la nube, lo que permite identificar a los atacantes más rápidamente y con más precisión, y expulsarlos de su entorno. El objetivo del equipo de CrowdStrike es conseguir que las empresas puedan reanudar su actividad más rápidamente y reducir el impacto de los ciberincidentes.

SERVICIOS DE RECUPERACIÓN DE ENDPOINTS

- Los servicios de recuperación de endpoints de CrowdStrike le ayudan a recuperarse rápidamente de los ataques y las amenazas persistentes avanzadas, sin interrumpir la actividad empresarial en absoluto.
- Estos servicios combinan la plataforma tecnológica y la inteligencia de amenazas líderes de CrowdStrike con un equipo de expertos en seguridad con dilatada experiencia que le ayudarán con la detección, el análisis y la corrección de los incidentes de seguridad conocidos y le facilitarán una rápida recuperación.

COMPROMISE ASSESSMENT

- El equipo Compromise Assessment de CrowdStrike identifica la actividad en curso y pasada del atacante en su entorno para poder contestar a una pregunta fundamental: "¿ha sufrido mi empresa una brecha?"
- El equipo Compromise Assessment cuenta con años de experiencia en respuesta a intrusiones de los atacantes más sofisticados, y emplea la potente plataforma Falcon combinada con inteligencia sobre ciberamenazas líder del sector y un servicio de threat hunting 24/7 para ofrecerle la evaluación mas completa de un compromiso en su entorno.

SUPERVISIÓN DE LA SEGURIDAD DE LA RED

- Este servicio ofrece una amplia supervisión de seguridad de la red para detectar las amenazas activas presentes en su entorno.
- Proporciona una amplia función de supervisión de la seguridad de la red para la detección, respuesta y threat hunting. El servicio se vale de la experiencia de los threat hunters de los servicios de CrowdStrike y de un dispositivo de red que detecta las amenazas presentes en su entorno.

¿POR QUÉ ELEGIR CROWDSTRIKE?

Equipo humano con experiencia demostrada: profesionales expertos en respuesta a incidentes, investigación de malware y ciberinteligencia que proporcionan servicios rápidos proactivos y de respuesta, análisis forense y recuperación de endpoints.

Inteligencia sobre el adversario: contará con investigaciones e informes actualizados de los atacantes y las tácticas, técnicas y procedimientos empleados contra su entorno.

Threat hunting sin igual: el servicio proactivo de threat hunting 24/7 amplía la búsqueda de actividad de ciberdelincuentes a todo el entorno.

Excelente tecnología: la exclusiva plataforma CrowdStrike Falcon proporciona protección de endpoints de nueva generación para detectar a los adversarios, expulsarlos rápidamente y evitar que vuelvan a entrar.

SERVICIOS DE RESPUESTA A INCIDENTES DE CROWDSTRIKE

¿DEBO SEGUIR MEJORANDO?

EVALUACIÓN DE LA MADUREZ EN CIBERSEGURIDAD

- Los servicios de CrowdStrike afirman que cumplir las normas no es sinónimo de estar protegido. En lugar de centrarse únicamente en el cumplimiento, el equipo de servicios se centra en la evaluación del nivel de madurez de la empresa, con la aportación de años de experiencia en la respuesta a amenazas.
- La metodología empleada no se limita a una auditoría estándar, sino que evalúa la madurez en ciberseguridad de la empresa en relación a su capacidad para prevenir, detectar y responder a los adversarios más sofisticados.

EVALUACIÓN DE SEGURIDAD DE ACTIVE DIRECTORY

- Reciba una revisión integral de su configuración de Active Directory (AD) y la configuración de directivas para evitar problemas en la infraestructura de AD.
- La evaluación de la seguridad de Active Directory es un servicio exclusivo de CrowdStrike diseñado para revisar la configuración de AD y de las directivas con el fin de identificar problemas que puedan aprovechar los atacantes.
- La evaluación incluye la revisión de la documentación, charlas con su personal, ejecución de herramientas propias y una comprobación manual de su configuración y ajustes de AD. El resultado es un informe detallado de los problemas descubiertos y de su impacto, así como medidas recomendadas para su mitigación y corrección.

EVALUACIÓN DE SEGURIDAD DE LA NUBE

- La evaluación de seguridad de la nube de CrowdStrike ofrece información práctica de los problemas de configuración de la seguridad y señala las diferencias respecto a la arquitectura de seguridad de la nube recomendada.
- Esta evaluación, que suma la experiencia de CrowdStrike en respuesta a incidentes a la de consultores de empresas líderes reconocidas en arquitectura de seguridad de la nube, le indica las acciones priorizadas que necesita para ampliar al máximo su capacidad de respuesta, detección y recuperación ante incidentes de seguridad de la nube.

EVALUACIÓN DE HIGIENE DE LAS TECNOLOGÍAS DE LA INFORMACIÓN (TI)

- Anticípese y descubra las vulnerabilidades para proteger su red antes de que ocurra una brecha.
- La evaluación de higiene de las tecnologías de información de CrowdStrike ofrece una mejor visibilidad de las aplicaciones, accesibilidad y gestión de cuentas dentro de la red, lo que le proporciona contexto global del tráfico de la red y las deficiencias de seguridad. Identificar las vulnerabilidades y los parches que no se han aplicado le permite proteger proactivamente su red antes de que se produzca un incidente.

PROGRAMA DE MEJORA DE LA CIBERSEGURIDAD

- Desarrolle e implemente un programa de mejora de la ciberseguridad tras una brecha para cerrar lagunas de seguridad y prevenir futuros ataques.
- El programa de mejora de la ciberseguridad de CrowdStrike está destinado a empresas que han sufrido una brecha recientemente y necesitan asistencia para desarrollar un plan de mejora de la ciberseguridad estratégico con el fin de evitar que se repita la situación.

OTRAS OFERTAS

Evaluación del centro de operaciones de seguridad (SOC):
mejore el nivel de madurez de su SOC e identifique y priorice las áreas de mejora.

Programa de seguridad en profundidad:
estudie en profundidad sus procesos, herramientas y recursos de ciberseguridad para determinar el nivel de madurez de su programa de seguridad de la información.

Desarrollo del programa de inteligencia de amenazas:
establezca un programa para gestionar la inteligencia de amenazas según vaya evolucionando el panorama de amenazas, los ciberdelincuentes a nivel global y las últimas tácticas, técnicas y procedimientos empleados.

SERVICIOS DE RESPUESTA A INCIDENTES DE CROWDSTRIKE

¿ESTOY PREPARADO?

EJERCICIO DE SIMULACIÓN TEÓRICA

- La experiencia del equipo de servicios de CrowdStrike en investigaciones de respuesta a incidentes para ciberamenazas sofisticadas le permite ofrecer una perspectiva realista en los ejercicios de simulación teórica.
- Los ejercicios han sido diseñados para simular un ataque selectivo y guiar a su empresa —ya sean los participantes ejecutivos o técnicos— por una simulación de incidentes convincente. Este ejercicio ofrece la experiencia de un ataque sin sufrir la interrupción de la actividad y los daños que supondría.

EJERCICIO DE PRÁCTICA REAL

- Este ejercicio ha sido diseñado para poner a prueba a las personas de la organización con el fin de asegurar que conocen su papel en caso de necesidad de respuesta a incidentes.
- En lugar de hablar de un ataque hipotético en grupo, el equipo de Servicios emplea sus herramientas y procesos para añadir realismo, proporcionando información específica a cada persona, como ocurriría durante la investigación de una brecha real. A continuación, el equipo le deja decidir cómo gestionar mejor la información. Al finalizar el ejercicio, tendrá una visión clara de las deficiencias de su proceso.

EJERCICIO DE EMULACIÓN DEL ADVERSARIO

- Esta prueba ofrece las ventajas de experimentar un ataque selectivo sofisticado, sin sufrir los daños que acarrea un incidente real.
- Para ello, un consultor de CrowdStrike experimentado imita las técnicas de un atacante actual e intenta conseguir acceso a la red de su empresa y poner en riesgo recursos concretos. Tras conseguir este objetivo, el equipo explica cómo se ha logrado y le ayuda a identificar las tácticas que puede emplear para evitar ataques similares en el futuro.

EJERCICIO EQUIPO ROJO/EQUIPO AZUL

- Prepare a su equipo de ciberseguridad y aprenda de expertos; un equipo atacará (rojo) y uno defenderá (azul) en su entorno.
- El objetivo del ejercicio equipo rojo/equipo azul de CrowdStrike es madurar el nivel de conocimientos de su equipo de seguridad en materia de threat hunting y procesos de respuesta a incidentes. Para ello, emplea un escenario de ataque selectivo comparable al del mundo real.

SERVICIOS DE PRUEBAS DE PENETRACIÓN

- El equipo de servicios utiliza técnicas de hackeo ético para localizar lagunas de seguridad mediante ataques de simulación y pruebas de penetración autorizados en distintos componentes de sus sistemas, redes y aplicaciones.
- Elija entre distintas opciones de pruebas según sus objetivos de seguridad particulares.

SERVICIOS GESTIONADOS, SOPORTE Y FORMACIÓN

- **FALCON COMPLETE™:** esta solución global de protección de endpoints y threat hunting se ofrece como servicio integral, totalmente gestionado, aprovechando el poder de la plataforma Falcon.
- **SOPORTE OPERATIVO PARA FALCON:** el soporte operativo ayuda a configurar y gestionar la plataforma Falcon para optimizar las operaciones de ciberseguridad.
- **FORMACIÓN SOBRE FALCON:** los servicios de formación y educación profesionales de CrowdStrike University (CSU) mejoran el conocimiento sobre ciberseguridad de su equipo y le ayudan a sacar el máximo rendimiento de la plataforma Falcon.

ACERCA DE LOS SERVICIOS DE CROWDSTRIKE

Los servicios de CrowdStrike dotan a las empresas de la protección y la experiencia que necesitan para defenderse y responder a los incidentes de seguridad. Gracias a la plataforma en la nube CrowdStrike Falcon® —con protección de endpoints de nueva generación, inteligencia sobre ciberamenazas e informes—, el equipo de servicios de CrowdStrike ayuda a los clientes a identificar, seguir el rastro y bloquear a los atacantes en tiempo real. Este exclusivo enfoque permite a CrowdStrike bloquear el acceso no autorizado más rápidamente y prevenir brechas futuras. CrowdStrike ofrece también servicios proactivos para que las organizaciones puedan mejorar su capacidad para anticiparse a las amenazas, preparar sus redes y detener los ataques.

Encontrará más información en **www.crowdstrike.com/services/**

Correo electrónico: **services@crowdstrike.com**