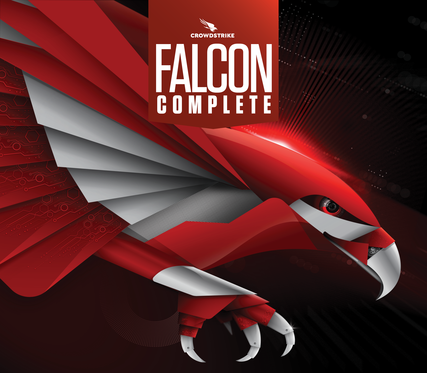

FALCON COMPLETE EN ACCIÓN

Una protección eficaz frente a las amenazas actuales requiere la vigilancia permanente de analistas cualificados.

CrowdStrike® Falcon Complete™ es un servicio gestionado de detección y respuesta a incidentes que ofrece investigación y respuesta quirúrgica 24/7/365.

Vea cómo Falcon Complete marca la diferencia para su empresa.

RESPUESTA A INCIDENTES DE MÍNIMOS	ACTIVIDAD DEL ADVERSARIO Tiempo transcurrido (H:MIN)	RESPUESTA A INCIDENTES DE LOS EXPERTOS DE FALCON COMPLETE
	0:00 El adversario obtiene las credenciales a través de **phishing**	
Malware bloqueado por la solución de protección de endpoints local Se genera una alerta de baja gravedad, pero se ignora al considerarse como no crítica	**0:02** El phishing conecta con el dominio malicioso e intenta desplegar el **malware** de segunda fase	**Malware bloqueado** por Falcon Prevent™ Se genera una alerta de baja gravedad
	0:30	El equipo de Falcon Complete **investiga la alerta** de baja gravedad El equipo de Falcon Complete lleva a cabo la clasificación del malware bloqueado y lo identifica con un grupo de autores de amenazas conocido por lanzar ataques de ransomware contra empresas del sector financiero El analista verifica que las directivas están adecuadamente configuradas para descubrir la actividad de adversarios que pueda producirse
	6:00 El **adversario inicia sesión** en el sistema **a través de RDP** con credenciales de usuario válidas	
	6:10 Advierte que el intento de acceso inicial no ha funcionado, sospecha que el endpoint tiene protección local, pone en práctica **tácticas sigilosas** y usa funciones nativas del sistema operativo para llevar a cabo un reconocimiento local	
El adversario identifica un nuevo **servidor de desarrollo que no está protegido** por el endpoint local	**7:30**	Sus intenciones se ven frustradas al **no encontrar sistemas desprotegidos**, continúa explorando y recurre incluso a la descarga de otras herramientas
El adversario **se dirige al servidor desprotegido** Será necesario borrar el servidor y recrear su imagen	**7:45**	El analista de Falcon Complete identifica la actividad del adversario e **inicia la investigación y respuesta**
	7:55	El analista de Falcon Complete aísla de la red el sistema afectado y **expulsa al adversario**
El adversario descarga el malware Mimikatz personalizado, vuelca las credenciales y **obtiene credenciales de administrador** Es necesario restablecer todas las cuentas de administrador a nivel global	**8:00**	El cliente recibe una escalación crítica para **restablecer la única cuenta de usuario afectada**
El adversario **se desplaza lateralmente** por la empresa Es necesario realizar una investigación para rastrear los pasos del adversario	**8:05**	El analista de Falcon Complete **elimina todas las herramientas y artefactos** que ha dejado atrás el adversario
	8:30	El cliente recibe una notificación con los detalles de la intrusión, incluidos los antecedentes y recomendaciones para mejorar su estado de seguridad a fin de **eliminar el riesgo de intrusiones similares en el futuro**
El adversario **introduce malware selectivo** y despliega mecanismos de **persistencia** mientras se desplaza lateralmente por la empresa Algunas actividades se bloquean y otras se registran como alertas de seguridad, pero el personal ya ha finalizado su jornada laboral	**18:45**	
Es necesario realizar una investigación para rastrear los pasos del adversario Será necesario borrar y recrear la imagen de muchos otros hosts		
El equipo de seguridad identifica alertas críticas y pone en marcha la respuesta de emergencia Al equipo le esperan unos días de simulacros de incendios	**31:30**	

RESULTADO DE LA RESPUESTA DE MÍNIMOS: GASTOS Y MOLESTIAS

Horas de laboriosa investigación

Recreaciones de imágenes complicadas y caras

No hay seguridad de si el adversario volverá

RESULTADO DE FALCON COMPLETE: RAPIDEZ Y EFICACIA

Intrusión neutralizada y solucionada en minutos

Sin intervención por parte del personal de TI

Sin interrupción de los procesos empresariales y los usuarios

Confianza en que la amenaza se ha solucionado completamente de la forma adecuada

CROWDSTRIKE

PARA OBTENER MÁS INFORMACIÓN SOBRE FALCON COMPLETE, VAYA A WWW.CROWDSTRIKE.COM/FALCON-COMPLETE