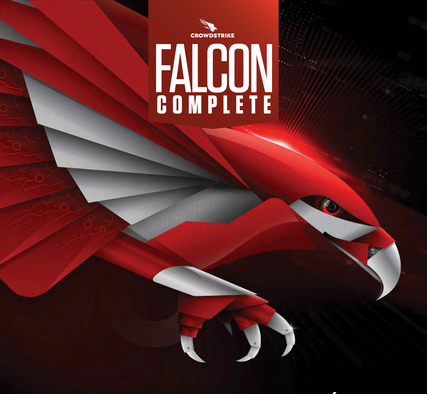

FALCON COMPLETE EN ACCIÓN

Defenderse contra las amenazas actuales requiere la vigilancia constante de analistas calificados.

CrowdStrike® Falcon Complete™ es un servicio de detección y respuesta administradas (MDR) que ofrece investigación especializada y respuesta quirúrgica 24x7x365.

Vea la diferencia que le brinda Falcon Complete.

RESPUESTA A INCIDENTES CON RECURSOS INTERNOS DISPONIBLES	ACTIVIDAD ADVERSARIA Tiempo transcurrido (HRS: MIN)	RESPUESTA A INCIDENTES ESPECIALIZADA FALCON COMPLETE
	0:00 El adversario obtiene credenciales através de **phishing**	
El **Malware es bloqueado** por la solución de protección de endpoint local Se genera una alerta de criticidad baja, pero se la ignora como no crítica	**0:02** Phish establece conexión con el dominio malicioso e intenta implementar el **malware** de segunda fase	Falcon Prevent™ **bloquea el malware** Se genera una alerta de baja criticidad
	0:30	El equipo de Falcon Complete **investiga la alerta** de baja criticidad El equipo de Falcon Complete identifica el malware bloqueado y lo califica como asociado con un grupo de agentes de amenazas conocidos por utilizar ransomware dirigido a organizaciones del sector financiero El analista verifica que las políticas estén configuradas correctamente para revelar actividades adversas que puedan estar en camino.
	6:00 **El adversario inicia la sesión** en el sistema **através de RDP** con credenciales de usuario válidas	
	6:10 El adversario se da cuenta de que el implante inicial ha fallado, sospecha que existe una protección de endpoint local implementada, activa **tácticas sensibles** y utiliza la funcionalidad nativa del sistema operativo para realizar el reconocimiento local.	
El adversario identifica un nuevo **servidor de desarrollo que no está protegido** por el endpoint local	**7:30**	El adversario se siente frustrado por no encontrar **ningún sistema desprotegido** y sigue intentándolo, incluso descargando herramientas adicionales
El adversario se **traslada al servidor desprotegido** Deberá limpiarse y formatearse el servidor	**7:45**	El analista Falcon Complete identifica la actividad del adversario e **inicia la investigación y respuesta.**
	7:55	El analista Falcon Complete aísla el sistema afectado de la red y **expulsa al adversario**
El adversario descarga el malware Mimikatz personalizado, realiza la descarga de las credenciales y **obtiene las credenciales de administrador** Todas las cuentas de administrador globales deben redefinirse	**8:00**	El cliente recibe un escalonamiento crítico para redefinir la **única cuenta de usuario afectada**
El adversario se **mueve lateralmente** dentro de la organización Se requiere una investigación para rastrear el movimiento del adversario	**8:05**	El analista Falcon Complete **elimina todas las herramientas y artefactos** restantes dejados por el adversario
	8:30	El cliente recibe una notificación con detalles de la intrusión, con detalles de contexto y recomendaciones para mejorar la posición de seguridad y **eliminar el riesgo de futuras intrusiones similares.**
El adversario pone en acción el **malware dirigido** e implementa mecanismos de **persistencia** a medida que se mueve lateralmente a través de la organización Algunas actividades están bloqueadas y otras se registran como alertas de seguridad, pero el equipo ya cerró el turno y se fue a casa	**18:45**	
Se requiere una investigación para rastrear el movimiento del adversario Deberá limpiarse y formatearse el servidor		
El equipo de seguridad identifica las alertas críticas y activa la respuesta de emergencia El equipo se dedica durante días a un simulacro de incendio	**31:30**	

RESULTADO CON RECURSOS INTERNOS: **RESPUESTA COSTOSA Y DISRUPTIVA**	RESULTADO CON FALCON COMPLETE: **RESPUESTA RÁPIDA Y EFICAZ**
Horas de trabajo de investigación intensiva	Intrusión contenida y corregida en minutos
Formateo complicado y costoso	Sin intervención del personal de TI
No se sabe al cierto si el adversario regresará o no	Sin interrupciones en los procesos comerciales o de los usuarios
	Confianza en que la amenaza ha sido controlada completa y correctamente