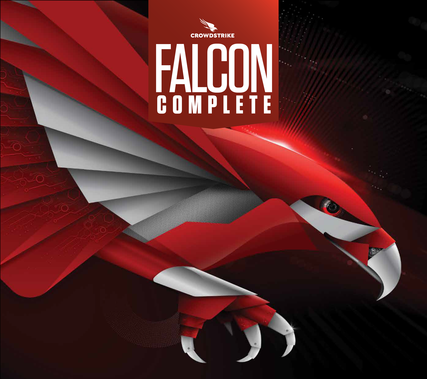

FALCON COMPLETE EM AÇÃO

Se defender contra ameaças atuais exige vigilância constante de analistas qualificados.

CrowdStrike® Falcon Complete™ é um serviço de detecção e resposta gerenciada (MDR) que oferece investigação especializada e resposta cirúrgica 24x7x365.

Veja a diferença que o Falcon Complete traz para você.

RESPOSTA A INCIDENTE COM RESURSOS INTERNOS DISPONÍVEIS	ATIVIDADE ADVERSÁRIA Tempo Decorrido (HRS:MIN)	RESPOSTA A INCIDENTE ESPECIALIZADA FALCON COMPLETE
	0:00 Adversário obtém credenciais por meio de **phishing**	
Malware é bloqueado pela solução de proteção de endpoint local Alerta de baixa criticidade é gerado, mas ignorado como não crítico	**0:02** Phish estabelece conexão com domínio malicioso e tenta implantar **malware** de segundo estágio	**Malware é bloqueado** pelo Falcon Prevent™ Alerta de baixa criticidade é gerado
	0:30	**O alerta** de baixa criticidade é **investigado** pela equipe Falcon Complete A equipe Falcon Complete realiza triagem do malware bloqueado e o identifica como associado a um grupo de agentes de ameaças conhecido por usar ransomware direcionado a organizações no setor financeiro O analista verifica se as políticas estão devidamente configuradas para revelar atividades adversas que podem estar a caminho
	6:00 **Adversário efetua login** no sistema **via RDP** com credenciais de usuário válidas	
	6:10 O adversário percebe que o implante inicial falhou, suspeita que há proteção de endpoint local em vigor, aciona **táticas sigilosas** e usa a funcionalidade nativa do sistema operacional para realizar o reconhecimento local	
O adversário identifica um novo **servidor de desenvolvimento que não está protegido** pelo endpoint local	**7:30**	O adversário está frustrado por não encontrar **nenhum sistema desprotegido** e continua explorando inclusive fazendo download de ferramentas adicionais
Adversário se **move para o servidor desprotegido** O servidor precisará ser limpo e formatado	**7:45**	O analista Falcon Complete identifica atividade adversária e **começa investigação e resposta**
	7:55	O analista Falcon Complete isola o sistema afetado da rede, e o **adversário é expulso**
O adversário baixa o malware personalizado Mimikatz, faz dumping (descarrega) de credenciais e **obtém credenciais de administrador** Todas as contas de administrador globais precisam ser redefinidas	**8:00**	O cliente recebe escalonamento crítico para **redefinir a única conta de usuário afetada**
O adversário se **move lateralmente** através da organização É necessária uma investigação para rastrear o movimento do adversário	**8:05**	O analista Falcon Complete **remove todas as ferramentas e artefatos** restantes deixados pelo adversário
	8:30	O cliente recebe uma notificação com detalhes da intrusão, incluindo detalhes do contexto e recomendações para melhorar a postura de segurança e **eliminar o risco de futuras intrusões semelhantes**
O adversário coloca em ação **malware direcionado** e implanta mecanismos de **persistência** à medida que se move lateralmente pela organização Algumas atividades estão bloqueadas e outras são registradas como alertas de segurança, mas a equipe já encerrou o expediente e foi para casa É necessária uma investigação para rastrear o movimento do adversário O servidor precisará ser limpo e formatado	**18:45**	
A equipe de segurança identifica alertas críticos e aciona resposta emergencial Equipe fica engajada em simulação de incêndio por dias	**31:30**	

RESULTADO COM RESURSOS INTERNOS: **RESPOSTA ONEROSA E DISRUPTIVA**	RESULTADO COM FALCON COMPLETE: **RESPOSTA RÁPIDA E EFICAZ**
Horas de trabalho intensivo e investigação	Intrusão contida e corrigida em minutos
Formatações complicadas e caras	Nenhuma intervenção da equipe de TI
Não há certeza se o adversário retornará ou não	Sem disrupção para os processos de negócios ou usuários
	Confiança de que a ameaça foi controlada completa e corretamente