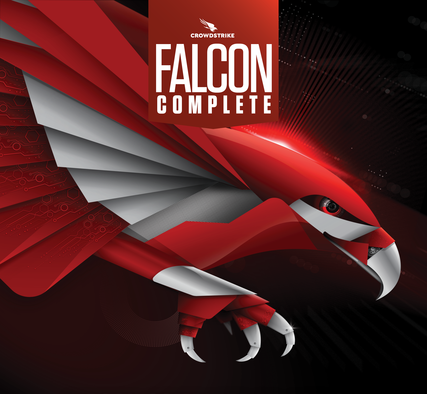

FALCON COMPLETE EN ACTION

La lutte contre les cybermenaces actuelles exige une vigilance constante de la part d'analystes expérimentés.

CrowdStrike® Falcon Complete™ est un service prêt à l'emploi de détection et d'intervention gérées, qui offre des fonctionnalités d'investigation poussée et d'intervention ultraprécise, 24 h/24 et 7 j/7, sans interruption.

Découvrez les avantages que Falcon Complete peut vous offrir.

INTERVENTION SUR INCIDENT « AU MIEUX »	ACTIVITÉ DU CYBER-ADVERSAIRE Temps écoulé (H:MIN)	INTERVENTION SUR INCIDENT POINTUE DE FALCON COMPLETE
	0:00 Le cyberadversaire obtient les identifiants au moyen d'une attaque de **phishing**	
Une solution locale de protection des endpoints **bloque le logiciel malveillant** Une alerte de faible gravité est générée, mais est ignorée car jugée non critique	**0:02** L'outil de phishing établit une connexion avec le domaine malveillant et tente de déployer un **logiciel malveillant** de second niveau	Falcon Prevent™ **bloque le logiciel malveillant** Une alerte de faible gravité est générée
	0:30	L'équipe Falcon Complete **enquête sur l'alerte** de faible gravité L'équipe Falcon Complete opère un tri et établit que le logiciel malveillant bloqué est associé à un groupe cybercriminel connu pour attaquer des entreprises du secteur financier avec des ransomwares Un analyste vérifie que les politiques sont configurées de façon à pouvoir détecter toute nouvelle attaque du cyberadversaire
	6:00 Le **cyberadversaire se connecte** au système **via RDP** à l'aide d'identifiants valides	
	6:10 Le cyberadversaire comprend que l'implantation initiale a échoué, présume que les endpoints sont protégés localement, lance une **attaque furtive** et utilise une fonctionnalité native du système d'exploitation pour effectuer une reconnaissance locale	
Le cyberadversaire identifie un nouveau **serveur de développement non protégé** par l'endpoint local	**7:30**	Frustré de ne trouver **aucun système non protégé**, le cyberadversaire continue son exploration et télécharge des outils supplémentaires
Le cyberadversaire **s'attaque au serveur non protégé** Le contenu du serveur doit être effacé et une nouvelle image système doit être créée	**7:45**	L'analyste Falcon Complete identifie l'activité du cyberadversaire et **démarre le processus d'investigation et d'intervention**
	7:55	L'analyste Falcon Complete isole le système compromis du reste du réseau et le **cyberadversaire est éjecté**
Le cyberadversaire télécharge un logiciel malveillant Mimikatz personnalisé, supprime les identifiants et **obtient des identifiants administrateur** Tous les comptes administrateur doivent être réinitialisés	**8:00**	Le client reçoit un message d'alerte urgent lui demandant de **réinitialiser le seul compte utilisateur compromis**
Le cyberadversaire **se déplace latéralement** au sein de l'entreprise Une investigation est requise pour retracer les déplacements du cyberadversaire	**8:05**	L'analyste Falcon Complete **supprime tous les outils et artefacts** que le cyberadversaire a laissés derrière lui
	8:30	Le client reçoit une notification contenant des détails sur l'intrusion (origine, évolution, etc.), ainsi que des recommandations pour renforcer le niveau de sécurité afin d'**éliminer le risque d'intrusions similaires à l'avenir**
À mesure qu'il se déplace latéralement dans l'entreprise, le cyberadversaire **installe des logiciels malveillants ciblés** et déploie des mécanismes de **persistance** Certaines activités sont bloquées, et d'autres sont consignées en tant qu'alertes de sécurité, mais les membres de l'équipe sont rentrés chez eux après leur journée de travail Une investigation est requise pour retracer les déplacements du cyberadversaire Le contenu de nombreux autres systèmes doit être effacé et de nouvelles images système créées	**18:45**	
L'équipe de sécurité identifie les alertes critiques et lance la procédure d'intervention d'urgence L'équipe va connaître plusieurs jours de lutte acharnée	**31:30**	

RÉSULTAT DE L'INTERVENTION « AU MIEUX » : INTERVENTION COÛTEUSE, QUI PERTURBE LES ACTIVITÉS

Des heures d'investigations laborieuses

Création fastidieuse et coûteuse de nouvelles images système

Aucune certitude quant à un éventuel retour du cyberadversaire

RÉSULTAT DE FALCON COMPLETE : INTERVENTION RAPIDE ET EFFICACE

Intrusion contenue et neutralisée en quelques minutes

Aucune intervention de l'équipe informatique

Aucune perturbation des processus métier ou des utilisateurs

Assurance que la cybermenace a été totalement et correctement prise en charge