CROWDSTRIKE

AUDIT DES COMPROMISSIONS

Identifiez les activités présentes et passées des cyberadversaires

DÉTERMINEZ SI VOTRE ENTREPRISE A ÉTÉ COMPROMISE

L'audit des compromissions (Compromise assessment) réalisé par les Services CrowdStrike® est conçu pour identifier les activités en cours ou passées des cyberadversaires dans l'environnement d'une entreprise. Il s'appuie sur les années d'expérience de l'équipe des Services dans la réponse aux intrusions par les cyberattaquants les plus avancés, ainsi que sur la puissante plateforme CrowdStrike Falcon®, des renseignements de pointe sur les cybermenaces et un Threat Hunting actif 24 heures sur 24. Ces forces conjuguées vous offrent l'audit le plus complet du secteur de l'environnement informatique de votre entreprise et répondent à une question cruciale : « Mon entreprise a-t-elle subi une intrusion ? ».

Une longue expérience des investigations menées dans le cadre d'interventions impliquant des menaces ciblées permet à l'équipe des Services d'offrir de précieux renseignements sur les tactiques, techniques et procédures employées par les cyberadversaires les plus sophistiqués. Ces connaissances et ce savoir-faire alliés à la technologie primée de protection des endpoints native au cloud de la plateforme Falcon permettent de réaliser un audit complet et poussé. Les Services CrowdStrike vont au-delà des détections classiques basées sur les indicateurs et de la surveillance ponctuelle pour offrir un audit des compromissions fondé à la fois sur une analyse approfondie des preuves informatiques historiques et sur une détection des menaces et un Threat Hunting en temps réel. Il est capital de connaître les événements passés et présents survenus sur vos endpoints pour savoir comment protéger votre environnement dans le futur.

PRINCIPAUX AVANTAGES

L'AUDIT DES COMPROMISSIONS DE CROWDSTRIKE OFFRE LES AVANTAGES SUIVANTS :

Limitation de la durée d'implantation : déterminez si les cyberadversaires ont infiltré vos défenses et se déplacent furtivement dans votre environnement.

Réduction des risques : bénéficiez d'une analyse approfondie qui réduit le risque de vol de vos actifs financiers, données clients ou propriété intellectuelle par des cyberadversaires.

Renforcement de la sécurité : identifiez proactivement les pratiques de sécurité inefficaces qui exposent votre entreprise à un risque accru.

AUDIT DES COMPROMISSIONS

PRINCIPAUX ATOUTS

UNE ÉQUIPE HAUTEMENT QUALIFIÉE

- Pour atteindre un tel niveau d'expertise et de compétence, l'équipe des services CrowdStrike a recruté « la crème de la crème » du monde de la cybersécurité, de l'intervention sur incident, des investigations informatiques et des opérations pour réaliser les audits des compromissions. L'équipe offre une perspective unique sur les techniques, tactiques et procédures (TTP) qu'utilisent aujourd'hui les attaquants les plus chevronnés.

OUTILS À LA POINTE DU SECTEUR

- **La plateforme Falcon** vous offre une visibilité en temps réel sur votre environnement. Elle identifie les compromissions potentielles et vous offre la possibilité de les éliminer. Il s'agit là d'un avantage indéniable par rapport aux audits habituels, qui ont recours à une approche classique d'investigation informatique, uniquement basée sur la recherche d'indicateurs de compromission.
- **Falcon Insight™** est la solution de détection et d'intervention sur les endpoints (EDR) de CrowdStrike. Elle offre une protection avancée native au cloud au sein d'un agent léger unique déployé sur chaque endpoint de votre environnement.
- **Falcon Forensics Collector (FFC)** est un outil « single-run » inter-plateforme non persistant qui collecte des données auprès de plus de 45 artefacts significatifs d'un point de vue criminalistique sur chaque endpoint. Les données sont agrégées et traitées dans le cloud CrowdStrike, où elles peuvent être analysées et comparées aux renseignements de CrowdStrike Intelligence, une solution conçue pour surveiller et identifier les tactiques, techniques et procédures des cyberadversaires.

APPROCHE COMPLÈTE

- L'audit combine analyse des preuves informatiques historiques par des experts et détection des menaces et Threat Hunting en temps réel, ce qui permet à CrowdStrike de repérer les activités des cyberadversaires sur l'endpoint et au sein du réseau.
- Un audit des compromissions CrowdStrike commence par la collecte et l'analyse efficaces des artefacts d'investigation en provenance des systèmes d'exploitation Microsoft Windows, macOS et Linux — sans nécessiter d'appliances sur site ou d'analyse des indicateurs actifs. En parallèle, la plateforme CrowdStrike Falcon assure une détection des menaces et une surveillance de l'environnement en temps réel, afin d'identifier les menaces avec et sans logiciels malveillants, ainsi que les indicateurs d'attaque.
- Un véritable audit des éventuelles activités malveillantes au sein de votre environnement ne peut être effectué sans un contexte historique complet basé sur des investigations, associé à une surveillance dynamique. Chaque environnement étant unique, l'équipe des Services collabore dès le départ avec votre équipe pour comprendre votre topologie réseau et découvrir les systèmes hébergés dans votre environnement.

À PROPOS DES SERVICES CROWDSTRIKE

Les Services CrowdStrike offrent aux entreprises la protection et l'expertise dont elles ont besoin pour se défendre contre les incidents de cybersécurité et y répondre efficacement. S'appuyant sur la plateforme native au cloud CrowdStrike Falcon®, qui assure une protection de nouvelle génération des endpoints, des opérations de collecte de renseignements et de génération de rapports sur les cybermenaces, ainsi qu'un Threat Hunting proactif 24 heures sur 24, 7 jours sur 7, l'équipe des services CrowdStrike aide les clients à identifier, suivre et bloquer les cyberadversaires en temps réel. Cette approche unique permet à CrowdStrike de bloquer plus rapidement les accès non autorisés et de prévenir de nouvelles intrusions. CrowdStrike offre également des services proactifs conçus pour permettre aux entreprises de rehausser leur capacité à anticiper les menaces, de préparer leurs réseaux et d'empêcher les intrusions.

Pour en savoir plus, consultez le site www.crowdstrike.fr/services/

E-mail : services@crowdstrike.com

ANALYSE ET RÉSULTATS EXPLOITABLES

CrowdStrike est conscient qu'un audit des compromissions n'a de sens que s'il fournit des résultats et des rapports d'analyse exploitables et adaptés à toutes les parties prenantes occupant des fonctions de gestion des risques d'entreprise et de la sécurité informatique. La documentation fournie par les consultants de CrowdStrike peut inclure :

Un rapport détaillé précisant si l'équipe a découvert des preuves d'une intrusion ciblée au sein de votre environnement, avec des recommandations pour véritablement renforcer votre sécurité

Un résumé écrit destiné à présenter les résultats, conclusions et recommandations les plus importants

La documentation technique de l'audit mené par l'équipe des Services CrowdStrike pour offrir à votre équipe technique les informations dont elle a besoin pour neutraliser, éliminer et confirmer les menaces identifiées par l'équipe des Services

D'autres documents sur les éléments découverts, notamment les logiciels malveillants de base, les scripts et fichiers suspects, les utilitaires d'accès à distance et les pratiques d'administration susceptibles d'introduire des risques.