CROWDSTRIKE

SERVICES PROACTIFS ET DE RÉPONSE À INCIDENTS CROWDSTRIKE

S'entraîner, réagir et remédier rapidement et efficacement à une intrusion

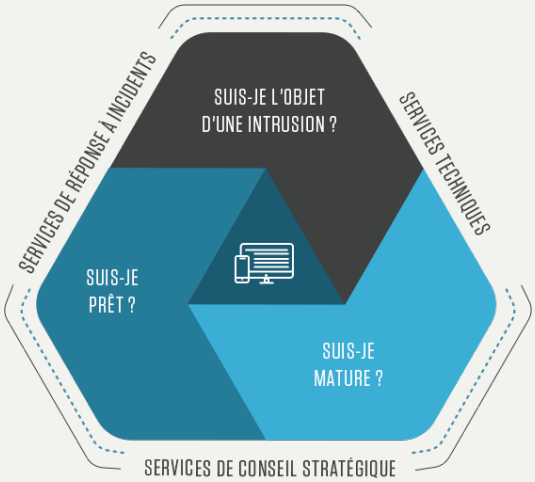
SERVICES PROACTIFS ET DE RÉPONSE À INCIDENTS CROWDSTRIKE

CHOISISSEZ LES SERVICES QUI CORRESPONDENT LE MIEUX AUX BESOINS DE VOTRE ENTREPRISE

Les services CrowdStrike® regroupent des offres proactives et de réponse à incidents qui jouent un rôle crucial dans l'amélioration du niveau de sécurité de votre entreprise et le blocage des intrusions. Ces services sont conçus pour permettre aux entreprises de répondre de façon efficace et rapide aux incidents de cybersécurité. Les clients bénéficient également d'un large éventail de services proactifs conçus pour améliorer leur niveau de cybersécurité global.

Pour ce faire, les services CrowdStrike réunissent une équipe de professionnels de la sécurité issus des services de renseignement, des forces de l'ordre et du secteur de la cybersécurité, des architectes et des ingénieurs des meilleures entreprises technologiques du monde entier, ainsi que des consultants en sécurité qui ont mené certaines des investigations sur les intrusions les plus complexes au monde.

Cette équipe s'appuie largement sur la plateforme CrowdStrike Falcon®, qui offre une protection révolutionnaire des endpoints, tout en favorisant la réponse à incidents en temps réel, les investigations informatiques approfondies et les renseignements sur les cybermenaces afin de garantir qu'aucune menace ne passe inaperçue. Les services CrowdStrike se distinguent en aidant les entreprises à anticiper, neutraliser et prévenir les dommages causés par un large éventail d'incidents de sécurité et de cyberattaques avancées, et surtout en les aidant à se protéger contre de futures attaques.



Les services proactifs et de réponse à incidents CrowdStrike peuvent être utilisés individuellement ou conjointement, de même que faire l'objet d'un contrat de service. Ce contrat est flexible : si vous constatez que vous n'avez pas besoin des services de réponse à incidents de CrowdStrike, vous pouvez utiliser vos heures de service disponibles pour profiter des services proactifs, qui sont tous conçus pour vous aider à améliorer votre niveau de sécurité.

APERÇU DES SERVICES CROWDSTRIKE

Les offres de services CrowdStrike permettent aux entreprises de renforcer leur niveau de sécurité en répondant à trois questions fondamentales :

SUIS-JE L'OBJET D'UNE INTRUSION ?

- Services de réponse à incidents
- Services de récupération des endpoints
- Évaluation des compromissions
- Surveillance de la sécurité du réseau

SUIS-JE MATURE ?

- Évaluation de la maturité de la cybersécurité
- Évaluation de la sécurité d'Active Directory
- Évaluation de la sécurité du cloud
- Évaluation du Centre des opérations de sécurité (SOC)
- Évaluation de l'hygiène IT
- Programme de renforcement de la cybersécurité
- Programme de sécurité approfondi

SUIS-JE PRÊT ?

- Exercice de gestion d'incident
- Simulation immersive de gestion de cyberattaque
- Exercice de simulation de l'adversaire
- Exercice Red Team / Blue Team
- Services de tests d'intrusion

SERVICES MANAGÉS, SUPPORT ET FORMATION

- Falcon Complete™
- Falcon Gold Standard
- Support opérationnel de Falcon
- Formations Falcon (CrowdStrike University)

SERVICES PROACTIFS ET DE RÉPONSE À INCIDENTS CROWDSTRIKE

SUIS-JE L'OBJET D'UNE INTRUSION ?

SERVICES DE RÉPONSE À INCIDENTS

- En cas d'intrusion, notre équipe d'intervention raccourcit les délais de résolution en vous informant sur les activités du cyberattaquant, vous permettant ainsi de reprendre vos activités plus rapidement. L'équipe des services de réponse à incidents CrowdStrike travaille en collaboration avec vos équipes pour gérer les incidents de sécurité critiques et mener des investigations afin de neutraliser les cyberattaques dans les plus brefs délais et mettre en œuvre une solution à long terme pour éviter que cela se reproduise.
- L'équipe de réponse à incidents de CrowdStrike adopte une approche de la réponse à incidents fondée sur des renseignements sur les cybermenaces, et allie une expérience pratique de la réponse à incidents, de l'investigation et de la correction à une technologie de pointe, en s'appuyant sur la plateforme cloud Falcon, qui permet d'identifier rapidement et précisément les cyberattaquants et de les neutraliser efficacement. L'équipe CrowdStrike s'efforce de remettre les organisations sur pied plus rapidement, tout en réduisant l'impact des cyberincidents.

SERVICES DE RÉCUPÉRATION DES ENDPOINTS

- Les services de récupération des endpoints de CrowdStrike (ERS - Endpoint Recovery Services) vous permettent de récupérer facilement à la suite d'attaques ou de menaces persistantes avancées, sans interruption de vos activités.
- Ce service allie la plateforme technologique de pointe et les renseignements sur les cybermenaces de CrowdStrike à une équipe d'experts en sécurité chevronnés pour faciliter la détection, l'analyse et la correction des incidents de sécurité connus, tout en permettant une récupération rapide.

ÉVALUATION DES COMPROMISSIONS

- L'équipe d'évaluation des compromissions de CrowdStrike identifie les activités actuelles et passées des cyberattaquants dans votre environnement pour répondre à la question suivante : « Mon entreprise a-t-elle subi une intrusion ? »
- L'équipe d'évaluation des compromissions compte de nombreuses années d'expérience dans la réponse aux intrusions perpétrées par les cyberattaquants les plus avancés. Elle s'appuie sur la puissante plateforme Falcon, des renseignements de pointe sur les cybermenaces et un Threat Hunting actif 24 heures sur 24, 7 jours sur 7 pour offrir l'évaluation la plus complète qui soit d'une compromission dans votre environnement.

SURVEILLANCE DE LA SÉCURITÉ DU RÉSEAU

- Ce service assure une surveillance approfondie de la sécurité du réseau afin de détecter les menaces actives présentes dans votre environnement.
- Il offre une vaste capacité de surveillance de la sécurité du réseau pour la détection, la réponse et le Threat Hunting. Il utilise à la fois l'expertise des threat hunters des services CrowdStrike et un dispositif réseau qui détecte les menaces présentes dans votre environnement.

POURQUOI CHOISIR CROWDSTRIKE

Expertise éprouvée : Une équipe d'experts composée de spécialistes de la réponse à incidents, de chercheurs en logiciels malveillants et de professionnels des renseignements sur les cybermenaces apporte une réponse rapide en cas d'incident et assure l'investigation, la récupération des endpoints et des services proactifs.

Renseignements sur les adversaires : Vous bénéficiez de renseignements et rapports parfaitement actualisés sur les auteurs de menaces qui ont pris votre environnement pour cible, ainsi que sur leurs techniques, tactiques et procédures.

Threat Hunting inégalé : Threat Hunting proactif, opérationnel 24 h/24 et 7 j/7, étend la recherche d'activités malveillantes à tout l'environnement.

Technologies de pointe : La plateforme unique CrowdStrike Falcon utilise des technologies de nouvelle génération pour protéger les endpoints et détecter les cyberadversaires, les expulser rapidement et les empêcher de revenir.

SERVICES PROACTIFS ET DE RÉPONSE À INCIDENTS CROWDSTRIKE

SUIS-JE MATURE ?

ÉVALUATION DU NIVEAU DE MATURITÉ DE LA CYBERSÉCURITÉ

- Les experts des services CrowdStrike sont conscients qu'être « conforme » ne signifie pas que vous êtes en sécurité. Plutôt que de se concentrer uniquement sur la conformité, l'équipe évalue le niveau de maturité de votre entreprise à travers une vision précise, complétée par des années d'expérience dans la réponse aux menaces.
- La méthodologie de l'équipe ne se limite pas à un audit standard : elle évalue la maturité de l'entreprise en matière de cybersécurité sur la base de sa capacité à prévenir et détecter les cyberattaques les plus avancées, ainsi qu'à y répondre.

ÉVALUATION DE LA SÉCURITÉ D'ACTIVE DIRECTORY

- Bénéficiez d'un examen complet de votre configuration Active Directory (AD) et des paramètres des règles afin de prévenir l'exploitation de l'infrastructure AD.
- L'évaluation de la sécurité d'Active Directory proposée par CrowdStrike est conçue de manière unique pour examiner la configuration et les paramètres des règles d'AD afin d'identifier les problèmes de configuration de sécurité susceptibles d'être exploités par les cyberattaquants.
- Cette évaluation comprend l'examen de la documentation, des discussions avec votre personnel, l'exécution d'outils propriétaires et un examen manuel de votre configuration et de vos paramètres d'AD. Une fois l'évaluation terminée, vous recevez un rapport détaillant les problèmes identifiés et leur impact, ainsi que des recommandations pour l'atténuation et la correction.

ÉVALUATION DE LA SÉCURITÉ DU CLOUD

- Le service d'évaluation de la sécurité du cloud (Cloud Security Assessment) de CrowdStrike fournit des informations utiles sur les erreurs de configuration de la sécurité et met en lumière les écarts par rapport à l'architecture de sécurité du cloud recommandée.
- Fondée sur l'expérience de CrowdStrike en matière de réponse à incidents et réalisée par des consultants ayant fait leurs classes auprès de leaders reconnus dans le domaine de l'architecture de sécurité du cloud, cette évaluation vous indique les actions prioritaires à mettre en œuvre pour optimiser vos capacités de prévention, de détection et de reprise des activités après un incident de sécurité dans le cloud.

ÉVALUATION DE L'HYGIÈNE IT

- Découvrez les vulnérabilités de manière proactive et protégez votre réseau avant qu'une intrusion ne se produise.
- Une évaluation de l'hygiène IT par CrowdStrike permet de bénéficier d'une meilleure visibilité sur les applications, l'accessibilité et la gestion des comptes au sein de votre réseau, offrant ainsi un contexte complet sur le trafic réseau et les failles de sécurité. L'identification des vulnérabilités et des correctifs manquants vous permet de protéger votre réseau de manière proactive avant qu'une intrusion ne se produise.

PROGRAMME DE RENFORCEMENT DE LA CYBERSÉCURITÉ

- Élaborez et mettez en œuvre un programme de renforcement de la cybersécurité après qu'une intrusion s'est produite afin de combler les lacunes en matière de sécurité et de prévenir d'autres intrusions.
- Le programme d'amélioration de la cybersécurité de CrowdStrike s'adresse aux entreprises qui ont récemment subi une intrusion et qui ont besoin d'aide pour élaborer un plan stratégique d'amélioration de la cybersécurité afin d'éviter qu'une autre intrusion se produise.

OFFRE COMPLÉMENTAIRES

Évaluation du Centre des opérations de sécurité (SOC) :
Améliorez le niveau de maturité de votre SOC en identifiant et hiérarchisant les domaines à améliorer.

Programme de sécurité approfondi :
Plongez dans vos processus, outils et ressources de cybersécurité pour déterminer la maturité de votre programme de sécurité.

SERVICES PROACTIFS ET DE RÉPONSE À INCIDENTS CROWDSTRIKE

SUIS-JE PRÊT ?

EXERCICE DE SIMULATION DE GESTION D'INCIDENT

- L'expérience avancée de l'équipe des services CrowdStrike dans la conduite d'investigations IR contre les cybermenaces sophistiquées apporte une perspective concrète au processus de simulation de gestion d'incident.
- Les exercices sont conçus pour simuler une attaque ciblée et guider votre entreprise, que les participants soient des dirigeants ou des membres de l'équipe technique, tout au long d'une simulation d'incident réaliste. Cet exercice permet de faire l'expérience d'une attaque sans les perturbations et dommages qui l'accompagnent.

SIMULATION IMMERSIVE DE GESTION DE CYBERATTAQUE

- Cet exercice est conçu pour tester les collaborateurs de l'entreprise afin de s'assurer qu'ils comprennent leur rôle dans le cadre d'un scénario de réponse à incidents.
- Au lieu de discuter d'une attaque hypothétique en groupe, l'équipe des services s'appuie sur vos outils et processus pour ajouter au réalisme, en fournissant notamment des informations spécifiques à des personnes précises, exactement comme cela se produirait lors de l'investigation d'une intrusion réelle. L'équipe vous laisse ensuite le soin de déterminer la meilleure façon de gérer ces informations. À l'issue de la mission, les vulnérabilités de votre processus seront clairement identifiées.

EXERCICE DE SIMULATION DE L'ADVERSAIRE

- Ce test offre l'avantage de faire l'expérience d'une attaque ciblée sophistiquée sans subir les dommages qui accompagnent un incident réel.
- Pour ce faire, un consultant CrowdStrike chevronné imite les techniques d'attaque actuelles pour tenter d'accéder au réseau de votre entreprise et de compromettre des ressources spécifiques. Une fois cet objectif atteint, l'équipe explique comment elle a procédé et vous aide à identifier les tactiques que vous pouvez employer pour aider à prévenir de futures attaques.

EXERCICE RED TEAM / BLUE TEAM

- Les membres de votre équipe de cybersécurité s'entraînent et apprennent auprès d'experts dans le cadre d'une simulation d'attaque de votre environnement informatique menée par la Red Team tandis que la défense est assurée par la Blue Team.
- L'exercice Red Team / Blue Team de CrowdStrike se concentre sur la connaissance de votre équipe de sécurité en matière de Threat hunting et des processus globaux de réponse à incidents au moyen d'un scénario d'attaque ciblée inspiré du monde réel.

SERVICES DE TESTS D'INTRUSION

- L'équipe des services CrowdStrike recourt au piratage éthique pour identifier les failles de sécurité et effectue des simulations d'attaque autorisées et des tests de pénétration sur différents composants de vos systèmes, réseaux et applications.
- Vous pouvez choisir parmi un large éventail d'options de test pour répondre à vos objectifs de sécurité spécifiques.

SERVICES MANAGÉS, SUPPORT ET FORMATION

FALCON COMPLETE™ :
Cette solution complète de protection des endpoints et de Threat Hunting est proposée sous la forme d'un service clé en main entièrement managé qui tire parti de la puissance de la plateforme Falcon.

FALCON GOLD STANDARD :
Vous aide à déployer, configurer et manager la plateforme Falcon et répondre aux alertes pendant les 90 premiers jours de votre expérience avec CrowdStrike.

SUPPORT OPÉRATIONNEL DE FALCON :
Ce support vous aide à déployer et configurer la plateforme Falcon de façon à optimiser vos opérations de cybersécurité.

FORMATION FALCON :
Les services de formation professionnelle de la CrowdStrike University (CSU) améliorent les connaissances de votre équipe de cybersécurité, vous permettant ainsi de tirer le meilleur parti de votre investissement dans la plateforme Falcon.

SERVICES PROACTIFS ET DE RÉPONSE À INCIDENTS CROWDSTRIKE

RETAINER DE SERVICES

SERVICES PROACTIFS ET DE RÉPONSE À INCIDENTS

Tous les services proactifs et de réponse à incidents de CrowdStrike sont disponibles dans le cadre d'un retainer de services CrowdStrike. Le retainer vous permet de faire rapidement appel à l'équipe dès lors que vous avez besoin d'une assistance pour la réponse à incidents. Sa structure permet en outre de planifier et d'offrir les services proactifs les mieux adaptés aux besoins de votre entreprise. Vous bénéficiez ainsi de services de réponse à incidents au moment où vous en avez besoin, de même que d'un plan conçu pour renforcer votre niveau de sécurité et tester votre état de préparation tout au long de l'année.

Retainer	Tier 1	Tier 2	Tier 3	Tier 4
Réponse à incidents à la demande	Oui	Oui	Oui	Oui
Délai de réponse (à distance)	8 heures	6 heures	4 heures	2 heures
Délai de réponse (sur site)	2 jours	2 jours	1 jour	1 jour
Heures de travail comprises	110	160	240	480

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 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 cyberattaquants 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.com/services/**

Adresse e-mail : **services@crowdstrike.com**