Produits CrowdStrike

CROWDSTRIKE

DÉTECTION ET INTERVENTION MANAGÉES (MDR) GUIDE D'ACHAT

INTRODUCTION

EN QUOI CONSISTENT LES SERVICES MDR ?

À l'heure actuelle, une pénurie chronique d'experts en cybersécurité et des compétences associées touche les entreprises de toutes tailles, et ce dans tous les secteurs d'activité à travers le monde. La situation est d'autant plus critique que les cyberadversaires affinent leurs techniques et lancent des attaques de manière toujours plus rapide et efficace. Les entreprises ont du mal à s'éloigner des approches préventives de la sécurité pour répondre aux besoins en matière de détection précoce, de Threat Hunting proactif et d'intervention rapide et efficace 24 heures sur 24, 7 jours sur 7. Constituer une équipe de sécurité dédiée pour assurer ces missions et lui donner les moyens d'agir peut être envisageable pour les grandes entreprises dotées de budgets conséquents. Il n'en reste pas moins que la plupart des entreprises n'auront pas les ressources suffisantes pour mener à bien ce type d'initiative.

Les services de détection et d'intervention managées (MDR, Managed Detection and Response) ont émergé pour répondre à cette demande du marché. Ils aident les entreprises par l'implémentation ou l'amélioration de fonctions de détection des menaces, de réponse à incident, de gestion de la sécurité et de surveillance continue.

Les fournisseurs de services MDR s'appuient entre autres sur les technologies de détection et d'intervention sur les endpoints (EDR, Endpoint Detection and Response) pour disposer d'une visibilité sur les événements liés à la sécurité de l'entreprise, permettant la détection des menaces et l'investigation des incidents. Des analystes surveillent l'apparition d'alertes et participent aux interventions requises. Les formes possibles d'intervention incluent l'investigation des alertes (tri), l'application des mesures nécessaires pour réduire les répercussions et les risques (atténuation) et, enfin, l'élimination totale des menaces et la restauration des endpoints au dernier état correct connu (correction).

Optez pour une solution MDR orientée résultats qui :

- Renforce votre équipe grâce à l'assistance d'experts
- Élimine les menaces en quelques minutes et assure la correction
- Réduit considérablement les risques et les coûts liés à la cybersécurité

POURQUOI LES ENTREPRISES ONT-ELLES BESOIN DE SERVICES MDR ?

La mise en œuvre d'un programme efficace de sécurité des endpoints peut être une tâche particulièrement complexe. Les outils nécessaires sont souvent difficiles à utiliser et exigent une équipe fournie pour les implémenter et en assurer la maintenance et le support. De ce fait, de nombreuses entreprises sont incapables de tirer pleinement parti des technologies de protection des endpoints qu'elles ont acquises. La situation est encore plus délicate pour les entreprises souhaitant assurer un niveau de sécurité élevé. Ce dernier impose en effet la mobilisation de davantage de ressources, dans la mesure où il peut être plus onéreux à entretenir et plus complexe à gérer.

En conclusion, de nombreuses entreprises ne parviennent pas à implémenter un programme de sécurité des endpoints de base, et encore moins un programme vraiment complet. La situation s'avère d'autant plus critique lorsque des incidents graves se produisent et que les entreprises n'ont ni le temps ni l'expertise nécessaires pour gérer la situation comme il se doit, mettant alors en péril leur intégrité.

Voici les problèmes que les services MDR permettent de résoudre :

- **Les entreprises éprouvent des difficultés à implémenter et configurer correctement les technologies qu'elles ont acquises.** Suivant la taille et la charge de travail de leurs équipes informatiques, certaines entreprises ne disposent pas forcément des outils ou de la bande passante nécessaires pour déployer rapidement et efficacement leur solution jusqu'aux endpoints. En outre, il arrive qu'elles ne bénéficient ni du temps, ni de l'expertise nécessaires pour configurer et ajuster les règles répondant à leurs besoins en matière de sécurité et permettant de protéger leurs endpoints, surtout face à des menaces et à un environnement qui évoluent en permanence. Ces lacunes peuvent entraîner le déploiement partiel et la configuration inadéquate d'une solution de sécurité des endpoints, ce qui crée des failles de sécurité invisibles qui rendent l'entreprise vulnérable face aux compromissions.

- **Le nombre d'alertes et d'incidents quotidiens est trop important.** Gérer le volume potentiellement considérable d'alertes générées par certains produits de sécurité des endpoints peut s'avérer très difficile, même pour les entreprises disposant d'une équipe de sécurité dédiée ou d'un centre SOC (Security Operation Center). Non seulement le traitement de ces alertes mobilise de la main-d'œuvre, mais 67 % des décideurs informatiques estiment que les opérations de sécurité sont autant ou plus compliquées aujourd'hui qu'il y a deux ans.[1] La plupart des entreprises souffrent malheureusement d'une pénurie aussi bien de talents que de compétences, laissant des alertes non validées et ouvrant la voie à des compromissions de grande envergure.

- **Les entreprises n'ont pas les ressources nécessaires pour prendre des mesures de correction efficaces en cas d'incident.** Les entreprises souffrant d'une pénurie de ressources et de compétences peuvent avoir du mal à déterminer à temps la nature et la portée des incidents. 80 % des décideurs informatiques estiment que la pénurie de personnel de sécurité rend leur entreprise plus vulnérable.[2] Les incidents peuvent alors ne pas être corrigés efficacement, résolus entièrement ou gérés suffisamment vite, laissant les entreprises vulnérables ou compromises. Répondre correctement à un incident demande des connaissances spécifiques et de l'expérience. La plupart des entreprises qui manquent des ressources nécessaires se voient forcées de restaurer les images d'endpoints en cas de problème. L'alternative consistant à associer manuellement différentes contremesures — comme le confinement du réseau, la prévention des hachages, la suppression, la modification ou la création de clés de Registre, ou encore l'arrêt, la désactivation et le redémarrage de services — semble tout sauf réaliste. Cela dit, la restauration d'images système ne garantit aucunement que l'incident d'origine est intégralement corrigé.

- **La mise en œuvre efficace d'un programme prend du temps.** Même si une entreprise dispose des moyens financiers suffisants pour concevoir un programme interne de sécurité des endpoints, la mise en œuvre d'une stratégie pleinement aboutie peut nécessiter un certain temps. La recherche et le recrutement des collaborateurs qualifiés, l'acquisition des technologies adaptées, la définition de règles et l'élaboration d'un processus de réponse à incident peuvent prendre des mois, voire des années. Par ailleurs, ces programmes sont rarement prioritaires sur d'autres projets informatiques urgents, ce qui ne fait que rallonger les processus d'implémentation pendant lesquels les entreprises restent vulnérables.

- **Il est difficile de recruter et de conserver les professionnels qualifiés nécessaires.** Réunir le personnel compétent requis pour sécuriser efficacement les endpoints peut s'avérer particulièrement compliqué pour certaines entreprises. Selon l'International Information System Security Certification Consortium, un organisme de certification américain, plus de 3,4 millions d'emplois de cybersécurité sont vacants à l'échelle mondiale.[3] Même pour les entreprises qui en ont les moyens, il peut être extrêmement difficile de recruter, former et retenir les collaborateurs et compétences indispensables pour faire face à un paysage de cybermenaces aussi avancées que sophistiquées. Cette pénurie d'expertise spécialisée est un problème qui touche l'ensemble du secteur.

QUELS SONT LES ÉLÉMENTS FONDAMENTAUX DES SERVICES MDR ?

Les services de détection et d'intervention managées visent à réduire le délai entre la détection et l'intervention de sorte à limiter la durée d'implantation des cyberattaquants et ainsi réduire efficacement le risque de compromission. La rapidité de correction dépend donc de la rapidité des étapes de détection et d'intervention.

Pour assurer un tel niveau de réactivité et ainsi garantir la sécurité de leurs clients, les fournisseurs de services MDR doivent offrir l'ensemble des éléments clés suivants : une plateforme robuste, un Threat Hunting continu piloté par une équipe d'experts, des fonctionnalités de surveillance et d'investigation 24 heures sur 24 et 7 jours sur 7, et des capacités de correction ultraprécise. En l'absence de l'un de ces éléments clés, il est beaucoup plus difficile d'appréhender le cycle de vie des attaques dans son intégralité et de restaurer rapidement le réseau au dernier état correct connu.

---

1 *Source :* ESG 2023 SOC Modernization and the Role XDR report (https://research.esg-global.com/reportaction/515201525/Toc)
2 *Source :* 2023 ESG SOC Modernization and the Role of XDR report (https://research.esg-global.com/reportaction/515201525/Toc)
3 *Source :* 2023 ESG SOC Modernization and the Role of XDR report (https://research.esg-global.com/reportaction/515201525/Toc)

PLATEFORME ROBUSTE

La fourniture de services MDR performants passe obligatoirement par une infrastructure technologique robuste. Cette plateforme doit pouvoir bloquer les attaques tout en capturant et en enregistrant l'activité des endpoints en temps réel, et ce afin de permettre des opérations d'analyse et de Threat Hunting plus approfondies.

Une plateforme robuste s'appuie sur les éléments suivants :

1. Une infrastructure cloud native et facile à déployer qui réduit les coûts et la complexité en offrant une rentabilité immédiate sans aucun matériel, logiciel ou configuration supplémentaire.
2. Un moteur de Machine Learning et d'analyse comportementale qui apporte une visibilité totale, en temps réel, et fournit des informations sur toute l'activité au sein de l'environnement.
3. Un agent léger unique qui fournit des données télémétriques détaillées en provenance de tout l'environnement, notamment les endpoints, les workloads cloud et les identités.

Bien entendu, pour que cette technologie offre une protection optimale, elle doit être entièrement déployée et correctement configurée. Le fournisseur de services MDR doit d'ailleurs mettre son expertise et ses bonnes pratiques au service du déploiement, de la configuration et du paramétrage de la plateforme. En effet, cela permettra d'optimiser le niveau de maturité de votre sécurité et vous assurera une rentabilité rapide, avec une intégration en quelques jours seulement, au lieu de plusieurs semaines ou mois.

THREAT HUNTING CONTINU PILOTÉ PAR UNE ÉQUIPE D'EXPERTS

La détection des menaces peut mettre en lumière tout un panel de vulnérabilités au sein de votre environnement informatique. La plupart du temps, cette détection s'appuie sur des algorithmes et des fonctions d'automatisation rapides, efficaces et capables de bloquer les attaques à l'exécution. Certaines attaques sont toutefois menées par des cyberadversaires humains qui comprennent bien les contremesures utilisées pour détecter leurs activités et font le nécessaire pour les contourner et rester cachés. La détection de ces attaques avancées et dissimulées nécessite d'adopter une approche plus proactive.

Grâce au Threat Hunting, des experts dédiés analysent en permanence les données à la recherche du moindre indice de menaces émergentes et d'attaques sophistiquées. Ces indices peuvent être le résultat de nouvelles tactiques, techniques et procédures (TTP) utilisées par les cyberattaquants, de l'utilisation d'identifiants volés pour se faire passer pour des utilisateurs légitimes, ou du détournement d'outils et de logiciels en local pour mêler des activités malveillantes aux tâches administratives quotidiennes de l'entreprise.

Tout service MDR qui ne combine pas détection humaine et prévention technologique risque de passer à côté des menaces connues survenant en périphérie et des attaques sophistiquées progressant dans l'ombre.

SURVEILLANCE ET INVESTIGATION 24 H/24 ET 7 J/7

Dès qu'une alerte a été créée, l'analyste en sécurité est chargé d'identifier les mesures à prendre pour y remédier. Certaines parties du processus d'analyse des cybermenaces peuvent être automatisées grâce à des techniques d'analyse comportementale ou en environnement sandbox, lesquelles permettent d'obtenir une recherche de menaces directement exploitable et des indicateurs de compromission personnalisés conçus pour les menaces auxquelles les entreprises sont confrontées.

Il est possible d'automatiser un grand nombre de tâches du processus d'analyse, mais pour apprécier véritablement la réalité, la portée et les incidences d'une attaque, une intervention humaine est nécessaire dans l'analyse des workloads automatisés.

Qui plus est, si un service MDR ne s'occupe que des alertes de sécurité les plus graves et ne tient pas compte des alertes de gravité moyenne et faible, son efficacité risque fort d'en pâtir. En effet, les attaques débutent bien souvent par une longue série d'incidents de faible gravité qui, s'ils ne sont pas interrompus, permettent aux cyberadversaires de s'infiltrer dans votre réseau et de s'y implanter. Un service MDR passe au crible la moindre détection ou alerte de sécurité (qui peut être le signe d'une attaque à plus large échelle) permettra de bloquer les intrusions au stade le plus précoce possible.

Détecter les attaques avancées et dissimulées nécessite d'adopter une approche plus proactive. Grâce à la traque des menaces, des experts dédiés analysent en permanence les données de sécurité des entreprises à la recherche du moindre indice de menaces émergentes et d'attaques sophistiquées.

CORRECTION ULTRAPRÉCISE

En cas d'alerte signalant une cybermenace avérée, une réponse à incident s'impose. Les étapes d'analyse et d'investigation doivent permettre d'obtenir le contexte nécessaire pour déterminer le type d'intervention à mettre en place.

La réponse à incident peut prendre de nombreuses formes, comme le retrait et l'isolement d'un endpoint compromis, dans le but de le rétablir à un état opérationnel antérieur. Pour de nombreuses entreprises, cela peut passer par la restauration d'une image sur cet endpoint. Toutefois, avec des informations contextuelles pertinentes, des analystes expérimentés et des outils efficaces, la correction peut rétablir le système à un état correct, et ce sans restauration de l'image système. Il s'agit là d'un atout majeur pour le fournisseur de services MDR, car l'incident peut être résolu sans intervention aucune du client. En plus de réduire les coûts et l'impact sur les activités, cette approche est plus rapide que la restauration complète de l'image d'un système.

La correction couvre l'étape finale de la réponse à incident, à savoir la reprise. Elle restaure les systèmes à leur état d'origine, tels qu'ils étaient avant l'attaque, en supprimant les logiciels malveillants, en nettoyant les entrées du Registre et en éliminant les intrus et les mécanismes de persistance. Cette étape finale est celle qu'il convient d'effectuer avec le plus grand soin. Dans le cas contraire, tout l'investissement réalisé lors des étapes précédentes d'un programme MDR n'aura, pour ainsi dire, servi à rien. Les cyberattaquants usent d'un nombre incalculable de techniques pour conserver l'accès au réseau une fois qu'ils sont parvenus à y pénétrer. Les tâches planifiées, les services de surveillance et les portes dérobées (backdoors) redondantes ne sont que quelques-unes des méthodes qu'ils utilisent pour s'assurer que leurs intrusions résisteront aux contremesures de quarantaine et de confinement de base.

Avec un éventail aussi varié de services relevant des MDR, il est essentiel de disposer d'une bonne compréhension des fonctionnalités à attendre en fonction des besoins spécifiques de votre entreprise.

QUELLES PERFORMANCES ATTENDRE DE VOTRE SERVICE MDR?

CrowdStrike a défini un nouvel indicateur en matière de cybersécurité, appelé « temps de propagation », sur la base de l'expérience acquise à aider des milliers d'entreprises à se protéger contre les menaces. Il s'agit du temps nécessaire à un intrus pour commencer à se déplacer latéralement en dehors de la tête de pont initiale, vers d'autres systèmes du réseau. En 2022, le temps de propagation moyen observé pour les cybercriminels était de 1 h 38 minutes.[5] Cette statistique ne donne toutefois qu'une image partielle de la situation : dans 36 % de ces intrusions, l'équipe OverWatch a observé que le cyberadversaire était parvenu à se déplacer latéralement vers d'autres hôtes en moins de 30 minutes.

En d'autres termes, le temps de propagation correspond à la fenêtre (étroite s'il en est) pendant laquelle une entreprise peut empêcher un incident de sécurité de se transformer en une véritable compromission. Le temps de propagation n'est évidemment pas le seul indicateur permettant de juger le degré de sophistication des cybercriminels, mais il constitue un moyen précieux pour les entreprises d'évaluer leurs capacités opérationnelles. Il est également utile pour les professionnels de la sécurité désireux d'évaluer leurs temps moyens de détection, d'investigation et de correction, appelés collectivement la « règle 1-10-60 ». CrowdStrike recommande ainsi aux entreprises d'œuvrer à atteindre les indicateurs de performances suivants :

- Détection d'une intrusion en 1 minute en moyenne
- Investigation et analyse en moins de 10 minutes
- Éjection du cyberadversaire en moins de 60 minutes

LA GARANTIE DE RÉSULTATS : UNE COMPOSANTE ESSENTIELLE POUR LES CLIENTS MDR

« Dans l'idéal, votre service d'intervention MDR doit intégrer la correction. Pour bloquer une intrusion avant qu'elle ne se transforme en compromission, il faut agir très vite. Cela peut nécessiter d'isoler un système affecté du reste du réseau, d'interrompre des processus en cours d'exécution, de supprimer des mécanismes de persistance du système de fichiers ou du Registre Windows, etc. »[2]

4 Blog Crowdstrike : Does Your MDR Deliver Outcomes — or Homework?
5 Global Threat Report 2023 de CrowdStrike

Les entreprises qui adoptent ce cadre ont plus de chances de pouvoir éjecter les cyberadversaires avant qu'ils ne s'étendent au-delà de leur point d'entrée initial, réduisant ainsi au maximum l'impact de l'intrusion. Les entreprises ont évidemment la possibilité d'ajuster le délai d'intervention cible selon leurs besoins spécifiques. Elles peuvent notamment tenir compte des types de cyberadversaires auxquels elles sont les plus susceptibles d'être confrontées, compte tenu de leur secteur d'activité et de l'orientation régionale de leurs opérations. Toutefois, par la mise en place d'une stratégie MDR, la règle 1-10-60 offre un cadre qui permet à n'importe quelle entreprise de disposer des fonctionnalités correspondant au niveau d'efficacité opérationnelle nécessaire pour lui permettre de bloquer les compromissions en toute confiance.

QU'ATTENDRE D'UN SERVICE MDR ?

Voici quelques questions à vous poser au moment de choisir un service MDR.

De quel type d'expertise disposent les analystes du service MDR ?
L'une des principales raisons d'investir dans un service MDR est de faire bénéficier votre personnel d'une expertise professionnelle, de compétences renforcées et d'un degré supérieur de maturité sans pour autant recruter de spécialistes particulièrement coûteux. CrowdStrike occupe une position privilégiée qui lui permet d'embaucher et de fidéliser des experts en Threat Hunting et des analystes en sécurité jouissant d'une vaste expérience de terrain dans tous les domaines, notamment le service public, le secteur privé, le renseignement et la défense. L'équipe de CrowdStrike fait montre d'une efficacité prouvée dans la recherche et la neutralisation des cybermenaces les plus sophistiquées.

Quel est le délai moyen d'intégration et d'adaptation de la solution MDR à vos besoins ?
Atteindre une certaine maturité en termes de sécurité n'est pas chose facile. Et vu le temps et l'énergie que demande la recherche d'une solution MDR adaptée, il est tout à fait légitime de s'attendre à une protection qui soit immédiatement efficace. Le délai qui sépare la prise de décision de la protection est généralement long et crée des failles de sécurité dans votre infrastructure. Avec CrowdStrike Falcon Complete, il s'écoule en moyenne 10 jours seulement entre les phases d'intégration et d'opérationnalisation, ce qui réduit considérablement la fenêtre de vulnérabilité de votre entreprise et vous permet de bénéficier au plus vite des avantages promis.

Quelles technologies préventives et automatisées sont intégrées à la solution MDR ?
Pour pouvoir répondre de manière adéquate aux besoins actuels et futurs de votre entreprise, votre solution MDR doit tirer parti de la puissance des technologies préventives et automatisées. Optimisée par l'architecture de sécurité cloud de CrowdStrike et des capacités d'intelligence artificielle inégalées, la plateforme CrowdStrike Falcon s'appuie sur des indicateurs d'attaque en temps réel, la recherche de menaces, l'évolution des techniques des cybercriminels et des données télémétriques enrichies récoltées à l'échelle de l'entreprise pour assurer une détection ultraprécise, une protection et une correction automatisées, un Threat Hunting de pointe et une observation priorisée des vulnérabilités. Elle permet en outre de bénéficier d'un déploiement rapide et évolutif, d'une protection et de performances de haut niveau, d'une complexité réduite et d'une rentabilité immédiate.

Votre service MDR s'accompagne-t-il d'une protection managée contre les menaces cloud liées à l'identité ?
Aujourd'hui, 80 % des compromissions impliquent des identifiants compromis. Mais malgré la prévalence des attaques basées sur l'identité, elles restent extrêmement compliquées à détecter grâce à des approches traditionnelles. Lorsque les identifiants d'un utilisateur valide ont été compromis et qu'un cyberadversaire usurpe l'identité de cet utilisateur, il est souvent bien difficile de différencier son comportement habituel de celui du cyberpirate. Falcon Complete Identity Threat Protection (ITP) comble cette lacune. Il s'agit du premier et du seul service de protection des identités entièrement managé qui offre une prévention fluide des menaces liées à l'identité en temps réel et sans interruption grâce à la mise en œuvre de règles pour les comptes managés et non managés, ainsi qu'à la gestion, la surveillance et la correction assurées par des experts.

MDR ET MSSP : QUELLE DIFFÉRENCE ?

De nombreuses entreprises se demandent si elles ont besoin d'un service MDR alors qu'elles font déjà appel à un fournisseur de services de sécurité managés (MSSP). Les offres des fournisseurs MSSP peuvent varier considérablement, mais en règle générale, elles se concentrent sur la gestion et la surveillance des outils de sécurité déployés au sein d'une entreprise. Cela comprend habituellement le tri de base des alertes de sécurité, ainsi que d'autres services tels que la gestion des technologies, des mises à niveau, de la conformité et des vulnérabilités.

Les fournisseurs de services MDR assurent quant à eux des services dont la portée est bien plus étroite et précise. Les services MDR permettent une intégration rapide et clé en main, généralement avec un dispositif technologique bien défini. Ils ont également des objectifs bien plus spécialisés, visant généralement à aider les entreprises à faire progresser leurs SOC dans différentes tâches du flux de détection ou d'intervention. Cette portée plus précise confère aux services MDR une valeur ajoutée immédiate, à faible coût et dans des délais très courts.

Votre service MDR bénéficie-t-il d'une recherche de menaces native et intégrée ?
Pour détecter et neutraliser le plus efficacement possible les menaces émergentes, les analystes en sécurité doivent disposer des connaissances les plus récentes sur les dernières tactiques, techniques et procédures utilisées actuellement par les cybercriminels. Les services MDR de CrowdStrike tirent parti des renseignements sur les menaces générés par l'équipe d'analystes experts en cybermenaces de CrowdStrike. L'équipe CrowdStrike Intelligence rassemble des chercheurs en sécurité, des anthropologues et des linguistes dont le rôle consiste à enrichir le processus MDR d'informations détaillées et mises à jour en continu sur les méthodes de plus de 200 cyberadversaires. Cette connaissance pointue des dernières tactiques, techniques et procédures permet à l'équipe CrowdStrike de mettre en place une détection et une intervention réellement efficaces.

De quelle manière votre fournisseur de services MDR compte-t-il communiquer avec votre équipe ?
Quel que soit le service MDR, il arrive toujours un moment dans le flux de détection, d'investigation ou d'intervention où vous devez reprendre les rênes. Communiquer ce transfert est un facteur de friction potentiel et peut entraîner l'introduction de nouveaux portails, consoles ou flux de travail susceptibles de ralentir les efforts d'intervention de votre équipe. Il est donc primordial d'utiliser une plateforme centrale qui permet une transmission fluide des informations entre le fournisseur de services MDR et le client. Le centre de messagerie de CrowdStrike réduit les frictions liées à la collaboration MDR et permet une communication fluide, transparente et sécurisée entre les analystes des services managés de CrowdStrike et les clients. Intégré à la plateforme Falcon, le centre de messagerie permet aux analystes de CrowdStrike de fournir aux clients des données en temps réel concernant les attaques en cours et les activités connexes. Les clients sont ainsi toujours tenus informés des intrusions et des mesures à prendre pour y remédier. Les communications étant bidirectionnelles, l'équipe CrowdStrike et les analystes du client peuvent dialoguer et collaborer librement au sein de la plateforme Falcon.

Parmi les différentes mesures et actions d'intervention, lesquelles incomberont au fournisseur de services MDR et lesquelles à vos équipes ?
Souvent trop vague, le concept d'« intervention » génère une confusion quant à la répartition exacte des tâches entre le fournisseur de services MDR et les équipes du client. Votre fournisseur de services MDR doit être en mesure d'isoler, de contenir et d'éradiquer le cyberattaquant de votre environnement. Pourtant, on observe généralement un transfert de responsabilité au niveau de la phase d'éradication, ce qui génère une charge de travail supplémentaire considérable pour le client. Falcon Complete gère cette dernière étape pour vous et va même plus loin en proposant, en plus de l'isolation et du confinement, une phase de correction. Nos équipes se chargent donc de supprimer les fichiers, artefacts et processus malveillants de l'environnement et de restaurer immédiatement votre infrastructure à un état opérationnel connu. Avec CrowdStrike, votre sécurité est donc assurée et votre charge de travail allégée.

Le service MDR est-il opérationnel 24 h/24 et 7 j/7 ?
Les cyberattaquants ne prennent pas de vacances, et votre service MDR ne devrait pas en prendre non plus. De nombreuses entreprises choisissent de mettre en place un service MDR en partie pour s'assurer une protection permanente contre les cybermenaces, surtout lorsque leurs équipes ne sont susceptibles d'être présentes que pendant les heures de bureau.

Le fournisseur de services MDR est-il en mesure de réduire vos risques tout en limitant vos coûts ?
Il est important de bien cerner les avantages que vous offrira votre solution MDR, notamment si elle vous aidera à réduire vos risques et à mieux comprendre l'impact des incidents sur les résultats financiers de votre entreprise. CrowdStrike n'a qu'une mission : bloquer les compromissions. Comme Falcon Complete gère le cycle de vie complet des incidents et assure la chaîne de responsabilité de tous les incidents de sécurité, les experts de CrowdStrike peuvent se consacrer exclusivement à la neutralisation des compromissions, 24 h/24 et 7 j/7. Qui plus est, une **étude d'impact économique menée par Forrester en 2021 à la demande de CrowdStrike** a démontré que Falcon Complete offre un retour sur investissement de 400 % et permet à votre entreprise d'économiser plus de 2 500 heures d'investigation par an.

Les services de correction ont pour but de restaurer de façon transparente les systèmes à leur état d'origine, tels qu'ils étaient avant une attaque, et ce en supprimant les logiciels malveillants, en nettoyant les registres, en éjectant les intrus et en éliminant les mécanismes de persistance — si possible en évitant d'avoir à restaurer les images de processus.

Quelles garanties avez-vous que le fournisseur de services MDR pourra assurer la protection de votre entreprise ?
En général, tous les fournisseurs de services MDR affirment pouvoir vous protéger des cyberattaques. Il ne faut donc pas hésiter à leur demander de vous en apporter la preuve. Si un fournisseur se montre réticent à prouver ses dires ou que sa démonstration n'est pas convaincante, la prudence est de mise. C'est pourquoi CrowdStrike a mis sur pied la **garantie de prévention des compromissions**. Le fait que CrowdStrike défende fermement l'efficacité de ses fonctionnalités de protection contre les compromissions, qui couvrent les coûts en cas de compromission, montre bien à quel point l'entreprise a confiance dans les capacités de son service MDR Falcon Complete à bloquer les compromissions.

Le service MDR a-t-il fait l'objet d'une validation indépendante ?
La procédure d'évaluation des solutions MDR est bien souvent fastidieuse et renvoie des messages contradictoires qui ne facilitent pas la prise de décision. Nombre d'entreprises semblent offrir les mêmes avantages et résultats. Dans le cadre de votre évaluation, il peut s'avérer utile de rechercher les validations indépendantes et d'utiliser ces analyses pour appuyer votre décision. CrowdStrike a été désigné leader dans les rapports de Forrester Wave et d'IDC MarketScape consacrés aux solutions MDR. Il a également obtenu la couverture de détection la plus complète lors des évaluations MITRE Engenuity ATT&CK® 2022 portant sur les fournisseurs de services de sécurité. Pensez à consulter les études de ces experts lors de l'évaluation des solutions MDR.

À quelle fréquence le fournisseur de services MDR intervient-il pour gérer, adapter et optimiser votre niveau de sécurité ?
L'amélioration et l'optimisation continues sont deux éléments indispensables dans la lutte contre les menaces actuelles. Face à des cyberadversaires qui gagnent quotidiennement en rapidité et en sophistication, il est absolument primordial que votre service MDR assure une part importante de la gestion et de l'adaptation de la plateforme, des règles et des processus en matière de détection et d'intervention managées. Cela garantira une optimisation cohérente du service qui sera alors en mesure de fournir des résultats probants en termes de neutralisation des compromissions.

FALCON COMPLETE : UNE SOLUTION MDR COMPLÈTE À L'EFFICACITÉ REDOUTABLE

CrowdStrike Falcon® Complete pour la détection et l'intervention managées (MDR) combine la puissance de la plateforme de sécurité Falcon, cloud native et à la pointe du secteur, avec l'efficacité, l'expertise et la protection 24 h/24 et 7 j/7 de l'équipe internationale d'experts en sécurité de CrowdStrike, qui surveille, trie et neutralise en continu les menaces ciblant les entreprises de nos clients.

Fonctionnalités	Service MDR Falcon Complete
Gestion, adaptation et optimisation 24 h/24 et 7 j/7	
Gestion par des experts	✓
Gestion proactive de la plateforme	✓
Conseiller en sécurité attitré	✓
Priorisation des groupes de ressources	✓
Expertise pluridisciplinaire	✓
Détection et prévention	
Surveillance continue avec visibilité en temps réel	✓
Investigation de toutes les détections (gravité faible/ moyenne/élevée/critique)	✓
Données, outils et processus spécialisés	✓
Protection managée des workloads cloud	✓
Prévention managée des menaces liées à l'identité	✓
Threat Hunting et recherche de menaces	
Recherche de menaces native et indicateurs de compromission intégrés	✓
Rapports de Threat Hunting trimestriels	
Visibilité totale sur l'arborescence de tous les endpoints	✓
Threat Hunting proactif par une équipe d'experts, 24 h/24 et 7 j/7	✓
Threat Hunting proactif par une équipe d'experts, 24 h/24 et 7 j/7	
Isolation et confinement de toutes les menaces	✓
Correction ultraprécise, interactive et proactive	✓

VOTRE SOLUTION MDR DOIT SOULAGER VOS ÉQUIPES, NON LES SURCHARGER

C'est au fournisseur de services MDR qu'incombe le plus gros du travail, non au client. Falcon Complete s'engage à fournir des résultats probants.

Lorsqu'un client fait appel à un fournisseur de services MDR, c'est avant toute chose pour éviter des compromissions préjudiciables. Comme de nombreux fournisseurs de services MDR ne sont pas en mesure de garantir cela, ils s'engagent à d'autres niveaux, en jouant par exemple sur la rapidité d'intervention des analystes en cas d'alerte critique. Si de tels accords de niveau de service (SLA) peuvent s'avérer utiles pour le suivi de l'efficacité à long terme ou peuvent effectivement limiter le risque de compromission en misant sur des délais d'intervention rapides, ils sont loin de remplir l'objectif premier recherché par les clients, à savoir bloquer les compromissions.

Falcon Complete intègre sa garantie hors pair de prévention des compromissions dès son déploiement. Celle-ci a pour but de rassurer les clients quant à la qualité des services et des résultats promis par CrowdStrike.

Il existe aujourd'hui un grand nombre de services MDR sur le marché. Si vous devez en choisir un pour aider l'équipe de sécurité de votre entreprise à remplir ses missions efficacement, il convient avant tout de bien connaître les capacités dont dispose votre équipe pour détecter, examiner et neutraliser les menaces, mais aussi ses faiblesses. Vous devez ensuite évaluer la capacité du service MDR à protéger à la fois les personnes, les processus et les technologies. Cela vous aidera à déterminer si vous hériterez en réalité d'une surcharge de travail en étant contraint d'effectuer des actions de suivi ou si vous pourrez compter sur votre fournisseur pour éradiquer et corriger les incidents, de même que neutraliser les compromissions qui menacent votre entreprise.

Demander une démonstration des services MDR Falcon Complete

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

À PROPOS DE CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq : CRWD), leader mondial de la cybersécurité, redéfinit la sécurité avec sa plateforme cloud native la plus avancée au monde, conçue pour protéger les ressources critiques des entreprises, à savoir les endpoints, les workloads cloud, les identités et les données.

Optimisée par l'architecture de sécurité cloud de CrowdStrike et une intelligence artificielle de pointe, la plateforme CrowdStrike Falcon® s'appuie sur des indicateurs d'attaque en temps réel, le renseignement sur les cybermenaces, l'évolution des techniques des cybercriminels et des données télémétriques enrichies récoltées à l'échelle de l'entreprise pour assurer une détection ultraprécise, une protection et une correction automatisées, un Threat Hunting de pointe et une observation priorisée des vulnérabilités.

Spécialement conçue dans le cloud au moyen d'une architecture à agent léger unique, la plateforme Falcon offre un déploiement rapide et évolutif, une protection et des performances de haut niveau, une complexité réduite et une rentabilité immédiate.

CrowdStrike : **We stop breaches.**

Suivez-nous : **Blog | Twitter | LinkedIn | Facebook | Instagram**