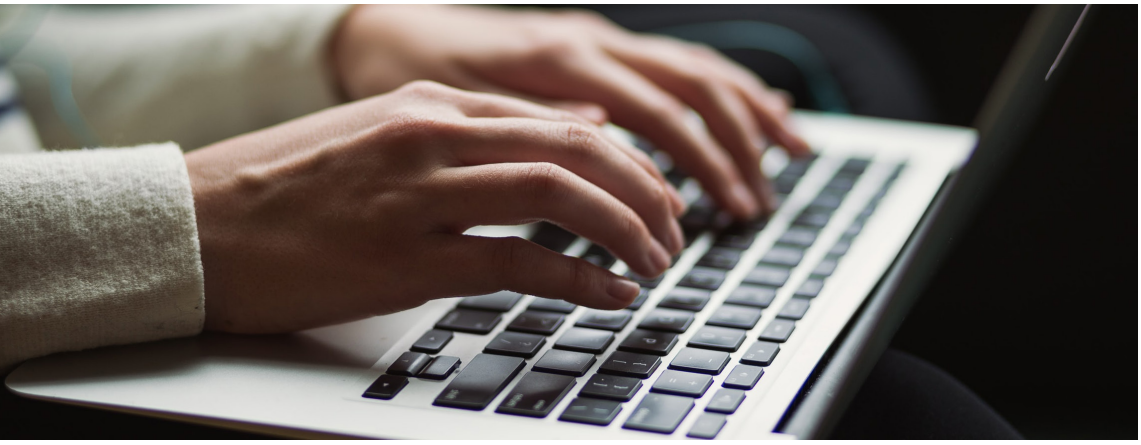
PRÉSENTATION DE SOLUTION

Secureworks®

Transformer la réponse aux incidents pour la préparation et la résilience



Le NIST définit la cyber-résilience comme « la capacité d'anticiper, de résister, de récupérer et de s'adapter à des conditions défavorables, un stress, des attaques ou des compromis sur des systèmes qui incluent des cyber-ressources »[1]. Cette définition souligne l'importance de dépasser la prévention de la sécurité pour adopter une stratégie qui repose non seulement sur la détection, mais aussi sur l'amélioration des fonctionnalités de réponse à l'échelle de l'organisation pour une réponse et une récupération plus efficaces.

Nouvelles réalités commerciales

Les responsables de la cybersécurité doivent aujourd'hui trouver un équilibre entre la cybersécurité et l'atténuation des risques d'une part, et les opérations commerciales et les efforts de transformation d'autre part. L'adoption accélérée de nouvelles technologies a donné lieu à un écosystème informatique de plus en plus complexe et à une surface d'attaque en expansion rapide. Si l'on ajoute à cela la pénurie de personnel et de compétences dans l'ensemble du secteur et des adversaires motivés qui évoluent rapidement, on comprend pourquoi 76 % des professionnels de la cybersécurité ont indiqué que la détection et la réponse aux menaces étaient plus ardues qu'il y a deux ans[2].

Dans ce nouvel environnement économique, reconnaître que les altérations ou les violations de données peuvent être inévitables est une condition fondamentale pour mettre en place un programme de réponse robuste et pour atteindre la cyber-résilience. Le cycle de réponse aux incidents (Secureworks Incident Response Life Cycle) (Figure 1) fournit un cadre pour

Le défi

Le rythme et l'ampleur du changement sont aujourd'hui sans précédent. Les organisations sont confrontées à des cyber-risques accrus, à mesure qu'elles adoptent des technologies destinées à permettre des opérations et des transformations commerciales qui attirent de plus en plus l'attention d'adversaires sans scrupule.

La solution

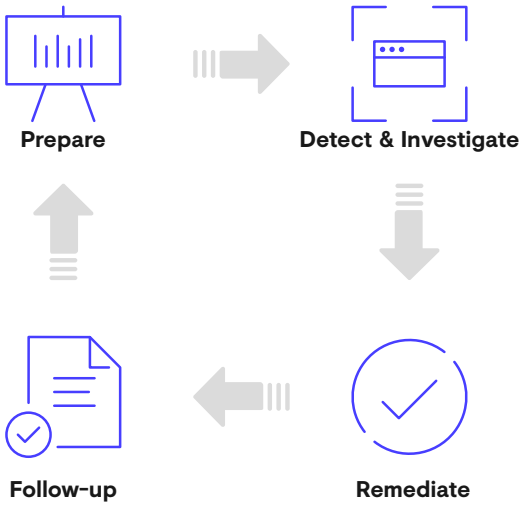
Le contrat Secureworks Incident Management Retainer est conçu pour aider les entreprises à repenser leur approche de la réponse aux incidents, en leur permettant d'adopter une approche globale et axée sur la résilience pour améliorer leur position de cyberdéfense, et en leur fournissant une assistance en cas d'urgence de cybersécurité.

[1] https://csrc.nist.gov/glossary/term/cyber_resiliency

[2] ESG Master Survey Results, The Threat Detection and Response Landscape, avril 2019

l'élaboration d'un programme de réponse aux incidents. Il souligne l'importance de coupler les fonctionnalités de réponse réactives et conventionnelles à une approche proactive et adaptative. Les activités de préparation et de suivi post-incident jouent un rôle essentiel dans la gestion efficace du risque de cybersécurité et, à terme, dans l'atténuation des interruptions et de l'impact durable sur les entreprises pendant et après les cyberincidents importants.

Figure 1. Cycle Secureworks de réponse aux incidents



Maturité de la réponse aux incidents

La préparation et la réponse proactive aux incidents étant reconnues comme des éléments essentiels du programme de cybersécurité d'une organisation, la préparation aux incidents devient l'un des principaux vecteurs de dépenses de sécurité[3]. Cependant, une récente étude ESG suggère que les organisations sont moins préparées aux incidents qu'elles ne le pensent[4].

L'étude montre que 92 % des personnes interrogées ont une opinion « bonne à excellente » de leur capacité à détecter rapidement les incidents et à y répondre. Seulement 68 % d'entre elles indiquent qu'elles ont mis en place un plan de réponse aux incidents. Elles sont encore moins nombreuses à l'exercer régulièrement[4]. Bien que des activités de préparation aient lieu, l'approche n'est souvent pas optimale pour renforcer la préparation et la résilience. Un examen plus approfondi de la préparation aux incidents montre une tendance aux activités tactiques, la conformité aux normes étant l'une des principales[4].

Les organisations peuvent faire améliorer leurs programmes et tirer davantage de valeur de la réponse proactive aux incidents en augmentant la fréquence et le périmètre des activités de préparation, tout en assurant une approche délibérée et organisée.

[3] Rapport ESG Research : Cybersecurity Services: omnipresent and heavily invested in, Déc. 2019
[4] ESG Master Survey Results, Incident Readiness Trends, août 2020

Comment Secureworks aide ses clients

Depuis plus de 14 ans, l'équipe Incident Response de Secureworks répond aux urgences en matière de cybersécurité et aide ses clients à s'y préparer. Au cours de cette période, notre équipe de réponse aux incidents a soutenu des milliers de projets de clients dans le monde entier. Nos consultants s'appuient sur plus de 20 ans d'expertise en sécurité opérationnelle de la société, une visibilité sur plus de 5 300 clients et plus de 20 ans de données d'attaques produites, analysées et validées par nos chercheurs et chasseurs de menaces Counter Threat Unit™ (CTU™).

Secureworks Incident Management Retainer

Le contrat Secureworks Incident Management Retainer est conçu pour permettre une approche complète et axée sur la résilience, afin d'améliorer votre position de cyberdéfense et de vous aider en cas d'urgence de cybersécurité. Secureworks propose un modèle par niveau qui s'adapte à vos objectifs métiers, tandis que les fonctionnalités avancées de gestion de programme fournissent l'expertise nécessaire pour définir et guider une approche proactive efficace.

Services de conseil proactifs

Le contrat Incident Management Retainer donne accès à un large éventail de services de conseil en matière de réponse aux incidents et de cybersécurité. Nos consultants s'appuient sur des années d'expérience et sur une connaissance approfondie des pratiques de pointe en matière de cybersécurité pour atténuer les risques et les impacts. Cette expertise est complétée par les connaissances collectives issues de milliers d'interventions, la toute dernière intelligence sur les menaces, les analytiques exclusives de cybersécurité et les méthodologies fondées sur les menaces. Une suite de services de préparation aux incidents fournit les éléments de base permettant d'élaborer et d'adapter un programme de réponse aux incidents et vos fonctionnalités de cyberdéfense.

Services de conseil et de préparation aux incidents

Animés par des experts de notre équipe de conseils proactifs en matière de réponse aux incidents.

Évaluez votre situation actuelle afin de renseigner la planification de la réponse et la conception du programme

Développez des plans, des politiques et des procédures de réponse aux incidents

Hiérarchisez les mesures et actions correctives

- **Évaluation de la préparation à la réponse aux incidents**
- **Développement/Vérification de la documentation sur la réponse aux incidents**

Ateliers et exercices

Dirigés par nos consultants en réponse aux incidents et nos chercheurs et chasseurs de menaces.

Découvrez les menaces et les pratiques d'excellence

Formez vos équipes aux procédures fondamentales

Passez en revue les enseignements tirés des précédents incidents

Entraînez-vous grâce aux scénarios et simulations fondés sur les menaces

- **Formation sur les notions de base de la réponse aux incidents**
- **Formation sur la sensibilisation et la préparation à la cybercriminalité**
- **Atelier sur les enseignements tirés**
- **Dossier d'information sur les menaces**
- **Dossier d'information sur la surveillance de la marque de l'exécutif**
- **Exercice de simulation**
- **Exercice fonctionnel**

Services de test et de validation

Assurés par notre équipe en charge des tests de sécurité contradictoires et les chasseurs de menace des équipes de réponse aux incidents et des opérations spéciales CTU.

Testez les systèmes, les applications, les personnes et les équipes

Identifiez la présence d'un acteur de menace existant

Remédiez aux lacunes et aux faiblesses

- Évaluation de la chasse aux menaces
- Test d'intrusion
- Tests de la sécurité des applications
- Tests « Red Team »
- **Gestion des failles de sécurité**

Fonctionnalités de gestion de programme

Outre des contrats de niveau de service (SLA) améliorés pour les réponses d'urgence, les programmes de gestion des incidents Secureworks Essential et Essential Plus comprennent des fonctionnalités avancées visant à garantir et à guider l'avancement et la gouvernance du programme. Ils comprennent à la fois des ateliers de prise en main et des contacts réguliers avec les experts en réponse aux incidents de Secureworks pour planifier, suivre les progrès et examiner la participation inter-organisationnelle à tous les niveaux, avant, pendant et après les urgences de cybersécurité.

Grâce à l'atelier annuel de planification de l'IMR (**Annual IMR Planning Workshop**), Secureworks aide à préparer une réponse efficace et efficiente en comprenant d'emblée les objectifs et la stratégie de cybersécurité de votre organisation.

- La formation sur les notions de base de la réponse aux incidents examine le processus de traitement et d'escalade des incidents, assure l'alignement de l'équipe d'intervention de Secureworks avec vos plans et processus existants, et identifie proactivement tous les domaines susceptibles d'entraver une intervention rapide et efficace.
- La formation sur la planification proactive des services (Proactive Services Planning) est l'occasion de discuter des objectifs et de la stratégie de cybersécurité de votre organisation afin de développer conjointement un plan proactif et une feuille de route définie mutuellement, pour tirer parti des services proactifs de Secureworks.

La formation sur les **révisions trimestrielles des services** (Quarterly Services Reviews) permet des interactions régulières avec les experts de l'équipe Secureworks Incident Response afin d'examiner les résultats, de fournir des recommandations et d'apporter des ajustements à la feuille de route des services proactifs. Notre programme Essentiel Plus comprend un Executive Briefing annuel à l'intention des dirigeants, donné par un membre senior de l'équipe de réponse aux incidents de Secureworks. Ce briefing, qui s'adresse à un public de cadres, vise à communiquer les idées, les progrès et les mises à jour dans le contexte des cyber-risques.

Réponse d'urgence aux incidents

Lorsqu'une urgence en matière de cybersécurité se produit, le contrat de gestion des incidents Incident Management Retainer prévoit des contrats de niveau de service (SLA) pour garantir une assistance rapide de la part des intervenants mondiaux en charge des incidents, qui sont prêts à intervenir dans divers scénarios de cybermenace. Le programme Secureworks de réponse d'urgence aux incidents (Emergency Incident Response) fournit une assistance pour divers types d'incidents, qu'il s'agisse de problèmes mineurs liés à un seul système informatique ou de situations de crise à grande échelle ou à l'échelle de l'entreprise, qui perturbent ou entravent considérablement les activités de l'entreprise.

Notre approche est collaborative et interactive. Nous collaborons avec votre équipe pour évaluer, comprendre et gérer la situation afin que vous puissiez prendre les mesures appropriées, et minimiser la durée et l'impact commercial d'une urgence en cybersécurité. Notre équipe fournit des fonctionnalités de criminalistique numérique, d'analyse des logiciels malveillants et d'intelligence sur les menaces, ainsi que les conseils et l'assistance nécessaires pour étudier et analyser les menaces, et y remédier rapidement.

L'équipe Secureworks Incident Response dispose des outils nécessaires pour fournir à votre organisation une assistance transversale à la direction des équipes de gestion des incidents afin de s'assurer que toutes les parties prenantes de la réponse à l'incident coordonnent leurs efforts et de mener tous les participants vers des objectifs de réponse définis conjointement.

Pour télécharger une fiche technique sur le programme **Incident Management Retainer**, **cliquez ici**

Si votre organisation a besoin d'une assistance immédiate, appelez notre **hotline mondiale de réponse aux incidents disponible 24x7** : **+33-0800-91-57-18**

Pour plus d'informations, composez le **1-877-838-7947** pour échanger avec un spécialiste Secureworks en charge de la sécurité **secureworks.com**

À propos de Secureworks
Secureworks® (NASDAQ : SCWX) est un leader mondial de la cybersécurité qui protège les avancées des clients grâce à Secureworks® Taegis™. Cette plateforme Cloud native d'analytique de la sécurité s'appuie sur plus de 20 ans de recherche et d'intelligence sur les menaces réelles pour améliorer la capacité des clients à détecter les menaces avancées, à rationaliser les investigations et collaborer à leur réalisation, et à automatiser les mesures appropriées.