kaspersky BRING ON THE FUTURE

Vous créez votre propre SOC ? Évitez cet écueil courant

À l'origine, le centre opérationnel de sécurité (SOC) était à la sécurité ce que le centre de contrôle était au voyage dans l'espace. Mais les temps ont changé. Aujourd'hui, le SOC est rationalisé, il inclut plusieurs composants de cybersécurité très efficaces et parfaitement intégrés, et il propose un champ d'action et des indicateurs qui ne pourraient être obtenus par une approche plus appropriée. Le SOC est une fonction centralisée pour la surveillance et l'analyse des menaces en continu, ainsi que pour l'atténuation et la prévention des incidents de cybersécurité.

Le rêve, n'est-ce pas ?

Mais aucun CISO de grande entreprise sensé n'investirait dans un simple rêve. Si la mise en place et l'exploitation d'un SOC interne sont clairement un objectif commun aux entreprises matures sur le plan informatique, au vu des conditions actuelles du marché mais aussi du panorama des menaces, la réalité est parfois en demi-teinte.

Écueils et approches fréquentes

Dans cet article, nous dévoilerons les écueils les plus courants auxquels sont confrontées les entreprises qui font le choix de créer leur propre SOC. Mais intéressons-nous d'abord à la façon dont les entreprises abordent ce casse-tête que peut être le SOC à l'heure actuelle.

Créer un SOC interne n'est pas toujours la solution la plus indiquée, car les organisations n'ont pas toutes les ressources nécessaires ne serait-ce que pour gérer la quantité d'alertes de menace générée. Rien de surprenant donc à ce que de nombreuses organisations choisissent d'externaliser les fonctionnalités SOC à un partenaire externe de confiance, libérant ainsi des collaborateurs cruciaux du service de sécurité informatique pour qu'ils se concentrent sur des tâches qui requièrent réellement leur attention directe.

SOC hybride : le meilleur des deux mondes ?

Une alternative consiste à adopter une approche hybride : employer des collaborateurs internes pour optimiser les ressources et maximiser l'expertise spécifique à l'entreprise, et faire appel à un partenaire externe pour les tâches plus communes (ou génériques). Il faut bien comprendre que l'approche hybride doit être holistique pour garantir la sécurité de l'organisation à 360 degrés, afin qu'il n'y ait jamais d'interruption et que rien ni personne ne puisse se faufiler dans les failles entre les services internes et les prestations externes.

La popularité croissante de l'approche hybride face au SOC interne est un signe évident de l'écueil dont nous allons parler aujourd'hui : les collaborateurs. Pour être exact, ce ne sont pas les collaborateurs eux-mêmes le problème, mais plutôt la difficulté à les trouver, à les recruter, à les former et à les retenir.

C'est tout bonnement impossible !

Un bref coup d'œil à la cartographie Cyberseek de l'offre et de la demande en cybersécurité vous permettra de comprendre en quoi c'est un problème. En janvier 2022, le rapport offre/demande était de 68 %, un chiffre qui n'a guère varié au cours des dernières années (et qui variera probablement peu dans les années à venir).

Si l'on se plonge dans les statistiques de Cyberseek, un domaine de compétences occupe clairement la première place de la liste des offres d'emploi non pourvues : l'opération et la maintenance, soit exactement le domaine d'expertise dans lequel vous souhaiterez recruter pour exploiter le SOC flambant neuf dans lequel vous venez d'investir.

Malheureusement, cet écueil (ignorer la dure réalité de la pénurie de compétences lors de l'élaboration de sa stratégie SOC) est de plus en plus redoutable. En effet, le volume, la complexité et la gravité des cybermenaces actuelles ne cessent de croître, ce qui pèse encore davantage sur les fardeaux que sont la documentation des processus, la mise en œuvre de technologies de base, etc. En bref, comment instaurer un SOC si vous ne parvenez pas à réunir une équipe capable de s'en occuper ?

En l'absence de solution à ce problème, même le SOC le plus complet pourrait n'être finalement qu'un « éléphant blanc », un investissement onéreux sans aucun bénéfice.

Les composants essentiels de votre SOC

- **Compétences**

Votre équipe SOC doit monter en compétence sur le terrain pour suivre l'évolution du panorama des menaces et protéger vos investissements dans les technologies du SOC

- **Threat intelligence**

Un SOC efficace est un SOC bien informé. Pour cela, il est absolument vital de disposer d'une Threat Intelligence précise, pertinente et contextuelle qui doit être disponible dans des formats compatibles avec les autres composants du SOC

- **Threat hunting**

La recherche proactive, plutôt que la découverte, est essentielle. Votre SOC doit être capable de détecter des campagnes de cyberespionnage et de cybercriminalité, ainsi que celles commanditées par les États, aussi bien nouvelles que notoires, visant vos systèmes d'information stratégiques, et ce en temps réel et sans interruption.

- **Analyse des programmes malveillants et cyberdiagnostic**

Recueillir des éléments de preuve et identifier les menaces n'est que la première étape. Votre SOC doit être capable d'analyser le comportement spécifique d'échantillons de programmes malveillants, de révéler le schéma complet de tout incident et d'appliquer efficacement les enseignements tirés

- **Évaluations de la sécurité**

L'environnement réel de votre SOC doit être soumis à des évaluations régulières de la sécurité afin de tester l'intégrité et l'efficacité de vos systèmes d'information

- **Tests de pénétration et exercices de simulation**

Les démonstrations pratiques de scénarios d'attaque possibles, informées par une Threat Intelligence contextuelle et pertinente, sont essentielles à l'évaluation précise du niveau actuel de préparation face aux incidents

Recruter dans votre SOC

Comme nous l'avons déjà évoqué avec la pénurie de compétences en cybersécurité à l'international, sans surprise, bon nombre de grandes entreprises considèrent le recrutement comme une difficulté majeure (si ce n'est la première d'entre elles) lors de la mise en place d'un SOC interne. Votre candidat idéal, qui possède déjà les compétences SOC adaptées à votre organisation, est souvent hors d'atteinte. Beaucoup d'organisations choisissent de former et de promouvoir des collaborateurs déjà présents en interne afin de combler les lacunes et de maintenir une continuité pendant la mise en place du SOC interne.

La concurrence débauche les effectifs de votre SOC ?

Malheureusement, retenir de tels collaborateurs est souvent difficile face à l'attrait d'une promotion externe. Il n'existe pas un seul CISO sur cette planète qui n'ait jamais connu la frustration de former quelqu'un pour un poste au sein du SOC interne, pour finalement le voir partir pour une meilleure rémunération.

Les cybercontraintes de la pandémie n'ont fait qu'accroître l'engouement pour la création de SOC internes, et l'on comprend aisément que le marché soit si enthousiasmé par le pouvoir que lui confère sa capacité à concrétiser de telles promesses au sein d'une entreprise.

Chez Kaspersky, nous comprenons les enjeux de la mise en place et de l'exploitation d'un centre opérationnel de sécurité interne. Et nous sommes extrêmement fiers des immenses progrès réalisés par les multinationales en matière de lutte contre les APT et autres menaces similaires lorsqu'elles décident de mener ce combat en interne.

C'est pourquoi nos services de conseil en SOC sont un pilier central de notre contribution à la lutte mondiale contre les cybermenaces avancées. Forts de plus de 20 années de recherche permanente de menaces, de technologies de protection leaders du marché, d'une expertise reconnue et d'une expérience éprouvée dans les projets de cybersécurité complexes, nous sommes à même de libérer le potentiel de votre SOC à tous les niveaux pour gagner en efficacité afin de vous protéger contre des menaces de plus en plus sophistiquées.

Le SOC Kaspersky, quant à lui, répond aux difficultés rencontrées par les entreprises particulièrement matures sur le plan informatique en leur fournissant l'expertise externe dont elles ont besoin pour s'assurer du retour sur cet investissement stratégique. Nous mettons à votre service nos connaissances (dont la Threat Intelligence) et nos équipements (dont une plateforme XDR unifiée), et nous nous engageons à développer les qualités de vos précieux collaborateurs afin que vos compétences internes soient toujours parfaitement alignées avec les caractéristiques internes avancées de votre propre SOC.

Adaptez la conception à l'équipe dont vous disposez, et attirez l'équipe dont vous avez besoin

Mais précipiter la mise en œuvre d'un SOC sans avoir résolu la question des effectifs est un écueil dans lequel les entreprises ne peuvent pas se permettre de tomber. Les responsables informatiques en entreprise doivent impérativement tenir compte des ressources humaines lorsqu'ils élaborent leur stratégie en vue de la création d'un SOC. Ne pas adapter les tâches impliquées dans l'exploitation et la surveillance du SOC à la disponibilité des compétences en cybersécurité est une erreur critique qui coûte cher.

Si vous êtes en mesure d'attirer les effectifs dont vous avez besoin pour gérer votre SOC interne, nous vous recommandons fortement de rechercher les compétences et les qualités suivantes :

- **Un esprit naturellement curieux**

Recherchez des collaborateurs qui sont naturellement enclins à chercher des réponses qui ont du sens dans un fatras de données fragmentées

- **Une faculté de concentration en situation de stress**

L'environnement SOC peut être éprouvant. Vous aurez besoin de collaborateurs dotés d'une capacité de concentration à toute épreuve, même sous une pression extrême (en cas d'incident)

- **D'excellentes connaissances en cybersécurité combinées à une vaste expérience pratique**

Au risque de paraître excessif, le SOC est le théâtre d'une guerre virtuelle. Vos collaborateurs SOC sont vos forces vives : ils devront être parés au combat et parfaitement entraînés

Si vous recherchez et renforcez ces qualités au sein de votre équipe SOC, vous vous rendrez compte que vous n'instaurez pas seulement un centre de sécurité, mais toute une culture d'entreprise positive qui attire et retient les collaborateurs dont vous avez besoin. Si vous recherchez et renforcez ces qualités, vous créerez une nouvelle réalité qui valorise la contribution de précieux experts en sécurité informatique. Dans cette culture, tout le monde est gagnant.

En savoir plus sur [les services de conseil en SOC de Kaspersky et/ou le SOC Kaspersky]

Actualités sur les cybermenaces : www.viruslist.fr
Actualités dédiées à la sécurité informatique : business.kaspersky.com
Sécurité informatique pour les PME : www.kaspersky.fr/small-to-medium-business-security
Sécurité informatique pour les entreprises : www.kaspersky.fr/enterprise-security
Portail de Threat Intelligence : opentip.kaspersky.com
Interactive Portfolio Tool (outil de catalogue interactif) : www.kaspersky.com/int_portfolio/fr

www.kaspersky.fr

Reconnu. Indépendant. Transparent. Nous nous engageons à construire un monde plus sûr où la technologie améliore notre vie. C'est pourquoi nous la sécurisons, afin que le monde entier dispose des possibilités infinies qu'elle nous offre. Adoptez la cybersécurité pour un avenir plus sûr.

Pour en savoir plus, rendez-vous sur www.kaspersky.fr/about/transparency

Proven.
Transparent.
Independent.