6 conseils pour créer un centre d’opérations de sécurité physique

Depuis que j’ai quitté l'armée britannique il y a cinq ans pour travailler dans le domaine de la sécurité des entreprise et de la gestion des risques, j’ai entendu de nombreux dirigeants plaider en faveur ou en défaveur de la création d’un centre des d’opérations de sécurité (en anglais : Security Operations Center ou SOC). Bien que les bénéfices d’un SOC soient évidents, à commencer par une sécurité renforcée et une meilleure visibilité des risques, toutes les entreprises ne ressentent pas le besoin de centraliser leurs opérations de sécurité ou ne sont pas prêtes à le faire.

Celles qui le sont entrent généralement dans l’une des deux catégories suivantes :

1. Elles ont atteint une taille critique en termes d’infrastructure, de personnel mais aussi de réputation, et nécessitent désormais une surveillance et un contrôle accrus.

2. Elles s’appuyaient auparavant sur un réseau de responsables de la sécurité au niveau régional et national pour identifier et gérer les risques au niveau local, mais ont désormais besoin d’une approche centralisée.

Les évènements et les défis de ces dernières années, qu’il s'agisse de l’augmentation des nouveaux risques dus à la pandémie de COVID-19 ou à la multiplication et à la sophistication des cyberattaques, plaident également en faveur de la mise en place d’un SOC.

Toutefois, mon expérience m’a appris que la mise en place d’un SOC nécessite avant tout que les responsables de la sécurité et des risques adoptent le bon état d’esprit. Vous trouverez ci-dessous six conseils clés pour vous aider à y parvenir. Gardez à l’esprit qu’il ne s’agit pas d’une liste exhaustive, mais plutôt d’un aperçu rapide de ce que vous, en tant que professionnel de la sécurité et des risques, devez savoir et faire pour centraliser vos opérations de sécurité.

© Dataminr 2022. PZ032422

Dataminr

N°1 : partez du principe que rien n'est acquis d'avance

Vous disposez probablement d'un réseau de sécurité existant sur lequel ou autour duquel vous pouvez construire votre SOC. Cependant, votre SOC représentera un nouveau modèle opérationnel avec de nouvelles méthodes de travail. Ne présumez donc pas que tous les employés de votre entreprise comprendront ce qu'est un SOC ou en quoi consiste que son rôle.

Au contraire, partez du principe que personne ne sait ce qu'est un SOC ni comment vous allez le créer. Dès le départ, essayez d'obtenir l'adhésion de toutes les parties prenantes du projet. Définissez vos messages avec soin et établissez des lignes de communication claires entre l'équipe en charge du SOC, les principaux services ainsi que les partenaires de votre entreprise.

N°2 : insistez sur l'importance de la rapidité et de la précision

Pour être performant, un SOC doit disposer d'informations précises en temps réel. Cependant, il peut être difficile de tester pleinement la précision et la rapidité des informations avant l'activation d'un SOC, et les dirigeants doivent être prêts à ce que des défaillances failles soient révélées en temps réel. Bien qu'il s'agisse de l'un des plus grands défis liés à la mise en place et au fonctionnement d'un SOC, c'est aussi l'un des plus faciles à résoudre.

Ne partez pas du principe que chaque information qui entre dans le SOC ne sera connue qu'au sein du SOC. Cette erreur fréquente a pour effet la rétention d'informations, par peur de déranger d'autres personnes. Pour l'éviter, acceptez que plusieurs petits dérangements vaillent toujours mieux qu'une grande déconvenue. Et faites-en un principe pour toute votre équipe.

Mettez en place des pratiques d'excellence. Déterminez par exemple :

- ce qui doit être fait immédiatement avec les informations
- quels sont les deuxièmes et troisièmes effets d'une décision
- qui d'autre dans l'entreprise, en dehors de l'écosystème de sécurité immédiat, doit connaître ces informations

N°3 : accordez de l'importance à la technologie. Et encore plus aux gens.

Il existe un éventail semble-t-il infini de technologies habilitantes pour les opérations de sécurité. Mais lorsqu'elles sont associées à des systèmes de surveillance interne, les technologies peuvent donner l'impression que ce sont elles qui mènent les opérations, plutôt que l'inverse. Gardez le contrôle en déterminant :

- ce qu'il faut pour créer ou conserver un certain degré d'anticipation

© Dataminr 2022. PZ032422

- ce qu'il faut pour identifier les événements au moment où ils se produisent
- comment permettre aux informations et aux renseignements de circuler, en associant ressources technologiques et humaines

Dans un monde idéal, l'intégration de la technologie serait parfaite, les flux de travail seraient continus et les informations ne se chevaucheraient pas... Malheureusement, les choses se passent rarement ainsi. Disposer d'un objectif ultime, d'un modèle opérationnel et d'une architecture de systèmes clairement définis et répartis autour des différentes personnes de votre SOC vous permettra de prendre vos décisions de façon éclairée.

n°4 : apportez de la valeur ajoutée

La sécurité est un centre de coût. La première question que se poseront les dirigeants de votre entreprise sera certainement « Combien ça coûte ? » Pour que cette conversation tourne à votre avantage, préparez un business plan qui détaille la véritable valeur d'un SOC dans l'ensemble de l'entreprise. Il est crucial d'aller au-delà de votre équipe et d'identifier les opportunités qui peuvent être communes à d'autres services de l'entreprise.

Voici les questions clés qui permettent de déterminer la valeur ajoutée d'un SOC :

- Où créer des relations, tangibles et intangibles, pour contribuer à l'analyse de rentabilité ?
- Comment aider les autres services de l'entreprise à fournir plus efficacement de la valeur sans menacer leurs propres compétences ou capacités ?
- Comment avec un peu d'imagination, exploiter une capacité existante et mettre en place des partenariats pour la soutenir ?

À première vue, il y a de fortes chances que la centralisation des opérations de sécurité et les gains d'efficacité qui en découlent donnent l'impression que la plupart des coûts d'un SOC seront couverts. Mais cette hypothèse coûtera plus cher que vous ne le pensez, surtout avec une sécurité 24 heures sur 24 et 7 jours sur 7. C'est pourquoi il est important de détailler la valeur apportée par votre SOC, et ce le plus clairement possible.

N°5 : intégrez la redondance dès le départ

On vous demandera inévitablement de faire plus que ce dont vous êtes capable. Cela signifie qu'il sera nécessaire de réserver du temps à votre équipe pour qu'elle traite les informations et réfléchisse de façon critique à leur impact. Les équipes qui fonctionnent sous une pression extrême ou qui travaillent en permanence commettent des erreurs et passent à côté de certaines choses.

© Dataminr 2022. PZ032422

Or, votre SOC ne peut se permettre ni l'un ni l'autre, surtout dans les premiers temps. Mais il faut du temps pour apprendre, ajuster et optimiser les nouveaux systèmes et flux de travail. Alors intégrez suffisamment de redondance opérationnelle afin de donner à votre équipe le temps nécessaire pour adapter ses capacités en fonction de la fluctuation des demandes. Elle sera alors en mesure de s'adapter ou d'accélérer le rythme de fonctionnement du SOC lorsqu'une crise surviendra.

N°6 : créez un SOC prêt pour les défis de demain

Il existe de nombreux débats sur l'opportunité de combiner les SOC de cybersécurité et les SOC de sécurité physique. J'ai déjà eu l'occasion de participer à quelques-unes de ces conversations et je sais, pour l'avoir vécu, combien il peut être compliqué de faire converger deux SOC distincts. Car ils sont construits sur des principes différents, segmentés par des fonctions différentes, peuvent se trouver dans des lieux différents et fonctionner sur la base de procédures opérationnelles différentes.

Lorsque vous créez votre SOC, pensez à la manière dont il pourrait devoir répondre aux futurs besoins de votre entreprise. Une technologie adaptée aujourd'hui ne le sera peut-être plus demain. L'argent économisé en investissant dans une technologie suffisante aujourd'hui mais potentiellement insuffisante demain peut vous obliger à repenser toute votre stratégie de sécurité.

Créez une feuille de route pour votre SOC et examinez celles de vos partenaires et fournisseurs. Ensuite, posez-vous les questions suivantes :

- mon entreprise est-elle susceptible de faire converger cybersécurité et sécurité physique dans un avenir proche ?
- comment faire avancer la conversation sur la convergence ?
- comment initier ou accélérer le changement plutôt que d'en bénéficier simplement ?

Plus important encore, comment protéger votre SOC contre les perturbations ou les risques majeurs à venir ?

Al Bowman est responsable des comptes d'entreprise chez Dataminr. Avant de rejoindre Dataminr, il a conçu, développé et dirigé le Centre de services de renseignement de Deloitte à Londres. Avant cela, il a servi dans l'armée britannique, où son dernier poste a été celui de directeur du centre mondial des risques et du renseignement de l'armée.

© Dataminr 2022. PZ032422

Dataminr