PLANIFIER ET METTRE EN PLACE VOTRE SOC

Bonnes pratiques pour la création d'un centre des opérations de sécurité (SOC) physique

DATAMINR PULSE

Introduction

Vous et votre équipe avez été chargés de mettre en place le premier centre des opérations de sécurité (SOC) physique de votre entreprise. Le projet est doté d'un sponsor exécutif, d'une étude de rentabilité et d'un budget solides, et vous êtes impatient(e) de construire un SOC performant pour faire face aux risques toujours plus complexes auxquels votre entreprise fait face. Ce livre électronique est conçu pour vous aider à réfléchir au personnel, aux processus, à la technologie et aux indicateurs de performance nécessaires à la création d'un SOC.

Les incidents à risque comme catalyseurs de l'action

Avant de prendre la décision de développer leur premier SOC, de nombreuses entreprises ont déjà connu un incident à risque, auquel leur équipe de sécurité physique a eu du mal à répondre. Ces incidents peuvent inciter la direction d'une entreprise à agir, et servent de base à l'analyse de rentabilité en faveur d'un investissement supplémentaire dans le service de sécurité de l'entreprise.

Voici quelques exemples d'événements à risque que nous avons pu observer chez nos clients et qui les ont tous conduits à créer leur premier SOC:

- Le PDG d'une entreprise était en réunion dans une succursale lorsqu'il a entendu des coups de feu à l'extérieur du bâtiment. Les agents de sécurité contractuels sur place ont verrouillé les portes des locaux en demandant aux gens de rester à l'intérieur, mais la situation était confuse et les employés avaient peur. Le PDG a ensuite appelé l'équipe de sécurité de l'entreprise, qui ignorait totalement qu'il y avait eu une fusillade à proximité des locaux.

- Un important tremblement de terre a secoué Mexico en 2017, détruisant des dizaines de bâtiments et tuant plusieurs centaines de personnes. Une grande entreprise américaine, implantée dans plusieurs zones de Mexico, a tenté de recenser rapidement les employés et les cadres concernés. Les informations dans la presse ont pris du temps à arriver et ne présentaient pas le niveau de détail dont l'équipe de sécurité avait besoin pour planifier ses mesures d'évacuation.

- Au cours des premières semaines de la pandémie de COVID-19, les commerçants ont dû faire face à une accumulation de règles sanitaires locales et nationales en constante évolution. Un géant américain de la distribution a rencontré des difficultés à dresser un tableau complet des restrictions réglementaires affectant ses magasins dans tout le pays. Par ailleurs, l'équipe de direction du distributeur a demandé à l'équipe de sécurité des rapports de situation quotidiens sur le nombre de cas de COVID-19, ce qui s'est avéré difficile à réaliser manuellement à partir de sources publiques.

La manière dont vous concevrez votre centre opérationnel de sécurité dépendra du budget, du profil de risque et des objectifs de votre organisation. Toute équipe de sécurité centralisée d'une entreprise présente quatre caractéristiques communes, quels que soient sa taille, son secteur d'activité ou son domaine de responsabilité:

- **Les informations en temps réel sont transmises à** l'équipe de sécurité et constituent un élément crucial pour la prise de décision
- **Les analystes étudient les** informations en temps réel et décident des mesures à prendre pour réduire les risques
- Les mesures de réduction des risques entrent dans des **processus** de flux de travail qui sont reproductibles, évolutifs et quantifiables
- L'équipe rend compte de **l'impact du SOC à l'entreprise** afin de stimuler les investissements dans le programme

En dépit de ces caractéristiques communes, il n'y a pas de solution « clés en main » pour concevoir ou développer un service de sécurité centralisé. La taille et les responsabilités du service de sécurité centralisé de votre organisation dépendront du profil de risque spécifique de votre entreprise, de sa tolérance au risque, de son leadership, de sa culture d'entreprise et d'autres facteurs.

Dataminr travaille en étroite collaboration avec des centaines de SOC parmi les plus performants au monde, ce qui nous permet d'avoir une vision unique des bonnes pratiques du secteur.

Nous avons vu des entreprises de taille similaire, dans le même secteur d'activité et avec un profil de risque comparable, concevoir leur équipe de sécurité centralisée de manière totalement différente. Dans un cas, une entreprise A a opté pour un grand centre des opérations de sécurité mondial, tandis qu'une entreprise B a privilégié une approche décentralisée, avec de petites équipes régionales intervenant chacune de façon autonome.

Au-delà de ces différences opérationnelles majeures, l'information en temps réel est indispensable aux équipes de sécurité afin qu'elles puissent assurer la sécurité de leur personnel et de leurs biens.

Examinons de plus près les différentes composantes d'une équipe de sécurité centralisée.

L'information en temps réel

Les informations en temps réel provenant de sources internes et externes constituent la pierre angulaire d'une équipe de sécurité performante. L'information en temps réel désigne les informations concernant un incident à risque spécifique et fournies le plus rapidement possible après l'événement initial, souvent, en quelques secondes.

Les informations peuvent provenir de plusieurs sources:

- D'outils internes:
  - Systèmes de contrôle d'accès
  - Vidéosurveillance
  - Dispositifs de sécurité des réseaux
- De circuits de communication directs avec l'entreprise:
  - Alias dédiés de messagerie sécurisée
  - Applications de sécurité
  - Outils de discussion instantanée
  - Numéro d'appel disponible 24 h/24 et 7 j/7
- De sources externes d'informations et d'actualités:
  - Outils de surveillance des réseaux sociaux
  - Fils d'actualité
- Plateformes d'information en temps réel telles que Dataminr Pulse

Ensemble, ces sources d'information en temps réel donnent aux équipes de sécurité – de l'analyste au chef de la sécurité (CSO) – une vision globale de l'ensemble des risques auxquels est exposée leur organisation. En période de crise, les équipes de sécurité sont évaluées en fonction de la qualité des informations en temps réel dont elles disposent et de leur rapidité à traiter ces informations et à réagir pour préserver la continuité des activités.

Les informations en temps réel sont transmises à d'autres plateformes de technologie au sein du SOC, telles que:

- Une plateforme de surveillance des risques intégrant des zones d'intérêt spécifique
- Une cartographie SIG et visualisation des données
- Un système de gestion des tickets de réponse aux incidents et du flux de travail
- Des outils de communication de masse
- Des plateformes d'information touristiques
- Un logiciel d'alerte de cybersécuritéC

Éléments clés pour l'élaboration d'un centre des opérations de sécurité - Planifier et mettre en place votre SOC

À LIRE ICI

L'intelligence artificielle intégrée au SOC

Combien de temps vos analystes sécurité consacrent-ils à la collecte d'informations ? Dataminr Pulse utilise l'intelligence artificielle pour aider vos analystes à réduire le temps passé à chercher des informations et en gagner pour les traiter.

En traitant à grande échelle plus de 150 000 sources d'information publiques – contenus sur les réseaux sociaux, capteurs en ligne, sites d'information, retransmission audio, deep web et dark web –, la plateforme d'intelligence artificielle de Dataminr peut fournir les premiers signes indicateurs de risques pour la continuité des activités.

La plateforme est fortement configurable : vous localisez les sites d'implantation de votre organisation et définissez les thèmes spécifiques qui vous intéressent afin de cibler les alertes les plus pertinentes selon les besoins de votre organisation.

Plusieurs centaines de grands centres des opérations de sécurité au niveau mondial, d'organismes publics, de groupes humanitaires et de journalistes travaillant dans plus de 650 grands organes de presse font confiance à Dataminr.

.

Le personnel

Les centres des opérations de sécurité sont dotés d'analystes et de gestionnaires qui travaillent ensemble pour formuler des recommandations visant à protéger les employés et les cadres, les partenaires et les clients, ainsi que les actifs de l'entreprise.

La taille d'un SOC est variable. En pratique, nous avons constaté:

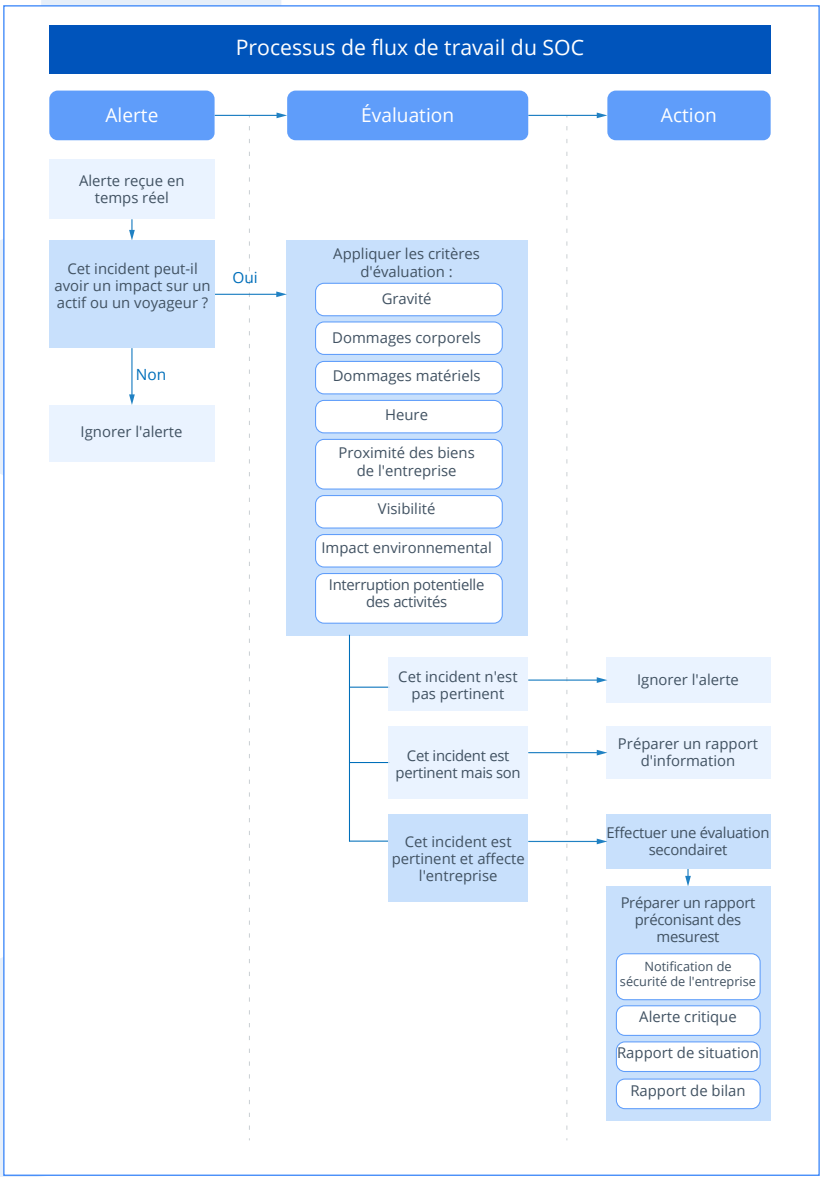
- De petites entreprises dont le service centralisé de sécurité ne compte que trois personnes travaillant la journée et qui font appel à un prestataire de services de sécurité infogérés pour couvrir les plages horaires en dehors des heures de travail ou en cas de crise
- Des entreprises de taille moyenne qui disposent d'une équipe centralisée limitée à cinq personnes, travaillant souvent sans SOC physique et qui assurent la sécurité de l'entreprise 24 h/24 et 7 j/7 en coordination avec des responsables de la sécurité régionaux
- De grandes entreprises disposant d'un centre des opérations de sécurité dédié à l'échelle mondiale comptant jusqu'à 30 personnes, opérant 24 h/24 et coordonnant les interventions avec les SOC régionaux et les responsables de la sécurité régionaux

Les responsables de SOC sont chargés de superviser et d'améliorer les flux de travail et processus du SOC, ainsi que d'en mesurer le succès. Ils restent calmes et modérés en toutes circonstances, tout en assumant la responsabilité de prendre les mesures appropriées à partir d'informations en temps réel en cas d'incident à risque.

Les processus de flux de travail

Fondamentalement, toutes les équipes de sécurité centralisées transforment les informations en temps réel en renseignements exploitables. Des flux de travail prédéfinis structurent le processus de transformation des informations en actions et contiennent des outils permettant de mesurer les performances de ces flux.

Les flux de travail d'un SOC peuvent être regroupés en trois grandes étapes : alerte, évaluation et action. **Voici un exemple de flux de travail que nous avons vu utilisé dans plusieurs SOC aujourd'hui:**



Les flux de travail sont établis à l'aide d'un système de gestion des incidents qui contient des outils permettant de mesurer le temps de réponse moyen et les performances d'une équipe. Par ailleurs, certains SOC utilisent d'autres outils de mesure pour évaluer l'efficacité et l'impact de l'équipe, comme les enquêtes de satisfaction auprès de leurs employés.

5 pièges à éviter lors de la création de votre centre des opérations de sécurité

REGARDER LA VIDÉO

L’impact des communiqués

Les équipes de sécurité ne génèrent pas de revenus pour l’entreprise. Il est donc important de consacrer des ressources pour mesurer l’impact positif d’un SOC et justifier la poursuite des investissements dans un tel programme.

Les responsables de SOC qui souhaitent voir augmenter les investissements dans leur programme doivent prévoir d’emblée des outils d’évaluation de l’efficacité et de reporting, ainsi qu’informer régulièrement leur équipe de direction sur l’impact et les performances du SOC.

Les équipes de sécurité sont confrontées à une tâche inédite : mesurer la valeur d’un risque qui a été réduit. L’ampleur potentielle de l’impact ne sera jamais pleinement réalisée, ce qui rend difficile l’estimation du coût d’un accident qui a été évité ou d’un risque qui a été minimisé.

Les principaux indicateurs de performance qu’il convient de mesurer sont les suivants:

- Le nombre total d’alertes en temps réel traitées par le SOC au cours de la période de référence
- Le nombre total de mesures de réduction des risques prises par le SOC au cours de la période de référence
- Un certain nombre de mesures de réduction des risques à fort impact prises pendant la période de référence
- Les notes de satisfaction des employés

Planifier l'avenir

Lorsqu'ils planifient l'avenir, il y a deux choses que les responsables de SOC peuvent faire pour garantir un investissement continu dans leur équipe.

En premier lieu, optimiser le travail du centre des opérations de sécurité, en s'éloignant d'une réponse réactive aux risques pour s'orienter vers une gestion proactive des risques et la résilience de l'entreprise. Utilisez les informations disponibles en temps réel et les données historiques sur les risques pour aider les dirigeants de votre entreprise à prendre des décisions plus éclairées.

Partagez l'accès aux informations en temps réel avec d'autres équipes de l'organisation chargées de réduire les risques, comme l'équipe de cybersécurité et l'équipe de gestion des risques, afin qu'elles puissent utiliser ces informations pour mieux anticiper les risques futurs.

Ensuite, adoptez une approche globale de la gestion des risques, de la résilience et de la continuité des activités, de la cybersécurité et de la sécurité physique, sachant que toutes ces équipes poursuivent un objectif similaire : anticiper, planifier et réduire les risques. Or, le fait de compartimenter la gestion de ces équipes en silos opérationnels peut involontairement créer des angles morts en matière de risque.

Face à la convergence croissante entre les risques liés à la cybersécurité et à la sécurité physique, de nombreuses entreprises étudient comment adopter de bonnes pratiques convergentes en matière de sécurité afin d'éliminer ces angles morts.

Les centres des opérations de sécurité sont essentiels pour les entreprises modernes qui souhaitent aborder la gestion des risques de manière quantifiée, reproductible et évolutive. Les alertes en temps réel de Dataminr Pulse constituent aujourd'hui la pierre angulaire de centaines de SOC d'entreprises hautement performants partout dans le monde.

En savoir plus

Demander une démo

Demandez une démonstration pour savoir comment disposer d'informations prédictives sur les événements et les risques à fort impact.

DEMANDER UNE DÉMO

Contactez-nous

Informations générales | info@dataminr.com
Assistance | support@dataminr.com

Pour tout savoir sur les SOC, rendez-vous sur notre plateforme Centre des opérations de sécurité