Près de 50 % des équipes SOC canadiennes se sentent submergées par le volume d'alertes de sécurité

Une étude de Trend Micro révèle le coût humain des centres d'opérations de sécurité insuffisamment équipés

Le 26 mai 2021 – Trend Micro Incorporated (TYO: 4704; TSE: 4704), leader mondial en matière de cybersécurité, a publié aujourd'hui les résultats d'une nouvelle étude qui révèle que les équipes responsables des centres d'opérations de sécurité (SOC) et des technologies de l'information (TI) souffrent de niveaux élevés de stress en dehors de la journée de travail, causés par la surcharge d'alertes.

L'étude, qui a interrogé 2 303 décideurs en matière de sécurité des TI et de SOC dans des entreprises de toutes tailles et de tous secteurs verticaux, dont 101 Canadiens, révèle que 70 % ont déclaré que leur vie privée est affectée par leur rôle dans la gestion des alertes aux menaces informatiques. Près de la moitié (46 %) des équipes de sécurité SOC/TI canadiennes sont submergées par le volume d'alertes de sécurité et 52 % admettent qu'elles n'ont pas entièrement confiance dans leur capacité à les hiérarchiser et à y répondre. Il n'est donc pas étonnant que les équipes passent jusqu'à 25 % de leur temps à traiter des faux positifs.

Ces conclusions sont corroborées par une étude récente de Forrester, selon laquelle « les équipes de sécurité manquent cruellement de personnel pour répondre aux incidents, alors qu'elles sont confrontées à un nombre croissant d'attaques. Les centres d'opérations de sécurité (SOC) ont besoin d'une méthode de détection et de réponse plus efficace. Par conséquent, XDR (pour *Extended Detection and Response* – en français, *Détection et remédiation entre les couches*) adopte une approche radicalement différente de celle des autres outils actuellement sur le marché. »

En dehors du travail, le volume élevé d'alertes empêche de nombreux responsables SOC canadiens de décrocher ou de se détendre, et les rend irritables avec leurs amis et leur famille. Au travail, ils sont amenés à désactiver les alertes (30 % le font occasionnellement ou fréquemment), à s'éloigner de leur ordinateur (46 %), à espérer qu'un autre membre de l'équipe intervienne (46 %) ou à ignorer complètement ce qui arrive (40 %).

« Nous avons l'habitude que la cybersécurité ne soit décrite en termes de personnes, de processus et de technologie », a déclaré la Dre Victoria Baines, chercheuse et autrice en matière de cybersécurité. « Trop souvent, cependant, les personnes sont dépeintes comme une vulnérabilité plutôt que comme un atout, et les défenses techniques sont privilégiées par rapport à la résilience humaine. Il est grand temps de renforcer notre investissement dans nos actifs de sécurité humaine. Cela signifie qu'il faut s'occuper de nos collègues et de nos équipes, et veiller à ce qu'ils disposent d'outils qui leur permettent de se concentrer sur ce que les humains font le mieux. »

Les conséquences de telles actions pourraient être désastreuses, compte tenu du fait que 65 % des répondants canadiens, et 74 % à l'échelle mondiale, sont déjà confrontés à une violation ou en prévoient une dans l'année, et que le coût moyen estimé par violation est de 235 000 dollars américains.

« Les membres de l'équipe SOC jouent un rôle essentiel sur la ligne de front virtuelle, en traitant et en répondant aux alertes de menaces pour que leurs organisations soient à l'abri de brèches potentiellement catastrophiques. Mais comme le montre cette étude, cette pression a parfois un coût personnel énorme », constate Bharat Mistry, directeur technique chez Trend Micro. « Pour ne pas perdre leurs meilleurs éléments à cause de l'épuisement professionnel, les entreprises doivent se tourner vers des plateformes de détection et de réponse aux menaces plus sophistiquées, capables de corréler et de hiérarchiser intelligemment les alertes. Cela améliorera non seulement la protection dans son ensemble, mais aussi la productivité des analystes et leur niveau de satisfaction professionnelle. »

Trend Micro Vision One est la solution aux difficultés rencontrées par les équipes SOC. Des alertes hiérarchisées et corrélées utilisant les données de l'ensemble de l'environnement informatique permettent aux équipes de consacrer leur temps à des tâches plus judicieuses. La réduction du nombre d'alertes et le renforcement des renseignements permettent aux équipes de retrouver un équilibre dans leur vie professionnelle et d'alléger le poids psychologique de la sécurité.

Veuillez consulter le rapport ci-joint (en anglais) pour en apprendre davantage.

Méthodologie de recherche
L'étude est basée sur des entretiens avec 2 303 décideurs en matière de sécurité des TI dans 21 pays. Au Canada, 101 décideurs en matière de sécurité des TI ont été interrogés. Cela comprend les responsables qui dirigent les équipes SOC (85 %) et ceux qui gèrent les SecOps au sein de leur équipe de sécurité informatique (15 %). Tous les répondants provenaient d'entreprises comptant plus de 250 employés.

À propos de Trend Micro
Trend Micro, leader mondial en matière de cybersécurité, contribue à sécuriser les échanges d'informations numériques à travers le monde. S'appuyant sur des décennies d'expertise en matière de sécurité, de recherche sur les menaces et

travers le monde. S'appuyant sur des décennies d'expertise en matière de sécurité, de recherche sur les menaces et d'innovation continue, Trend Micro protège des centaines de milliers d'entreprises et des millions d'individus grâce à des solutions de sécurité connectées pour les environnements Cloud, les Endpoints, les appareils et les réseaux. En tant que leader de la cybersécurité dans le nuage et en entreprise, la plateforme offre une vaste gamme de techniques de défense contre les menaces avancées, optimisées pour des environnements tels que AWS, Microsoft et Google, ainsi qu'une visibilité centrale pour une détection et une réponse qui sont à la fois meilleures et plus rapides. Avec plus de 6 700 employés dans 65 pays, Trend Micro permet aux entreprises de simplifier et sécuriser leur monde connecté. www.TrendMicro.com.

---

https://newsroom.trendmicro.ca/Pres-de-50-des-equipes-SOC-canadiennes-se-sentent-submergees-par-le-volume-dalertes-de-securite