La dimension humaine de la cybersécurité

Imaginez le pire scénario.

Une attaque sophistiquée par ransomware a totalement paralysé votre datacenter. Vos équipes commerciales, votre service client et votre département financier sont à l'arrêt. En votre qualité de RSI, vous avez la responsabilité de restaurer les systèmes, mais vous vous trouvez dans une impasse.

Votre équipe, déjà surchargée, a enchaîné des semaines de travail en s'accordant très peu de pauses ou de congés. Certains de vos experts sont ***allés jusqu'à pointer 36 heures d'affilée*** sans dormir. Vous craignez que la fatigue ne les amène à prendre de mauvaises décisions qui pourraient éventuellement compromettre leurs efforts de restauration.

Vous avez désespérément besoin de ressources supplémentaires capables d'intervenir immédiatement et de vous aider à résoudre le problème. Mais où trouver de telles ressources ?

Ce scénario ressemble au début d'un roman, mais il s'inspire en réalité des expériences véritablement vécues par les clients Dell. Il met en évidence un problème majeur dans l'environnement de cybersécurité actuel : l'élément humain.

Des données récentes indiquent que le secteur souffre d'une pénurie de près de 5 millions de professionnels de la sécurité. Même si le manque de ressources se fait plus cruellement ressentir au cours d'un incident, les solutions sont ancrées davantage en amont.

Commencer par constituer et développer un vivier de talents

La première étape pour vous assurer que vous disposez des ressources dont vous avez besoin consiste à créer un vivier de talents :

Stages et recrutement dans les établissements d'enseignement supérieur

Les universités et les écoles techniques locales peuvent libérer un flux régulier de jeunes talents. Au fil du temps, ces jeunes peuvent devenir des collaborateurs capables de créer un fort impact.

Formation et développement continus

Malgré des contraintes de temps et des restrictions budgétaires constantes, les professionnels de la cybersécurité doivent s'adapter à l'évolution des outils et des menaces.

Priorité à la fidélisation

Les praticiens talentueux sont très demandés, surtout s'ils ont une certaine expérience dans la gestion d'une attaque. Si vous ne parvenez pas à fidéliser vos meilleurs talents, quelqu'un d'autre s'en chargera.

Même une équipe solide peut ne pas suffire à gérer le stress lié à la gestion d'une attaque. Il est donc important d'anticiper les choses en prévoyant une assistance supplémentaire avant que vous en ayez besoin :

Évaluation des ressources tierces

Les cabinets de conseils en cybersécurité et de recrutement de personnel d'appoint peuvent aider votre équipe à la fois dans les opérations du quotidien et au cours d'incidents. Même si vous n'avez pas besoin de leurs services dans l'immédiat, il est important d'établir des relations avec ces entreprises afin d'avoir accès à ces ressources en cas de besoin.

Dell propose un certain nombre de services qui peuvent compléter les équipes existantes, notamment les services de CISO virtuel (vCISO), de réponse aux incidents et de conseils en cybersécurité.

Utiliser AI

Tirez parti des nouvelles fonctionnalités d'IA intégrées aux outils de cybersécurité, telles que l'analyse des journaux, la détection des anomalies, le tri des alertes de faible priorité ou l'entraînement spécialisé, afin de combler la pénurie de ressources et de répondre aux besoins opérationnels, et libérer ainsi du temps aux membres de l'équipe pour leur permettre de se concentrer sur des tâches plus importantes.

C'est au cours d'une cyberattaque que le manque de ressources pèse le plus lourdement

Comme le montre le scénario présenté ci-dessus, une cyberattaque de grande ampleur peut paralyser votre entreprise en mettant à l'arrêt les principaux systèmes et opérations métier. Chaque minute qui passe coûte de l'argent à l'entreprise, et l'équipe de cybersécurité subit une énorme pression pour résoudre le problème.

Veiller à ce que vos équipes soient le mieux préparées possible aura un impact direct sur la réponse aux incidents et sur le stress qui pèse sur l'équipe.

N'oubliez pas que la formation ne doit pas se limiter aux professionnels de la sécurité, mais bien s'étendre à tous les employés, car ils constituent la première ligne de défense.

Tout ceci met en évidence une problématique centrale : les cyberdéfenseurs sont avant tout humains. Ils ont leurs limites, et lorsque ces limites sont dépassées, même les professionnels les plus talentueux peuvent échouer. La fatigue mentale, le stress et l'épuisement professionnel sont devenus des facteurs critiques dans la posture de cybersécurité.

Bien qu'il n'existe pas de solution miracle, les stratégies suivantes peuvent se révéler très utiles :

Constituer une équipe solide et un vivier de talents

La solution la plus fondamentale à ce problème est de ne pas le laisser devenir une urgence : il est essentiel de constituer une équipe solide épaulée par des remplaçants.

Anticipation d'une attaque du côté humain

Les plans de réponse aux incidents sont essentiels et doivent IMPÉRATIVEMENT comprendre des plans de gestion du personnel, de planification et de gestion des arrêts de travail/congés des employés.

Utilisation de ressources tierces

Des consultants externes en cybersécurité peuvent vous aider à renforcer votre équipe. Par exemple, les services de réponse aux incidents de Dell peuvent dépêcher une équipe d'experts sur place en quelques heures, prête à évaluer la situation, à contenir les menaces et à prendre immédiatement des mesures correctives. Nous avons aidé de nombreux clients à se relever de cyberattaques.

L'IA peut vous aider, mais ce n'est pas une solution miracle

L'IA offre l'extraordinaire promesse d'améliorer les outils et les programmes de cybersécurité. Ses capacités s'étendent de l'analyse prédictive au développement de programmes de formation personnalisés, voire à la résolution des menaces en amont, avant qu'elles ne se propagent.

Plus important encore, l'IA peut fournir aux défenseurs un système de support en temps réel lors d'un incident. Les modèles d'apprentissage automatique entraînés sur des données d'attaque historiques peuvent recommander des actions basées sur des événements passés d'une nature similaire.

À mesure que les solutions de traitement du langage naturel s'intégreront aux outils de cybersécurité, les analystes pourront interagir directement avec leurs systèmes, identifier les menaces et déployer des solutions.

L'IA peut également surveiller les schémas comportementaux pour signaler les situations où un analyste humain commet régulièrement des erreurs (peut-être par épuisement) et demander une rotation d'équipe ou une vérification.

Même si les outils de cybersécurité intègrent rapidement des outils d'IA plus sophistiqués, bon nombre des fonctionnalités les plus puissantes sont encore en cours de développement. N'oubliez pas qu'à l'heure actuelle, l'IA ne peut remplacer les compétences d'un praticien expérimenté, ***en particulier s'il possède déjà l'expérience d'une attaque***.

Quelques recommandations pour exploiter le potentiel de l'IA :

Comprendre comment les outils peuvent vous assister dans vos opérations de sécurité

Analysez en détail les outils d'IA et mettez-les en œuvre là où ils peuvent être les plus efficaces. La détection des menaces avancées, l'automatisation des tâches répétitives et l'utilisation de l'IA dans la gestion des identités constituent des atouts potentiels.

> Les bonnes pratiques consistent à s'entourer d'un partenaire qui gère la réponse aux incidents, la résolution des problèmes et la récupération sur la base d'un contrat. »
>
> ***Jason Rosselot***
> *VP, Cybersecurity and Business Unit Security Officer, Dell Technologies*

Anticiper l'avenir de l'IA

Apprenez à déterminer à quel moment de nouvelles capacités seront disponibles et comment elles profiteront à l'équipe, puis élaborez un plan de mise en œuvre.

Intégrer l'IA à la planification des effectifs

L'automatisation réduit les tâches manuelles, ce qui signifie que la composition de votre équipe de sécurité devra peut-être évoluer. Vous aurez peut-être besoin de ressources plus expérimentées pour analyser et exploiter les informations de sécurité, plutôt que de simplement les compiler. Adaptez vos stratégies de recrutement et de perfectionnement en conséquence.

L'IA est appelée à jouer un rôle central dans vos opérations de cybersécurité, si ce n'est déjà le cas. N'oubliez pas cependant que rien ne peut remplacer un praticien qualifié et expérimenté. Vous devriez vous fixer comme objectif d'utiliser l'IA pour automatiser les opérations et renforcer l'efficacité de vos ressources humaines, afin de prévenir les attaques et de minimiser leur impact lorsqu'elles se produisent.

Atteindre la maturité en matière de cybersécurité : une étape à la fois

Comme tout ce qui touche à la cybersécurité, aborder la dimension humaine est un parcours, et non une destination. Les efforts progressifs, voire même chaque petit progrès, font la différence et s'additionnent au fil du temps. L'important est de garder à l'esprit que même les meilleurs outils technologiques et de sécurité ne doivent en fin de compte leur efficacité qu'aux personnes qui les utilisent.

DELL Technologies

Produits et solutions Dell qui peuvent vous aider

Solution Dell proposée	Description
Services de réponse aux incidents	Une équipe d'experts en cybersécurité certifiés par le secteur, prête à réagir rapidement en cas de cyberattaque. Nous travaillons à vos côtés pour éliminer les menaces jusqu'au retour à la normale.
Cybersecurity Advisory Services	Des conseils d'experts qui peuvent vous aider à identifier et corriger les zones d'ombre de votre stratégie de sécurité, à protéger vos actifs et vos données, et à assurer une vigilance et une gouvernance en continu.
vCISO	Responsable de la sécurité virtuelle des systèmes d'information et expert en cybersécurité qui peut vous aider à identifier et gérer les risques mais aussi à prendre des décisions stratégiques.
Managed Detection and Response	Réduit les efforts manuels et rationalise les opérations de sécurité quotidiennes en fournissant une surveillance, une détection des menaces, une procédure d'enquête et une réponse rapide sur l'ensemble des points de terminaison, du réseau et du Cloud. Les clients choisissent la plateforme XDR qui leur convient (SecureWorks® Taegis™ XDR, CrowdStrike Falcon® XDR ou Microsoft Defender XDR) et reçoivent des conseils d'experts, des rapports trimestriels et jusqu'à 40 heures de réponse aux incidents par an.

Découvrez comment relever certains des défis actuels majeurs en matière de cybersécurité sur **dell.com/cybersecuritymonth**