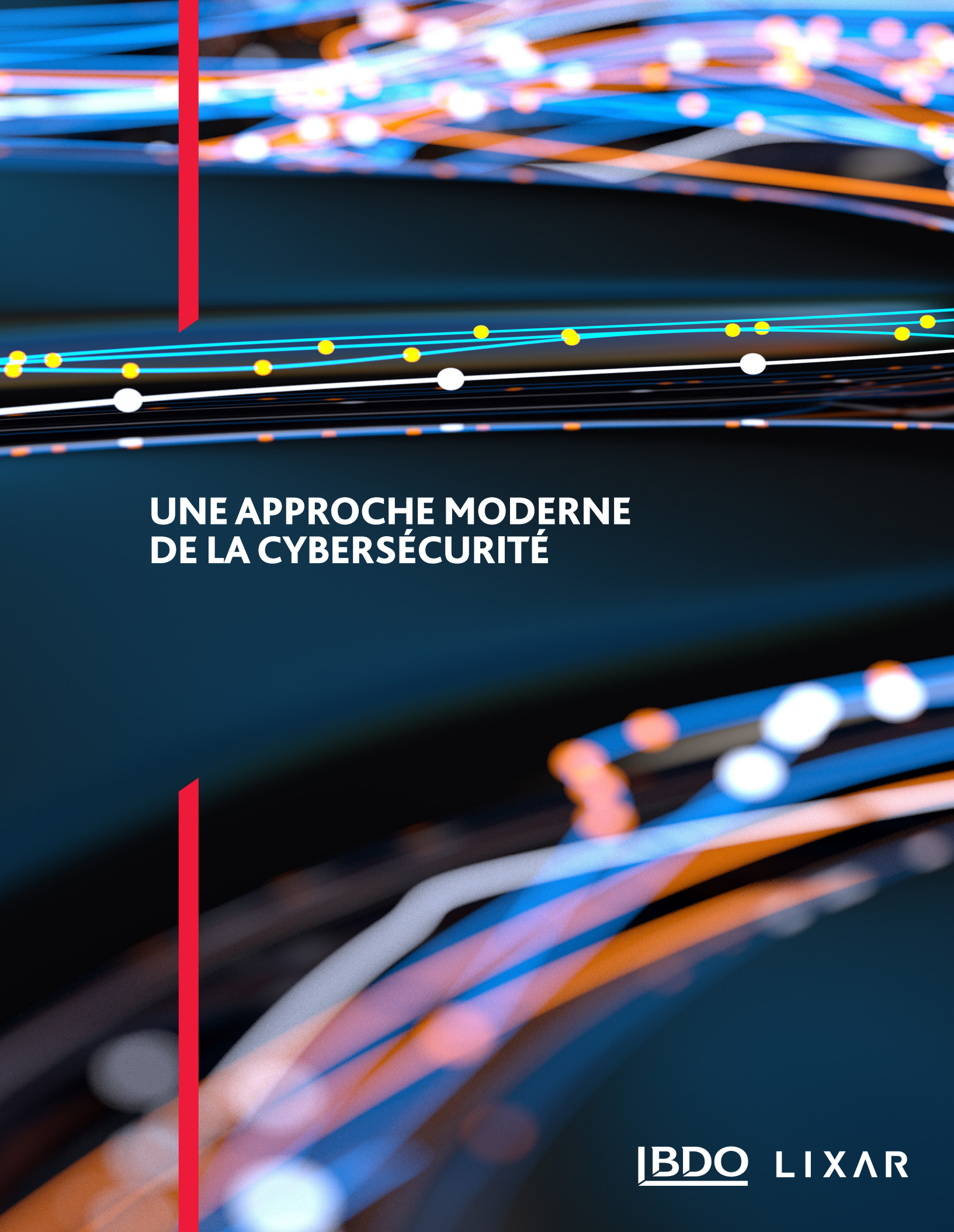


UNE APPROCHE MODERNE DE LA CYBERSÉCURITÉ

BDO LIXAR

La cybersécurité est l'un des sujets de l'heure pour les organisations qui procèdent à l'adoption rapide de technologies modernes et à la migration numérique.

Les organisations qui exercent leurs activités dans l'environnement numérique grandissant doivent composer avec la gestion toujours plus complexe des besoins et des compétences technologiques élevés de leurs employés, de leurs clients et des organismes de réglementation tout en veillant à protéger leurs plateformes technologiques et leurs données contre les cybercriminels.

Au vu des nouvelles exigences imposées à un rythme effarant et des capacités disponibles, les organisations doivent faire face à des difficultés sans précédent en matière d'adaptation aux conditions numériques évoluant rapidement. Il n'est pas question ici d'une seule technologie révolutionnaire, mais bien d'une réorientation plus rapide que jamais de l'ensemble des activités humaines vers un point commun de dépendance au numérique.

Du point de vue de la sécurité, chaque migration de nouveau service vers l'espace numérique qu'effectue une entreprise s'accompagne de risques. Les professionnels de la cybersécurité peinent à suivre le rythme des entreprises qui cherche à améliorer continuellement leur technologie dans un objectif de croissance, et cela s'en ressent dans leurs programmes. À cela s'ajoutent les défis du recrutement effectué à partir d'un bassin de talents disproportionné par rapport à la demande ainsi que les efforts constants devant être déployés en vue de retenir les talents existants. Dans ces conditions, il est difficile pour les organisations de rester au diapason et de maintenir une solide posture en matière de sécurité.

Toutefois, tout n'est pas sombre. Ces mêmes technologies à l'origine de la transformation numérique accélérée des entreprises (comme l'infonuagique) sont sur le point de provoquer une transformation tout aussi importante du point de vue de la sécurité. Ce livre blanc s'intéresse aux domaines où la cybersécurité intelligente est mise à contribution et à la manière dont celle-ci permet aux organisations d'être mieux protégées que jamais.

DES DÉFIS COMMUNS

Les équipes chargées de la sécurité et les organisations ont du mal à optimiser leur posture en matière de sécurité pour plusieurs raisons. Voici quelques difficultés que connaissent toutes les organisations dans le contexte actuel :

Solutions trop complexes – Dans bien des cas, les solutions sont excessivement complexes et il est difficile de les exploiter d'une manière optimale et utile. Les organisations qui peinent à mettre au point et à exploiter une solution sont souvent contraintes de se tourner vers les services professionnels coûteux des fournisseurs ou d'avoir recours à d'autres technologies pour combler les lacunes, ce qui peut mener à une prolifération des technologies et à une hausse des coûts.

Prolifération des technologies – Ajouter des technologies visant à combler des lacunes en matière de visibilité nécessite mûre réflexion. L'organisation sera-t-elle en mesure d'acquérir les talents et les compétences nécessaires à l'exploitation de la solution? Cette solution entraîne-t-elle à son tour d'autres problèmes? Les coûts liés à l'utilisation de la nouvelle solution ont-ils été évalués?

Hausse des coûts – Les redondances et les chevauchements technologiques font augmenter les coûts de gestion connexes. Il est souvent difficile de rationaliser les technologies et d'éliminer les duplications puisque d'autres besoins opérationnels jugés prioritaires ont préséance. Le cycle se poursuit, ce qui mène à des inefficacités que les organisations ne peuvent se permettre de subir et introduit des angles morts dans leur programme de sécurité.

Acquisition de compétences – Le recrutement de professionnels compétents en cybersécurité est un défi en soi; il faut à la fois attirer de grands talents pour diverses technologies, leur fournir les outils dont ils ont besoin et assurer leur rétention. Les facteurs qui expliquent la pénurie de ressources en sécurité sont nombreux : manque de professionnels formés, explosion de la demande, manque d'investissements historiques des entreprises, épuisement professionnel lié au manque d'effectif, augmentation du volume et de la complexité des menaces, nouvelles difficultés découlant de l'automatisation et du télétravail.

Lassitude face aux alertes – Les équipes de sécurité consacrent trop de temps à répondre à des alertes non fondées. Ces fausses alertes sont souvent causées par des capteurs mal configurés ou des seuils d'alerte réglés à de trop hauts niveaux. Les alertes mineures ou non fondées distraient et surchargent les équipes qui doivent sans cesse y réagir, ce qui augmente le risque d'atteinte à la sécurité et de roulement du personnel.

Les difficultés que nous venons de décrire sont très répandues dans le domaine de la cybersécurité. Les organisations se rendent rapidement compte qu'il n'existe aucune solution sur le marché qui permet d'éliminer tous les risques. Or, celles qui adoptent une approche fondée sur les risques pour élaborer des programmes de sécurité peuvent obtenir un avantage considérable à ce titre en employant des technologies performantes (p. ex., les solutions de sécurité de Microsoft), des processus rigoureux (p. ex., en gestion des incidents) et des talents qualifiés (p. ex., dans l'utilisation des outils).

QUE PEUVENT FAIRE LES ORGANISATIONS?

Les organisations qui adoptent des solutions modernes fondées sur des plateformes infonuagiques, l'intelligence artificielle et les renseignements gagnent en confiance et réduisent davantage leurs risques lorsqu'elles tirent pleinement profit de la convivialité et de la portée qu'offre la sécurité dans l'environnement informatique moderne. Cette façon de faire ouvre la voie à des possibilités sans précédent en matière de cybersécurité. Poursuivez votre lecture pour savoir en quoi les technologies émergentes sont à l'origine d'un nouveau paradigme et comment les processus intelligents permettent d'alléger les fardeaux sans pour autant augmenter les coûts et les difficultés des organisations.

Plateformes infonuagiques

MS Azure

Solutions intégrées

MS Defender for Endpoint

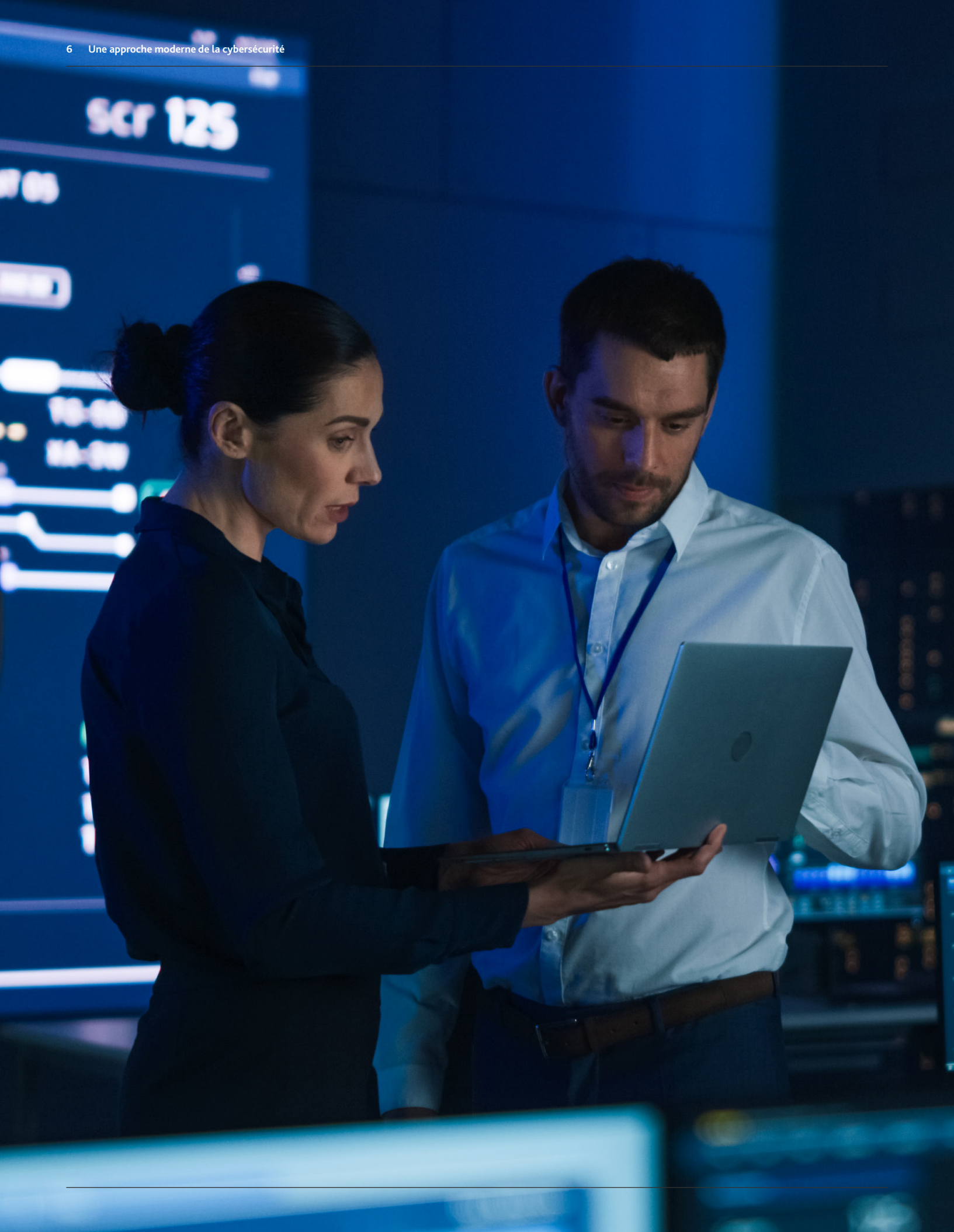
Alimentées par les renseignements sur les menaces

LES CAPACITÉS ÉMERGENTES EN RENFORT

Plateformes infonuagiques – Le choix d'une plateforme infonuagique de première qualité, telle que Microsoft Azure, est la pierre angulaire d'un programme de sécurité infonuagique moderne, réalisable et fonctionnel. On ne saurait suffisamment insister sur l'importance d'une plateforme infonuagique pour votre sécurité. Les fournisseurs de ces services réussissent à offrir à leurs clients des cadres et des processus de sécurité à la fine pointe en concentrant leurs efforts sur les capacités de détection des plateformes, contrairement aux fournisseurs tiers, et en tirant profit de leurs moyens financiers qui leur permettent de créer de telles solutions exhaustives. On ne pourrait trouver meilleur connaisseur de l'application Microsoft Azure que Microsoft lui-même. Bien que les solutions de tierces parties aient une place dans l'écosystème, seuls les fournisseurs de services d'expérience qui accordent la priorité à la sécurité peuvent permettre aux clients de tirer pleinement profit des capacités fondamentales des plateforme.

Solutions intégrées – Les fournisseurs de solutions ont compris qu'il fallait passer de la détection fondée sur les signatures à la détection fondée sur les comportements afin d'avoir une meilleure vue des menaces. Pour ce faire, ils intègrent leurs capacités en vue de les rendre plus intelligentes et plus fiables, pour ainsi obtenir de meilleurs résultats. L'utilisation d'une solution de détection et de réponse des terminaux est un exemple de technologie intégrée permettant de relier et de détecter les activités suspectes qui ne sont pas relevées par une solution centrale de gestion des informations et des événements liés à la sécurité. En concentrant vos efforts sur les comportements aux terminaux plutôt que sur les signatures tout en tirant profit des renseignements sur les menaces, les alertes que vous recevrez seront de meilleure qualité et plus fiables.

Renseignements sur les menaces – Les organisations qui utilisent judicieusement les renseignements sur les menaces peuvent mieux privilégier leurs investissements et leurs projets en matière de sécurité puisqu'elles sont au fait des menaces les plus probables et les plus graves qui planent sur elles. Elles peuvent ainsi améliorer leur sécurité, accélérer leurs efforts de réhabilitation et déceler des attaques dont elles auraient autrement pu ignorer l'existence.


scr 125

UNE APPROCHE PRATIQUE POUR RÉDUIRE LE FARDEAU

Nous constatons souvent que les organisations adoptent une approche tactique à court terme afin de mettre en place des capacités de sécurité habituellement en réponse à des atteintes, à des vérifications ou à des conseils de fournisseurs ou de services professionnels. Cette façon de faire comporte des risques considérables du point de vue de l'efficacité globale, des coûts et de la dotation en personnel, et peut même nuire à la sécurité.

BDO propose donc aux organisations l'approche suivante en vue d'améliorer leur posture en matière de sécurité.

Permettre les enquêtes – La première étape consiste à vérifier si vous avez les autorisations d'accès et les moyens techniques nécessaires pour mener efficacement des enquêtes et prendre les mesures appropriées lorsque des problèmes de sécurité sont portés à votre attention. À cette fin, BDO s'occupe de préparer votre environnement pour faire en sorte que l'information nécessaire à la surveillance des menaces soit disponible, accessible et fournie en temps opportun.

Prioriser les alertes intégrées – Les technologies les plus fiables et les plus intégrées sont priorisées en vue d'optimiser votre visibilité à tous les égards. Nous privilégions les technologies intégrées telles que les plateformes infonuagiques, une solution de détection et de réponse des terminaux et les solutions permettant d'intégrer un filtrage basé sur les renseignements sur les menaces.

Améliorer les processus opérationnels – Pour assurer la qualité, la durabilité et la production de résultats positifs pour l'organisation, il est essentiel de disposer de processus internes. Une organisation qui peut compter sur des alertes de grande qualité doit également être en mesure d'y réagir. Par exemple, les organisations qui n'ont pas mis en place un processus d'intervention en cas d'incident bien documenté et compris risquent de prendre plus de temps que les autres à contenir les menaces et à s'en rétablir.

Amélioration des cas d'utilisation – Une fois les éléments fondamentaux du système de sécurité bien en place, BDO en étend la portée en y ajoutant des couches supplémentaires de surveillance relative aux applications, à la logique applicative ou aux menaces internes. Nous mettons en place des cas d'utilisation personnalisés en vue de repérer les menaces dans l'ensemble de vos surfaces d'attaque, ce qui maximise votre visibilité sur les événements susceptibles de compromettre la sécurité.

Assurer la durabilité – Chez BDO, nous évaluons sans cesse le marché et la pile technologique connexe afin de maximiser l'efficacité, l'efficience et la valeur que nous offrons à nos clients. Toute organisation souhaitant maintenir une bonne posture en matière de sécurité doit assurer sa durabilité, utiliser les bons outils et préserver le niveau approprié de compétences. Il est essentiel que vos programmes de sécurité disposent d'une défense en profondeur. Vous devez être en mesure de distinguer les cas où il est préférable de reconfigurer une technologie de ceux où il convient de la remplacer, en fonction des conditions du marché et de votre situation actuelle.

Une évolution majeure s'est entamée. Les technologies de plus en plus intelligentes bouleversent complètement le secteur de la sécurité. Les programmes de sécurité modernes évoluent plus rapidement que jamais, et les organisations qui n'hésitent pas à mettre à contribution les technologies actuelles, à adopter une approche intelligente et à recourir à des conseillers d'expérience comme ceux de BDO seront plus à même de s'adapter et de s'améliorer rapidement.

PERSONNES-RESSOURCES

ROCCO GALLETTO
Associé et chef national, Services en cybersécurité
BDO Lixar
416 729-2609 / rgalletto@bdo.ca

ROB PHILPOTTS
Directeur, Services de gestion et d'intervention en matière de cybermenaces
BDO Lixar
437-237-3502 / rphilpotts@bdo.ca

BRAD ELLISON
Directeur général, Managed Services Group
630-286-8196 / bellison@bdo.com

STEVE COMBS
Directeur, Infrastructure Solutions Group
713 576-3417 / scombs@bdo.com

À propos de BDO Lixar

BDO Lixar est le service-conseil en technologie de BDO Canada. Nous sommes un fournisseur de solutions technologiques de bout en bout qui aide les entreprises à s'améliorer et à croître.

Nos équipes ont aidé nos clients à innover grâce aux données et à l'intelligence artificielle, la cybersécurité, les stratégies numériques, les solutions de milieu de travail moderne et le développement d'applications, reposant sur le cadre d'adoption de l'infonuagique de BDO Lixar. Qu'il s'agisse de réaliser des économies, de gagner en efficacité, de fournir des idées ou d'anticiper des résultats, nous nous sommes engagés à aider nos clients à composer avec l'environnement technologique changeant, tout en restant concurrentiels et en continuant à croître. Nous possédons une expertise reconnue dans un large éventail de secteurs et offrons des solutions novatrices, stables et extensibles qui permettent de régler les problèmes les plus complexes et de saisir les occasions de croissance.