L'avenir de la cybersécurité

Nous proposons ici une analyse des résultats de notre étude mondiale Pulse 2023. L'objectif ? Fournir aux MSSP des éclairages concrets sur les problématiques d'aujourd'hui.

W / T H®
secure

Introduction

L'étude de marché WithSecure™ Pulse 2023 a été menée auprès de 3 072 professionnels IT de 12 pays. Les professionnels interrogés étaient des décideurs en sécurité, des influenceurs en sécurité ou encore des responsables d'achat de produits et de services en sécurité.

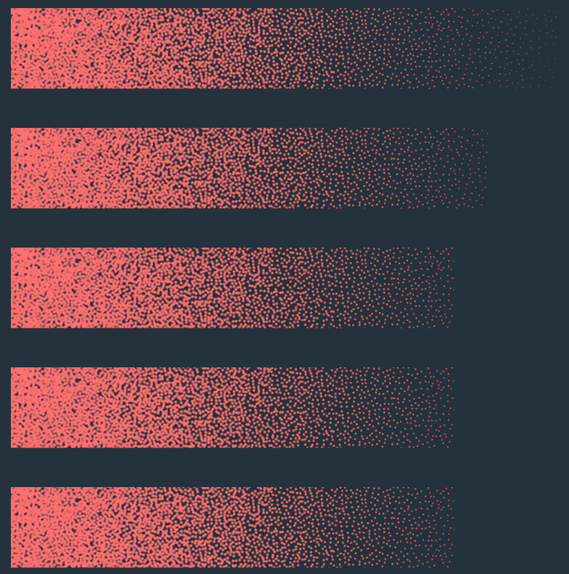
Nous leur avons posé une série de questions sur leurs priorités et préoccupations pour l'année 2023. Nous avons évoqué avec eu plusieurs thématiques comme les violations de données, les changements de fournisseur et les questions budgétaires.

Les priorités de 2023

Les participants se sont globalement accordés sur le caractère essentiel de la détection et de la réponse aux menaces. La préoccupation n°1 porte sur la prévention des violations de données ; la seconde, sur la protection contre les malwares et ransomwares.

Les cinq principales priorités techniques pour 2023

D'après notre enquête Pulse 2023, voici les 5 grandes priorités techniques des leaders de la cybersécurité pour 2023 :



34% Prévenir les violations de données

29% Assurer la protection contre les malwares et les ransomwares

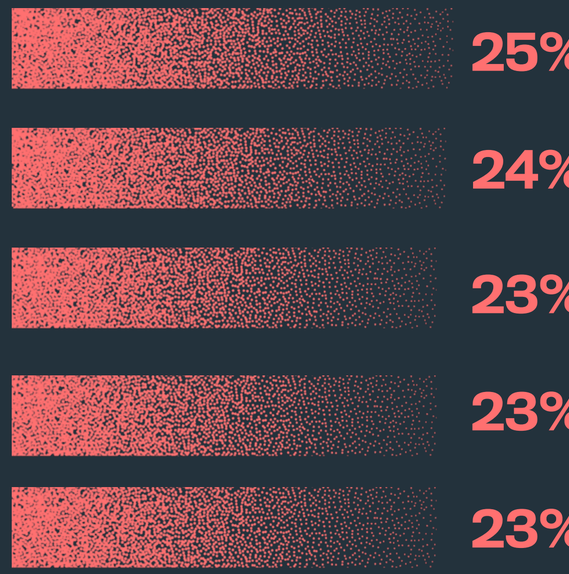
27% Prévenir les menaces avancées ciblant la messagerie comme le phishing ou les attaques BEC

27% Assurer la sécurité des applications de collaboration cloud comme Office 365 et Salesforce.

26% Assurer la sécurité d'un écosystème de plus en plus diversifié d'appareils, de services et de logiciels.

Les cinq principaux enjeux de la sécurité pour 2023

Voici les cinq grands enjeux de la sécurité pour les entreprises en 2023 :



25% Sécuriser le travail à distance/le travail hybride

24% Accélérer et optimiser la réponse aux cyberincidents

23% Sensibiliser les employés aux cyber-risques et à la cybersécurité

23% Assurer la continuité des opérations, sans interruption

23% Instaurer une culture d'entreprise qui priorise la sécurité

Certains aspects négligés

Selon Peter Page, Head of Solution Consulting chez WithSecure™, les aspects de sécurité les plus essentiels sont, paradoxalement, absents des priorités mentionnées : « il y a des compétences et des pratiques qui manquent à de nombreuses organisations ».

Pour chaque entreprise cliente, il est conseillé de comparer la liste des priorités aux compétences de cybersécurité qui font défaut à l'entreprise. Ces compétences manquantes ont souvent plus d'importance que les priorités perçues. Vous pouvez aider vos clients en mettant en évidence les aspects de leur sécurité qu'ils ont laissés de côté.

WithSecure™ Elements, notre offre unique de cybersécurité, comprend la protection des endpoints, l'EDR (Endpoint Detection and Response), la gestion des vulnérabilités et la protection collaborative. Cette solution complète a été conçue pour répondre à tous les besoins de sécurité de vos clients. Nos partenaires peuvent aussi intégrer leurs propres services à Elements, pour proposer à leurs clients une solution encore plus performante.

Violations de données

La prévention des violations de données apparaît comme la priorité technique n°1. Des divergences ont toutefois été constatées sur cette question entre les influenceurs et les décideurs IT.

Divergences

44 % des influenceurs IT considèrent la « prévention des violations de données » comme la problématique la plus importante, Pour 38% du top management, il s'agit également de la priorité technique n°1, mais seuls 29 % des décideurs IT adoptent cette position. Il existe donc des dissensions au sein des entreprises. Lorsque vous communiquez avec vos clients, veillez à ce qu'il existe un consensus au sein de leur entreprise. Encouragez vos interlocuteurs à échanger avec leur équipe de sécurité.

Pour prévenir les violations de données, WithSecure™ se comporte comme le prolongement de votre équipe de sécurité. Nous sommes disponibles à tout moment, en cas de besoin. Avec le service « Elevate to WithSecure », vous pouvez bénéficier d'une aide supplémentaire pour faire face aux cas les plus complexes. Nous nous engageons à fournir ce support 24h/24, 7j/7. C'est bien en cela que nous nous différencions de nos concurrents.

Changer de fournisseur

Changer de fournisseur de sécurité est une démarche complexe, qui exige du temps et des ressources financières. Pour autant, plus de 30 % des professionnels interrogés ont changé de fournisseur de sécurité au cours des six derniers mois. Et 30 % prévoient de le faire dans les six prochains mois. Quelles sont donc les raisons qui motivent ces changements de fournisseurs ?

Au-delà de la simple question du coût

Les changements de fournisseur ne sont pas seulement motivés par la question du coût. Seuls 13,2% des participants ont évoqué le prix comme principale motivation. 21,8 % ont cité le support 24h/24 et 7j/7, tandis que 16,7 % ont déclaré que ce changement était motivé par un problème de confiance.

Jusqu'à récemment, même lorsque les organisations étaient insatisfaites des performances de leur fournisseur, elles hésitaient à sauter le pas, compte-tenu de la complexité du processus de changement. Mais il est devenu de plus en plus facile de changer de fournisseur et les entreprises se montrent aujourd'hui moins frileuses.

Si vous évoquez un changement de fournisseur avec l'un de vos prospects, expliquez-lui qu'il convient d'acter la décision le plus tôt possible, idéalement au moins 12 mois avant la date d'expiration du contrat en cours. D'après notre expérience, les migrations les plus réussies commencent au plus tard un an avant la fin de contrat.

Les dépenses de sécurité

Pour de nombreuses entreprises, le coût est une problématique centrale. Il ne s'agit pas seulement de dépenser le moins possible, mais de déterminer le montant correct à investir pour obtenir les meilleurs résultats au prix le plus bas. D'après notre enquête, même si le coût reste un facteur décisif, il occupe désormais moins d'importance dans le processus décisionnel que par le passé.

Augmentation des dépenses de sécurité

Face à l'augmentation des cyber-risques, de nombreuses entreprises choisissent d'augmenter leurs dépenses en cybersécurité. D'ici 2024, le marché mondial de la sécurité IT devrait représenter 174,7 milliards de dollars.

Ce constat est corroboré par nos recherches. 87,9 % des entreprises européennes ayant participé à notre enquête Pulse 2023 ont indiqué qu'elles prévoyaient d'augmenter leurs dépenses de sécurité au cours des 12 prochains mois. Seuls 8,3 % des professionnels interrogés estimaient que leur organisation était déjà suffisamment protégée ou bien envisageaient de réduire leur budget de cybersécurité.

« Combien devons-nous dépenser pour la cybersécurité ? »

C'est la question qui taraude l'esprit de nombreux professionnels IT. Selon Paul Brucciani, Head of Product Marketing chez WithSecure™, la réponse dépend de plusieurs facteurs, comme le niveau de risque que l'entreprise est prête à accepter et les perturbations commerciales qu'elle peut tolérer.

Teemu Myllykangas, Director of B2B Product Management chez WithSecure, explique : « Je dis toujours qu'il est essentiel de débuter par un budget d'au moins 5 %, mais c'est sans aucune limite : plus la sécurité est vitale pour le client, plus ce pourcentage doit être élevé. Et vice versa. »

Pour autant, ce chiffre ne fait pas l'unanimité. Selon Paul Brucciani, pour les entreprises qui considèrent la sécurité comme essentielle, les dépenses de cybersécurité représentent généralement 12 à 15 % du budget informatique. Il n'existe donc pas de chiffre magique. Pour chaque entreprise, divers facteurs spécifiques doivent donc être pris en compte. »

WithSecure™ peut aider à réaliser ces estimations en calculant l'espérance de perte annuelle, la probabilité d'un incident de cybersécurité et les conséquences probables d'une attaque grave. Une fois ces calculs effectués, il est possible de déterminer quel montant l'entreprise doit allouer à la cybersécurité.

Quel que soit le montant que vos clients décident de consacrer à la sécurité, WithSecure™ propose des modèles de tarification flexibles adaptés à leurs besoins. Nous proposons notamment une licence annuelle, un abonnement mensuel et une sécurité basée sur l'utilisation.

Conclusion

Comme le montre l'enquête Pulse 2023, la sécurisation du travail distant et hybride constitue un enjeu de sécurité majeur pour de nombreuses entreprises, tout comme la nécessité d'accélérer et d'optimiser la réponse aux cyberincidents. WithSecure™ Elements dispose de puissantes capacités prédictives, préventives et réactives qui permettent de faire face à ces problématiques.

En tant que partenaire, vous pouvez répondre aux besoins de nombreux clients via la seule plateforme WithSecure™, avec un niveau d'efficacité opérationnelle que les autres fournisseurs sont tout simplement incapables de proposer.

Endpoint Protection et Endpoint Detection and Response sont de puissants outils qui répondent à la priorité numéro 1 des professionnels : la prévention des violations de données. Ces outils sont également très efficaces contre les ransomwares, les malwares, les menaces basées sur la messagerie et le phishing.

WithSecure™ Elements Collaboration Protection offre une sécurité fiable pour les applications de collaboration cloud comme Office 365 et Salesforce. Enfin, WithSecure™ Elements Vulnerability Management permet d'assurer en toute simplicité la sécurité d'un écosystème diversifié d'appareils, de services et de logiciels.

Notre plateforme Elements a été conçue avec et pour nos partenaires, pour faciliter au maximum l'activation de nouveaux services. Les MSSP peuvent se baser sur notre technologie pour proposer leurs propres prestations. Nous vous fournissons même un support de pointe pour la conception de vos services.

En choisissant le programme de partenariat WithSecure™, vous aurez également accès à Elevate to WithSecure™, un service de support 24h/24, 7j/7, qu'aucun autre fournisseur ne propose.

Notre objectif est de vous aider à progresser en tant que fournisseur de services managés. Pour ce faire, notre programme de partenariat comprend un volet de développement des compétences. Nous permettons également le cross-sell et l'up-sell, avec des produits et services en développement continu.

L'enquête Pulse 2023 offre un aperçu des priorités, préoccupations et attentes des professionnels IT pour cette année. En tant que membre du Programme Partenaires WithSecure™, vous serez plus que jamais en mesure de répondre à ces préoccupations. Vous pourrez même dépasser les attentes de vos clients. SI vous avez la moindre question au sujet de cette enquête, n'hésitez pas à nous contacter. C'est en travaillant ensemble que nous pourrons créer un cyberespace plus sûr.

Qui sommes-nous ?

WithSecure™ est le partenaire européen de référence en matière de cybersécurité depuis plus de 30 ans. Nous accompagnons les fournisseurs de services informatiques, les MSSP et des multinationales, qui nous font confiance, à travers des modèles commerciaux flexibles et adaptés au marché. Nous leur fournissons une cybersécurité axée sur les résultats, pour les protéger en toutes circonstances et garantir le bon fonctionnement de leurs activités. Notre protection basée sur l'IA sécurise les endpoints et protège les environnements cloud. Nos outils intelligents de détection et de réponse sont pilotés par des experts qui identifient les risques, assurent une recherche proactive des menaces et neutralisent les attaques en temps réel. Un service de consulting expert est également disponible pour les entreprises qui souhaitent renforcer leur résilience.

WithSecure™, anciennement F-Secure Corporation, a été fondée en 1988 et est cotée au NASDAQ OMX Helsinki Ltd.

W / T H®
secure