Sécurité du Cloud

Protégez votre entreprise, vos services et vos produits

Dans l'environnement de menaces fluctuantes et en évolution rapide d'aujourd'hui, les entreprises doivent relever des défis de plus en plus difficiles pour protéger efficacement leurs actifs tout en maintenant une expérience utilisateur accessible et transparente. Notre équipe peut vous aider à identifier les lacunes de votre architecture de sécurité, à réduire la partie à risque, à améliorer la précision des alertes aux menaces, à automatiser les tâches de sécurité à forte intensité manuelle et à réduire les coûts.

Priorités urgentes pour sécuriser le cloud

- Développement d'une architecture de référence de cybersécurité cohérente de bout en bout — un modèle holistique issu des meilleures pratiques est essentiel pour établir une gouvernance flexible et adaptative
- Déploiement d'une solution SIEM (Security Information and Event Management) et SOAR (Security Orchestration, Automation and Response) de premier ordre telle que Microsoft Sentinel — une solution d'automatisation complète capable d'unifier les solutions ponctuelles et la couverture disjointe
- Réalisation d'une évaluation de la cybersécurité de la préparation au cloud pour les charges de travail des systèmes sur site, afin de s'assurer que toutes les conditions préalables nécessaires sont en place avant la migration vers le cloud

Valeur ajoutée

- Des informations importantes sur vos systèmes actuels de cybersécurité
- Sensibilisation de votre équipe aux outils et technologies les plus récents
- Planifiez votre stratégie de sécurité de nouvelle génération et la manière de la mettre en œuvre

Chiffres clés

- Notre équipe a aidé des dizaines d'entreprises à améliorer leur cybersécurité
- Les faux positifs peuvent être réduits de 60 à 70 % avec Sentinel
- D'ici 2023, 90 % des solutions SIEM auront des capacités qui ne seront fournies que via le cloud

Les bénéfices

- Les charges de travail critiques peuvent être migrées vers le cloud en toute sécurité
- L'automatisation améliorée de la surveillance et des alertes libère du personnel pour une réponse plus rapide aux menaces
- Réduction des coûts de sécurité

Passez à l'action

Solutions tactiques : Un atelier de deux heures structuré autour de la résolution de problèmes. Commencez par le problème à résoudre, et non par la solution finale.

Évaluation de la gouvernance : Un programme de trois jours pour analyser votre cadre de cybersécurité existant et déterminer les avantages de la mise en œuvre d'un système SIEM/SOAR.

Plan de sécurisation du cloud : Identifier les forces et les faiblesses de votre architecture de sécurité existante et créer une architecture de référence réalisable et adaptée au cloud.

Feuille de route pour votre avenir : Créez un plan de transition réalisable pour avancer par étapes définies afin de remédier aux déficiences, de combler les failles et d'améliorer la détection des menaces existantes.

Notre solution

Nos experts en sécurité du cloud travailleront avec votre équipe d'infrastructure pour analyser votre cadre de sécurité actuel. Plus important encore, nous travaillerons avec votre équipe pour développer un plan de sécurité basé sur des normes et une feuille de route de conformité afin de garantir que votre cybersécurité et votre gouvernance sont prêtes pour le cloud.

Savoir par où commencer

Quelles sont mes priorités en matière de sécurisation du cloud ?

Premièrement, créer une architecture de référence en matière de cybersécurité afin de fournir un plan directeur pour la sécurisation et la surveillance de toutes les charges de travail critiques, qu'elles soient sur site ou dans le cloud. Deuxièmement, utiliser pleinement la technologie SIEM et SOAR pour améliorer les opérations de sécurité. Troisièmement, consolider et éliminer les anciennes solutions en utilisant des solutions cloud plus efficaces et moins coûteuses.

Quelles solutions de sécurité mes concurrents mettent-ils en œuvre ?

La technologie SIEM est désormais largement déployée pour assurer la détection des menaces, la conformité et la gestion des incidents de sécurité. Les grandes entreprises utilisent la technologie SOAR pour automatiser la gestion des volumes élevés d'alertes.

Quelles sont les fonctionnalités de sécurisation du cloud dont mes utilisateurs métier ont le plus besoin ?

Recherchez ces fonctionnalités auprès de votre fournisseur de services cloud : Pare-feu de périmètre avancé, intégration Active Directory, systèmes de détection d'intrusion avec journalisation des événements, cybersécurité des clients non gérés, SecOps du cloud hybride et cryptage des données entreposées.

Mon architecture de sécurisation est trop coûteuse

La surveillance et la remontée d'alertes sont souvent les composants les plus coûteux des SecOps* car ils nécessitent une allocation importante de temps de la part des SecAdmin. Pour réduire les coûts, étudiez les nouvelles technologies SOAR qui peuvent automatiser une grande partie de ce travail.

* Personne en charge de l'approche de gestion qui met en relation les équipes de sécurité et d'opérations.

Nous rencontrons trop de faux positifs

Les faux positifs sont le fléau des SecOps. Mais l'apprentissage automatique et l'IA peuvent réduire considérablement les faux positifs. Ces fonctionnalités se trouvent généralement dans les solutions SIEM avancées.

Mon équipe de sécurité ne travaille pas actuellement avec Microsoft Azure

Peu d'équipes SecOps peuvent couvrir toutes les bases dans le monde en évolution rapide de la cybersécurité d'Azure. C'est pourquoi il est important de s'associer à un spécialiste de la cybersécurité qui peut aider votre équipe à rester à jour et à se concentrer sur les priorités les plus importantes.

⚠ La problématique

"J'ai besoin d'une meilleure approche, plus définie, pour rester à la pointe des défis de sécurité en constante évolution."

Les opportunités

Identifier les risques liés au cloud

Effectuez une évaluation de votre architecture de sécurité actuelle pour identifier les failles et les risques à corriger.

Former votre équipe

Mettez à jour les compétences de votre équipe en organisant des séances d'information sur les principaux composants de sécurité d'Azure.

Développer des directives de sécurité du cloud

Créez un plan directeur pour la mise en œuvre de la cybersécurité et identifiez les meilleures pratiques dans votre entreprise.

Entraînement de vos outils

Configurez les outils d'apprentissage automatique et d'IA pour améliorer lla détection des shémas et réduire les faux positifs.

Établir une bonne gouvernance

Priorisez les objectifs de gouvernance et créez des indicateurs clés de performance automatisés pour faciliter le suivi de la sécurité et de la conformité.

Faites équipe avec les meilleurs

Concevez votre architecture de sécurité avec un partenaire stratégique de Microsoft.

74 %

des entreprises utilisent des produits SIEM pour automatiser les alertes de cybersécurité

2 à 3 jours

pour effectuer une mise en œuvre initiale d'un SIEM de cybersécurité (Sentinel)

43 %

de toutes les cyberattaques visent les petites entreprises