Optimisation de DatAlert

Renforcez proactivement votre sécurité pour mieux faire face à des menaces en constante évolution.

L'équipe de réponse aux incidents Varonis regroupe des analystes en cybersécurité internes disposant d'une vaste expérience en matière de détection et de réponse aux menaces. **Demandez-nous une session personnalisée** pour profiter de l'expertise de notre équipe et de notre produit. Vous pourrez ainsi optimiser votre utilisation de DatAlert et améliorer vos mesures de détection proactive des menaces.

- Offre gratuite pour nos clients DatAlert.
- Sessions animées par des experts de la sécurité spécialisés dans le domaine et le secteur
- Augmentation du ROI en matière de sécurité dans l'ensemble de l'écosystème

Comment ça marche

Le processus d'optimisation de DatAlert suit une méthodologie éprouvée pour vous aider à utiliser Varonis encore plus efficacement. Nos experts en sécurité vous aideront à :

- Établir des workflows de réponse aux alertes adaptés à votre environnement
- Optimiser DatAlert pour votre environnement et créer des alertes sur mesure
- Mettre en place une réponse automatisée pour bloquer les ransomwares
- Préparer et former votre équipe à la gestion des incidents avancés

★★★★★

Nos clients nous décernent **4,9/5 étoiles** sur **Gartner Peer Insights.**

« Le service client de Varonis est incroyable. Je n'ai rencontré une assistance aussi performante chez aucun autre fournisseur. L'équipe est extraordinairement motivée pour vous aider à utiliser le produit au mieux de ses capacités, de la façon la plus adaptée à tous vos besoins. »

Ingénieur en sécurité d'un fournisseur d'énergie américain

Lire l'étude de cas →

Voici les experts de l'équipe d'optimisation de DatAlert.

Matthew Radolec
Directeur de la réponse aux incidents et des opérations cloud

Ian Levy
Analyste sécurité en chef

Ian McIntyre
Expert réponse aux incidents en chef

Pierre-Antoine Failly-Crawford
Expert réponse aux incidents en chef

Résultats de la prestation

Créez une infrastructure de sécurité résiliente.

- Personnalisez les modèles de menaces en fonction de votre environnement, de vos données et de votre mission.
- Configurez votre canal d'alerte préféré (e-mail, journaux système ou SIEM).
- Intégrez les alertes de Varonis dans votre écosystème de sécurité, notamment avec les processus opérationnels et intégrations système (par ex. : SIEM, SOAR, etc.).

Bénéficiez de l'aide d'experts lors de vos investigations.

- Configurez des réponses automatisées à l'aide de scripts sur mesure.
- Formez l'équipe de sécurité pour qu'elle puisse mener des enquêtes en fonction du contexte, traquer les menaces et créer des alertes personnalisées.
- Recevez des recommandations pour améliorer la détection et la réponse.

Suivez l'évolution des menaces.

- Activez les mises à jour Varonis pour actualiser automatiquement les modèles de menaces dès que nécessaire.
- Activez le système de surveillance en ligne pour améliorer l'assistance produit et l'aide à la réponse aux incidents.
- Mettez en place des réunions régulières avec l'équipe de réponse aux incidents pour optimiser vos processus en place.

Demandez votre session d'optimisation de DatAlert.

Contactez l'équipe Varonis qui gère votre compte ou ouvrez un ticket auprès de notre équipe de réponse aux incidents.

Contactez-nous