Varonis permet à une équipe de sécurité composée d'une seule personne de gagner 400 heures par an : explications

ÉTUDE DE CAS

« Il est impossible pour une petite équipe de dégager assez de temps pour étudier les données et réaliser des analyses approfondies. Varonis nous apporte une aide inestimable sur ce point. C'est une solution incontournable pour doper l'efficacité d'une seule personne. »

À PROPOS DE CETTE ÉTUDE DE CAS :

Notre client est un hôpital américain. À sa demande, nous ne mentionnons aucun nom ni aucun lieu dans cette étude.

EN BREF

LES PROBLÈMES

- Limiter la menace posée par les ransomwares, qui pourraient mettre en danger la vie des patients
- Protéger les informations médicales personnelles et concernées par la loi HIPAA des menaces venues de l'intérieur et de l'extérieur
- Corriger les risques en s'appuyant sur une seule personne dédiée à la sécurité

LA SOLUTION

La plateforme de sécurité des données la plus solide :

- **DatAdvantage** permet de déterminer les fichiers sur lesquels les utilisateurs disposent d'un accès trop important et d'appliquer en toute sécurité un modèle de moindre privilège
- **DatAlert Suite** permet de surveiller en continu les données et systèmes, et de générer des alertes

RÉSULTATS

- Plus de 400 heures économisées chaque année
- Visibilité sur les serveurs sur site permettant à une seule personne de faire face aux ransomwares
- Tranquillité d'esprit depuis 2009 grâce à une solution de sécurité qui s'adapte aux besoins croissants de l'hôpital

Les problèmes

Protéger des systèmes essentiels susceptibles de sauver des vies

Pour les hôpitaux et entreprises du monde de la santé, la neutralisation des attaques des ransomwares constitue une véritable question de vie ou de mort.

En septembre 2020, une équipe de secours a dû emmener un patient dont le pronostic vital était engagé dans un autre hôpital que celui prévu, près de 30 km plus loin, car l'établissement le plus proche avait été compromis. Le patient est malheureusement décédé, et les médecins estiment que l'heure de retard induite par ce changement a contribué à cette fin tragique.

Un prestataire de santé américain, dont nous tairons le nom à sa demande, a bien compris ce risque et a par conséquent choisi de travailler avec Varonis depuis 2009.

> « Les malwares figurent parmi nos principales inquiétudes », explique le responsable de la sécurité. Un ransomware pourrait nous paralyser… ou pire. Toute attaque contre un hôpital peut poser un risque pour la sécurité des patients. Si un ransomware venait à nous paralyser pendant une semaine ou deux, cela poserait de graves difficultés à nos patients.
>
> La menace ne se limite pas aux ransomwares. Si nous ne luttons pas efficacement contre les menaces venues de l'intérieur et l'exfiltration de données, des données personnelles et informations médicales personnelles pourraient être prises en otage, et le chiffrement des fichiers pourrait causer de nombreux dégâts. »

Il est de notoriété publique que les équipes de sécurité des hôpitaux sont restreintes. Dans ce cas précis, une seule personne est chargée de protéger les données contre les attaques de ransomwares et d'assurer la conformité aux réglementations HIPAA et PHI.

> « Un grand nombre de nos fichiers contiennent des informations médicales personnelles et sont régis par les règles de sécurité HIPAA. Nous devons nous assurer que seules les personnes en ayant besoin peuvent y accéder. Sans solution comme celle proposée par Varonis, nous ne pourrions vraiment pas savoir qui accède aux fichiers et qui devrait y accéder. »

Même pour une équipe plus nombreuse, cette tâche serait chronophage. Pour une personne seule, elle est tout bonnement impossible, et c'est bien pour cette raison que l'hôpital a choisi Varonis.

> « Sans Varonis, les journées ne seraient pas assez longues pour me permettre de sécuriser notre réseau. C'est une tâche impossible pour une personne seule. »

> « Un ransomware pourrait nous paralyser… ou pire. Toute attaque contre un hôpital peut poser un risque pour la sécurité des patients. »

La solution

Visibilité et alertes pour les fichiers et systèmes stratégiques

DatAdvantage pour Windows aide ce responsable de la sécurité à évaluer, prioriser et limiter les risques de sécurité les plus importants pour les serveurs sur site de l'hôpital. Si un fichier est surexposé (accessible à tous) ou qu'un utilisateur commence à consulter, déplacer ou supprimer des données qu'il ne manipule pas habituellement, Varonis en informe le responsable de la sécurité en temps réel.

L'hôpital a par la suite ajouté **DatAdvantage pour Directory Services** à sa plateforme de sécurité. Cette solution prend en charge Active Directory et lui permet de disposer d'une visibilité complète sur les accès aux données des systèmes les plus stratégiques. DatAdvantage contribue à cette stratégie en détectant et corrigeant les problèmes de sécurité liés aux droits, groupes imbriqués et héritages.

> « Nous avons commencé avec DatAdvantage et avons ajouté la prise en charge de Directory Services, qui surveille les changements intervenant dans Active Directory. Nous en avions besoin, car nous ignorions jusque-là quels changements étaient effectués, par qui, où et comment. »

L'hôpital a également ajouté **DatAlert Suite** à sa pile de sécurité. En mettant au jour les menaces potentielles dans la chaîne d'attaque avant qu'elles ne s'aggravent, DatAlert joue un rôle central dans sa lutte contre les ransomwares.

> « DatAlert garde un œil sur tout ce qui se passe sur nos serveurs de fichiers et sur Active Directory. S'il détectait un ransomware ou une violation, nous en serions immédiatement informés. »

Mais même avec ces solutions, une seule personne chargée de la sécurité rencontrerait des difficultés pour arrêter seule une attaque ciblée. Dans ce type de situation, mieux vaut appeler la cavalerie : **c'est là que l'équipe de réponse aux incidents de Varonis entre en scène**.

> « Le produit d'un fournisseur a été compromis. L'équipe de réponse aux incidents nous a aidés à confirmer que le hacker n'avait pas été plus loin que cet appareil. Sans Varonis, cette tâche aurait été bien plus longue et difficile. »

> « DatAlert garde un œil sur tout ce qui se passe sur nos serveurs de fichiers et sur Active Directory. S'il détectait un ransomware ou une violation, nous en serions immédiatement informés. »

Résultats

400 heures économisées chaque année

D'après ce responsable de la sécurité, Varonis permet à une personne seule de gagner du temps, **au moins un jour de travail complet par semaine, soit plus de 400 heures par an.**

> « Il est impossible pour une petite équipe de dégager assez de temps pour étudier les données et réaliser des analyses approfondies. Varonis nous apporte une aide inestimable sur ce point. C'est une solution incontournable pour doper l'efficacité d'une seule personne.
>
> Le temps que je gagne me permet de me concentrer sur d'autres problèmes et de passer en revue des alertes sur lesquelles je n'aurais autrement pas le temps de me pencher. »

Ces gains sont appréciables, mais la tranquillité d'esprit apportée par la solution est un atout encore plus précieux. Le fait de savoir qu'ils peuvent verrouiller les données et appeler rapidement l'équipe de réponse aux incidents tranquillise le responsable de la sécurité et les dirigeants.

> « La situation actuelle en matière de sécurité n'est pas propice à la détente. Presque chaque jour, nous entendons parler d'un hôpital qui s'est fait pirater ou infecté par un ransomware. Je dors mieux en sachant que je dispose des outils nécessaires pour empêcher qu'un problème ne dégénère. »

L'hôpital réfléchit à ses prochaines actions et cherche à prendre des précautions supplémentaires pour protéger les données et la vie de ses patients. Pour atteindre cet objectif, le responsable de la sécurité espère ajouter rapidement davantage de solutions Varonis à son arsenal.

« Varonis a déjà détecté des comptes obsolètes, des droits incorrects et d'autres risques. Nous étudions la possibilité d'installer Automation Engine et sans doute Data Classification Engine peu après. »

« Le temps que je gagne me permet de me concentrer sur d'autres problèmes et de passer en revue des alertes sur lesquelles je n'aurais autrement pas le temps de me pencher. »

Varonis aide les petites équipes à garder la tête hors de l’eau.

Gagnez en visibilité, renforcez la sécurité des données et apaisez vos inquiétudes avec une équipe expérimentée à vos côtés.

DEMANDER UNE DÉMO