Comment Varonis permet à un groupe industriel français de se mettre en conformité avec NIS2

« La plateforme Varonis nous donne la possibilité d'avoir enfin de vraies pratiques sécurisées pour protéger notre donnée.

Témoignage

Notre client est un groupe industriel indépendant basé en France.

Points clés

Les défis

- Revoir des pratiques de protection de la donnée non sécurisées
- Sécuriser des répertoires ouverts sur Internet
- Apporter une visibilité sur la data

La solution

- Mettre en place une identification et une classification des données
- Remonter des incidents de sécurité Data Classification Engine
- Automatiser la résolution des problèmes liés à la donnée

Les résultats

- De 7,5 millions de répertoires ouverts à 19 000 avec accès restreints 99 % de permissions cassées réparées
- Une visibilité à 360° sur la donnée
- Un renforcement de la sécurité de l'Active Directory

Les défis

Des problématiques cyber non considérées

Ce groupe industriel français, quasi centenaire, a pris conscience de l'importance de la cybersécurité lorsque Saint Gobain a été victime de NotPetya.

En 2018, cette entreprise familiale décide donc de la création d'un poste de RSSI. D'autant que, depuis 2015, ce groupe, qui compte 7 sites de production en Europe, en Amérique du Nord et en Asie, ainsi que 22 sites commerciaux, opère sa transformation numérique et se tourne vers l'usine 4.0, connectée à Internet, les outils en mode SaaS...

A son arrivée, le nouveau RSSI constate que tout reste à faire : il n'y avait jusqu'alors aucune gouvernance cyber, puisque les problématiques cyber n'étaient pas considérées.

> **« Avant mon arrivée, il y avait des fuites de données sans arrêt. C'était tellement peu sécurisé que même Google arrivait à référencer des documents confidentiels »**
>
> **« A ma prise de poste fin 2018, j'ai découvert que nous étions dans le cliché de l'entreprise du secteur industriel : un legacy très important et des pratiques dangereuses en matière d'hygiène informatique. Par exemple, depuis une usine en Chine, il était possible d'accéder aux machines-outils en France ou aux Etats-Unis » précise le RSSI.**

VARONIS

La visibilité de la donnée

Dans les premiers mois, le RSSI travaille en mode pompier, à gérer les départs de feu ici et là. Mais, à plus long terme, « *l'entreprise avait besoin de projets structurants pour gagner des points de vie* ». A commencer par un important besoin de visibilité autour de la donnée et de l'usage qui en est fait.

> **En général je ne pouvais même pas dire où se trouvait la donnée, confidentielle ou non. Je parle ici de toute la donnée de la vie de l'entreprise, des données personnelles du salarié que l'on trouve chez les RH aux données de production des pièces dans telle ou telle usine.**

La solution

Data Security Platform de Varonis

Après de premiers contacts avec des commerciaux de Varonis, le groupe commence à installer la plateforme de POC de l'éditeur le 28 juin 2021. Le 2 juillet, lors de la première session de formation, la plateforme remonte deux incidents majeurs. D'un côté, un serveur ouvert sur Internet était scanné en permanence. De l'autre, un utilisateur quittait l'entreprise avec 3000 fichiers finance.

A l'époque, l'enjeu de visibilité se manifestait surtout quand les directeurs métiers venaient challenger le RSSI.

> **Les responsables métiers me demandaient quand on allait être piraté, je leur répondais à l'époque que la vraie question, était « depuis quand nous étions piratés.**

En effet, à ce moment-là, l'entreprise ne pouvait savoir s'il y avait un intrus sur son réseau, si quelqu'un d'extérieur avait accès aux données du groupe.

> **Nous avons ainsi pu tester l'équipe forensic de Varonis et tout cet aspect réponse à incident. Ils ont été en mesure d'analyser l'incident et de nous donner tous les éléments pour pouvoir le corriger au plus vite.**

Des répertoires ouverts aux quatre vents

Varonis assure donc une visibilité nouvelle pour le groupe sur ses données, à commencer par les serveurs de fichiers. Le RSSI s'aperçoit en effet que l'entreprise a 92 To de données dans 7,5 millions de répertoires. Et 4 millions de fichiers ouverts à tous, impliquant la possibilité d'accès par des personnes extérieures à l'entreprise.

Il n'était pas humainement possible que l'équipe du RSSI, composé d'un alternant et de lui-même, puisse traiter un tel volume de fichiers et de répertoires. Au début, le responsable cybersécurité s'attaque manuellement aux plus gros répertoires, mais « *rien qu'à trier, c'était déjà un cauchemar* ». Sans parler d'identifier et de classifier la donnée contenue dans ces fichiers.

Là encore, Varonis est arrivé en renfort, puisque la plateforme est en mesure, par OCR notamment, d'identifier les données, notamment celles à caractère personnelle (IBAN, passeport, permis de conduire…) ou encore les mots de passe renseignés en clair dans les documents. Avec l'aide de Varonis et de revues régulières des propriétaires et des droits, le groupe a été en mesure de réduire le nombre de répertoires ouverts à 19 000, avec des accès précis.

De l'importance d'une bonne configuration de l'AD

En outre, Varonis aide également le RSSI à garantir les bonnes configuration de l'AD. Car le groupe étant une entreprise familiale bien implantée localement, les salariés ont tendance à y faire carrière. Pendant une trentaine d'années dans la société, ces employés occupent diverses fonctions dans divers services, amassant les droits d'accès. Or, quand un stagiaire arrive, pour des questions de simplicité, lui est fournie une copie du profil de cette personne qui a trente ans d'historique. Autant de problèmes de configuration qui, une fois la plateforme de Varonis installée, font remonter des incidents de sécurité.

> **Avant mon arrivée, il y avait des fuites de données sans arrêt. C'était tellement peu sécurisé que même Google arrivait à référencer des documents confidentiels.**

Les résultats

Une automatisation sur l'ensemble du périmètre

L'industriel utilise désormais Varonis sur Sharepoint Onprem et Online, sa vingtaine d'outils de serveurs de fichiers, Teams, OneDrive et Active Directory, Azure et on premise. La plateforme a longtemps été la première source de remontée d'incidents de sécurité. Aujourd'hui, c'est l'outil anti-phishing qui émet le plus d'alertes, preuve que Varonis a permis de sécuriser les données du groupe. Ainsi, le groupe bénéficie d'une visibilité complète sur sa donnée.

> **Si vous me demandez là quelle quantité de données j'ai sur l'ensemble des serveurs ou un seul serveur, je peux vous sortir le chiffre. Je sais combien j'ai d'utilisateurs, à l'utilisateur prés. Je peux voir tout ce qui dévie de la politique de sécurité, par exemple si un compte ne respecte pas la password policy, ça va être remonté automatiquement.**

> **La plateforme m'offre une visibilité complète sur le nombre d'utilisateurs, le volume de données, les déviations par rapport à la politique, les OS obsolètes... Auparavant cela me prenait trois à quatre semaines pour obtenir ces informations par le biais de l'équipe infra. Je les obtiens désormais en trois clics. C'est un gain de temps inestimable.**

Une aide à la conformité

En tant qu'entreprise exerçant au sein de l'Union Européenne, nous devons entrer en conformité avec la directive NIS2. Varonis nous accompagne sur ce chemin en assurant la protection accrue de toutes nos données.

Notamment en détectant le fait que des données soient exfiltrées ou chiffrées massivement. Là encore, l'automatisation joue un rôle prépondérant, puisque les outils de sécurité mis en place par le RSSI vont désactiver automatiquement le compte suspect et déconnecter la machine.

> **Varonis est et va continuer d'être un très bon outil pour maintenir une gouvernance conforme autour de la data.**

Un plan d'action a été défini avec Varonis pour ajouter d'autres outils, de sorte à identifier les propriétaires de la données, archiver automatiquement les données obsolètes et supprimer les accès non légitimes.

> **Un été, l'automatisation mise en place avec les équipes Varonis a sauvé mes vacances. C'est vous dire à quel point je souhaite la poursuite de notre collaboration.**

> **Varonis nous permet rien de moins que de nous conformer à NIS2. C'est un enjeu crucial pour notre groupe et sa reconnaissance sur le marché.**

Attribuez automatiquement les droits d'accès réellement.

Automatisez votre gestion de la data pour une meilleure sécurité et conformité.

Demandez une démo