Étude de cas

QOSTODIAN PRIME™

Desjardins devient encore plus précis dans sa traque aux menaces internes

Desjardins

« Les autres outils suivent le mouvement des fichiers. Avec Prime, j'identifie l'origine d'un élément de donnée spécifique et je vois comment il s'est propagé d'une personne à l'autre au fil du temps – sans travail manuel. **Personne d'autre sur le marché ne fonctionne de cette façon. »**

Frederic Michaud,
Directeur principal, Évolution de la menace et innovation en sécurité de l'information,

Industrie
Services financiers, Banque

Cas d'utilisation
Prévention des menaces internes

Produit
QOSTODIAN PRIME

Le Mouvement Desjardins est le 1er groupe financier coopératif au Canada et le 5e au monde. Desjardins offre une gamme complète de produits et services aux particuliers et aux entreprises à travers son vaste réseau de distribution, ses plateformes virtuelles et ses filiales.

Défi

Classée parmi les banques les plus sûres d'Amérique du Nord par le magazine Global Finance, la confiance des clients est la pierre angulaire du Mouvement Desjardins. Propulsé par les meilleur talents internes et des solutions de cybersécurité de premier plan, Desjardins excelle dans la conformité aux réglementations canadienne et considéré comme une référence mondiale.

Au cours des quatre dernières années, Desjardins a investi massivement dans la numérisation de son offre de produits. Parallèlement, l'équipe de sécurité de Desjardins a mis en place une stratégie proactive pour protéger les données sensibles à travers toutes les technologies partenaires et leurs plateformes.

Frédéric Michaud, directeur principal chez Desjardins dans la division Menaces cybersécurité, approuve, met en œuvre et gère des outils, des processus et des analyses pour prévenir les menaces internes et la cyberfraude. Selon Frédéric, tous les outils ne se valent pas :

> **« Le problème de la plupart des logiciels est qu'ils se concentrent sur les fichiers, les postes de travail et les serveurs. Mais, lorsque vous effectuez une surveillance des menaces internes, vous vous souciez des utilisateurs, du comportement des gens. »**

Travailler avec d'autres outils signifiait que l'équipe de Frédéric devait effectuer d'importants travaux manuels lors des analyses. Au moyen d'appels téléphoniques, de visites au bureau et de suivis, une équipe interne a créé son propre cadre de triage et a travaillé à rebours pour déterminer le flux de données entre près de 50000 employés. Dans une organisation aussi massive que Desjardins, traquer ces informations et déterminer leur origine et mode de propagation n'a pas une tâche facile.

En plus de ces enquêtes fastidieuses, Frédéric et son équipe manquaient d'indicateurs clairs des niveaux de risque attachés à chaque élément mentionné dans les rapports. Il devenait donc ardu d'éliminer les faux positifs.

Solution

Afin d'accélérer les enquêtes, Frédéric a cherché une solution qui pourrait aider ses analystes de sécurité à :

- Faire une « chasse aux menaces » plus précise en réduisant le bruit et en triant en fonction du risque
- Suivre les informations sensibles quand elles se propagent entre les personnes
- Obtenir des résultats exploitables qui permettent de gagner du temps

Qostodian Prime™ en chiffres

	Outil précédent de Desjardins	Prime
Risque	Vues limitées du risque	Niveaux de risque quantifiés Suivi des employés à haut risque
Suivi	Fichiers seulement	Comportement de l'utilisateur Éléments de données
Enquête	Analyse manuelle laborieuse	Vue automatisée du mouvement des données entre les personnes au fil du temps

Après avoir évalué plusieurs fournisseurs, il a remarqué quelque chose d'étonnant : une seule solution sur le marché – Qostodian Prime – traque les éléments de données. Toutes les solutions concurrentes suivent les fichiers. Pourtant, les fichiers, ou les conteneurs pour les données, changent continuellement.

Avec Prime, Frédéric effectue désormais des recherches pour des éléments de données. Il peut voir chaque employé dans l'organisation ayant eu accès à ces données et comment les données se sont propagées de personne à personne, dans le temps. Selon Frédéric :

> **« Je peux localiser l'origine de ces données, voir quand elles sont sorties d'un environnement et remonter jusqu'à la première personne qui a fait une erreur, sans travail manuel. Chaque fois que nous trouvons une anomalie, il est vraiment facile de comprendre d'où elle provient. »**

Lors de l'exécution de recherches sur des mots clés spécifiques, Frédéric et son équipe tirent parti de la fonction de "hachage" de Prime, qui leur permet de rechercher des informations sensibles sans les stocker dans une base de données.

Frédéric a également découvert que, malgré la numérisation de documents volumineux et de tous les types de fichiers sur les postes de travail, les e-mails, OneDrive, etc., Prime avait la puissance nécessaire pour faire le travail 20 fois plus rapidement que les technologies concurrentes.

Résultats

Prime fournit à Frédéric et à son équipe la pleine contextualisation des résultats d'analyse. Armée de rapports qui suivent les informations sensibles entre les personnes et qui listent les prochaines étapes de façon claire, l'équipe réagit avec rapidité et confiance, rendant le travail manuel désuet.

L'équipe d'analystes de sécurité de Fréedéric traque désormais les menaces plus efficacement, en triant avec précision pour faire face aux plus gros risques. Il ajoute:

> **« Je peux déterminer en quelques secondes si quelque chose pose problème ou non. Prime nous permet de hiérarchiser les menaces des plus malveillantes aux moins malveillantes en toute confiance. Une plus grande productivité et une meilleure efficacité de mon équipe équivaut à une meilleure sécurité pour nos membres. »**

Les rapports de Prime aident également la direction à garder un œil sur la situation dans son ensemble. «En plus des données granulaires, qui nous permettent de surveiller les employés à risque et de garantir qu'ils respectent les politiques et les procédures, je peux également prendre du recul et évaluer les informations au niveau macro pour gérer efficacement les risques, » explique Frédéric.