Questions et réponses #4-15 à la demande de renseignements 1000464174 Solution de gestion de la fraude d'entrepri

La modification à cette demande de renseignements est émise pour répondre aux questions suivantes soumises durant la période de soumissions, conformément à la demande de renseignements.

Q4) Nombre d'utilisateurs qui devraient utiliser l'application de la gestion de la fraude d'entreprise (GFE)? Combien de privilèges différents sont attendus?

R4) Quelque 200 utilisateurs utilisent environ 25 profils LDAP (protocole allégé d'accès annuaire) avec divers privilèges.

Q5) Quel est le volume estimatif de données saisies sur une base quotidienne? La demande de propositions mentionne environ 40 000 utilisateurs surveillés.

R5) Veuillez noter que l'Agence du revenu du Canada a émis une demande de renseignements et non une demande de propositions. À l'heure actuelle, l'Agence compte environ 40 000 utilisateurs surveillés qui génèrent environ 25 millions de transactions par jour dans les applications surveillées. À l'heure actuelle, l'Agence capte en moyenne environ 2,4 millions de mégabits (Mo) de trafic sur le réseau par heure. L'Agence prévoit élargir l'utilisation de la gestion de la fraude d'entreprise (GFE) et prévoit que la capacité devra augmenter à 4 millions de mégabits (Mo) par heure dans le trafic saisi.

Q6) Lesquels des systèmes de l'Agence doivent être intégrés afin de surveiller les activités des utilisateurs?

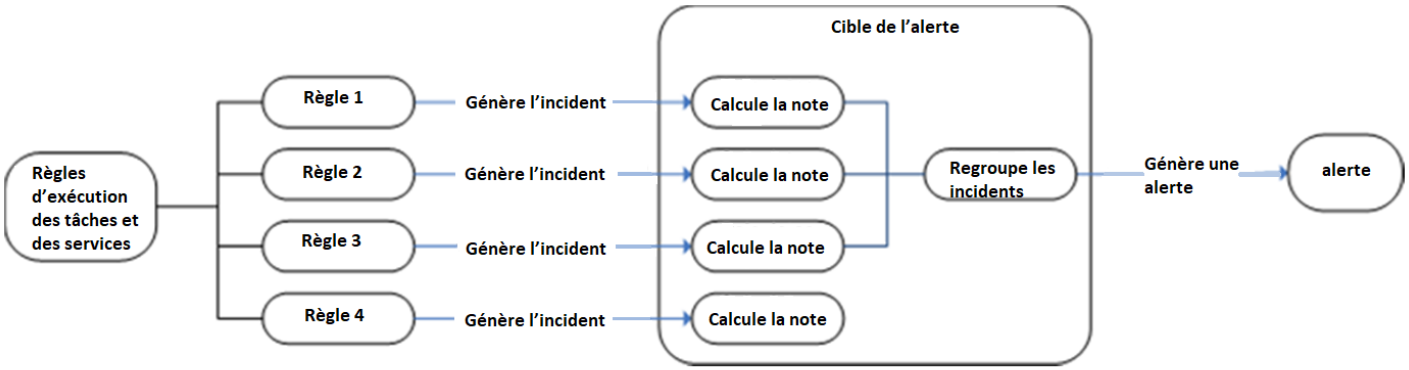
R6) Les cinq plateformes énumérées à la section 4.1 de la demande de renseignements devraient être intégrées pour surveiller les activités des utilisateurs.

Q7) Quelles sont les attentes relatives au calendrier du projet en ce qui a trait à la sélection des fournisseurs et à la mise en œuvre?

R7) Les attentes relatives au calendrier du projet en ce qui a trait à la sélection des fournisseurs seront déterminées au cours d'une demande de propositions, si l'Agence décide de procéder à un processus d'approvisionnement par l'intermédiaire d'une demande de propositions. En ce qui concerne la mise en œuvre du lancement, on s'attend à ce qu'une nouvelle solution soit entièrement mise en œuvre et soit opérationnelle d'ici l'été 2026.

Q8) Pouvez-vous fournir votre flux de travail actuel ou les diagrammes de flux de travail souhaités?

R8) Consultez le diagramme du flux de travail ci-dessous.



Q9) Quel est votre échéancier pour le lancement du projet?

R9) Si l'Agence décide de procéder à une demande de propositions, on s'attend à ce que le projet commence à l'été 2024.

Q10) Quelles sont les règles d'affaires existantes dans la GFE actuelle ou les règles d'affaires souhaitées à analyser?

R10) Les règles d'affaires comprennent la détection des accès des employés aux renseignements de nature délicate des contribuables dans les applications de l'Agence qui ne font pas partie de leur charge de travail. Par exemple, détecter les accès d'un employé à son propre compte de contribuable ou à des comptes de contribuable avec lesquels l'employé a une relation personnelle. Les cas d'utilisation comprennent également la détection des transactions frauduleuses effectuées par les employés dans les applications de l'Agence. Par exemple, la détection de faux dossiers ou de modifications non autorisées dans les registres comptables qui entraînera ultimement un avantage financier pour l'employé. La solution actuelle de la GFE de l'Agence a la capacité de personnaliser les nouvelles règles d'affaires, qui sont entièrement codées à l'interne par la TI afin de répondre aux exigences précises de l'Agence. En raison de la nature délicate des règles d'affaires, les exigences précises des règles d'affaires ne peuvent pas être communiquées.

Q11) Combien d'appareils sont censés surveiller?

R11) L'Agence surveille actuellement 60 adresses IP uniques (serveurs d'applications et de bases de données) ainsi qu'un ordinateur central en production.

Q12) Combien d'emplacements sont censés être surveillés?

R12) À l'heure actuelle, l'Agence surveille les hôtes dans deux centres de données. Toutefois, à mesure que les applications passent au nuage, l'Agence devra surveiller les appareils hébergés sur les fournisseurs de services infonuagiques.

Q13) Y a-t-il des utilisateurs qui travaillent à domicile?

R13) Oui, les utilisateurs sur place et à distance doivent être surveillés. Les utilisateurs de la GFE doivent également être en mesure d'accéder à la solution de la GFE sur place et à distance. La solution actuelle surveille le côté de l'application, de la base de données et de l'ordinateur central de la conversation, et non le trafic hébergé par les utilisateurs. (P. ex., une personne qui visite cbc.ca par l'intermédiaire de son navigateur ne serait pas vue par les captures de l'Agence, car elle n'atteint jamais l'un des hôtes surveillés de l'Agence.) Toutefois, les nouvelles solutions peuvent fonctionner en étant installées sur le système de l'utilisateur, mais cela serait une divergence de la configuration actuelle.

Q14) Qu'est-ce qui déclenche une enquête pour que les données soient analysées?

R14) Les transactions des utilisateurs surveillés sont saisies, déchiffrées et analysées par rapport aux règles d'affaires prédéfinies par la solution de la GFE actuelle. Si la transaction des utilisateurs surveillés enfreint une règle d'affaires, une alerte est créée avec une cote de risque qui déclenche une enquête préliminaire des transactions des utilisateurs surveillés. Si cela est justifié, une enquête officielle est ensuite lancée.

Q15) Est-ce qu'on s'attend à une migration des données du système existant?

R15) Oui, on s'attend à ce que les données existantes soient migrées vers une nouvelle solution. Les données existantes comprennent les renseignements historiques sur les cas et les alertes, la configuration de règles d'affaires, les données de surveillance saisies et les données sources.