Sommaire de gestion · Octobre 2026

Rapport mensuel de cybersécurité

Entreprise de services professionnels · Deux bureaux au Québec

Un nouveau compte ayant accès aux dossiers de projets partagés échappait à la politique d'authentification multifacteur. Un portable a cessé de communiquer. Son état de protection reste inconnu.

Du 1er au 31 octobre · Heure du Québec · Publié le 2 novembre 2026

Octobre en bref

6 / 6
Détections examinées sur les postes
Un fichier mis en quarantaine

47 / 48
Postes qui communiquent
Dernier signal du portable le 19 oct.

51 / 52
Comptes visés par la politique d'AMF
Les 3 administrateurs sont couverts

Décision du client · Échéance du 3 novembre

Protéger la connexion du nouvel utilisateur.

Le responsable TI du client doit autoriser l'ajout du compte à la politique d'authentification multifacteur (AMF). Si l'inscription est impossible d'ici le 3 novembre, il doit décider s'il suspend les connexions interactives jusqu'à ce que l'utilisateur soit prêt.

Ce qui a changé en octobre

Alerte sur un poste	Un poste a mis un programme d'installation potentiellement indésirable en quarantaine. DITC a vérifié la mise en quarantaine et l'analyse de suivi. Les éléments examinés justifiaient la fermeture de l'alerte sur ce poste.
Correctifs	44 des 48 postes respectaient la cible de mise à jour, contre 41 pour le même parc en septembre. Il reste trois écarts connus et un poste dont l'état est inconnu. Il s'agit du portable qui a cessé de communiquer.

Portée de cet exemple

DITC examine les alertes des postes pendant les heures convenues, les relevés de correctifs et les politiques de connexion. Le client autorise les changements aux comptes. Le contenu des boîtes courriel, les charges infonuagiques et une enquête complète sur incident sont hors mandat.

Analyse des alertes · Octobre 2026

Pourquoi l’alerte a été fermée

Le 14 octobre, l’agent de protection a mis un fichier en quarantaine. Le poste a continué de communiquer jusqu’à la fin du mois. Le portable hors ligne est un autre appareil.

Résultat de l’examen des six détections

4 Tâches administratives autorisées · 1 Outil de mise à jour vérifié · 1 Fichier mis en quarantaine

Cinq événements correspondaient à des activités autorisées. Un logiciel potentiellement indésirable a été détecté et mis en quarantaine. Aucun incident n’a été confirmé parmi les six détections examinées.

De la détection à la fermeture

Date et heure	Constats et interprétation
14 OCT. 9 h 12	**L’agent a mis le fichier en quarantaine.** L’événement CrowdStrike identifiait un programme d’installation sur un seul poste. Le journal des actions confirmait la mise en quarantaine.
14 OCT. 9 h 37	**DITC a examiné l’activité du poste.** Les événements de processus consultés montraient le téléchargement. DITC n’y a relevé aucune trace d’exécution du programme sur ce poste.
14 OCT. 10 h 26	**L’analyse de suivi s’est terminée.** L’analyse n’a relevé aucune autre détection. DITC a vérifié que l’agent communiquait et a fermé l’alerte en consignant l’événement, la quarantaine et le résultat de l’analyse.
31 OCT. Fin du mois	**DITC a vérifié si la détection s’était répétée.** Le poste a continué de communiquer. Aucune détection correspondante n’est réapparue dans les données disponibles jusqu’à la clôture du mois.

Quand rouvrir le dossier

Une détection correspondante sur un autre appareil, une preuve d’exécution ou l’échec de la quarantaine entraînerait un nouvel examen et un avis au responsable de la sécurité du client. La conclusion porte sur les données consultées pour ce poste.

Plan d’action · Octobre 2026

Trois mesures de sécurité à prendre

La première décision concerne un compte utilisateur. Les deux autres mesures visent le portable hors ligne et les correctifs en retard. Chaque responsable doit consigner une preuve avant de fermer son suivi.

Responsable et échéance	Mesure et preuve de clôture
03 NOV. Responsable TI du client	**Protéger un compte actif sans privilège administratif** Appliquer la politique d’AMF approuvée et consigner une connexion réussie qui respecte cette exigence. Si l’accès est suspendu, consigner le blocage et poursuivre le suivi jusqu’à la vérification de l’AMF.
04 NOV. Responsable du site client	**Localiser le portable vu le 19 octobre** Confirmer qui détient le portable. Après la reconnexion, DITC vérifie que l’agent communique et que les correctifs ont été analysés. Si le portable reste introuvable, aviser le responsable de la sécurité du client le jour même et garder le dossier ouvert.
06 NOV. Responsable des postes, DITC	**Régler les trois écarts de mise à jour connus** Coordonner les deux redémarrages. Tester le correctif reporté avec le responsable de l’application avant de le déployer. Fermer chaque écart sur preuve d’une nouvelle analyse conforme à la cible.

Vérification de fin de mois

Comment lire les chiffres de couverture

Visibilité des postes	Signaux CrowdStrike comparés à l’inventaire NinjaOne. Un poste est compté comme actif s’il a communiqué dans les 24 heures précédant le 31 octobre à 23 h 59, heure du Québec. Le portable hors ligne reste parmi les 48 postes.
Couverture des comptes	Politiques effectives de connexion de Microsoft Entra ID comparées aux 52 comptes utilisateurs actifs. Les trois comptes administrateurs étaient couverts. Les comptes invités et de service sont exclus du calcul.
Cible de mise à jour	Le poste doit avoir été analysé par NinjaOne dans les 24 heures et n’avoir aucun correctif de sécurité du système approuvé depuis plus de 14 jours en attente. L’état du portable hors ligne reste inconnu.

Suivi du 9 novembre

DITC et le responsable TI du client feront le point sur les trois mesures. Consigner séparément tout compte suspendu ou appareil retiré pour expliquer une variation du nombre total. Reporter les mesures en cours avec un responsable et une nouvelle échéance.