Livre blanc

La fraude de la part des candidat·es dans l'embauche en entreprise

Un cadre de gestion des risques pour les responsables des ressources externes

Mars 2026

Table des matières

À quel moment l’embauche s’est-elle mise à exiger du travail d’enquête?

La fraude de la part des candidat·es n’est pas un problème nouveau. L’embellissement des CV, le gonflement des références et l’exagération de l’expérience font partie des réalités de l’embauche depuis des décennies. Ce qui change fondamentalement, c’est l’infrastructure derrière la fraude : des réseaux organisés qui orchestrent des opérations de placement coordonnées, des outils d’intelligence artificielle (IA) qui génèrent des CV soignés et qui accompagnent les candidat·es en temps réel pendant les entrevues en direct, ainsi qu’un environnement de travail à distance qui a éliminé de nombreux signaux en personne sur lesquels les gestionnaires d’embauche se fiaient, sans les remplacer par quoi que ce soit d’équivalent.

Voilà pourquoi la fraude de la part des candidat·es persiste, et pourquoi il devient plus difficile de la déceler. Parfois, elle est flagrante. Le plus souvent, elle est ordinaire. Un CV correspond presque parfaitement à la description du poste. Les antécédents professionnels sont techniquement vérifiables, mais pas nécessairement ceux sur lesquels l’entrevue s’est appuyée. L’emplacement d’un·e travailleur·se ou ses plages de disponibilité ne correspondent pas à ce qui avait été convenu. Dans bien des cas, la personne est en mesure d’effectuer le travail. La fausse déclaration porte sur l’employeur réel de la personne, sur son lieu de travail ou encore sur la manière dont le travail est effectué.

La plupart des organisations ne sont pas conçues pour détecter ces situations. L’embauche repose sur une base de bonne foi. Un·e gestionnaire qui évalue un·e candidat·e veut croire que la personne devant lui·elle est réellement celle qu’elle prétend être. Lorsque quelqu’un se présente bien, communique avec assurance et possède un CV qui correspond au poste, le réflexe est de se sentir rassuré, non de mener un interrogatoire. Ce réflexe n’a rien d’une naïveté; c’est ainsi que commencent des relations de travail efficaces. Toutefois, il s’agit aussi de la brèche que la fraude de la part des candidat·es vise précisément à exploiter. Les gestionnaires d’embauche ne participent au processus d’embauche que de manière ponctuelle, et non à temps plein, et il·elles ne voient qu’un échantillon limité de CV chaque année. Lorsqu’un dossier paraît excellent sur papier, la pression est bien réelle; les petites incohérences se trouvent rationalisées et ne prennent tout leur sens qu’après coup, une fois que les coûts ont déjà été absorbés.

Des opérations sophistiquées et des scénarios à fort retentissement existent bel et bien, surtout dans des environnements de travail à distance. Cependant, l’exposition aux risques la plus courante ne suppose pas un architecte de la fraude. Elle découle plutôt de lacunes simples dans la vérification, de transitions maladroites entre les équipes et de processus d’embauche conçus pour la rapidité plutôt que pour la détection.

Les programmes de ressources externes sont au cœur de cette exposition aux risques. Les canaux d'embauche de contractuel·les sont généralement plus ouverts que ceux utilisés pour le recrutement d'employé·es permanent·es. Le rythme des placements est plus élevé, les périodes de vérification sont plus courtes et la multiplication des intermédiaires crée des failles de sécurité que des acteurs sophistiqués exploitent.

Les programmes d'employeur officiel (EOR) et d'agent officiel (AOR) présentent un risque particulier : les gestionnaires d'embauche du·de la client·e repèrent et sélectionnent les travailleur·ses souhaité·es, mais il·elles ne disposent généralement pas des capacités de détection de fraude au sein du service de recrutement d'une agence de dotation en personnel ou de la fonction d'embauche des employé·es permanent·es du·de la client·e. Il en résulte une surface d'exposition aux risques plus importante, que la plupart des organisations n'ont pas évaluée au regard du contexte actuel des menaces.

Plusieurs facteurs expliquent cette augmentation du risque :

1. Les gestionnaires sont souvent soumis·es à une forte pression pour pourvoir les postes afin d'atteindre les résultats attendus. Les CV conçus pour correspondre à un poste donné peuvent paraître parfaitement harmonisés avec les résultats recherchés.
2. Les gestionnaires ne consultent que les CV liés à leurs postes actuels, sans visibilité sur l'ensemble du marché de l'embauche; il·elles ne voient donc pas les tendances récurrentes que les agences de dotation en personnel constatent en analysant des milliers de candidatures.
3. Confiance : les personnes ont généralement tendance à croire que ce qu'elles entendent est vrai.
4. Leurs propres préjugés peuvent aussi intervenir; par exemple, lorsque la personne a été recommandée par un·e collègue ou qu'elle présente des références particulièrement convaincantes.

Ce document s'adresse aux responsables des programmes de ressources externes, qu'il·elles relèvent du service des ressources humaines, du service d'acquisition de talents, du service des achats ou d'une fonction dédiée à la main-d'œuvre. Il propose un cadre de compréhension des six principaux mécanismes de fraude actuellement actifs dans l'embauche, un modèle d'évaluation des coûts réels, une architecture de défense pratique et un outil d'autoévaluation pour analyser votre situation actuelle.

Les organisations les mieux placées pour gérer ce risque sont celles qui considèrent la fraude de la part des candidat·es comme un enjeu de gestion des risques organisationnels, et non comme un simple contretemps lié à l'embauche, et qui investissent en conséquence.

À propos de l'auteur

Kent McCrea,
Chef de la direction et président de procom

Kent McCrea possède plus de 15 années d'expérience à la tête de l'une des principales entreprises de dotation en personnel au Canada, fournissant des services-conseils et des solutions de main-d'œuvre à bon nombre des plus grandes organisations nord-américaines. À mesure que les capacités de l'IA se perfectionnent et se généralisent, il apporte une perspective unique sur l'évolution du paysage de la dotation en personnel, grâce à une connaissance approfondie des tendances émergentes du marché et des mutations du secteur.

Avec les contributions de
Wendy Kennah,
Chef de l'exploitation

RÉSUMÉ

La menace est systémique. La fraude de la part des candidat·es se déploie désormais à trois niveaux : des individus opportunistes, des organisations commerciales structurées et des acteurs étatiques, chacun utilisant six mécanismes distincts qui exploitent les failles présentes tout au long du cycle d'embauche.

Les programmes de ressources externes sont exposés de façon disproportionnée. Un rythme de placement plus élevé, des périodes de vérification plus courtes, des transitions multipartites et des capacités limitées de détection de fraude au niveau des gestionnaires d'embauche font des canaux d'embauche des contractuel·les une cible privilégiée pour les groupes de fraude organisés. Les programmes d'EOR et d'AOR, dans le cadre desquels les gestionnaires du·de la client·e sélectionnent des travailleur·ses sans disposer d'une infrastructure de présélection dédiée, présentent un niveau de risque plus élevé.

Le coût est plus élevé que ce que la plupart des organisations reconnaissent, car les pertes les plus courantes sont aussi les moins visibles. Les frictions habituelles liées à l'embauche sont absorbées sans être réellement mesurées. Les pertes dues à la fraude salariale sont considérées comme des erreurs d'embauche. Les dommages opérationnels découlant du cumul d'emplois ou de la sous-traitance non autorisée sont attribués à des problèmes de rendement. Seuls les incidents catastrophiques, notamment le vol de propriété intellectuelle, les sanctions réglementaires ou les rançongiciels, forcent les organisations à s'attaquer à la fraude qui les sous-tend. À ce stade, un simple placement a déjà engendré des dommages indirects se chiffrant en millions.

La protection contre la fraude exige une approche intégrée tout au long du cycle d'embauche. Une atténuation efficace de la fraude repose sur la superposition de contrôles fondés sur la technologie, les processus et l'expertise humaine, et ce, à chacune des quatre phases du cycle d'embauche : avant l'embauche, pendant l'embauche, durant l'affectation et après l'embauche. Les organisations qui concentrent leurs vérifications dans une seule phase ou qui s'appuient sur un seul type de contrôle créent des failles prévisibles que des fraudeur·ses sophistiqué·es chercheront à exploiter.

Commencez par évaluer votre posture de risque. Le cadre d'autoévaluation présenté à la section 5 permet aux organisations d'évaluer leurs contrôles actuels par rapport au contexte de menaces et de déterminer où les failles génèrent la plus grande exposition au risque.

Principaux cadres présentés dans ce document

Ce document présente cinq cadres interconnectés :

1. **les trois niveaux de menace,** qui classent les acteur·rices de la fraude selon leur sophistication et leur incidence;
2. **les six mécanismes de fraude,** soit une taxonomie des schémas d'attaque actifs dans le recrutement;
3. **le continuum des coûts,** qui présente quatre niveaux d'exposition organisationnelle allant des coûts liés aux frictions aux pertes catastrophiques;
4. **le modèle de protection du cycle d'embauche,** c'est-à-dire une architecture en quatre phases et trois modalités pour des contrôles intégrés de la fraude;
5. **l'autoévaluation de la posture face au risque de fraude,** un outil diagnostique pour évaluer les protections actuelles.

Section 1 : le nouveau paysage de la fraude

Perspective clé :

La plupart des organisations conçoivent leurs processus d'embauche pour repérer les individus opportunistes (niveau 1). Ces contrôles offrent une protection minimale contre les opérations de fraude organisées (niveau 2) et pratiquement aucune protection contre les acteurs soutenus par des États (niveau 3). Les canaux de ressources externes, qui fonctionnent avec des volumes plus élevés, des cycles de vérification plus courts et des transitions multipartites, sont ceux où ce décalage est le plus facile à exploiter.

Trois niveaux de menace

Catégorie	*Type d'acteur*	*Motivation*	*Niveau de sophistication*	*Difficulté de détection*	*Incidence sur l'entreprise*
Niveau 1	Individus opportunistes	Gain financier personnel, avancement professionnel	Faible à moyen	Relativement facile	Faible à moyen
Niveau 2	Opérations organisées	Fraude commerciale à grande échelle	Moyen à élevé	Modéré	Moyen à élevé
Niveau 3	Acteurs soutenus par des États	Financement d'armement, espionnage, attaques visant les chaînes d'approvisionnement	Très élevé	Très difficile	**Grave**

La taxonomie de la fraude : six mécanismes dans l'acquisition de talents

Il ne s'agit pas de nouveaux types de fraude. Il s'agit de modes d'attaque bien établis, raffinés au fil de décennies dans les services financiers, les chaînes d'approvisionnement et la cybersécurité, qui migrent maintenant vers le recrutement. Chaque mécanisme ci-dessous précise le secteur où il a été développé et où les contre-mesures les plus avancées existent. Ces parallèles sont pertinents : les enseignements tirés de ces domaines permettent de déterminer les stratégies efficaces pour se prémunir contre les variantes utilisées dans le recrutement.

1 ***Falsification des références des candidat·es***
Falsification des certifications, des antécédents d'emploi ou des qualifications.

2 ***Fraude d'identité et usurpation d'identité***
La personne rencontrée en entrevue n'est pas celle qui effectue réellement le travail.

3 ***Sous-traitance non autorisée et substitution de travailleur·ses***
Un travailleur délègue secrètement une partie ou la totalité de son travail à des tiers non déclarés.

4 ***Cumul d'emplois et conflits non déclarés***
Des travailleur·ses occupent simultanément plusieurs postes à temps plein sans le déclarer.

5 ***Fausse déclaration de lieu ou d'accès***
Des travailleur·ses déclarent faussement leur emplacement physique.

6 ***Surestimation des compétences et fausse déclaration assistée par l'IA***
Des candidat·es font de fausses déclarations sur leur niveau de compétence réel grâce à des évaluations assistées par l'IA.

1. Falsification des références des candidat·es

Parallèle sectoriel : Fraude liée aux produits contrefaits (chaîne d'approvisionnement sectorielle)

Définition : Falsification des diplômes, des certifications professionnelles, des antécédents professionnels ou des qualifications techniques.

Surface d'attaque : Phase préembauche (tri des CV, examen des candidatures, qualification initiale)

Ces cas de fausse déclaration sont généralement le fait d'une seule personne et ne sont pas toujours malveillants; toutefois, il s'agit néanmoins d'une forme de fraude.

Cela peut se manifester par un·e candidat·e dont les compétences paraissent adéquates sur papier, mais dont l'expérience sectorielle n'est peut-être pas la bonne, ou encore par une expérience acquise à l'étranger qui ne se transpose pas nécessairement à la réalité nord-américaine.

Dans d'autres cas, le CV, les références, les échantillons de projets, les titres professionnels et la formation sont fabriqués ou, pire encore, volés. La personne qu'il·elles affirment avoir eu comme supérieur·e peut être un·e ami·e, et les lieux de travail déclarés dans le système de vérification des antécédents professionnels ne correspondent pas au CV.

Indicateurs de détection :

- Numéros de certification dont le format semble valide, mais qui ne figurent dans aucune base de données officielle de l'organisme émetteur
- Emploi dans des entreprises ayant une empreinte numérique minimale ou une existence brève
- Explications techniques vagues ou incohérentes lors de discussions approfondies
- Connexions LinkedIn principalement avec d'autres personnes présentant des profils professionnels similaires
- Nouveau profil LinkedIn sans photo et ne comportant que peu de relations, de publications ou d'interactions
- Références qui n'ont pas travaillé aux mêmes endroits aux mêmes périodes, ou référence n'ayant pas occupé un poste de direction et n'étant donc vraisemblablement pas le·la gestionnaire du·de la candidat·e
- Références ne laissant aucune trace numérique (LinkedIn, courriel professionnel, etc.)

2. Fraude d'identité et usurpation d'identité

Parallèle sectoriel : Vol d'identité et fraude par prise de contrôle de comptes (services financiers)

Définition : La personne rencontrée en entrevue n'est pas celle qui effectue réellement le travail, ce qui peut résulter de mandataires d'entrevue, de substitutions vidéo rendues possibles par des vidéos truquées (deepfake), de tactiques d'appât et substitution après l'embauche ou encore de profils synthétiques créés à partir de renseignements personnels volés.

Surface d'attaque : Phase d'entrevue jusqu'à la période de travail initiale

La fraude d'identité exploite l'écart entre les entrevues virtuelles et le travail réel. Les mandataires d'entrevue représentent la variante la plus simple. La technologie des vidéos truquées (deepfake) en temps réel permet désormais d'échanger les visages pendant les appels vidéo avec un mouvement des lèvres synchronisé, contournant ainsi les politiques de vérification visuelle et d'activation de la caméra.

Scénario — vol de salaire : Une entreprise embauche un·e ingénieur·e en infrastructure infonuagique présentant de solides références. En quelques semaines, le·la nouveau·elle employé·e éprouve des difficultés à accomplir des tâches élémentaires et évite les appels vidéo. Au bout de six semaines, il·elle est licencié·e pour des raisons de rendement. Une enquête menée après le départ révèle une identité volée. La personne qui occupait le poste n'était pas celle qui avait passé les vérifications. Le coût total, comprenant le salaire versé sous une identité frauduleuse, le recrutement, l'intégration, les retards de projet et la nouvelle embauche, dépasse 65 000 $ sans recours réel possible.

Scénario — espionnage et exposition réglementaire : Une entreprise de logiciels-services embauche un·e développeur·se principal·e après trois solides entrevues vidéo. Après son intégration, plusieurs signaux d'alerte s'accumulent : une communication écrite de moindre qualité, des appels audio seulement de façon persistante et des habitudes de travail laissant supposer un autre fuseau horaire. Six mois plus tard, un audit de sécurité révèle que des référentiels de code ont été clonés de manière systématique sur des serveurs externes. L'identité de la personne embauchée avait été volée. La personne qui effectuait réellement le travail se trouvait à l'étranger. Le montant total des dommages (réarchitecture du système, sanctions réglementaires, notification des client·es) dépasse 8 millions de dollars.

Indicateurs de détection :

- Évitement constant des appels vidéo ou des rencontres en personne après l'embauche
- Incapacité d'utiliser l'équipement fourni par l'entreprise
- Qualité des communications incohérente avec le rendement observé durant l'entrevue
- Modes de travail incompatibles avec le fuseau horaire déclaré
- Lacunes techniques qui se manifestent après l'embauche malgré une entrevue concluante
- Utilisation inhabituelle d'un réseau privé virtuel (RPV) ou accès à partir d'emplacements géographiques inattendus ou d'adresses IP itinérantes

Contexte réel

En 2024, le département de la Justice des États-Unis a inculpé plusieurs personnes dans le cadre de stratagèmes visant à placer des travailleur·ses étranger·ères du secteur informatique à des postes à distance au sein d'entreprises américaines en utilisant des identités américaines volées. Les procureur·es ont décrit des opérations générant des millions de dollars en salaires frauduleux, dont les recettes étaient dans certains cas détournées pour soutenir des programmes étrangers sanctionnés. Ces affaires illustrent la convergence de la fraude d'identité, de la fausse déclaration de lieu et d'objectifs associés à des acteurs étatiques, tels que décrits dans les mécanismes 2 et 5 ainsi que dans le modèle de menace de niveau 3.

3. Sous-traitance non autorisée et substitution de travailleur·ses

Parallèle sectoriel : Fraude par sociétés fictives (services financiers); substitution de sous-traitant·es (marchés publics)

Définition : Un·e travailleur·se embauché·e délègue secrètement une partie ou la totalité de son travail à des tiers non déclarés. Le·la client·e croit recevoir un travail effectué par une personne connue et vérifiée, mais le travail est en réalité effectué par des parties inconnues et non vérifiées, n'ayant aucune obligation contractuelle.

Surface d'attaque : Post-embauche (phase d'exécution du mandat)

La sous-traitance repose sur plusieurs motivations : l'arbitrage des capacités (le·la travailleur·se embauché·e n'est pas en mesure d'exécuter le travail et agit comme intermédiaire), l'arbitrage des coûts (un·e développeur·se local·e sous-traite à l'étranger ou localement, et empoche la différence de taux) et la captation d'accès (le fait de donner à des tiers non déclarés un accès aux systèmes du·de la client·e). Dans toutes les variantes, des individus inconnus, sans vérification des antécédents et sans obligations contractuelles, accèdent aux systèmes de production grâce à des identifiants partagés, invisibles pour le·la client·e.

Indicateurs de détection :

- Accès simultané aux systèmes à partir de plusieurs emplacements géographiques
- Style ou approche de codage incohérent entre les différents produits de travail
- Travail soumis à des heures inhabituelles pour le fuseau horaire déclaré
- Adresses IP associées à des services de RPV ou à des centres de données
- Style de communication ou maîtrise linguistique ne correspondent pas au rendement observé durant l'entrevue
- Refus d'activer la caméra lors des réunions
- Ne répond pas aux appels et insiste pour rappeler afin de se donner le temps de mettre la bonne personne en ligne

4. Cumul d'emplois et conflits non déclarés

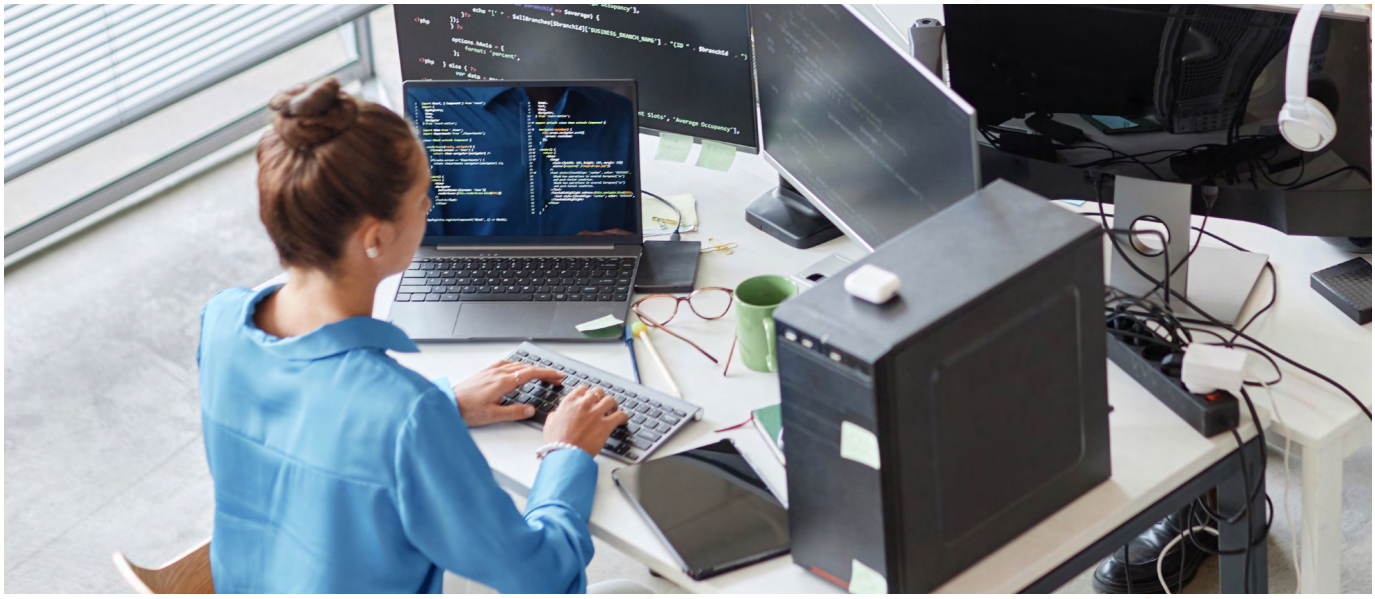
Parallèle sectoriel : Menaces internes (cybersécurité); fraude liée aux conflits d'intérêts (gouvernance d'entreprise)

Définition : Des travailleur·ses occupent simultanément plusieurs postes à temps plein sans le déclarer, ce qui entraîne une attention divisée, des conflits d'horaires et des conflits d'intérêts potentiels. Cette situation se distingue du cumul d'emplois autorisé ou du travail à temps partiel déclaré.

Surface d'attaque : Post-embauche (gestion continue du mandat)

Le risque se manifeste sur un continuum. Au niveau le plus bas, un emploi secondaire non déclaré crée des conflits de temps et d'attention qui entraînent une baisse du rendement. À l'autre extrémité, des postes occupés simultanément chez des concurrent·es direct·es entraînent des fuites d'informations et une violation potentielle des obligations fiduciaires. Même sans intention malveillante, des travailleur·ses cumulant plusieurs emplois confronté·es à des incidents critiques simultanés chez plusieurs employeurs ne peuvent répondre adéquatement à aucun d'eux. Les raccourcis qui en résultent (révisions superficielles du code, lacunes dans la documentation, contournements de sécurité) s'accumulent au fil du temps.

Les outils d'IA ont ajouté une couche de complexité à cette situation. Les utilisateur·rices qui maîtrisent l'IA peuvent accomplir leur travail en une fraction du temps attendu selon les repères de productivité d'avant l'IA, ce qui leur permet de satisfaire aux exigences de production de plusieurs postes au cours d'une semaine normale de travail. Cela soulève une véritable question encore sans réponse : lorsqu'un·e travailleur·se fournit un rendement de pleine qualité dans deux postes à la fois, le préjudice découle principalement de l'absence de divulgation plutôt que de la qualité du travail fourni. Le risque opérationnel le plus immédiat est l'inverse : des gestionnaires qui ne sont pas encore familiarisé·es avec ce qu'un·e travailleur·se assisté·e par l'IA peut produire peuvent établir des échéanciers qui laissent une capacité importante non détectée et non utilisée pour l'organisation



qui la rémunère. Qu'un cumul d'emplois rendu possible par l'IA dégrade la production ou ne fasse que redistribuer une capacité excédentaire, la non-divulgation demeure l'enjeu déterminant.

L'ampleur du problème est documentée. Dans un article publié en 2021, le Wall Street Journal a brossé le portrait du phénomène du cumul d'emplois, en interviewant des cols blancs occupant secrètement plusieurs postes à temps plein en télétravail. Le journal a vérifié leurs déclarations à l'aide de lettres d'offre, de talons de paie concomitants et de courriels professionnels. Les travailleur·ses ont indiqué gagner entre 200 000 $ et 600 000 $ par année grâce à ces postes simultanés. Depuis lors, cette pratique s'est développée : les communautés Reddit dédiées comptent désormais plus de 500 000 membres, où les participant·es s'entraident ouvertement pour gérer les conflits d'horaires de réunions, contourner les logiciels de surveillance du télétravail, échapper aux bases de données de vérification de l'emploi et éviter d'être repéré·es par leurs employeurs.

Indicateurs de détection :

- Indisponibilité récurrente à certaines heures sans explication
- Annulations fréquentes de réunions à la dernière minute; demandes persistantes de participation uniquement par audio
- Incapacité de participer à des réunions ou à des appels téléphoniques à court préavis
- Baisse de la qualité du travail au fil du temps, avec des livrables qui semblent précipités
- Présence sur LinkedIn ou dans des répertoires professionnels indiquant un autre employeur que celui apparaissant dans les dossiers
- Absence totale de présence sur LinkedIn, ou antécédents professionnels qui changent sans explication
- Horaires de travail inhabituels, avec des périodes d'activité intense suivies de longues périodes d'inactivité

Réaction des employeurs

Plusieurs grands employeurs ont procédé à des licenciements collectifs pour cause de cumul d'emplois non déclaré et d'utilisation de logiciels de simulation d'activité, des incidents suffisamment importants pour attirer l'attention des principaux médias économiques. Equifax a développé un produit commercial (Talent Report Work Inform) spécialement conçu pour détecter les travailleur·ses cumulant plusieurs emplois, signe que le problème a atteint une ampleur suffisante pour justifier l'existence d'un marché dédié à la détection.

5. Fausse déclaration de lieu ou d'accès

Parallèle sectoriel : Fraude liée à la provenance dans les chaînes d'approvisionnement; violations des contrôles des exportations

Définition : Des travailleur·ses déclarent faussement leur emplacement physique et effectuent leur travail depuis des lieux non déclarés ou non approuvés, ce qui entraîne des violations de la souveraineté des données, des risques en matière de contrôle des exportations et des risques pour la sécurité de l'information.

Surface d'attaque : Entrevue, intégration et opérations courantes

Le lieu détermine les obligations fiscales de l'employeur en matière de paie, les lois applicables en matière de confidentialité (Règlement général sur la protection des données [RGPD], Health Insurance Portability and Accountability Act [HIPAA]), les violations éventuelles des réglementations en matière de contrôle des exportations (International Traffic in Arms Regulations [ITAR], Export Administration Regulations [EAR]) et le respect des exigences contractuelles des client·es. Un·e travailleur·se qui accède aux données de citoyen·nes de l'Union européenne depuis une juridiction non approuvée contrevient au RGPD, que l'employeur en ait connaissance ou non. Un·e travailleur·se qui effectue un travail lié à la protection soumis à l'ITAR depuis l'extérieur des États-Unis engage sa responsabilité pénale.

L'infrastructure permettant de masquer le lieu réel s'est considérablement développée. Des fermes d'ordinateurs portables, c'est-à-dire des installations physiques abritant des dizaines d'ordinateurs exploités à distance, permettent à des travailleur·ses de donner l'impression d'être basé·es localement alors qu'il·elles travaillent depuis l'étranger. Des réseaux de proxys résidentiels redirigent le trafic Internet par l'entremise de véritables adresses IP résidentielles situées dans les emplacements ciblés. La détection nécessite une surveillance active plutôt que des présomptions passives.

Indicateurs de détection :

- Géolocalisation de l'adresse IP incompatible avec le lieu de travail déclaré ou qui change fréquemment
- Heures de connexion systématiquement décalées par rapport au fuseau horaire déclaré
- Arrière-plan vidéo incohérent (éclairage, architecture, indices saisonniers)
- Adresse d'expédition de l'appareil différente du lieu déclaré dans le CV
- Modèles de latence réseau incompatibles avec la proximité déclarée

6. Surestimation des compétences et fausse déclaration assistée par l'IA

Parallèle sectoriel : Fraude académique (secteur de l'éducation); fraude liée aux qualifications (certifications professionnelles)

Définition : Des candidat·es font de fausses déclarations sur leur niveau de compétence réel grâce à des évaluations assistées par l'IA, des entrevues coachées et des tests à domicile réalisés par d'autres personnes, ce qui leur permet de passer la présélection pour des fonctions dont il·elles ne peuvent pas s'acquitter de manière autonome.

Surface d'attaque : Phase d'évaluation et d'entrevue

Les outils d'IA ont modifié ce que les candidat·es peuvent affirmer et démontrer au cours d'un processus d'embauche. Les évaluations techniques à réaliser à domicile et les entrevues asynchrones, autrefois des indicateurs fiables des capacités, peuvent maintenant être accomplies avec une aide importante de l'IA, ce qui rend plus difficile la distinction entre une expertise réelle et un résultat produit à l'aide d'instructions bien formulées.

En pratique, cela ne s'apparente que rarement à une fraude manifeste. Le plus souvent, cela reflète des candidat·es dont la confiance dans la production augmentée par l'IA dépasse leurs propres capacités autonomes. L'écart devient visible non pas par une forme de surveillance, mais par le simple déroulement naturel du processus d'embauche.

Indicateurs de détection :

- Difficulté à expliquer leur travail ou leur raisonnement avec leurs propres mots lors des conversations de suivi
- Baisse notable du rendement lors du passage d'entrevues en vidéoconférence à des rencontres sur site
- Travail fourni dans des délais qui ne correspondent pas à l'ancienneté déclarée du·de la candidat·e
- Réponses qui paraissent soignées dans des contextes structurés, mais qui manquent de profondeur lorsqu'on les explore dans une conversation
- Mouvements oculaires laissant croire que la personne lit une source hors écran plutôt que de faire appel à un rappel réel ou à une réflexion authentique
- Arrière-plans flous ou virtuels qui masquent l'activité, surtout lorsqu'ils s'accompagnent de mouvements visibles en périphérie
- Audio provenant d'un appareil différent du flux vidéo, un signe fréquent qu'une deuxième personne fournit les réponses en temps réel

Les mécanismes ci-dessus produisent rarement un « événement frauduleux » unique et évident. Ils génèrent plutôt une série de coûts qui se répartissent entre le recrutement, les équipes de prestation et l'intervention en sécurité, puis qui se retrouvent classés sous d'autres catégories. Cette mauvaise classification explique pourquoi les mêmes schémas se répètent d'un poste, d'un·e fournisseur·se ou d'un canal à l'autre sans qu'une exigence de réponse uniforme ne s'impose.

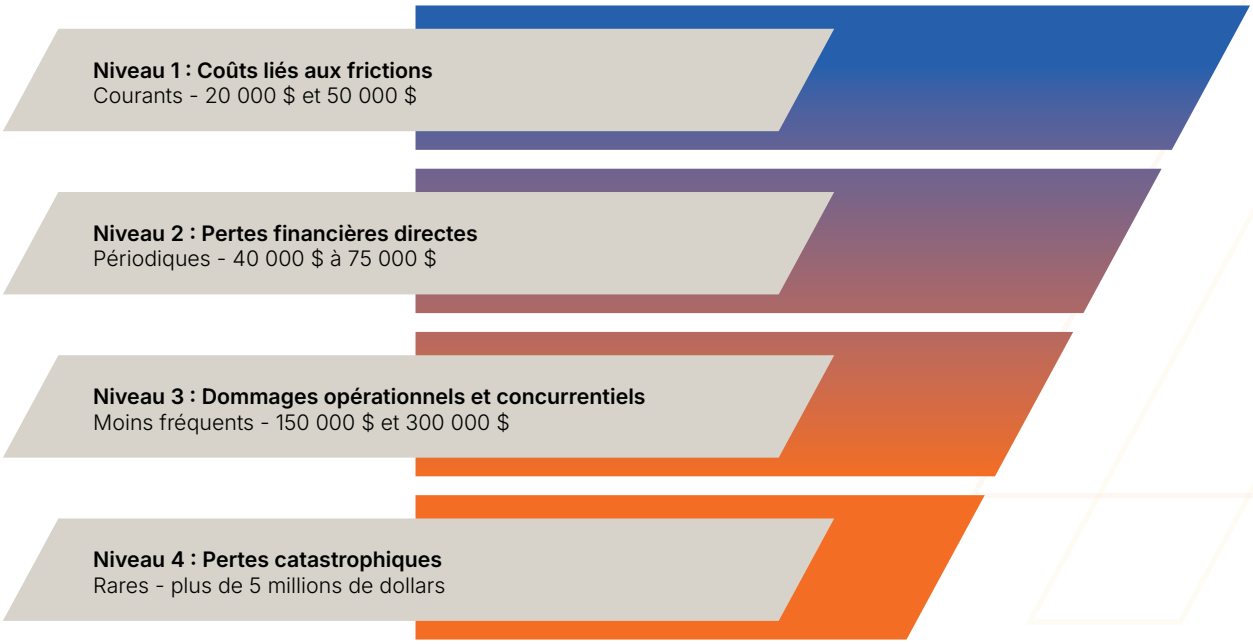
Section 2:
le coût réel de la fraude

Au-delà du calcul lié à une « erreur d'embauche »

La fraude de la part des candidat·es ne s'annonce pas d'elle-même. Elle se manifeste sous la forme d'une erreur d'embauche, d'un projet retardé, d'un dépassement budgétaire ou d'un incident lié aux données demeuré inexpliqué, le tout classé et clos sans que la cause sous-jacente ne soit jamais mise au jour. Il en résulte que la plupart des organisations absorbent des pertes financières bien réelles attribuables à la fraude tout en les mesurant comme s'il s'agissait de tout autre chose.

Ces coûts se regroupent en quatre strates, chacune ayant sa propre probabilité et exigeant une réponse adaptée.

Le continuum des coûts liés à la fraude



Niveau 1 : Coûts liés aux frictions

Courants, car la plupart des organisations les absorbent régulièrement

Un·e candidat·e frauduleux·se qui réussit la présélection, intègre l'organisation, offre un rendement insuffisant puis quitte reproduit en tout point le scénario d'une erreur d'embauche. Le·la candidat·e et l'agence de recrutement sont rémunéré·es. La recherche d'un·e remplaçant·e commence. Aucun signalement de fraude n'est déposé, car aucune fraude n'a été reconnue.

Le coût direct d'un placement qui échoue, qu'il s'agisse des frais de recrutement, du temps d'intégration, des perturbations de projet ou du remplacement, se situe généralement entre **20 000 $ et 50 000 $**. Dans des programmes qui placent 50 travailleur·ses ou plus par année, cela survient plusieurs fois par trimestre. Cela ne donne pas l'impression d'une exposition à la fraude. Cela donne l'impression d'une variabilité dans l'embauche. Cette mauvaise classification est le problème; elle fait en sorte que la cause profonde n'est jamais traitée et que le schéma se répète.

Niveau 2 : Pertes financières directes

Periodic – Organizations making 50+ placements annually

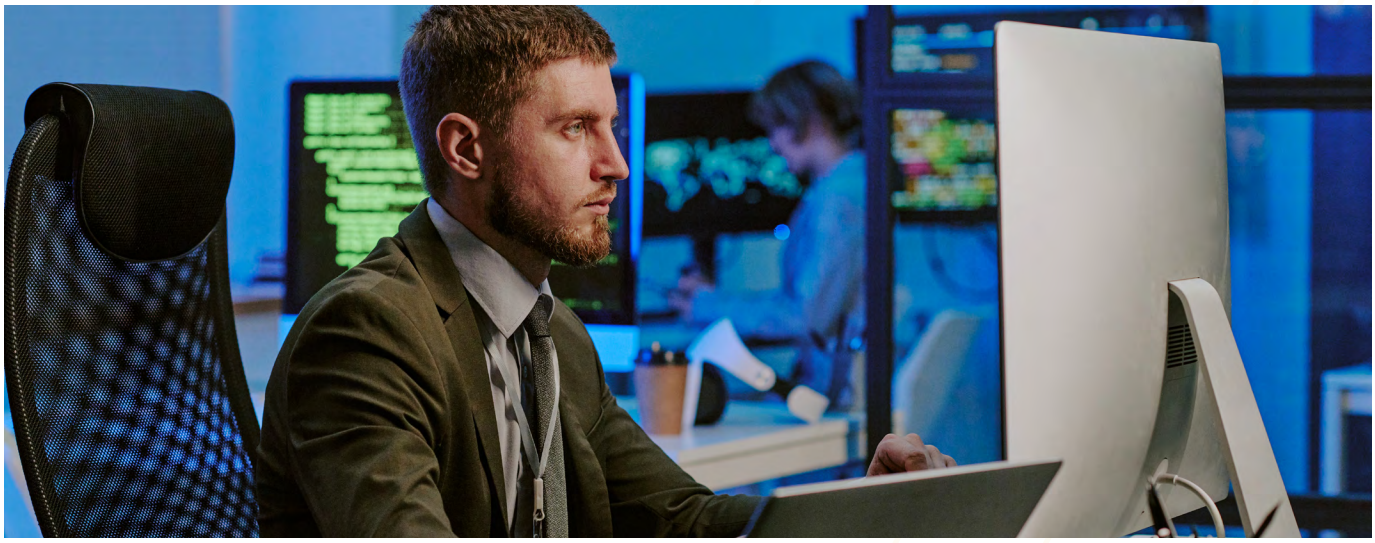
Un·e candidat·e ayant des titres professionnels fabriqués ou une identité falsifiée perçoit trois à quatre périodes de paie avant que les incohérences ne ressortent, ce qui représente généralement entre 15 000 $ et 35 000 $ en vol direct de paie par incident. En ajoutant les frais de recrutement déjà payés, les coûts d'intégration absorbés et le coût de la recherche de remplacement, un seul incident représente de **40 000 $ à 75 000 $** en pertes récupérables.

Les opérations de fraude ciblent délibérément cette strate. Les montants sont suffisamment élevés pour être rentables à grande échelle, mais assez modestes pour que la plupart des équipes des achats ferment l'incident au lieu d'examiner le schéma qui s'y rattache. C'est précisément sur cela que comptent les réseaux de fraude organisés : chaque incident est traité individuellement, signalé comme une erreur d'embauche, géré comme une fin de mandat anticipée, brièvement soumis à une escalade, puis clos. L'incident suivant, six semaines plus tard, avec un·e fournisseur·se différent·e et un poste distinct, reçoit le même traitement. Personne ne les relie entre eux, parce que personne ne cherche à travers les incidents, mais seulement à l'intérieur de chacun d'eux.

Le signe révélateur n'est presque jamais un seul événement. Il s'agit plutôt du regroupement d'éléments : plusieurs départs soudains au cours d'un trimestre, un schéma de candidat·es qui réussissent la présélection mais échouent dans les soixante premiers jours, ou des échecs de rendement inexpliqués concentrés dans une catégorie de compétences ou un canal de recrutement. Les organisations qui suivent ces incidents de manière isolée continueront d'en absorber les pertes. Celles qui les suivent comme un schéma au niveau du programme en trouveront la source.

Toutefois, la fraude de niveau 2 ne se manifeste pas toujours par des placements qui échouent. Un·e candidat·e ayant fabriqué ses antécédents professionnels, mais possédant réellement les compétences nécessaires pour occuper le poste, peut ne jamais être détecté·e. Son identité est réelle et vérifiable. Ses références sont valides, souvent parce que les personnes mentionnées les connaissent personnellement ou parce que les postes réellement occupés à l'étranger sont difficiles à vérifier de manière indépendante. Ce qui est faux, c'est l'expérience précise sur laquelle la décision d'embauche a été fondée : les dix années d'expérience locale en entreprise qui ont justifié le taux, les fonctions propres au domaine qui ont fait de ce·tte candidat·e la personne préférée, ou la progression de carrière donnant à penser qu'il·elle possède une maîtrise institutionnelle qu'il·elle n'a peut-être pas.

Il·elle s'intègre, exécute adéquatement le travail et demeure en poste. Aucun départ, aucune plainte, aucun incident. Or, l'organisation a pris une décision d'embauche et de rémunération sur une base qui n'a jamais été exacte, payant potentiellement un taux de niveau supérieur pour une expérience de niveau intermédiaire, écartant des candidat·es possédant des titres professionnels locaux légitimes ou plaçant une personne dans un niveau de confiance ou d'accès que son parcours réel n'aurait pas justifié. La fraude ne s'annonce pas, car rien n'échoue de manière visible. Elle demeure simplement à l'intérieur du programme, sans être détectée, aussi longtemps que le placement se poursuit.



Niveau 3 : Dommages opérationnels et concurrentiels

Moins fréquents, mais nettement plus coûteux par incident

Un·e travailleur·se cumulant plusieurs emplois, facturant à temps plein à un taux de niveau supérieur tout en répartissant son attention entre deux postes ou plus, génère plusieurs coûts qui se cumulent, et la plupart des organisations n'en perçoivent que le premier.

Le premier de ces coûts est une capacité rémunérée qui ne se concrétise jamais pleinement. Le travail peut être de qualité, mais il ne correspond pas à un engagement à temps plein. Ce qui manque, c'est la disponibilité pour les demandes urgentes, la concentration soutenue sur des problèmes complexes et la présence quotidienne qu'un placement de niveau supérieur est censé offrir. Lorsque l'attention est divisée, les transitions constantes entre des environnements similaires mais distincts augmentent la probabilité d'erreurs subtiles. Il ne s'agit pas d'erreurs attribuables à de l'incompétence. Ce sont les erreurs d'une personne compétente qui opère à la limite de sa capacité cognitive.

Le deuxième coût est le coût d'opportunité; c'est celui que la plupart des programmes ne quantifient jamais. Un placement de niveau supérieur n'est pas rémunéré uniquement pour des livrables. Il est rémunéré pour l'apport et le rendement qu'une personne hautement compétente et pleinement engagée est censée générer au cours d'une année. Lorsque cette capacité est discrètement redirigée vers un autre employeur, l'organisation ne reçoit pas de rabais; elle finance la seconde source de revenus de quelqu'un tout en assumant l'intégralité du coût du poste.

Le troisième coût est celui qui n'apparaît dans presque aucun cadre de fraude : la perte de transfert de connaissances. Un·e travailleur·se de niveau supérieur, dont la capacité est divisée, n'assure pas le mentorat des développeur·ses débutant·es, ne participe pas aux discussions d'architecture et n'apporte pas son expertise accumulée au travail quotidien de l'équipe qui l'entoure.

Dans un environnement où l'IA accélère le rythme de prestation, l'écart entre une personne de niveau supérieur réellement présente, qui guide l'utilisation des outils d'IA, révise ce qu'ils produisent et élève la capacité des personnes qui l'entourent, et une personne physiquement absente tout en facturant comme si elle était à temps plein n'est pas seulement un écart de capacité. C'est un écart de capacité cumulatif qui touche chaque membre de l'équipe qui aurait dû apprendre de lui·elle. Même si la qualité du travail est exceptionnelle, si le·la candidat·e ne travaille que 20 heures plutôt que 40, une question se pose : qu'aurait-il·elle pu accomplir en travaillant à temps plein?

L'IA rend ces trois coûts plus difficiles à détecter et plus difficiles à attribuer. Un·e utilisateur·rice qui maîtrise l'IA peut produire un résultat convaincant en une fraction des heures facturées, ce qui signifie que le signal de qualité révélant normalement un engagement réduit peut ne pas apparaître du tout. Cependant, un enjeu plus profond apparaît au-delà du problème de détection : si un·e travailleur·se de niveau supérieur fournit un rendement acceptable grâce à l'IA en vingt heures par semaine, l'organisation ne reçoit pas ce pour quoi elle paie; elle ne reçoit qu'une fraction de ce qu'il·elle pourrait produire en étant pleinement engagé·e. Le résultat semble adéquat par rapport aux attentes fixées avant que l'IA ne transforme ce qui était possible.

Le coût complet d'un incident de cumul d'emplois à un niveau supérieur se situe couramment entre **150 000 $ et 300 000 $**, en salaires perdus, en reprises de travail et en production perdue. Dans des programmes comportant plusieurs placements simultanés de ce niveau, cela devient une exposition budgétaire importante. Dans certains cas, cela accroît aussi le risque que des tiers inconnus accèdent aux systèmes et aux données du·de la client·e, déclenchant des coûts d'enquête et des pénalités potentielles.

Niveau 4 : Pertes catastrophiques

Rares, mais d'une gravité telle qu'elles peuvent menacer l'existence même de l'organisation

Vol de propriété intellectuelle, rançongiciels facilités par un·e complice infiltré·e, violations des contrôles à l'exportation ou de la souveraineté des données liées à une fausse déclaration de lieu, ou infiltration menée par des acteurs étatiques. Les dommages se chiffrent en millions, voire en dizaines de millions de dollars : sanctions réglementaires, règlements juridiques, résiliations de contrats clients et atteinte à la réputation dont la réparation prend des années. L'asymétrie est frappante. **Un seul placement frauduleux de 50 000 $ peut entraîner plus de 5 millions de dollars en dommages indirects.**

Voici une autre possibilité :

Vol de propriété intellectuelle, rançongiciel facilité par un·e complice infiltré·e, violations du contrôle des exportations ou de la souveraineté des données découlant d'une fausse déclaration du lieu de travail, ou infiltration commanditée par un État au moyen d'un·e travailleur·se placé·e. Les dommages se chiffrent en millions, voire en dizaines de millions de dollars : sanctions réglementaires, règlements juridiques, résiliations de contrats clients et atteinte à la réputation dont la réparation prend des années.

Ce qui distingue catégoriquement le niveau 4 des niveaux précédents n'est pas seulement l'ampleur des dommages, mais bien l'incertitude. Dans tous les autres scénarios, l'organisation sait ce qui a mal tourné. Un placement inadéquat prend fin. Un·e travailleur·se cumulant plusieurs emplois est identifié·e. Un CV falsifié est découvert. L'incident a des contours définis. Il peut être circonscrit, examiné et clos.

Au niveau 4, cette clarté est souvent absente. Lorsqu'un·e travailleur·se ayant des affiliations non divulguées ou une identité fabriquée a eu accès pendant des mois ou des années aux systèmes, aux bases de code, aux données du·de la client·e ou aux communications internes, l'organisation ne peut pas déterminer pleinement ce qui a été consulté, copié, observé ou communiqué à l'externe. L'enquête elle-même devient un coût important, entre l'analyse criminalistique, l'examen juridique, les obligations de notification réglementaire et l'information des client·es, et ce, avant même qu'un seul dollar de dommages directs soit comptabilisé. De plus, comme l'étendue réelle de l'accès ne pourra peut-être jamais être reconstituée avec certitude, l'organisation se retrouve à gérer un risque résiduel qu'elle ne peut quantifier avec précision.

C'est cette ambiguïté qui crée l'asymétrie. Un seul placement frauduleux de 50 000 $ peut déclencher cinq millions de dollars ou plus en dommages ultérieurs, non pas parce que la fraude était sophistiquée, mais parce que l'accès qu'elle a permis était étendu, parce que la période d'exposition était longue, et parce que l'organisation ne dispose d'aucun moyen fiable pour délimiter ce qui a été compromis. La réponse n'est pas proportionnelle à l'incident d'origine. Elle est proportionnelle à tout ce que ce placement a pu toucher.

La vraie question

La question n'est pas de savoir si votre organisation fera face à de la fraude de la part des candidat·es. Dès qu'une organisation atteint un volume de placements important, les coûts liés aux frictions deviennent presque inévitables et les pertes financières directes deviennent probables.

La question est la suivante : **où votre organisation se situe-t-elle sur ce continuum, et vos mécanismes de protection sont-ils adaptés à votre profil de risque réel?**

La plupart des organisations absorbent les coûts des niveaux 1 et 2 sans les mesurer. Certaines subissent les dommages associés au niveau 3 sans les relier à la fraude. Pratiquement aucune organisation n'a évalué son exposition aux scénarios du niveau 4, là où le risque est le plus asymétrique : faible probabilité, incidence catastrophique.

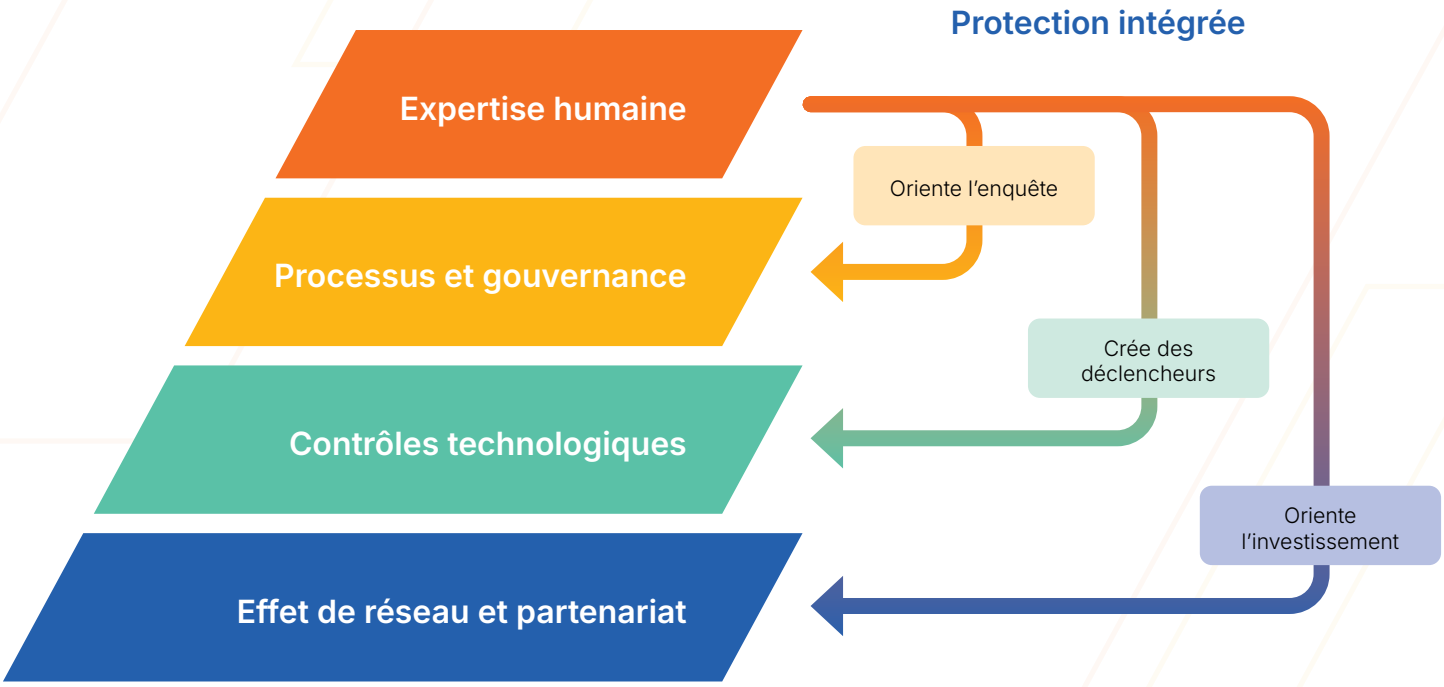
Section 3:
LE MODÈLE DE PROTECTION DU CYCLE D'EMBAUCHE

Une protection efficace contre la fraude exige des mécanismes de contrôle à chaque étape du cycle d'embauche et du cycle de travail, et non uniquement au moment de l'embauche. Les organisations qui concentrent la vérification dans une seule phase créent des lacunes prévisibles que des acteur·rices sophistiqué·es exploitent.

	Avant l'embauche	*Durant l'embauche*	*Intégration*	*Après l'embauche*
Technologie	• Outils de vérification des accréditations • Détection d'anomalies dans les CV et profils • Filtrage de l'identité numérique	• Entrevues vidéo avec vérification d'identité • Évaluations techniques surveillées • Systèmes d'enregistrement d'entrevues	• Vérification d'identité et contrôles biométriques • Contrôles d'enregistrement des appareils • Attribution d'accès fondée sur les fonctions	• Suivi des connexions et des emplacements • Suivi de l'activité des systèmes • Détection d'anomalies réseau
Processus	• Vérifications structurées des accréditations • Examen normalisé des CV • Vérification des références	• Entrevues en plusieurs étapes • Démonstrations techniques en direct • Questions vapprofondies sur l'expérience	• Confirmation d'identité • Intégration sécurisée • Configuration contrôlée des accès aux systèmes	• Révisions des accès • Vérifications du rendement par les gestionnaires • Surveillance des conflits ou de la sous-traitance
Expertise humaine et normes culturelles	• Sensibilisation des recruteur·ses à la fraude • Culture de vérification chez les gestionnaires • Examen critique des déclarations des candidat·es	• Panels d'entrevues techniques et comportementales • Questions de suivi approfondies • Formation des intervieweur·ses à la détection de fraude	• Validation du travail initial par les gestionnaires • Encourager la divulgation des contraintes • Renforcer la responsabilisation	• Escalade des signaux d'alerte par les gestionnaires • Reconnaître la fraude comme un risque lié au rendement • Culture de sensibilisation à la sécurité

Dans chaque phase, les mécanismes de contrôle se répartissent en trois modalités :

- **Technologie :** Vérifications automatisées, authentification biométrique, analyses comportementales, géolocalisation, outils tiers et tests
- **Processus :** Entrevues structurées, protocoles d'accès progressifs, coordination interfonctionnelle entre les RH, la sécurité et le service juridique
- **Expertise humaine et normes culturelles :** Formation des intervieweur·ses (vérification d'identité, reconnaissance de vidéos truquées (deepfake), questions approfondies permettant de déjouer des réponses préparées), obligation d'entrevues en personne, sensibilisation aux indicateurs de fraude et pratiques organisationnelles comprenant des politiques de caméra activée, des interactions en personne et une collaboration en direct, qui créent des points de vérification continus.



La troisième modalité, soit le facteur humain, est celle dans laquelle la plupart des organisations sous-investissent, et pourtant, c'est elle qui détermine l'efficacité des deux autres. La technologie est la plus facile à acquérir, les processus nécessitent une transformation organisationnelle, mais les compétences humaines et les normes culturelles constituent la couche résistante à la fraude, un obstacle que les opérations sophistiquées ne peuvent contourner. Des intervieweur·ses formé·es capables d'amener les candidat·es à s'éloigner de réponses répétées, des gestionnaires aptes à repérer les comportements d'évitement et des pratiques organisationnelles qui rendent la tromperie prolongée difficile à maintenir constituent les éléments clés qui comblent les lacunes de la technologie et des processus.

Cela est particulièrement important pour les programmes de ressources externes. Les organisations qui gèrent un grand nombre de contractuel·les par l'entremise de plusieurs agences de dotation en personnel et de prestataires de services d'EOR se heurtent à un défi additionnel : la capacité de détection des fraudes peut varier considérablement au sein de leur chaîne d'approvisionnement, et l'organisation cliente elle-même peut manquer de visibilité sur les contrôles appliqués de manière constante et ceux qui se dégradent lorsque le rythme d'embauche s'accélère.

Phase 1 : Préembauche – construire des pipelines fiables

La protection la plus efficace contre la fraude commence avant même l'ouverture d'une demande.

Entretenir des réseaux de talents fiables. Établissez et entretenez des relations avec des bassins de talents connus et vérifiés, que ce soit par l'intermédiaire de partenaires en dotation en personnel, de réseaux d'ancien·nes élèves ou de communautés de pratique. Les candidat·es provenant de canaux fiables présentent un risque de base inférieur à celui des personnes qui postulent sans relation préalable.

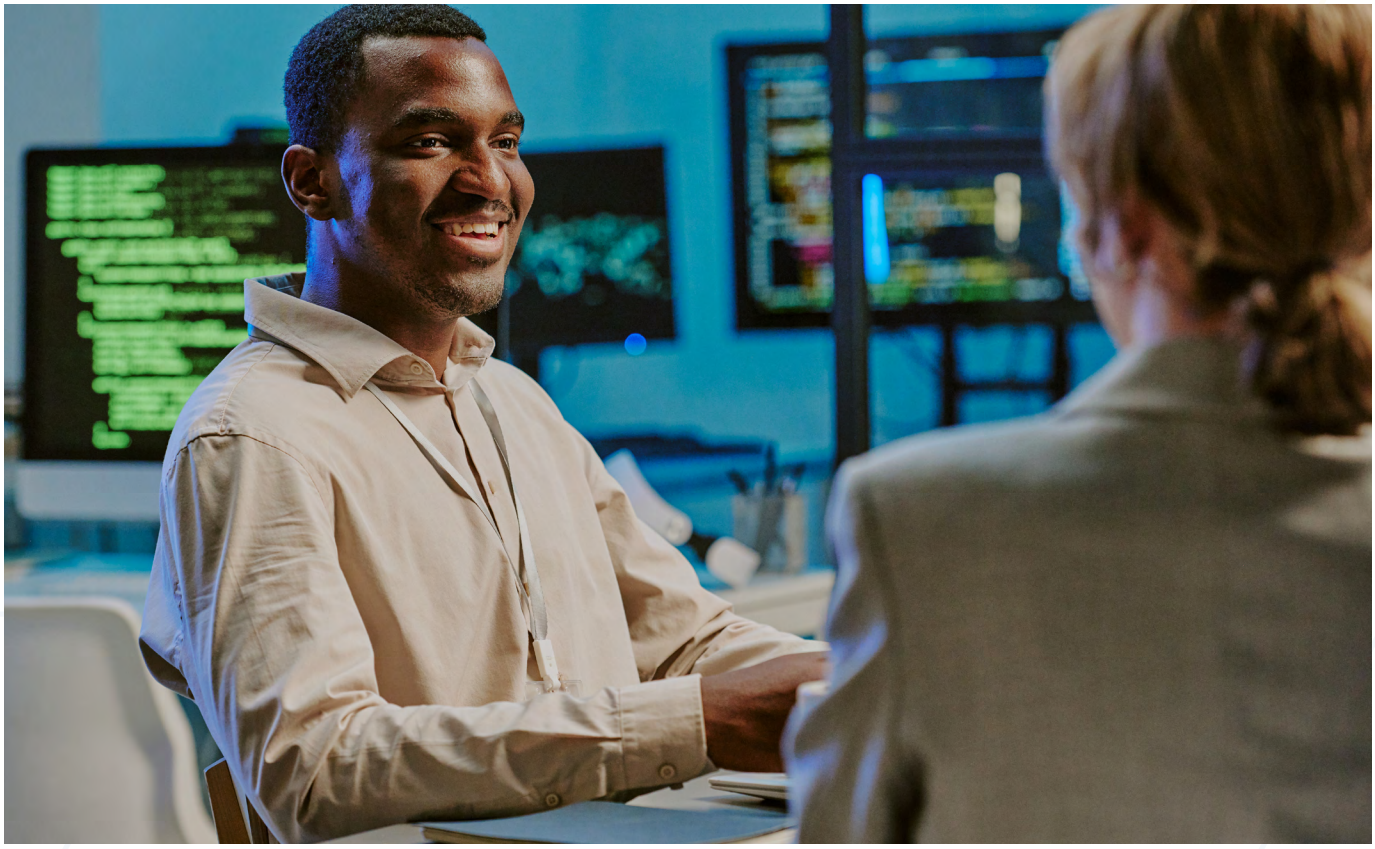
Vérifier les partenaires et les fournisseurs de recrutement. Lorsque vous recourez à des agences de dotation en personnel ou à des prestataires de services d'EOR, évaluez leur capacité de détection des fraudes. La norme de vérification la plus faible de votre chaîne d'approvisionnement devient, en pratique, votre norme. Les exigences contractuelles doivent préciser les obligations de réduction de la fraude, les garanties et les dispositions d'indemnisation.

Combler l'écart lié aux sources directes. La plupart des organisations disposent d'un mécanisme de recrutement direct dans le cadre duquel les gestionnaires d'embauche repèrent et approchent des travailleur·ses en-dehors des canaux fournisseurs. Veillez à ce que cette source soit soumise aux mêmes mécanismes de protection contre la fraude que les sources internes et celles des fournisseurs. Dans les programmes d'EOR ou d'AOR, où les gestionnaires du·de la client·e sélectionnent eux·elles-mêmes les travailleur·ses, cet écart constitue souvent la vulnérabilité la plus négligée.

Enfin, maintenez des normes fermes et n'empruntez aucun raccourci; dans bien des cas, certain·es prestataires de services d'EOR ou d'AOR peuvent vouloir contourner les vérifications d'antécédents, la vérification d'identité ou même les CV, alors que chacun de ces éléments peut constituer un point de détection de fraude. Veillez à ce qu'aucune lacune ne se crée à la source.

Définir les profils de risque propres aux postes. Tous les postes n'exposent pas au même niveau de risque de fraude. Les postes à distance nécessitant un accès aux systèmes, les postes traitant des données sensibles et les programmes de ressources externes à volume élevé exigent des contrôles renforcés. Calibrez l'investissement en fonction du risque.

Établir des politiques d'utilisation de l'IA avant d'en avoir besoin. Définissez les situations dans lesquelles l'aide de l'IA est acceptable dans votre processus d'embauche et celles dans lesquelles elle est disqualifiante, puis communiquez ces limites aux candidat·es.



Phase 2 : Embauche – Vérification du·de la candidat·e en temps réel

La phase d'entrevue et d'évaluation est celle où la surestimation des compétences, l'usurpation d'identité et les entrevues par procuration sont les plus susceptibles de réussir, et celle où les contrôles en temps réel sont les plus efficaces pour les détecter.

Imposer au moins une interaction en direct sous supervision. Qu'elle se déroule en personne ou par vidéo surveillée, au moins une évaluation doit avoir lieu dans des conditions empêchant le·la candidat·e de recevoir une aide externe. Ce contrôle unique permet de contrer les personnes qui passent les tests par procuration et le coaching hors écran.

Mettre en place la vérification d'identité dès le début. Utilisez un rapprochement entre égoportrait et pièce d'identité gouvernementale avant ou pendant le processus d'entrevue, et non après l'envoi d'une offre. Le déploiement précoce de la vérification d'identité permet d'éviter d'investir beaucoup de temps et de ressources dans des candidat·es qui ne sont peut-être pas ceux·elles qu'il·elles prétendent être.

Former les gestionnaires d'embauche aux indicateurs de fraude. Les mouvements oculaires laissant supposer une lecture hors écran, les artefacts audio provenant d'écouteurs, des angles de caméra inhabituels, des réponses répétées qui s'effondrent lors de questions de suivi approfondies et la réticence à activer la vidéo sont autant de signaux d'alerte observables que des intervieweur·ses non formé·es ne détectent pas. Cette formation est particulièrement essentielle pour les gestionnaires d'embauche des client·es dans le cadre des programmes d'EOR ou d'AOR, car il·elles constituent souvent le seul point de vérification humaine du processus.

Utiliser des évaluations techniques avec confirmation biométrique. Pour les postes techniques, associez les évaluations de compétences à l'enregistrement de la séance, au verrouillage du navigateur ou à une vérification biométrique confirmant que la personne passant le test est bien celle qui se présentera au travail.

Effectuer une analyse du profil numérique et de l'adresse IP. Recoupez l'emplacement déclaré par le·la candidat·e avec son adresse IP lors des entrevues à distance. Vérifiez la cohérence de son empreinte numérique, qu'il s'agisse de l'historique LinkedIn, des contributions GitHub ou de sa participation à des communautés professionnelles, avec l'expérience déclarée. Soumettez les profils peu étoffés ou récemment créés à un examen approfondi.

Phase 3 : Préentrée en fonction et intégration – combler l'écart de vérification

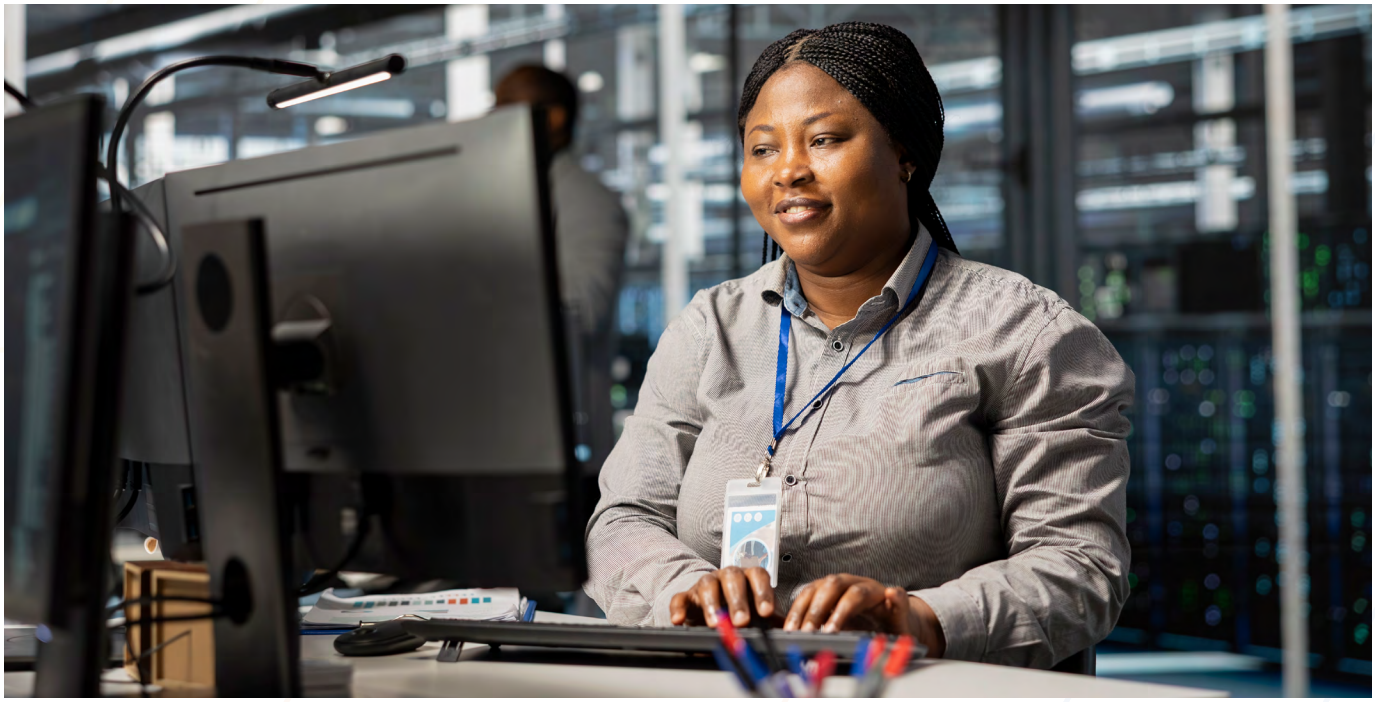
La période entre l'acceptation de l'offre et le début effectif du travail constitue une fenêtre de vulnérabilité critique.

Effectuer des vérifications de références approfondies. Communiquez avec des références repérées au moyen de recherches indépendantes, et non exclusivement celles fournies par le·la candidat·e. Vérifiez l'identité et le poste de la référence au moyen d'annuaires d'entreprise ou de LinkedIn plutôt que de vous fier aux numéros fournis par le·la candidat·e.

Procéder à la vérification des antécédents et de la formation. Confirmez les antécédents professionnels, les diplômes et les antécédents judiciaires par le biais de services de vérification tiers. Recoupez les résultats avec les déclarations faites pendant le processus d'embauche, et non seulement avec l'information fournie dans la candidature.

Vérifier de nouveau l'identité lors de l'intégration. Confirmez que la personne qui reçoit l'équipement, les identifiants et l'accès aux systèmes est bien celle qui a passé l'entrevue. Vérifiez que l'adresse d'expédition de l'appareil correspond à l'emplacement déclaré du·de la candidat·e, les écarts constituant un indicateur documenté d'usurpation d'identité ou de sous-traitance non autorisée. Bien souvent, des incohérences liées à l'identité peuvent être repérées dans des documents complémentaires comme des pièces d'identité, des chèques ou des formulaires fiscaux.

Mettre en place des protocoles d'accès progressifs. Accordez les autorisations système de façon progressive, selon les exigences du poste et la fiabilité démontrée durant les 90 premiers jours. Donner un accès complet dès le premier jour aux systèmes sensibles, aux référentiels de code et aux données des client·es maximise les risques de dommages si une fraude est détectée ultérieurement.



Phase 4 : Post-embauche – Vérification continue

Plusieurs vecteurs de fraude, notamment la surestimation des compétences, la sous-traitance non autorisée et le cumul d'emplois non déclaré, ne sont détectables que par une surveillance continue.

Déployer la géolocalisation et l'analyse d'adresses IP. Recoupez les emplacements de connexion avec l'emplacement déclaré du·de la travailleur·se et les dossiers RH. Les télétravailleur·ses frauduleux·ses génèrent fréquemment des alertes de « déplacements improbables » (des connexions provenant de régions opposées du pays à quelques minutes d'intervalle), ce qui survient en cas de dysfonctionnement de la configuration du RPV.

Surveiller les schémas de latence réseau. Une latence anormalement élevée ou incohérente lors des appels vidéo et des connexions aux systèmes peut indiquer un routage du trafic par une infrastructure de proxys ou des points relais situés à l'étranger, signe caractéristique de la sous-traitance non autorisée.

Exiger des interactions périodiques en personne. Même pour les postes à distance, les journées de présence sur site prévues, les événements d'équipe ou les rencontres avec les client·es créent des points de contact permettant de vérifier l'identité, ce qui empêche les travailleur·ses par procuration ou les remplaçant·es non autorisé·es de s'introduire.

Utiliser l'analyse comportementale et la surveillance des activités. Détectez les anomalies, notamment des schémas de connexion inhabituels, l'accès à des données en dehors du périmètre du poste, des transferts massifs de données ou des schémas d'activité qui ne correspondent pas à ceux d'une seule personne.

Suivre la constance du rendement. Un écart important et durable entre le rendement démontré en entrevue ou durant la période probatoire et la qualité du travail effectué par la suite constitue un indicateur important de surestimation des compétences. Des points de contrôle structurés à 30, 60 et 90 jours, comportant des tâches nécessitant une démonstration en direct et sans assistance, permettent de déceler ces écarts avant que la dépendance organisationnelle ne s'accentue.

Maintenir les pratiques de vérification culturelle. Les normes organisationnelles établies durant l'intégration, qu'il s'agisse des attentes liées à la caméra activée, des séances de travail collaboratives ou des interactions au sein de l'équipe, doivent perdurer au-delà des premières semaines. Lorsque ces pratiques culturelles s'érodent au fil du temps, la pression de vérification continue qu'elles exercent diminue également. Les organisations qui maintiennent ces pratiques de façon constante signalent une détection plus précoce d'anomalies comportementales et de schémas d'évitement révélateurs d'une fraude potentielle.

Intégration à l'échelle des phases et des partenaires

Aucune phase ne fournit une protection complète, et aucune organisation au sein de la chaîne d'approvisionnement ne dispose d'une visibilité totale. La valeur du modèle repose sur le renforcement des mécanismes de contrôle dans ces deux dimensions.

Tout au long du cycle de vie, chaque phase soutient les autres : la qualité du recrutement avant l'embauche réduit le nombre de candidat·es frauduleux·ses qui entrent dans le processus; les contrôles en temps réel lors des entrevues permettent de repérer ceux·elles qui passent entre les mailles du filet; la vérification lors de l'intégration comble les lacunes avant que l'accès ne soit accordé; la surveillance après l'embauche permet de détecter ce qui a été manqué lors des phases précédentes.

Pour être efficace, la chaîne d'approvisionnement doit permettre une circulation fluide des informations entre les partenaires. Les journaux d'adresses IP et de géolocalisation provenant du prestataire de services d'EOR, les observations d'entrevues du·de la gestionnaire d'embauche du·de la client·e, les signaux comportementaux relevés par le·la prestataire de services de dotation en personnel et les anomalies d'accès aux systèmes relevées par l'équipe de sécurité informatique du·de la client·e génèrent tous des signaux de fraude, mais seulement s'ils sont communiqués, corrélés et suivis d'actions. Les organisations qui considèrent la vérification effectuée par chaque partenaire comme un silo indépendant créent la même faille que lorsqu'elles concentrent les contrôles dans une seule phase du cycle de vie, soit des fragments d'un schéma qu'aucune partie ne peut voir dans son ensemble.

Les organisations les plus efficaces dans ces deux dimensions présentent une caractéristique commune : elles opèrent à un volume suffisant pour repérer des schémas récurrents. Un·e gestionnaire d'embauche qui observe un·e candidat·e coaché·e risque de ne pas déceler le signal. Une agence de dotation en personnel qui place des candidat·es chez un·e seul·e client·e risque de ne pas percevoir le schéma récurrent chez plusieurs client·es. Une organisation qui traite chaque année des milliers de placements, pour plusieurs client·es dans divers secteurs et régions, développe des capacités en matière de renseignement sur les menaces, de références comportementales et de reconnaissance des schémas qui rendent chaque phase et chaque partenaire plus efficaces.

Il s'agit de l'expertise humaine propre à cette modalité, déployée à grande échelle. Elle ne peut être reproduite par la seule technologie, développée sans volume opérationnel, ni atteinte sans une intégration délibérée à l'ensemble de la chaîne d'approvisionnement.

Section 4 : évaluer votre posture de sécurité

De la sensibilisation à l'évaluation des risques liés aux menaces

En cybersécurité, la discipline qui transforme la sensibilisation en action est l'évaluation des risques liés aux menaces, une analyse structurée qui détermine à quoi vous êtes exposé·e, quels mécanismes de contrôle sont en place et où les écarts créent des vulnérabilités exploitables.

La plupart des organisations ont mis en place certaines mesures d'atténuation de la fraude, mais ne les ont jamais testées sous pression dans le contexte actuel des menaces. Les procédures de vérification conçues il y a cinq ans peuvent traiter les menaces de niveau 1, mais négliger les vecteurs d'attaque de niveaux 2 et 3. Les mécanismes de contrôle peuvent exister sur papier, mais se dégrader lorsque le rythme des embauches s'accélère. La réponse interfonctionnelle nécessaire pour détecter et contenir une fraude sophistiquée, englobant les RH, la sécurité, le service juridique et la direction de l'entreprise, n'a peut-être jamais été mise en œuvre.

Les quatre questions ci-dessous constituent un cadre de départ.

1. Quelle est votre surface d’attaque?

Votre surface d’attaque est définie par votre volume de placements, les types de postes, les canaux de recrutement et votre modèle de main-d’œuvre. Cartographiez-la :

- Combien de placements de ressources externes réalisez-vous chaque année, et pour quels types de postes?
- Quelle proportion est à distance? Quels postes donnent accès aux systèmes, exposent à des données sensibles ou comportent des implications réglementaires?
- Quel est votre taux historique de détection de fraude, et dans quelle mesure êtes-vous certain·e qu’il reflète réellement ce qui se produit dans votre programme plutôt que seulement ce qui a été suffisamment visible pour remonter à la surface?
- Avez-vous mesuré vos coûts des niveaux 1 et 2, c’est-à-dire les pertes liées aux frictions et les salaires volés que la plupart des programmes absorbent comme des variations d’embauche sans les classer comme liés à la fraude?
- Avez-vous évalué votre exposition des niveaux 3 et 4, soit les dommages opérationnels et les scénarios catastrophiques?
- Combien de canaux de recrutement alimentent vos ressources externes, et quels sont ceux dont les mécanismes de vérification au point d’entrée sont les plus faibles?
- Avez-vous déterminé quels postes dans votre programme reposent encore sur des attentes de productivité et de production calibrées selon des repères antérieurs à l’IA, et si ces attentes créent un écart de capacité indétectable pour des travailleur·ses qui maîtrisent l’IA et qui sont employé·es simultanément ailleurs?

Cette dernière question représente une nouvelle dimension de surface d’attaque qui n’existait pas il y a cinq ans. Un·e travailleur·se facturant des heures à temps plein pour un poste dont la charge de travail a été établie avant que la productivité assistée par l’IA devienne la norme peut fournir un résultat acceptable tout en redirigeant une part importante de sa capacité vers un second employeur, sans qu’aucun signal comportemental ne soit détectable par les mécanismes de suivi actuels. Cartographier votre surface d’attaque aujourd’hui exige de prendre explicitement en compte cet écart.

La plupart des organisations qui réalisent cette évaluation pour la première fois découvrent qu’elles absorbent des coûts liés à la fraude qu’elles n’avaient jamais catégorisés comme tels, et que leur exposition aux niveaux supérieurs est plus importante que prévu.

2. Que vous apprend votre historique d'incidents?

L'examen des incidents constitue le fondement d'une protection adaptative. Chaque cas confirmé, quasi incident ou anomalie inexpliquée génère des informations qui valident vos mécanismes de contrôle ou révèlent des écarts.

Commencez par ce que vous savez : les placements où une fraude a été confirmée, les travailleur·ses licencié·es pour fausse déclaration et les mandats qui ont pris fin en raison d'écarts de rendement inexpliqués. Examinez ensuite les cas ambigus, comme le·la contractuel·le qui a quitté abruptement après 60 jours, le·la nouvel·le employé·e dont le rendement a chuté brusquement après sa période probatoire ou le·la candidat·e qui a refusé toute interaction en personne avant de disparaître.

Ensuite, faites quelque chose que la plupart des programmes n'ont jamais fait : repasser en revue les douze derniers mois de fins de mandat anticipées et de départs liés au rendement, et vous demander si chacun d'eux a été examiné pour repérer des indicateurs de fraude avant d'être clos. Dans la plupart des cas, la réponse sera non. Ils étaient systématiquement classés par défaut comme des erreurs d'embauche. Aucune liste de vérification d'indicateurs de fraude n'a été appliquée. Aucune analyse de schémas n'a été réalisée à travers les incidents. Si cela décrit votre programme, l'historique des incidents dont vous disposez est incomplet, et les schémas qu'il pourrait révéler demeurent invisibles.

Pour chaque incident, trois questions sont importantes :

- **Où a-t-il été détecté, et où aurait-il pu être détecté plus tôt?** L'écart entre le point de détection réel et le point de détection le plus précoce est une mesure directe de l'efficacité du mécanisme de contrôle.
- **Quel a été le coût total, y compris les coûts que vous n'aviez pas classés comme liés à la fraude?** Le remplacement du·de la titulaire du poste, les retards de projet, les dommages causés aux client·es, le temps consacré aux enquêtes et les mesures de remédiation en matière de sécurité sont fréquemment absorbés par les budgets d'exploitation généraux plutôt que rattachés à l'incident qui les a provoqués.
- **Les renseignements ont-ils été diffusés ou cloisonnés?** Si les connaissances acquises lors d'un incident restent confinées au·à la gestionnaire d'embauche qui l'a vécu, l'organisation n'apprend rien. La capacité de repérer des schémas exige des données consignées de manière systématique.

Transformer les processus de départ en renseignements sur la fraude

Les processus de départ standard comprennent rarement une évaluation structurée visant à déterminer si la fraude a pu constituer un facteur contributif. Lorsqu'un·e contractuel·le est licencié·e pour des raisons de rendement, la catégorisation par défaut est « erreur d'embauche » et non « indicateur potentiel de fraude ». La mise à jour des processus de départ afin d'y inclure une courte liste de contrôle des indicateurs de fraude (écarts d'identité, écarts de rendement inexpliqués entre l'entrevue et l'exécution, anomalies dans le profil numérique, irrégularités liées à l'emplacement ou à l'accès) transforme les processus RH courants en source de renseignements. Au fil du temps, ces données révèlent les vecteurs actifs dans votre environnement et les points faibles de vos mécanismes de contrôle du cycle de vie.

Un ajout important à cette liste de vérification consiste à évaluer si les schémas de production et de disponibilité du·de la travailleur·se correspondaient à un engagement unique à temps plein, ou si le profil observé, notamment une activité en rafales, une disponibilité incohérente, des erreurs liées au changement de contexte ou une qualité de travail variant fortement selon le type de tâche, correspond plutôt à une attention divisée entre plusieurs postes simultanés. Cela ne mènera pas, dans la plupart des cas, à une conclusion confirmée. Toutefois, au fil du temps et à travers plusieurs départs, cela révèle si le cumul d'emplois constitue un vecteur actif dans votre programme et quels types de postes y sont les plus exposés.

Ce simple changement de processus ne coûte rien à mettre en œuvre et génère la base de données sur les incidents dont dépendent toutes les autres améliorations.

3. Où se trouvent les vulnérabilités?

Cartographiez vos contrôles actuels par rapport aux quatre phases du cycle de vie et déterminez les lacunes :

- **Préembauche :** Recrutez-vous à partir de canaux fiables et vérifiés, ou assumez-vous l'intégralité du risque associé à des pipelines entrants ouverts? Avez-vous évalué les capacités de détection des fraudes de vos agences de dotation en personnel et de vos prestataires de services d'EOR?
- **Embauche :** La vérification d'identité, l'évaluation supervisée en direct et l'analyse du profil numérique sont-elles exécutées de manière systématique, ou sont-elles omises sous la pression des délais de placement?
- **Intégration :** Les vérifications des antécédents, la vérification indépendante des références et la reconfirmation de l'identité sont-elles effectuées avant l'octroi d'un accès complet aux systèmes?
- **Post-embauche :** Disposez-vous d'une surveillance continue (analyse de géolocalisation, schémas de latence, analyse comportementale et suivi du rendement), ou la vérification prend-elle fin lors de l'intégration?

Le constat le plus courant est une dégradation de la couverture tout au long du cycle de vie : contrôles raisonnables lors de l'embauche, exécution incohérente lors de l'intégration et surveillance post-embauche minimale. Il s'agit d'une sécurité périmétrique solide, mais sans détection des menaces internes, ce qui correspond exactement à l'écart que les opérations sophistiquées sont conçues pour exploiter.

Une lacune que les cadres de suivi actuels n'abordent pas pleinement concerne le·la travailleur·se dont l'identité est vérifiée, mais dont les antécédents professionnels sont fabriqués, qui exécute adéquatement son travail et ne génère aucune anomalie comportementale. Le suivi post-embauche tel qu'il est pratiqué actuellement repère la dégradation du rendement, les anomalies d'accès et les signaux d'alerte comportementaux. Il ne repère pas le·la travailleur·se qui facture correctement, produit un résultat acceptable et n'est tout simplement pas la personne que son CV prétend représenter. Cette exposition échappe à ce que le suivi comportemental peut révéler, et exige que les mécanismes de vérification des antécédents professionnels décrits à la section 3 aient été appliqués correctement avant le placement, puisqu'il n'existe aucun mécanisme fiable de détection post-embauche pour ce type de situation.

4. Pouvez-vous combler les écarts en interne ou devez-vous faire appel à des compétences externes?

Les équipes de cybersécurité sont confrontées à une décision classique : développer ou acheter. Certaines compétences gagnent à être développées en interne, tandis que d'autres, notamment le renseignement sur les menaces, la surveillance continue et la réponse aux incidents, sont plus efficaces lorsqu'elles sont confiées à des spécialistes opérant à une échelle qui génère de meilleures données.

La même décision s'applique ici. L'atténuation de la fraude nécessite une technologie de vérification, des processus exécutés de manière constante à chaque phase de l'embauche, une expertise en enquête et des renseignements sur les menaces mis à jour en continu. Les questions qui éclairent la décision :

- Quel est le taux actuel de tentatives de fraude dans votre secteur et dans vos types de postes, et avez-vous accès à des données intersectorielles permettant d'établir une comparaison?
- Comment vos procédures de vérification se comparent-elles à celles d'organisations ayant des volumes de placements et des profils de risque similaires?
- À quand remonte la dernière fois où vos mécanismes de contrôle ont été soumis à des tests de résistance face aux tactiques actuelles de niveaux 2 et 3, y compris la fraude aux entrevues assistée par l'IA et le cumul d'emplois organisé?
- Vos gestionnaires d'embauche, y compris les gestionnaires du·de la client·e qui sélectionnent des contractuel·les dans des programmes d'EOR et d'AOR, savent-il·elles reconnaître un·e candidat·e préparé·e et disposent-il·elles de procédures d'escalade claires lorsqu'un élément semble problématique?
- Votre équipe est-elle en mesure de distinguer une opération de fraude organisée d'un·e candidat·e légitime simplement nerveux·se dont la connexion est mauvaise?
- Votre volume de placements est-il suffisant pour que la vérification soit exécutée de manière uniforme pour chaque embauche, ou les mécanismes de contrôle se dégradent-ils sous la pression des délais de placement?
- Disposez-vous d'une capacité interne dédiée à l'analyse des schémas de fraude dans l'ensemble de votre programme, ou les connaissances liées aux incidents demeurent-elles cloisonnées auprès du·de la gestionnaire d'embauche qui a été confronté·e à ces incidents?
- Votre suivi post-embauche est-il suffisamment robuste pour repérer les vecteurs que les mécanismes de contrôle préembauche manquent, ou votre processus de vérification prend-il fin, dans les faits, au moment de l'intégration?

Si vous ne pouvez pas répondre à ces questions avec certitude, il s'agit d'une vulnérabilité qu'il convient de comprendre avant qu'elle ne soit exploitée.

Section 5 : AUTOÉVALUATION DE LA POSTURE FACE AU RISQUE DE FRAUDE

Utilisez ce cadre pour évaluer la vulnérabilité actuelle de votre organisation à la fraude de la part des candidat·es tout au long du cycle d'embauche. Il s'agit d'une version autoadministrée de l'évaluation des risques liés aux menaces décrite dans la section 4, conçue pour mettre rapidement en évidence les écarts et hiérarchiser les domaines sur lesquels se concentrer. Répondez à chaque question en toute honnêteté en fonction des pratiques réelles, et non des politiques documentées. Des mécanismes de contrôle qui existent sur papier, mais qui se dégradent sous la pression de l'embauche, ne sont pas des mécanismes opérationnels.

Mécanismes de contrôle préembauche

- Recrutez-vous des candidat·es par l'entremise de canaux fiables et vérifiés, ou vous appuyez-vous principalement sur des pipelines entrants ouverts où la qualité et l'intégrité du bassin de candidat·es demeurent inconnues?
- Avez-vous évalué les capacités de détection des fraudes de vos agences de dotation en personnel et de vos prestataires de services d'EOR? Vos contrats comprennent-ils des exigences précises en matière d'atténuation de la fraude, de garanties et d'indemnisation?
- Avez-vous défini des profils de risque propres aux postes afin de calibrer l'intensité de la vérification en fonction de l'exposition à la fraude de chaque poste, en tenant compte des accès aux systèmes, de la sensibilité des données et du statut de travail à distance?
- Vos canaux de recrutement direct, où les gestionnaires d'embauche repèrent et engagent des travailleur·ses en dehors des programmes de fournisseur·ses, reçoivent-il·elles les mêmes mécanismes de contrôle contre la fraude que les candidat·es provenant de fournisseur·ses, ou ce recrutement direct crée-t-il un point d'entrée non contrôlé?
- Disposez-vous d'une politique encadrant l'usage de l'IA, documentée et explicite, qui précise dans quelles étapes du processus d'embauche l'assistance de l'IA est acceptable et dans quelles étapes elle est disqualifiante, et cette politique est-elle communiquée aux candidat·es avant le début des évaluations?
- Avez-vous évalué quels postes de votre programme reposent encore sur des attentes de charge de travail calibrées selon des repères de productivité antérieurs à l'IA, créant ainsi des écarts potentiels de capacité qu'un·e travailleur·se maîtrisant l'IA pourrait exploiter tout en maintenant un emploi parallèle?

Contrôles en cours d'embauche

- Les entrevues comportent-elles au moins une interaction en direct, supervisée, dans laquelle le·la candidat·e ne peut recevoir aucune aide externe, humaine ou assistée par l'IA?
- Mettez en œuvre la vérification d'identité, comprenant l'authentification de documents, la correspondance biométrique et la corroboration de l'identité (comparaison d'un égoportrait et d'une pièce d'identité gouvernementale), avant ou durant le processus d'entrevue plutôt qu'après l'émission d'une offre.
- Les évaluations techniques sont-elles effectuées en direct par des expert·es internes avec confirmation biométrique, ou par l'entremise d'exercices à faire à domicile sans surveillance?
- Effectuez-vous une analyse du profil numérique et de l'adresse IP, en comparant le lieu déclaré à l'adresse IP utilisée lors de l'entrevue et en vérifiant la présence professionnelle pour assurer sa cohérence avec l'expérience affirmée?
- Vos gestionnaires d'embauche, y compris les gestionnaires du·de la client·e dans les programmes d'EOR et d'AOR qui peuvent constituer le seul point de vérification humaine, sont-il·elles formé·es pour reconnaître les indicateurs de fraude, qu'il s'agisse d'un·e candidat·e coaché·e, d'une personne interviewée assistée par l'IA ou d'un CV rédigé avec une aisance supérieure à celle que la personne démontre en entrevue?
- Vérifiez-vous les diplômes directement auprès des établissements émetteurs ou vous fiez-vous à la documentation fournie par le·la candidat·e?

Contrôles lors de l'intégration

- Les références sont-elles contactées par l'entremise de canaux vérifiés de manière indépendante plutôt qu'à l'aide des numéros fournis par le·la candidat·e?
- Les vérifications des antécédents et des diplômes sont-elles effectuées avant l'octroi d'un accès complet aux systèmes?
- Le processus d'intégration comprend-il une revérification de l'identité, afin de confirmer que la personne recevant le matériel et les identifiants est bien celle qui a passé l'entrevue?
- L'adresse d'expédition de l'appareil correspond-elle au lieu déclaré par le·la candidat·e?
- Mettez-vous en place des protocoles d'accès progressif, limitant les autorisations système durant une période probatoire initiale?
- Une évaluation structurée à 30, 60 et 90 jours permet-elle de vérifier si les compétences démontrées correspondent au rendement observé lors de l'entrevue?

Surveillance post-embauche

- Disposez-vous de capacités d'analyse de la géolocalisation et des adresses IP permettant de comparer les lieux de connexion avec le lieu déclaré par le·la travailleur·se?
- Vos systèmes peuvent-ils détecter des accès simultanés à partir de plusieurs lieux géographiques ou des déplacements improbables?
- Surveillez-vous les schémas de latence réseau lors des appels vidéo et des connexions système afin de détecter des indices de routage du trafic par une infrastructure de proxy?
- Exigez-vous des interactions périodiques en personne, même pour les postes à distance, afin de créer des points de contact pour la vérification d'identité?
- Surveillez-vous les anomalies comportementales, par exemple des schémas de travail incompatibles avec une seule personne, des variations dans le style de communication, des accès inhabituels aux données, des transferts massifs ou des profils d'activité en rafales suivies de silences, laissant croire à une attention divisée entre plusieurs postes simultanés?
- Vos gestionnaires sont-il·elles formé·es pour reconnaître la signature précise du cumul d'emplois, non seulement une dégradation du rendement, mais aussi une disponibilité incohérente, des erreurs liées au changement de contexte et un résultat dont la qualité est adéquate, mais dont le volume demeure limité par rapport à celui d'un·e travailleur·se pleinement engagé·e?

Processus de départ et consignation des incidents

- Lorsque des travailleur·ses sont licencié·es pour rendement insuffisant, en particulier au cours des six premiers mois, votre processus de départ évalue-t-il si une fraude pourrait avoir été un facteur contributif?
- Vérifiez-vous la présence d'indicateurs de fraude au moment lors du licenciement : divergences d'identité, écarts de rendement inexpliqués, irrégularités liées à l'emplacement ou à l'accès, anomalies dans le profil numérique?
- Votre évaluation de fin de mandat inclut-elle un examen visant à déterminer si le volume de production du·de la travailleur·se, ses profils de disponibilité et ses erreurs liées au changement de contexte correspondaient à un engagement unique à temps plein, ou si le profil observé s'apparente plutôt à une attention divisée entre plusieurs postes simultanés?
- Les incidents de fraude confirmés et soupçonnés sont-ils consignés dans un système centralisé ou l'information demeure-t-elle cloisonnée?
- Effectuez-vous une analyse post-incident afin de déterminer à quelle étape du cycle de vie la fraude aurait pu être détectée plus tôt?
- Les données sur les incidents sont-elles examinées périodiquement afin de mettre en évidence des schémas à travers les postes, les canaux de recrutement, les zones géographiques ou les fournisseur·ses, plutôt que d'être évaluées au cas par cas?
- Les enseignements tirés des examens d'incidents servent-il·elles à actualiser le processus d'embauche, ou chaque incident est-il clos sans apprentissage organisationnel?

Préparation organisationnelle

- L'atténuation de la fraude est-elle traitée comme une priorité de gestion des risques d'entreprise, avec une responsabilisation transversale entre les services des achats, des ressources humaines, de sécurité et juridique, ou repose-t-elle uniquement sur une fonction dépourvue de l'autorité ou de la visibilité nécessaires pour agir à travers les autres?
- Disposez-vous d'un plan d'intervention en cas d'incident documenté pour les cas de fraude présumée concernant les candidat·es, associant les RH, la sécurité, le service juridique et la direction de l'entreprise?
- Êtes-vous en mesure de quantifier votre exposition actuelle à la fraude sur l'ensemble du continuum des coûts, des niveaux 1 à 4, ou gérez-vous un risque que vous n'avez jamais mesuré formellement?
- À quand remonte la dernière mise à l'épreuve de vos contrôles par rapport aux tactiques actuelles des niveaux 2 et 3?
- Savez-vous si votre programme est actuellement touché par de la fraude, ou votre réponse dépend-elle uniquement de ce qui a été suffisamment visible pour remonter à la surface?

Évaluer votre posture

Note	Signification
Majoritairement « Oui »	Vous disposez de protections de base en place. Concentrez-vous sur une exécution cohérente malgré la pression liée à l'embauche et vérifiez que vos contrôles traitent les menaces des niveaux 2 et 3, et pas seulement celles liées à l'embellissement des CV.
Résultats mitigés	Vous présentez des écarts pouvant être exploités. Utilisez le cadre d'évaluation des risques liés aux menaces de la section 4 pour déterminer les écarts qui présentent le plus grand risque compte tenu de votre secteur d'activité, des types de postes et du volume de placements, puis déterminez si leur comblement nécessite un investissement interne, des capacités externes ou les deux.
Majoritairement « Non »	Votre exposition non analysée est importante. Commencez par la cartographie de la surface d'attaque à la section 4 : comprenez votre volume de placements, les profils de risque des postes et votre position sur le continuum des coûts. Cette évaluation est la condition préalable à toute autre décision.

Conclusion

Le paysage des menaces liées à la fraude de la part des candidat·es continue d'évoluer, tant sur le plan de la sophistication et de l'ampleur, que sur celui des outils à la disposition des attaquant·es et des protecteur·rices. Les cadres présentés dans ce document, à savoir la taxonomie en six mécanismes, le continuum des coûts, le modèle de protection du cycle d'embauche et l'autoévaluation de la posture face au risque de fraude, constituent une base pour évaluer et traiter ce risque.

Trois principes devraient guider les étapes suivantes. Premièrement, considérez la fraude de la part des candidat·es comme un enjeu de gestion des risques d'entreprise relevant de la responsabilité de plusieurs services, et non comme un simple inconvénient pour les RH qui est géré par une seule équipe. Deuxièmement, évaluez vos contrôles par rapport à l'environnement de menaces actuel, et non par rapport à celui qui existait lorsque vos procédures de vérification ont été conçues. Troisièmement, reconnaissez que les protections les plus efficaces reposent sur une combinaison de technologies, de processus et d'expertise humaine tout au long du cycle d'embauche et chez tous les partenaires de votre chaîne d'approvisionnement. L'expertise humaine, qui est la plus difficile à développer, est celle qui détermine l'efficacité des deux autres composantes.

Les organisations les mieux placées pour gérer ce risque sont celles qui considèrent l'atténuation de la fraude non pas comme un ensemble de contrôles statiques, mais comme une capacité qui s'adapte aussi rapidement que les menaces auxquelles elles sont confrontées, et qui reconnaissent la concentration particulière des risques dans leurs programmes de ressources externes.

Pour discuter de la posture de risque de fraude de votre organisation, demandez une évaluation confidentielle des risques liés aux menaces