TROUSSE D'OUTILS DE L'OACI SUR LA MENACE INTERNE

GÉNÉRALITÉS

La présente trousse d'outils, conçue par le groupe de travail chargé de la formation du Groupe d'experts de la sûreté de l'aviation, vise à aider les organisations actives dans le domaine de l'aviation à mieux se protéger contre la menace interne, un phénomène en constante évolution. Comme il est indiqué dans le document de l'OACI *État du contexte de risque mondial de sûreté de l'aviation civile* (Doc 10108 – Diffusion restreinte), les terroristes cherchent systématiquement à exploiter les vulnérabilités des contrôles de sûreté pour perpétrer des actes d'intervention illicite contre l'aviation, utilisant notamment pour ce faire des éléments internes.

Qui sont les éléments internes ?

Les éléments internes sont les personnes employées à temps plein ou à temps partiel (y compris les sous-traitants, les temporaires et les indépendants) dans ou pour le secteur de l'aviation, à qui leur fonction confère un accès privilégié à des lieux ou à des objets sécurisés ou à des informations sensibles relatives à la sûreté ou donne une connaissance de ces lieux, objets et informations que d'autres n'ont pas.

Qu'est-ce que la menace interne ?

La menace interne renvoie au risque de voir une personne employée travaillant dans le secteur de l'aviation perpétrer ou faciliter un acte d'intervention illicite grâce à l'avantage tactique que son autorisation d'accès lui donne.

Quels peuvent être les motifs d'agir d'un élément interne ?

Un élément interne peut perpétrer ou faciliter un acte d'intervention illicite par inconscience, négligence ou malveillance. Une méconnaissance des politiques et des procédures ou le laisser-aller (approche laxiste des politiques et procédures) peuvent l'amener à faciliter involontairement un acte d'intervention illicite par négligence, passivité ou non-respect des politiques et procédures de sûreté.

Par ailleurs, un élément interne malveillant – celui qui commet délibérément un acte d'intervention illicite – peut être motivé par plusieurs facteurs combinés liés à une vulnérabilité personnelle, à sa vie privée ou à certaines situations, tels que l'appât du gain, l'idéologie, le désir de vengeance, le besoin de reconnaissance ou la coercition.

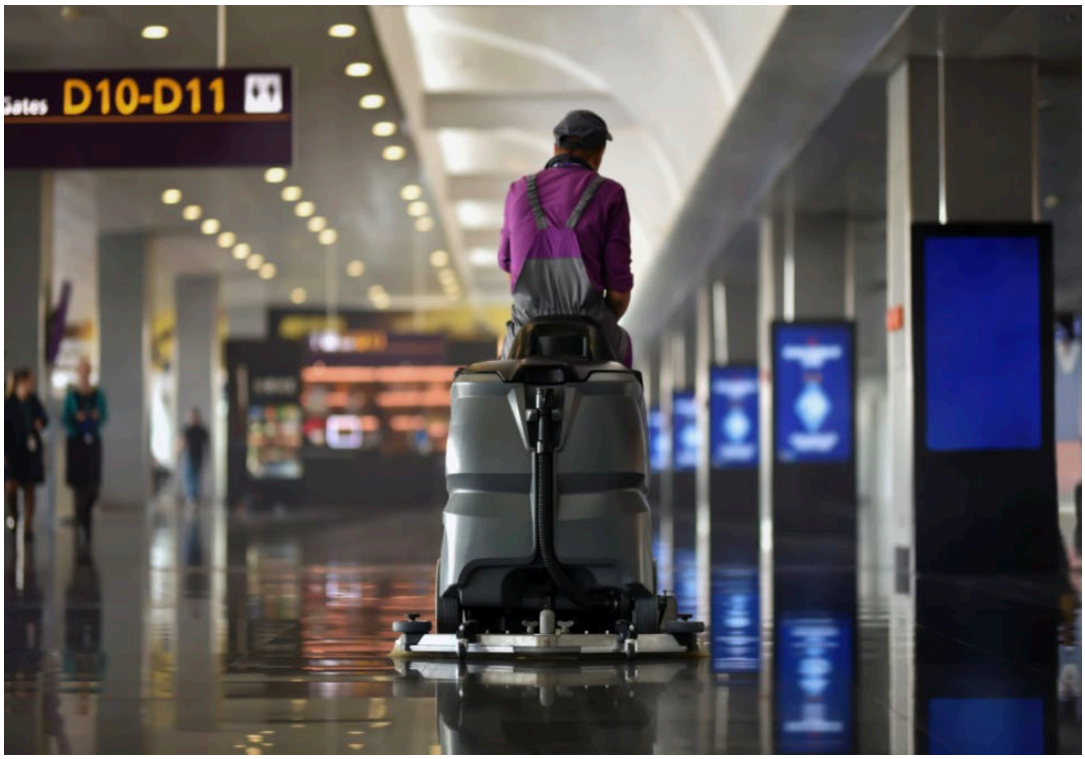
Un élément interne malintentionné peut avoir délibérément cherché à entrer dans une organisation pour y commettre un acte d'intervention illicite ou avoir acquis l'intention de le faire alors qu'il est déjà employé par cette organisation (et avoir été par exemple recruté par une partie tierce souhaitant tirer parti de sa position de confiance).

Comment un élément interne peut-il agir ?

Un élément interne peut commettre tout acte d'intervention illicite (p. ex. détruire un aéronef en service, introduire à bord d'un aéronef ou dans un aéroport une arme, un engin dangereux ou une matière dangereuse à des fins criminelles). Il peut divulguer des informations confidentielles, faciliter l'accès à une zone réglementée, remplir son rôle de manière inadéquate et permettre ainsi l'introduction d'articles interdits dans une zone réglementée, aider des personnes extérieures à entrer dans un système informatique ou une autre infrastructure numérique[1], etc.

MESURES D'ATTÉNUATION

Il existe tout un éventail de mesures et de politiques touchant au personnel et à la sûreté qui peuvent aider les organisations à amoindrir la menace interne. En général, ces mesures visent à réduire le risque qu'il y a de recruter des personnes susceptibles de présenter un problème pour la sûreté du fait de leurs actes, à réduire autant que possible la probabilité que les employés en place deviennent un problème, à réduire le risque d'actes malveillants internes et à protéger les avoirs de l'organisation.



[1] Par infrastructure numérique, on entend des biens essentiellement liés aux communications mobiles et par internet

Les mesures et outils d'atténuation de la menace interne peuvent être regroupés selon les catégories suivantes.

VÉRIFICATION DES ANTÉCÉDENTS ET VALIDATION

Politiques et procédures : Des politiques et des procédures rigoureuses en matière de vérification des antécédents (y compris l'identité de la personne recrutée, son expérience professionnelle, son casier judiciaire et ses études) sont un élément essentiel de tout cadre visant à limiter la menace interne. Ces politiques et procédures doivent être claires et concises et devraient être régulièrement revues.

Vérification initiale des antécédents : Tous les employés qui ont besoin d'avoir accès sans être accompagnés au côté piste et aux zones de sûreté à accès réglementé, ainsi que les personnes ayant accès à des informations sensibles relatives à la sûreté, doivent se soumettre à une vérification de leurs antécédents[2] selon les modalités décidées par l'autorité compétente.

Cette vérification initiale devrait couvrir :

- l'identité de l'intéressé (qui fournira par exemple un passeport, une carte d'identité, un extrait d'acte de naissance, etc.) ;
- le casier judiciaire (dans toute la mesure permise par les lois et les règlements locaux) ;
- les références (pour vérifier l'éthique de travail et l'aptitude générale des candidats à des emplois) ;
- le parcours professionnel (p. ex. employeurs précédents, études, etc.).

Vérification périodique des antécédents : Cette vérification des antécédents devrait être répétée et mise à jour régulièrement dans le cadre des vérifications cycliques du personnel sur le plan de la sûreté. Une bonne pratique consiste à le faire chaque fois qu'un permis d'identification aéroportuaire est renouvelé.

Ceux qui commettent un acte (d'intervention) illicite en profitant de l'accès ou de la connaissance qu'ils ont en qualité d'élément interne acquièrent souvent l'intention de commettre l'acte après avoir été recrutés. De plus, dans bien des cas, ils peuvent s'être déjà fait remarquer par la direction (p. ex. en raison de manquements à la discipline ou d'une performance professionnelle insatisfaisante), ce qui devrait être pris en considération au moment de revérifier les antécédents.

Validation continue : Un processus de validation continue devrait être encouragé, en collaboration avec les autorités compétentes (et, le cas échéant, avec les autorités d'autres États). Il s'agit ici d'évaluer si une personne continue de satisfaire aux conditions exigibles pour son emploi.

[2] Norme 3.5.2 de l'Annexe 17 – *Sûreté de l'aviation* (Douzième édition, Amendement n°18)

Vérification renforcée des antécédents : Il pourrait être utile de faire vérifier les données relevant du renseignement (et toute autre information pertinente disponible relative à l'aptitude d'une personne à exercer une fonction). Ainsi, un État peut collaborer avec les autorités nationales compétentes concernées pour incorporer certaines données renforcées dans le processus à plusieurs niveaux de vérification et de validation.

De même, si un membre du personnel décèle un comportement suspect ou inhabituel chez une personne, il convient de contacter les autorités locales compétentes et les services de sûreté concernés, car une vérification approfondie des antécédents pourrait être nécessaire au niveau du renseignement.

FORMATION ET SENSIBILISATION

Formation de sensibilisation : La sensibilisation à la sûreté et la formation à la culture de la sûreté devraient être encouragées pour tout le personnel. Cela permettra de s'assurer que tout le personnel connaît les politiques, les normes, les lignes directrices et les procédures de sûreté et comprend leur raison d'être, qui est de maintenir un niveau élevé de sûreté. Cette formation permettra également aux personnes nouvellement recrutées d'acquérir la capacité de déceler et de signaler sans risque tout comportement suspect à l'autorité compétente ou à l'agent ou organe des services répressifs approprié, éventuellement de manière anonyme.

Intégration de la formation : La sensibilisation à la sûreté pourrait être intégrée à la formation initiale et à la formation régulière déjà existante, ainsi qu'être introduite dans des documents de sensibilisation, des ateliers, des séances d'information, etc., afin de favoriser une culture de la sûreté de l'aviation qui soit solide et efficace.

Formation propre à certains rôles : Pour certaines catégories de personnel, notamment les chefs de service, les gestionnaires et les personnes responsables des questions de sûreté en rapport avec le personnel, une formation plus approfondie et propre à leur rôle sera nécessaire pour viser des résultats plus ciblés.

Campagnes de sensibilisation : Des messages graphiques couvrant les principaux aspects de la sûreté devraient être conçus pour être affichés dans les organisations et les aéroports et servir de rappel visuel au personnel.

MESURES RELATIVES AU CONTRÔLE D'ACCÈS

Inspection-filtrage : Des mesures visant à contrôler l'accès devraient être mises en place pour veiller à ce que les personnes autres que les passagers, de même que les articles qu'elles transportent, fassent l'objet d'une inspection-filtrage avant qu'elles n'entrent dans une zone de sûreté à accès réglementé[3]. Elles devraient comprendre des contrôles aléatoires et imprévisibles pour contrebalancer la connaissance que les éléments internes ont des procédures et réduire le risque que des articles interdits ne soient introduits côté piste, y compris par des membres du personnel.

Politiques et procédures : Les politiques et procédures devraient être claires et comprendre :

- la désactivation de l'insigne d'identification des employés qui ont quitté l'organisation (par suite de démission, de départ à la retraite, etc.) ;
- la limitation du droit d'accès aux zones réglementées pour les détenteurs de laissez-passer en fonction des stricts besoins opérationnels ;
- une protection adéquate du périmètre et des points de contrôle d'accès afin de veiller à ce que l'inspection-filtrage du personnel à des fins de sûreté ne soit pas contournée ;
- le cas échéant, la mise en place de protocoles de supervision et une large utilisation de caméras en circuit fermé pour les activités opérationnelles.

[3] Norme 4.2.5 de l'Annexe 17 – *Sûreté de l'aviation* (Douzième édition, Amendement nº 18).

Révision des listes d'accès : Il est recommandé que les procédures de délivrance des cartes d'identification aéroportuaire soient revues pour s'assurer que l'employé qui demande à avoir accès à une certaine zone en a effectivement besoin pour son travail.

PATROUILLES

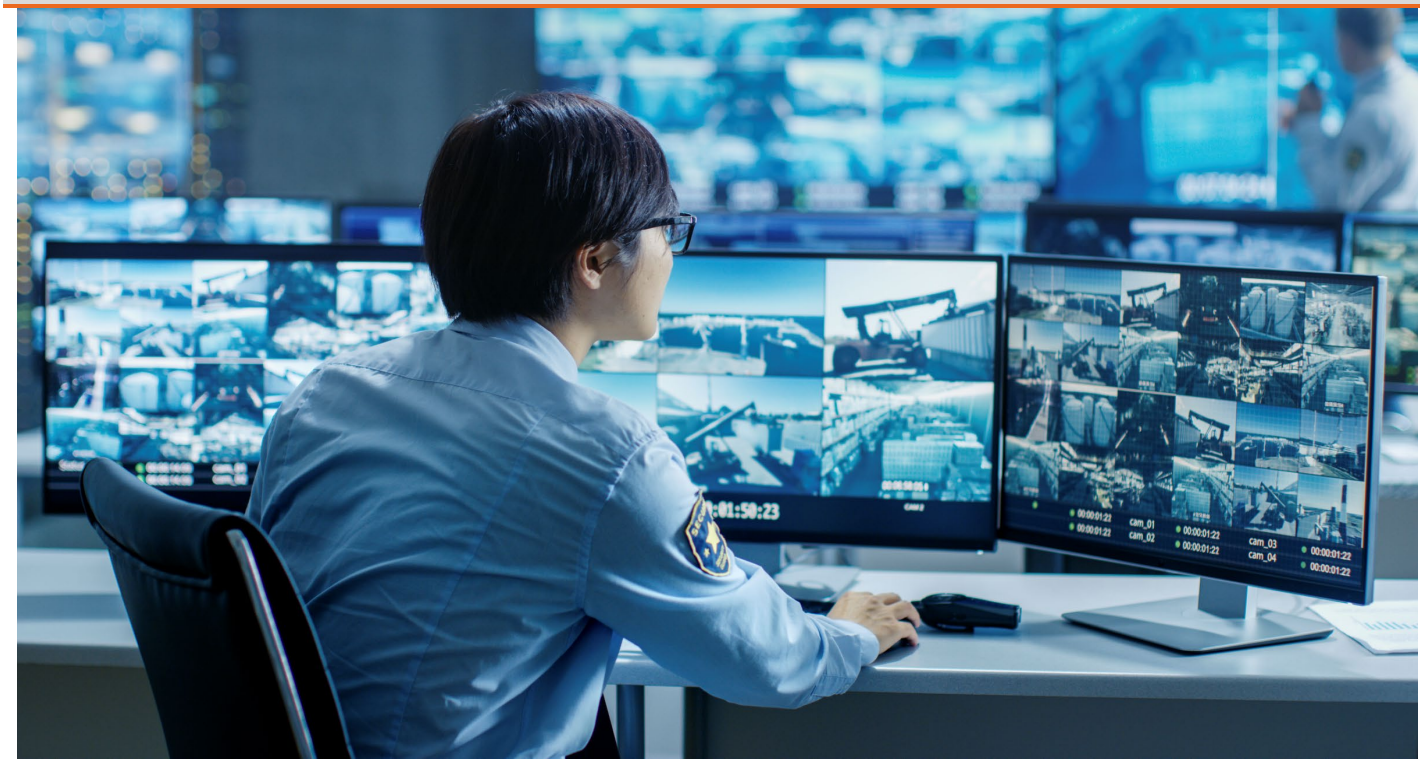
Caractère aléatoire et imprévisible : Les patrouilles devraient être effectuées de manière aléatoire et imprévisible (p. ex. vérifications par sondage), afin qu'elles ne puissent être évitées ou contournées à la suite d'une action de reconnaissance hostile ou de l'intervention d'une personne ayant une connaissance interne de ces patrouilles. Elles devraient aussi porter sur la surveillance, outre du personnel aéroportuaire, des passagers et des autres acteurs aéroportuaires, ainsi que des infrastructures aéroportuaires et des marchandises, de façon à déceler tout signe d'activité inhabituelle ou de sûreté déficiente.

Les patrouilles peuvent être efficaces comme moyen de dissuasion visuel si ses membres portent un uniforme et utilisent des véhicules identifiés. Il se peut aussi que les patrouilles assurent une surveillance renforcée si elles sont effectuées de manière discrète.

SURVEILLANCE ET SUIVI

Méthodes : Concernant les processus et les employés, le contrôle de la qualité et le suivi propres à la menace interne peuvent jouer un rôle déterminant pour prévenir les incidents de sûreté et les actes d'intervention illicite ou y réagir rapidement. Les méthodes de surveillance comprennent les caméras en circuit fermé, la tenue de registres (p. ex. demandes d'accès) et la surveillance au sol par du personnel de sûreté.

Les chefs de service jouent également un rôle essentiel dans la détection et la surveillance des activités et des comportements inhabituels des personnes qu'ils supervisent.



Données : Dans certaines organisations, les données relatives aux employés se retrouvent dans divers journaux d'application logicielle, qui enregistrent les actions des employés. Il peut ressortir de ces données numériques certains comportements au travail et on peut ainsi s'en servir pour déceler une éventuelle intention malveillante au sein du personnel aéroportuaire (p. ex. un membre du personnel qui entre dans une zone sans que son travail le justifie).

Ces applications pourraient inclure :

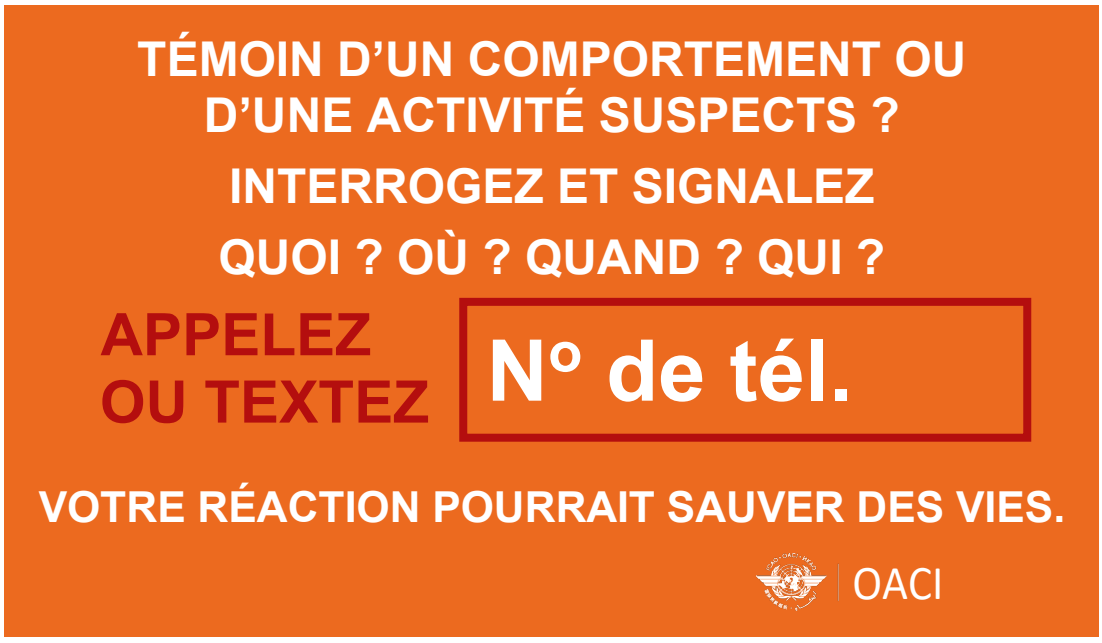
- des registres physiques d'entrée/sortie, concernant essentiellement l'accès à un espace physique donné, et l'heure de cet accès ;
- des données de connexion et déconnexion, en s'intéressant surtout aux informations concernant l'heure et l'utilisateur ;
- des journaux d'application de messagerie ;
- des journaux d'application de base de données.

MÉCANISMES DE NOTIFICATION

Notifier les comportements suspects : Les mécanismes de notification devraient faire intervenir toute personne travaillant dans l'organisation, et pas seulement celles qui sont directement affectées à des tâches relatives à la sûreté, car les employés de l'organisation sont ses « yeux », ses « oreilles » et sa « voix ».

On peut mettre en place des mécanismes de notification de sorte que les employés puissent signaler sans risque tout comportement ou incident suspect au moyen d'un texto, d'un courriel, d'un appel téléphonique, d'un canal de communication interne ou en parlant à quelqu'un en personne. Ces notifications devraient recevoir une réponse claire, efficace et rapide.

Des messages anonymes ou confidentiels peuvent être très utiles pour aider à atténuer les menaces internes potentielles et à établir une réelle culture de la sûreté dans l'organisation.

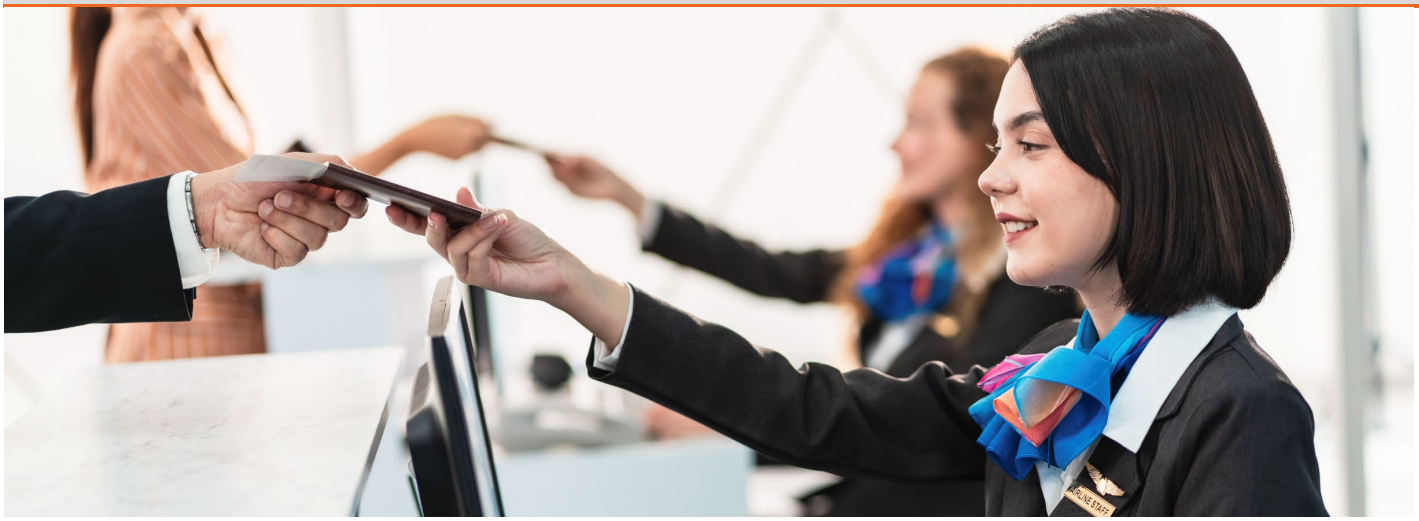


ANALYSE COMPORTEMENTALE[4]

Analyse comportementale : Elle peut être un outil utile pour aider à réduire la menace interne. Elle se fonde sur la prémisse que quelqu'un peut montrer des signes de comportement suspect ou inhabituel, et que ces signes peuvent être détectés par des personnes dûment formées.

Formation : Une formation qui familiarise le personnel à ce qui constitue une activité suspecte ou un comportement inhabituel et lui expliquant comment le signaler peut être utile.

La formation à l'analyse comportementale devrait être donnée à un large éventail de personnes, notamment les personnes responsables de la délivrance des laissez-passer, celles qui effectuent la vérification des antécédents ou celles qui font de l'inspection-filtrage. Cependant, c'est l'ensemble du personnel qui pourrait bénéficier de ce type de formation dans le cadre d'une action générale de sensibilisation à la sûreté.



CULTURE DE LA SÛRETÉ [5]

Une culture de la sûreté solide et efficace : L'instauration d'une culture positive de la sûreté dans tout le secteur de l'aviation est essentielle si l'on veut réduire les menaces internes et obtenir des résultats réels et solides en matière de sûreté. Le personnel peut être :

- motivé et informé des risques que représente la menace interne au moyen de réunions régulières sur les menaces et les questions de sûreté au sens large ;
- formé pour détecter et signaler les comportements anormaux ou suspects ;
- une source précieuse d'informations sur les vulnérabilités et sur les moyens d'y remédier.

[4] L'analyse comportementale consiste à appliquer des techniques permettant de reconnaître des caractéristiques comportementales, notamment des signes physiologiques ou gestuels dénotant un comportement anormal (une combinaison de signes verbaux et non verbaux), afin de déceler les personnes pouvant avoir l'intention de commettre un acte d'intervention illicite.

[5] On trouvera des renseignements supplémentaires sur la culture de la sûreté (y compris les ressources de l'OACI en la matière) sur le site web de l'OACI consacré à la question : www.icao.int/Security/Security-Culture

LEADERSHIP ET STRATÉGIE

Leadership fort : Il est essentiel que les responsables comprennent qu'ils ont un rôle à jouer en montrant l'exemple s'agissant des actes et des comportements positifs en matière de sûreté attendus du personnel. Il convient d'encourager le personnel et la direction à communiquer librement et les responsables devraient avoir une bonne compréhension des pressions qui s'exercent au quotidien sur le personnel dans le cadre de son travail et des risques internes résultant de ces pressions.

Un cadre (p. ex. gestionnaire de rang supérieur) qui fait siens les principes de risque de sûreté, approche les politiques de sûreté selon un modèle descendant et illustre par son comportement celui qui est attendu de tous sera plus à même de promouvoir une approche plus conforme et plus cohérente de la sûreté dans l'ensemble de l'organisation, contribuant ainsi davantage encore à réduire les menaces internes.

Stratégie : Il est recommandé d'avoir une stratégie d'atténuation de la menace interne (approuvée par la direction) pour aider le personnel à comprendre comment déceler et signaler les comportements suspects sur le lieu de travail.

La stratégie peut également inclure des politiques, des lignes directrices et des procédures relatives au personnel. Il s'agit notamment des mesures à prendre avant le recrutement et tout au long de la période d'emploi dans l'organisation. La stratégie et les politiques associées devraient être revues régulièrement avec toutes les principales parties prenantes.

Tous documents cadres[6], manuels et éléments indicatifs peuvent être autant d'outils supplémentaires utiles.

[6] Par exemple, www.cpni.gov.uk/insider-risks/insider-risk-mitigation-framework

FACTEURS HUMAINS

Performance et facteurs humains : Les organisations doivent comprendre comment la performance humaine peut aider à atténuer la menace interne. Cela veut notamment dire être conscient de la façon dont les facteurs humains peuvent avoir une incidence sur les individus, qui peuvent intentionnellement ou non mettre à profit leur accès privilégié pour rendre possible un acte d'intervention illicite. Les responsables et la haute direction devraient :

- développer une meilleure intelligence des capacités humaines et de la façon dont celles-ci peuvent aider à atténuer le risque d'actes malveillants internes ;
- comprendre les limites humaines et la façon dont elles peuvent être prises en compte pour s'assurer qu'elles n'ont pas d'incidence sur la performance professionnelle ;
- faciliter la notification par le personnel des problèmes de sûreté et des comportements suspects ;
- comprendre le lien entre les facteurs humains, la culture de la sûreté et la motivation ;
- assurer la disponibilité des ressources nécessaires au personnel ;
- veiller à ce que le personnel de supervision soit en mesure d'identifier les signes de stress et de fatigue afin d'y faire face rapidement ;
- éviter le laxisme dans les activités quotidiennes.

TECHNOLOGIES AVANCÉES[7]

Détection de traces d'explosifs (ETD): L'utilisation d'équipements ETD peut ajouter un degré de sûreté supplémentaire aux procédures normales d'inspection-filtrage des non-passagers et/ou aux contre-mesures de sûreté aléatoires et imprévisibles utilisées dans l'ensemble de la zone de sûreté à accès réglementé, contribuant ainsi à atténuer la menace interne.

Chiens détecteurs d'explosifs (EDD): On peut utiliser des brigades canines pour de multiples fins, dont des contrôles de sûreté dans toutes les zones de l'aéroport (côté ville, côté piste, passagers, non-passagers, bagages, fret, etc.), le quadrillage des zones de sûreté à accès réglementé et l'application de mesures de sûreté aléatoires et imprévisibles.

Intelligence artificielle (IA) : L'utilisation par un personnel formé de systèmes fondés sur l'intelligence artificielle peut aider à déceler les tendances et les activités anormales. Par exemple, les solutions modernes de gestion des incidents peuvent aider à déceler les incidents et à faire la différence entre situations banales et menaces imminentes, telles que les tentatives d'entrée par effraction dans les zones sécurisées.

[7] L'application de technologies avancées peut aider à atténuer le risque interne grâce à des normes de détection renforcées pour les procédures d'inspection-filtrage en place aux fins de la sûreté et/ou grâce à des degrés de sûreté supplémentaires venant s'ajouter au niveau de base quand ils sont appliqués de manière aléatoire et imprévisible dans l'ensemble du système aéroportuaire.

— FIN —