مجموعة أدوات الإيكاو بشأن التهديدات من الداخل

معلومات عامة

صُممت مجموعة الأدوات هذه، التي استحدثتها مجموعة عمل التدريب التابعة لفريق خبراء أمن الطيران، لمساعدة المؤسسات التي تعمل في بيئة الطيران على التفاعل بشكل أفضل مع التهديدات من الداخل التي تتطور باستمرار. وكما أشير إليه في بيان الإيكاو بشأن سياق المخاطر العالمية في مجال أمن الطيران (الوثيقة Doc 10108 – مقيّدة التوزيع)، يتطلع الإرهابيون باستمرار إلى استغلال أوجه الضعف في مراقبة الأمن ويرتكبون أفعال تدخل غير مشروع ضد الطيران، وهو أمر يمكن تيسيره عبر استغلال العناصر من الداخل

من هم العناصر من الداخل؟

العناصر من الداخل هم موظفون بدوام كامل أو دوام جزئي (بمن فيهم المتعاقدون والموظفون المؤقتون والموظفون لحسابهم الخاص) يعملون في قطاع الطيران أو لصالحه ويمنحهم دورهم إمكانية وصول مميزة إلى مواقع أو بنود مؤمنة و/أو معرفة بها أو إلى معلومات أمنية حساسة.

ما هو التهديد من الداخل؟

يشير التهديد من الداخل إلى الخطر الناجم عن قيام موظفي قطاع الطيران بفعل تدخل غير مشروع أو تسهيلهم له من خلال استخدام دخولهم المصرح به، ما يمنحهم بالتالي ميزة تكتيكية

ما هو السبب المنطقي للعنصر من الداخل؟

يمكن أن يقوم العناصر من الداخل بفعل تدخل غير مشروع أو بتسهيله بسبب الافتقار إلى الوعي أو فرط الثقة أو التهاون. وقد يسبب الافتقار إلى الوعي بالسياسات والإجراءات والتهاون (نهج التراخي في السياسات والإجراءات) تسهيل العناصر من الداخل عن غير قصد لفعل التدخل غير المشروع بسبب إهمالهم أو تقاعسهم أو فشلهم في اتباع السياسات والإجراءات الأمنية.

من ناحية ثانية، قد يكون العناصر الخبيثون من الداخل – أي الذين يتخذون قراراً مدروساً بالقيام بفعل غير مشروع – مدفوعين بمزيج من مواطن الضعف الشخصية وأحداث الحياة والعوامل الظرفية، من قبيل الكسب المالي أو الإيديولوجيا أو الثأر أو الرغبة في الاعتراف أو الإكراه.

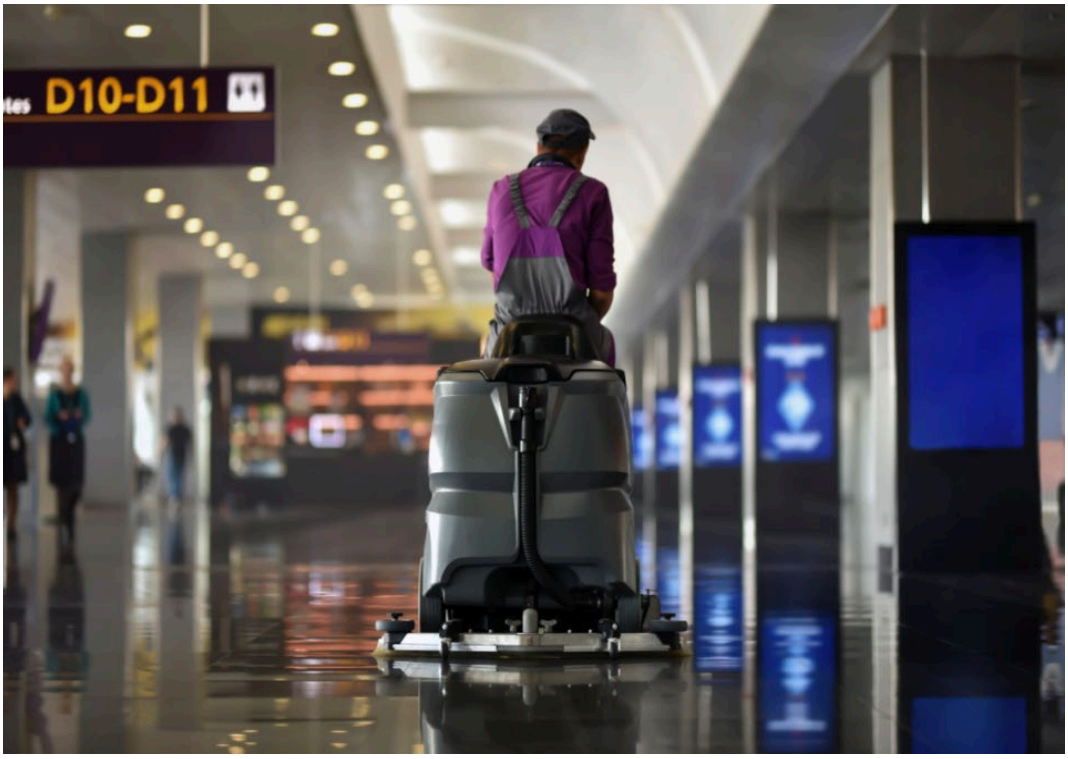
وقد يسعى العناصر الخبيثون من الداخل عمداً للانضمام إلى إحدى المؤسسات من أجل القيام بأفعال تدخل غير مشروع أو اكتساب النية للقيام بذلك أثناء عملهم (مثلاً التوظيف من قبل طرف ثالث لاستغلال منصبهم الموثوق)..

كيف يمكن أن يتصرف العنصر من الداخل؟

يمكن أن يقوم العناصر من الداخل بأفعال تدخل غير مشروع (مثل تدمير طائرة موضوعة في الخدمة، أو إدخال سلاح أو جهاز خطر أو مادة خطرة معدة لأغراض إجرامية على متن الطائرة أو في المطار). ويمكن للعناصر من الداخل تبادل معلومات سرية، أو تسهيل الدخول إلى المناطق المقيّدة، أو أداء دورهم بصورة غير كافية تمكّن من إدخال مواد محظورة إلى المناطق المقيّدة، أو مساعدة أطراف خارجيين على الوصول إلى نظم الحواسيب أو أي بنية أساسية رقمية أخرى[1]، وما إلى ذلك.

تدابير التخفيف

’ يمكن لمجموعة من التدابير والسياسات الأمنية الشخصية أن تساعد المؤسسات على التخفيف من التهديدات التي يشكلها العناصر من الداخل. وبوجه عام، تسعى هذه التدابير إلى الحد من مخاطر تعيين موظفين يمكن أن تسبب أفعالهم مخاوف أمنية، والتقليل إلى أدنى حد ممكن من احتمال أن يصبح الموظفون الحاليون هاجساً أمنياً، والحد من مخاطر نشاط العناصر من الداخل، وحماية ممتلكات المؤسسة.



[1] تعني البيئة الأساسية الرقمية الممتلكات المتعلقة أساسًا بالاتصالات المتنقلة واتصالات شبكة الإنترنت

يمكن تجميع تدابير وأدوات التخفيف من تهديدات العناصر من الداخل ضمن المجالات التالية

التحريات الشخصية والتدقيق

السياسات والإجراءات: تعتبر السياسات والإجراءات المتينة بشأن التحريات الشخصية، بما في ذلك هوية الموظفين وخبرة العمل السابقة والتاريخ الجنائي والخلفية التعليمية، حجر الزاوية في أي إطار يهدف إلى التخفيف من التهديدات التي يشكلها العناصر من الداخل. ويجب أن تكون هذه السياسات والإجراءات واضحة وموجزة وأن يتم استعراضها بشكل دوري.

التحريات الشخصية الأولية: يجب على جميع الموظفين الذين يحتاجون إلى الدخول إلى منطقة التحركات الجوية (الجانب الجوي) وإلى المناطق الأمنية المقيدة بدون حراسة، والأشخاص الذين تتوفر لهم إمكانية الحصول على معلومات أمنية حساسة أن يخضعوا للتحريات الأمنية الشخصية[2] من جانب السلطة المختصة.

ينبغي أن تشمل التحريات الشخصية الأولية ما يلي:

- الهوية (مثلاً تقديم جواز سفر، بطاقة الهوية، سجلات الولادة، إلخ)؛
- السجل الجنائي (إلى الحد الأقصى الذي تسمح به اللوائح والقوانين المحلية، إلخ)؛
- مراجعة خطابات التزكية (لإثبات حُسن الأخلاقيات في العمل ومدى ملائمة الموظف موضوع التحريات بوجه عام، إلخ)؛
- السجل الوظيفي (مثلاً أصحاب العمل السابقين، السجل التعليمي، إلخ)

التحريات الشخصية: ينبغي تكرار التحريات الشخصية وتحديثه بانتظام كجزء من عمليات الكشف الأمني الشخصية الدورية. ومن الممارسات الجيدة تحديث التحريات الشخصية كلما دعت الحاجة إلى تجديد تصاريح الدخول إلى المطار.

وغالباً ما يكون لدى أولئك الذين يرتكبون أفعالاً غير مشروعة أو أفعال تدخل غير مشروع النية للقيام بذلك بعد تأمين وظيفتهم. بالإضافة إلى ذلك، قد يكون عدد كبير من الأعضاء من الداخل قد استرعوا انتباه الإدارة بالفعل (مثلاً عن طريق المخالفات المسلكية والأداء السيء)، وهو ما ينبغي أن يؤخذ في الاعتبار أثناء عملية التحريات الشخصية..

التدقيق المتواصل: ينبغي التشجيع على عملية التدقيق المتواصل بالتعاون مع السلطات المختصة المعنية (وعند الاقتضاء، مع السلطات في الدول الأخرى). والهدف من ذلك هو تقييم استمرار أحد الموظفين بالوفاء بالمتطلبات الوظيفية المنطبقة .

[2] القاعدة القياسية 3-5-2 في الملحق السابع عشر – أمن الطيران (الطبعة الثانية عشرة، التعديل (18))

التحريات الشخصية المحسّنة: يمكن أن يكون التحريات الشخصية الذي يشمل الاستخبارات (وأي معلومات أخرى ذات صلة ومتاحة عن ملاءمة الشخص للعمل في وظيفة معينة) مفيداً. وبالفعل، يمكن أن تتعاون الدول مع السلطات الوطنية المختصة لإدراج بعض البيانات المحسنة في التحريات الشخصية المتعدد المستويات وعملية التدقيق.

وبالمثل، إذا حدد الموظفون سلوكاً مريباً أو غير عادي لدى شخص معين، ينبغي عندئذ الاتصال بالسلطات الأمنية ذات الصلة والسلطات المختصة المحلية، نظراً إلى أنه قد يلزم إجراء تحريات شخصية استخباراتية محسنة .

التدريب والتوعية

التدريب على الوعي الأمني: يجب تشجيع جميع الموظفين على التدريب على الوعي الأمني والتدريب على ثقافة الأمن. وسيساعد ذلك على ضمان معرفة جميع العاملين بالسياسات والمعايير والمبادئ التوجيهية والإجراءات الأمنية، وكذلك فهم غرضها المتمثل في الحفاظ على مستوى عالٍ من الأمن. وسيتيح هذا التدريب أيضاً للموظفين الجدد تنمية القدرة على تحديد أنماط السلوك المريبة والإبلاغ عنها بأمان إلى السلطة المختصة أو إلى المسؤول عن إنفاذ القانون، بما في ذلك عن طريق وسائل مغفلة.

تكامل التدريب: يمكن إدراج الوعي الأمني في التدريب المتكرر الأولي والقائم أو من خلال استخدام مواد حملة التوعية وحلقات العمل وجلسات الاستماع وما إلى ذلك، من أجل تعزيز ثقافة أمنية قوية وفعالة في قطاع الطيران.

التدريب المرتبط بأدوار الموظفين: بالنسبة لبعض الموظفين، بما في ذلك على سبيل المثال لا الحصر المديرون والمسؤولين عن الأمن الشخصي، يكون التدريب المتعمق والمرتبط بأدوار الموظفين مناسباً لتكييف النتائج المرجوة للتدريب.

حملات التوعية: ينبغي أن يتم إعداد الرسائل البصرية التي تغطي جوانب الأمن الرئيسية من أجل عرضها داخل المؤسسات وبيئات المطارات لكي تكون بمثابة رسائل تذكير مرئية للموظفين.

تدابير مراقبة المنافذ

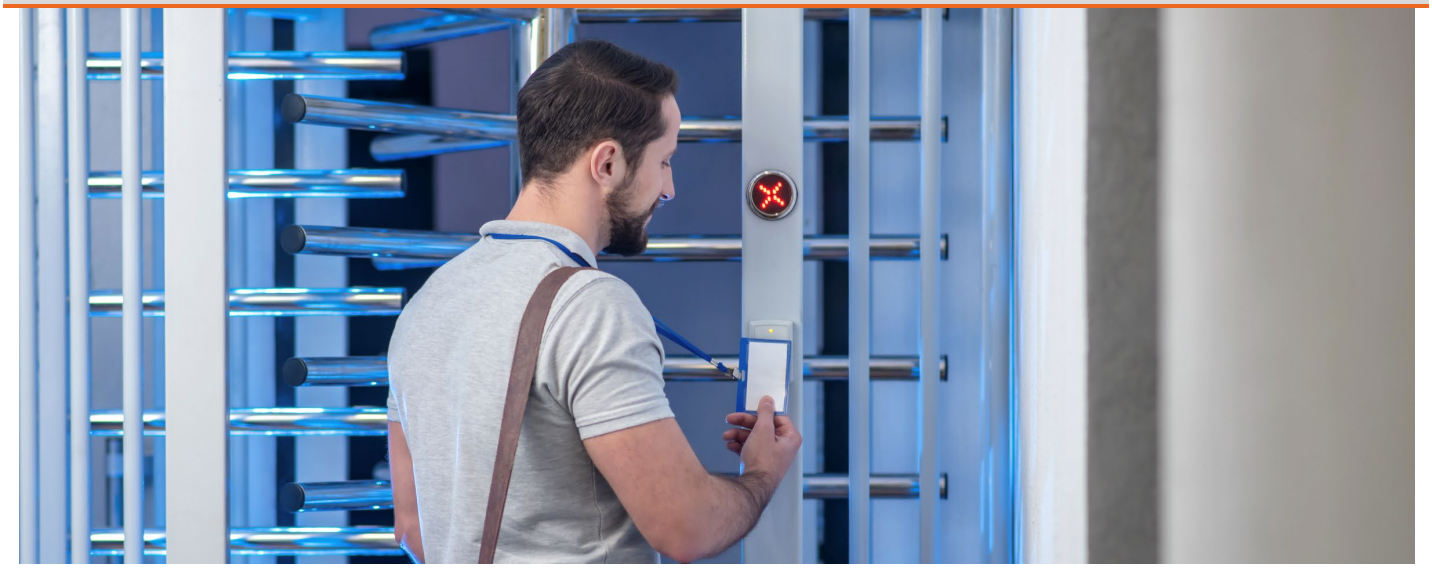
الكشف الأمني: ينبغي وضع تدابير مراقبة المنافذ لضمان إجراء الكشف الأمني على جميع الأشخاص الآخرين غير الركاب، وعلى الأشياء التي يحملونها، وذلك قبل دخولهم إلى المناطق الأمنية المقيّدة في المطار[3]. وينبغي أن يتضمن هذا الكشف الأمني أساليب كشف عشوائية وغير متوقعة للمساعدة على التعويض عن المعلومات الداخلية والحد من احتمال نقل المواد المحظورة إلى منطقة التحركات المراقبة (الجانب الجوي)، بما في ذلك عندما يحملها الموظفون

السياسات والإجراءات: ينبغي أن تكون السياسات والإجراءات واضحة وأن تشمل ما يلي:

- تعطيل مفعول شارات تعريف هوية الموظفين الذين غادروا المؤسسة (مثلاً، المستقيلون، المتقاعدون، إلخ.)؛
- وتقييد حقوق حاملي تراخيص الدخول إلى المناطق المقيدة استناداً إلى احتياجات تشغيلية صارمة;
- ;توفير الحماية الكافية لمحيط المطار ونقاط مراقبة المنافذ لضمان عدم التمكن من تجاوز الكشف الأمني للموظفين؛
- تنفيذ بروتوكولات المراقبة وتوسيع نطاق استخدام كاميرات الدائرة التلفزيونية المغلقة للأنشطة التشغيلية، أن وجدت.

[3] القاعدة القياسية 4-2-5 في الملحق السابع عشر – أمن الطيران (الطبعة الثانية عشرة، التعديل (18))

استعراض قوائم الدخول: يوصى باستعراض إجراءات إصدار تصاريح التعريف الخاصة بالمطار للتأكد من أن الموظف الذي يطلب السماح بالدخول إلى منطقة معينة لديه حاجة تشغيلية لهذا الدخول



الدوريات الأمنية

دوريات أمنية عشوائية وغير متوقعة: ينبغي تنفيذ الدوريات الأمنية بطريقة عشوائية وغير متوقعة (كعمليات التفتيش الموقعية)، بحيث لا يمكن تفادي الدوريات أو تجاوزها نتيجة استطلاع عدائي أو معلومات داخلية. بالإضافة إلى ذلك، ينبغي ألا يقتصر تركيز الدوريات الأمنية على مراقبة موظفي المطار فحسب، بل أن يشمل الركاب والجهات المعنية في المطار والبنية الأساسية للمطار والبضائع بحثاً عن علامات على نشاط غير عادي أو حالة أمنية سيئة.

يمكن أن تكون الدوريات الأمنية فعالة بوصفها رادعاً بصرياً إذا كان الموظفون يرتدون الزي الرسمي ويستخدمون مركبات تحمل علامات. وكبديل عن ذلك، يمكن للدوريات الأمنية أن توفر مراقبة معززة إن أجريت بطريقة سرية

المراقبة والرصد

الأساليب: يمكن أن تؤدي مراقبة ورصد جودة العمليات والموظفين المتعلقة بالتهديدات من الداخل دوراً هاماً في تجنب الوقائع الأمنية وأفعال التدخل غير المشروع أو التصدي السريع لها. وتشمل أساليب المراقبة كاميرات الدوائر التلفزيونية المغلقة، واستعراض سجلات النُظم (مثلاً طلبات الدخول)، والمراقبة التي يقوم بها الموظفون على الأرض.

ويقوم المراقبون أيضاً بدور حاسم في التعرف على الأنشطة وأنماط السلوك غير العادية للموظفين الذين تمارس الرقابة عليهم ورصدها

البيانات: في بعض المؤسسات، يمكن إيجاد بيانات الموظفين في مختلف سجلات تطبيقات البرمجيات التي تسجل أفعال الموظفين. ويمكن للبيانات الرقمية أن تسلط الضوء على أنماط العمل وأن تستخدم كأداة لتحديد ما إذا كان هناك سوء نية في أوساط موظفي المطار (مثلاً دخول مناطق لا يوجد حاجة تشغيلية لدخولها).

ويمكن أن تشمل التطبيقات ما يلي:

- سجلات دخول/خروج مادية، مع تركيز رئيسي على الوقت والدخول إلى الأماكن المادية؛
- وسجلات تسجيل الدخول/تسجيل الخروج، مع التركيز على وثائق الاعتماد المتطابقة من حيث الوقت والمستخدمين؛
- وسجلات تطبيق البريد الإلكتروني؛
- وسجلات تطبيق قاعدة البيانات

آليات الإبلاغ

الإبلاغ عن سلوك مريب: ينبغي أن تشمل آليات الإبلاغ جميع الأشخاص في المؤسسة – وليس فقط الأشخاص المعنيين مباشرة بالشؤون الأمنية. وهذه آليات هامة لأن الموظفين هم بمثابة "عيون" و"آذان" و"صوت" المؤسسة.

يمكن وضع آليات الإبلاغ بحيث يتمكن الموظفون من الإبلاغ عن أنماط السلوك أو الوقائع المريبة عن طريق النصوص أو رسائل البريد الإلكتروني أو المخابرات الهاتفية أو قنوات التواصل الداخلي، أو بالتحدث شخصياً إلى أحد ما. وينبغي أن تحصل التقارير الأمنية على ردّ واضح وفعال وسريع.

يمكن أن يكون الإبلاغ المجهول الهوية أو السري مفيداً للغاية في المساعدة على التخفيف من التهديدات المحتملة من الداخل وعلى ترسيخ ثقافة أمنية فعالة في المؤسس .

الكشف عن السلوك [4]

الكشف عن السلوك: يمكن أن يشكل الكشف عن السلوك أداة مفيدة في التخفيف من التهديدات من الداخل. ويستند الكشف إلى فرضية مفادها أن الناس قد تظهر عليهم مؤشرات تدل على سلوك مشبوه أو غير عادي، وأن هذه المؤشرات يمكن أن يلتقطها أشخاص حصلوا على التدريب الملائم.

التدريب: إن منح الموظفين فهماً لما يعتبر نشاطاً مريباً أو سلوكاً غير عادي، ولكيفية الإبلاغ عنه، يمكن أن يشكل أداة مفيدة.

ينبغي تقديم دورات التدريب على الكشف عن السلوك لمجموعة واسعة من العاملين، بمن فيهم على سبيل المثال لا الحصر، المشاركون في إصدار التصاريح، وفي التحريات الشخصية، والكشف الأمني. ومع ذلك، يمكن أن يستفيد جميع الموظفين من هذا النوع من التدريب كجزء من التدريب على الوعي بالأمن العام

ثقافة الأمن [5]

ثقافة أمنية متينة وفعالة: يعتبر ترسيخ ثقافة أمنية إيجابية في جميع أنحاء قطاع الطيران أساسياً للتخفيف من التهديدات من الداخل وتحقيق نتائج أمنية فعالة وقوية. وقد يكون الموظفون:

- مدفوعين ومطلعين على المخاطر من الداخل من خلال إحاطات إعلامية منتظمة بشأن التهديدات والمسائل الأمنية الأوسع نطاقاً؛
- ومدربين على تحديد أنماط السلوك الشاذ أو المريب والإبلاغ عنها؛
- ومصدراً قيّماً للمعلومات بشأن مواطن الضعف وكيفية التصدي لها

[4] الكشف عن السلوك هو عبارة عن تطبيق تقنيات تشمل الاعتراف بالخصائص السلوكية، بما في ذلك على سبيل المثال لا الحصر الإشارات الفيزيولوجية أو الإيحائية التي تدل على سلوك شاذ (مجموعة من الإشارات الشفوية وغير الشفوية) لتحديد هوية الأشخاص الذين لديهم النية المحتملة لارتكاب فعل تدخل غير مشروع.

[5] يمكن الاطلاع على مزيد من المعلومات عن ثقافة الأمن (بما في ذلك مصادر ثقافة الأمن) في الموقع الشبكي لثقافة الأمن في الإيكاو على العنوان www.icao.int/Security/Security-Culture/

القيادة والاستراتيجية

القيادة القوية: من الأهمية بمكان أن يدرك القادة دورهم في إبداء أفعال وأنماط سلوك أمنية إيجابية متوقعة من القوة العاملة لديهم. وينبغي التشجيع على التواصل المفتوح بين الموظفين والإدارة وأن يكون لدى القادة فهم للضغوط اليومية التشغيلية التي تمارس على القوة العاملة والمخاطر من الداخل التي قد تشكلها تلك الضغوط.

ومن شأن المسؤول التنفيذي (مثلاً مدير رفيع المستوى)، الذي يتولى زمام أمور مبادئ المخاطر الأمنية، وينفذ نهجاً تنازلياً إزاء السياسات الأمنية، ويجسّد أنماط السلوك المتوقعة، أن يرجّح تعزيز نهج أكثر امتثالاً واتساقاً عبر المؤسسة، ما يساعد أكثر على التخفيف من التهديدات من الداخل

الاستراتيجية: يوصى باعتماد استراتيجية (تؤيدها القيادة) لتخفيف التهديدات من الداخل من أجل مساعدة الموظفين على فهم كيفية التعرف على أنماط السلوك المريب داخل مكان العمل وكيفية الإبلاغ عنها.

وقد تشمل الاستراتيجية أيضاً السياسات الداخلية والمبادئ التوجيهية والإجراءات المتعلقة بالموظفين. وهذه تشمل إجراءات يتعين اتخاذها قبل التوظيف وطوال المدة التي يقضيها الموظف في المؤسسة. وينبغي استعراض الاستراتيجية والسياسات المرتبطة بها بانتظام مع جميع الجهات المعنية الرئيسية.

يمكن أن تعتبر الوثائق الإطارية[6] والكتيّبات والمواد الإرشادية بمثابة أدوات مفيدة إضافية

[6] مثلاً www.cpni.gov.uk/insider-risks/insider-risk-mitigation-framework

العوامل البشرية

الأداء البشري والعوامل البشرية: يجب أن يكون لدى المؤسسات فهم للكيفية التي يمكن بها للأداء البشري أن يساعد على التخفيف من التهديدات من الداخل. ويشمل ذلك أن نكون على علم بالكيفية التي يمكن أن تؤثر بها العوامل البشرية على الأفراد، الذين قد يستخدمون عن قصد أو عن غير قصد قدرتهم الفريدة على الوصول الى المعلومات لإحداث فعل تدخل غير مشروع. وينبغي على القادة والإدارة العليا القيام بما يلي:

- تطوير فهم للقدرات البشرية وكيف يمكنها أن تساعد على التخفيف من مخاطر الأنشطة من الداخل؛
- وفهم القيود البشرية وكيف يمكن تكييفها لضمان عدم تأثر الأداء بها؛
- وتسهيل الأمور على الموظفين للإبلاغ عن الشواغل الأمنية وأنماط السلوك المريبة؛
- وفهم الصلة بين العوامل البشرية وثقافة الأمن والتحفيز؛
- وضمان توافر الموارد اللازمة للموظفين؛
- وضمان تمكّن الموظفين المشرفين من تحديد علامات التوتر والإرهاق من أجل التعامل معها على الفور؛
- وتفادي التهاون في الأنشطة اليومية.

التكنولوجيات المتقدمة [7]

الكشف عن آثار المتفجرات (ETD): يمكن أن يضيف استخدام كاشفات آثار المتفجرات طبقة إضافية من الإجراءات القياسية للكشف الأمني للأشخاص غير الركاب و/أو الإجراءات الأمنية المضادة العشوائية وغير المتوقعة التي تستخدم في جميع أنحاء المنطقة المقيدة، ما يساعد بالتالي على التخفيف من التهديدات من الداخل.

[7] يمكن ان يساعد تطبيق التكنولوجيات المتقدمة على التخفيف من خطر العناصر من الداخل عن طريق زيادة معايير الكشف خلال عملية الكشف الأمني و/أو إضافة طبقات من الأمن فوق خط الأساس الأمني عند تطبيقه بطريقة عشوائية وغير متوقعة في جميع أنحاء بيئة المطار

كلاب الكشف عن الأجهزة المتفجرة: يمكن أن تخدم فرق كلاب الكشف عن الأجهزة المتفجرة في أغراض عديدة من قبيل: الكشف الأمني في جميع مناطق المطار (المنطقة المفتوحة للجمهور، منطقة التحركات الجوية، الركاب، الأشخاص غير الركاب، الأمتعة، البضائع، إلخ)، ومسح المناطق الأمنية المقيدة، وتوفير الوسائل اللازمة لتنفيذ تدابير أمنية عشوائية وغير متوقعة .

الذكاء الاصطناعي (AI): يمكن أن يساعد استخدام موظفين مدربين على نظم الذكاء الاصطناعي في تحديد الاتجاهات والأنشطة غير العادية. مثلاً، يمكن أن تساعد الحلول الحديثة لإدارة الوقائع في تحديد الوقائع والتمييز بين الأحداث العادية والتهديدات الوشيكة الحدوث، مثل محاولات اقتحام المناطق الأمنية.

—انتهى—