ICAO

SECURITY AND FACILITATION

تبادل المعلومات الإلكترونية

نُشر تحت سلطة الأمين العام

٢٠٢٤، الإصدار رقم ١

منظمة الطيران المدني الدولي

جدول المحتويات

الاختصارات

ANSP	مقدمو خدمات الملاحة الجوية
CAA	سلطة الطيران المدني
CERT	فريق الاستجابة لطوارئ أنظمة الكمبيوتر
CIShP	سياسة تبادل المعلومات الإلكترونية
CSIRT	فريق الاستجابة للحوادث الأمنية الإلكترونية
CTI	المعلومات التحليلية عن التهديدات الإلكترونية
FIRST	منتدى فرق الاستجابة للحوادث والأمن
ICAO	منظمة الطيران المدني الدولي
IoC	مؤشرات الاختراق
IPR	حقوق الملكية الفكرية
ISAC	مركز تبادل المعلومات وتحليلها
ISMS	نظام إدارة أمن المعلومات
IT	تكنولوجيا المعلومات
OSINF	المعلومات مفتوحة المصدر
OSINT	المعلومات التحليلية مفتوحة المصدر
SOC	مركز العمليات الأمنية
TLP	بروتوكول الإشارات الضوئية
TTP	الأساليب والتقنيات والإجراءات
UAS	نظام (نُظُم) الطائرات غير المأهولة

الموجز التنفيذي

تُظهر أفضل الممارسات المتبعة في مجالي السلامة الجوية وأمن الطيران أهمية تبادل المعلومات والدور الذي يؤديه ذلك في الحد من التهديدات والمخاطر التي يتعرض لها الطيران المدني. وبالمثل، فإن تبادل المعلومات الإلكترونية يتسم بالقدر ذاته من الأهمية.

يشكل تبادل المعلومات الإلكترونية أمراً بالغ الأهمية لإدارة المخاطر الإلكترونية في مجال الطيران المدني. فهو يعزز إرساء ثقافة قوية للأمن الإلكتروني تشجّع بدورها على التعاون والثقة. كما أنه يمكّن من الوعي بالأحوال والظروف المحيطة وإدارة المخاطر الإلكترونية، سواء التشغيلية والتكتيكية، والتخطيط الاستراتيجي.

وتقدم هذه الوثيقة إرشادات للدول والجهات المعنية في القطاع بشأن وضع خطة لتبادل المعلومات الإلكترونية، تشمل توصيات بشأن بلورة السياسات وتخصيص الموارد واتخاذ الخطوات العملية نحو تنفيذ ممارسات التبادل وتحسينها بشكل مستمر.

وتورد الوثيقة أيضاً وصفاً للمتطلبات المسبقة لتبادل المعلومات الإلكترونية في صناعة الطيران. وتسرد أنواعاً مختلفةً من المعلومات الإلكترونية التي يمكن تبادلها. كما تورد أيضاً مناقشةً لجوانب التحليل والضمانات فيما يخص تبادل المعلومات الإلكترونية، مع التأكيد على ضرورة تقييم مستوى الثقة في المصدر ومصداقية المعلومات.

تحلّ هذه الوثيقة محل إرشادات منظمة الطيران المدني الدولي – الإيكاو (ICAO) المنشورة سابقاً حول استخدام بروتوكول الإشارات الضوئية (TLP) في الطيران المدني. وهي توفر قواعد لتبادل المعلومات الإلكترونية في صناعة الطيران استناداً إلى النسخة الأحدث من قاعدة بروتوكول الإشارات الضوئية ونوع المعلومات التي يتم تبادلها وتاريخ/وقت تبادل المعلومات والجهات المتلقية (مثل الوكالات الحكومية والمشغلين ومقدمي الخدمات).

بشكل عام، تسلط الوثيقة الضوء على أهمية تبادل أنواع مختلفة من المعلومات الإلكترونية في قطاع الطيران المدني مع مراعاة التحليل والضمانات وتصنيف المعلومات بواسطة العلامات المناسبة لتعميم المعلومات بشكل فعّال على الجهات المعنية.

وتتماشى هذه الإرشادات مع استراتيجية الإيكاو للأمن الإلكتروني في الطيران[1] وخطة عمل الأمن الإلكتروني[2] المرتبطة بها، وهي تلبي الحاجة إلى تبادل المعلومات الإلكترونية. وتتماشى المعلومات الواردة في هذه الوثيقة مع المبادئ العامة لتوجيهات الإيكاو بشأن تبادل معلومات ذات الصلة بالسلامة الجوية وأمن الطيران، الواردة في وثيقتي "دليل أمن الطيران" (Doc 8973 – مقيدة التوزيع) و"دليل إدارة السلامة" (Doc 9859).

[1] https://www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx
[2] https://www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx

التعاريف

الضمان. الإجراءات المقررة والمنهجية اللازمة لتوفير الثقة الكافية بأن المنتج أو العملية تفي باشتراطات معينة.

وسيلة إيصال الهجوم. وسيلة الوصول التي يستخدمها المهاجم لبدء الهجوم.

التحقق من الصحة. تدابير للتحقق من الادعاء المتعلق بهوية فرد أو مستخدم أو برنامج أو عملية أو نظام أو جهاز.

التوافر. الإتاحة للوصول أو الاستخدام عند الطلب من قبل فرد مأذون له أو مستخدم أو برنامج أو عملية أو نظام أو جهاز.

الأمن الإلكتروني في مجال الطيران. مجموعة التقنيات والضوابط والتدابير والعمليات والإجراءات والممارسات المصممة لضمان السرية والسلامة والتوافر والحماية الشاملة وقدرة الأصول الإلكترونية على التصدي للهجوم و/أو التلف و/أو التدمير و/أو التعطيل و/أو الوصول غير المأذون به و/أو الاستغلال.

السرية. خاصية عدم إتاحة أي أصل من الأصول أو الكشف عنه لفرد أو مستخدم أو برنامج أو عملية أو نظام أو جهاز غير مأذون له.

أصل إلكتروني. البنود الرقمية والمادية التي لها قيمة من حيث الأعمال والعمليات والسلامة الجوية وأمن الطيران والكفاءة و/أو السعة، مثل الأنظمة والمعلومات والبيانات والشبكات والأجهزة والبرامج والمعدات والعمليات والبرامج الثابتة والموظفين المختصين/ المعتمدين والموارد الإلكترونية الأخرى.

هجوم إلكتروني. الاستخدام المتعمد للوسائل الإلكترونية لتعطيل الأصول الإلكترونية أو تغييرها أو تدميرها أو الوصول إليها دون إذن.

حدث إلكتروني. أي حدث يمكن ملاحظته في شبكةٍ أو نظام.

واقعة إلكترونية. حدث أو سلسلة أحداث إلكترونية تؤثر سلباً على السلامة الجوية وأمن الطيران وكفاءته و/أو سعته.

تخفيف المخاطر الإلكترونية. مجموعة (أو واحد) من ضوابط الأمن التي تهدف إلى تقليل المخاطر الإلكترونية المرتبطة بتهديد أو موطن ضعف إلكتروني معين، مع مراعاة تأثيرها على السلامة الجوية وأمن الطيران وكفاءته و/أو سعته.

قدرة الشبكة الإلكترونية على الصمود. قدرة الأصول الإلكترونية على الحفاظ على الوظائف الحيوية في ظل ظروف معاكسة أو ضغوط، والتعافي من تلك الظروف المعاكسة.

المخاطر الإلكترونية. احتمال حدوث نتائج غير مرغوب فيها ناجمة عن وقوع حدث إلكتروني.

تقييم المخاطر الإلكترونية. عملية مستمرة تقوم على تحديد المخاطر الإلكترونية وتحليلها وتقييمها.

إدارة المخاطر الإلكترونية. العملية المستمرة القائمة على تحديد التهديدات والمخاطر الإلكترونية والتخفيف من حدتها ومعالجتها ورصدها، وفقاً لتقييم المخاطر.

التهديد الإلكتروني. أي حدث إلكتروني محتمل يمكن أن يؤثر سلباً على السلامة الجوية وأمن الطيران وكفاءته و/أو سعته.

أمن المعلومات. الحفاظ على سرية المعلومات وسلامتها وتوافرها.

تبادل المعلومات. العملية التي يُقدم خلالها أحد الكيانات المعلومات إلى كيان آخر واحداً كان أو أكثر لتسهيل اتخاذ القرارات القائمة على التحسب للمخاطر ولتعزيز أفضل الممارسات.

السلامة. خاصية دقة الأصل واكتماله والتي تؤكد ماهية هذا الأصل.

الشدة. مؤشر نوعي لحجم التأثير السلبي الناتج عن تهديد ما.

الجهة الفاعلة للتهديد. الكيان الذي يكون مسؤولاً، بشكل جزئي أو كامل، عن أي واقعة تؤثر أو يحتمل أن تؤثر على أي مؤسسة أو نظام.

١ – المقدمة

١-١ الأسباب الداعية إلى تبادل المعلومات الإلكترونية

يشمل تبادل المعلومات عنصراً بالغ الأهمية لدعم إدارة المخاطر الإلكترونية في مجال الطيران. في عالم اليوم المترابط بعضه ببعض، تشكل التهديدات الإلكترونية مخاطر كبيرة على قطاع الطيران المدني. ويمكن للهجمات الإلكترونية أن تستهدف أي جانب من جوانب منظومة الطيران، من أنظمة إدارة الحركة الجوية إلى أنظمة بيانات الركاب، مما قد يؤدي إلى تعطيل العمليات التشغيلية وربما تعريض سلامة الركاب وأمنهم للخطر. ولذلك، تتطلب الإدارة الفعالة للمخاطر الإلكترونية نهجاً تعاونياً ينطوي على تبادل المعلومات بين الجهات المعنية.

تؤكد الدروس المستفادة من السلامة الجوية وأمن الطيران على أن ثقافة تبادل المعلومات سيقلل إلى حد كبير من المخاطر التي يتعرض لها الطيران المدني من قبل الجهات الفاعلة الخبيثة. في قطاع الطيران، ثبت أن تبادل المعلومات يشكل أداةً قيّمةً في إدارة المخاطر التي تهدد سلامة وأمن الطيران. وينطبق المبدأ نفسه على الأمن الإلكتروني للطيران. فمن خلال تبادل المعلومات الإلكترونية، يمكن للأطراف المعنية اكتساب فهم أفضل للتهديدات الإلكترونية التي تواجهها، وتحديد مواطن الضعف، واتخاذ التدابير المناسبة لمنع الهجمات الإلكترونية ضد الطيران المدني أو التخفيف من حدتها.

يُعدّ تبادل المعلومات أيضاً جانباً أساسياً من جوانب إرساء ثقافة قوية للأمن الإلكتروني. فوجود ثقافة قوية للأمن الإلكتروني يسهل التعرّف بشكل فعّال على التهديدات الإلكترونية والتصدي لها. ويُعد تبادل المعلومات جزءاً لا يتجزأ من هذه الثقافة لأنه يعزز الشفافية والتعاون والثقة بين الجهات المعنية. ويضمن التبادل الفعّالة للمعلومات الإلكترونية حصول جميع الجهات المعنية على البيانات اللازمة لاتخاذ القرارات المستنيرة وتقرير الإجراءات المناسبة والتخفيف من حدّة التهديدات الإلكترونية و/أو التصدي للحوادث الإلكترونية والتعافي منها.

لا تقتصر المعلومات الإلكترونية على المعلومات العملية ذات الصلة بالمسائل الإلكترونية تحديداً، بل تشمل أي نوع من المعلومات التحليلية ذات التأثير المحتمل على المخاطر الإلكترونية على الطيران المدني. ولا يقتصر تبادل المعلومات الإلكترونية على المعلومات التحليلية الخاصة بالمسائل الإلكترونية. فهي تشمل أي معلومات هامة من شأنها أن تساهم في تحديد المخاطر الإلكترونية في قطاع الطيران المدني والتخفيف من حدتها. على سبيل المثال، يمكن للمعلومات المتعلقة بالاختراقات الأمنية المادية أو التهديدات الداخلية أو السياق الجغرافي السياسي أو مواطن الضعف في التكنولوجيا أو في سلاسل التوريد أن تساعد الجهات المعنية على فهم التهديدات والمخاطر الإلكترونية والتخفيف من حدّتها بشكل أفضل.

ومن شأن تبادل المعلومات الإلكترونية أن يسهّل ما يلي:

- **التخطيط الاستراتيجي** بهدف بناء قدرات الأمن الإلكتروني في قطاع الطيران. فمن خلال تبادل المعلومات، يمكن للجهات المعنية تحديد الثغرات في قدرات الأمن الإلكتروني لديها ووضع الاستراتيجيات المناسبة لتحسين مرونتها في التصدي للمخاطر الإلكترونية. ويضمن التخطيط الاستراتيجي أن يظل قطاع الطيران يتمتع بالحماية والمرونة في مواجهة التهديدات الإلكترونية، كما يضمن أن تكون الجهات المعنية مستعدة للتصدي للحوادث الإلكترونية المحتملة والتعافي منها.
- **الوعي بالأحوال والظروف المحيطة** في كل من العمليات اليومية وأثناء وقوع حادث إلكتروني. ومن خلال تبادل المعلومات الإلكترونية، يمكن للأطراف المعنية اكتساب فهم أفضل لوضع الأمن الإلكتروني لديها، والمشهد العام للتهديدات الإلكترونية، ومواطن الضعف المحتملة في أنظمتها. ومن شأن ذلك أن يُمكّن الجهات المعنية من تحديد المخاطر المحتملة واتخاذ التدابير المناسبة لمنع وقوع الحوادث الإلكترونية أو التخفيف من أثرها.
- **الإدارة التشغيلية والتكتيكية للمخاطر الإلكترونية** تحسباً للتهديد الإلكتروني وللتصدي له. من خلال تبادل المعلومات، يمكن للجهات المعنية تحديد التهديدات الإلكترونية ووضع استراتيجيات مناسبة لإدارة المخاطر.
- **إدارة الأزمات** أثناء وقوع حادث إلكتروني، حيث أن التبادل الفعّال للمعلومات يمكّن الجهات المعنية من تنسيق استجابتها واتخاذ التدابير المناسبة للتخفيف من أثر الحادث.

من الضروري الإقرار بأن التبادل الفعّال للمعلومات يقوم على الثقة بين المشاركين. وتهدف هذه الإرشادات إلى دعم بناء الثقة المطلوبة لتشجيع مجموعة من المشاركين على التغلب على ترددهم الطبيعي عند تبادل المعلومات. ويتضمن ذلك وضع مجموعة من القواعد والإجراءات المشتركة التي تفهمها كل الأطراف داخل مجموعة التبادل وتتفق عليها وتلتزم بها. والتوصل إلى توافق في الآراء حول ماهية المعلومات الإلكترونية التي سيتم تبادلها وكيفية تبادلها وطرق توزيعها سيسهل من تبادل المعلومات بشكل فعّال بين المشاركين.

تمثل هذه الإرشادات استكمالاً للعمل الموسّع الذي قامت به الإيكاو فيما يخص الأمن الإلكتروني في الطيران. وهي تدعم الركيزة ٥ "تبادل المعلومات" الواردة في استراتيجية الإيكاو للأمن الإلكتروني في الطيران، والبند ٥-١ في خطة عمل الأمن الإلكتروني، الذي يطلب من الإيكاو وضع إرشادات بشأن تبادل المعلومات الإلكترونية.

ويُعتبر محتوى هذه الوثيقة مُكمّلاً للمواد الإرشادية المستقلة التي نشرتها الإيكاو سابقاً بشأن استخدام بروتوكول الإشارات الضوئية في الطيران المدني، ويحلّ محلها. كما تتضمن الوثيقة أيضاً إرشادات بشأن استخدام الإصدار ٢ المحدّث من قاعدة بروتوكول إشارات المرور الضوئية[٣]، التي وضعها منتدى فرق الاستجابة للحوادث والأمن (FIRST)، كوسيلة لتبادل المعلومات الإلكترونية في الطيران المدني.

١-٢ سياق تبادل المعلومات الإلكترونية

قبل التطرق إلى تبادل المعلومات الإلكترونية، من الضروري أولاً شرح دورة حياة المعلومات التحليلية الإلكترونية بشكل عام.

دورة حياة المعلومات التحليلية الإلكترونية هي عملية أساسية متكررة تُستخدم في مجال تحليل المعلومات. وتخدم كل خطوة في هذه الدورة غرضاً هاماً لضمان تحويل المعلومات من بيانات خام إلى معلومات تحليلية تحمل فائدةً بحيث تسهّل عملية صنع القرار وتعزز الأمن الإلكتروني وتدعم الأهداف الاستراتيجية التنظيمية المختلفة.

وتبادل المعلومات (ويُسمى أيضاً "تعميم المعلومات" في الشكل ١ أدناه) هو جزء من دورة حياة المعلومات التحليلية الإلكترونية التي تشمل الخطوات التالية:

١- **التخطيط والتوجيه:** الخطوة الأولى في جمع المعلومات الإلكترونية وتحليلها تتمثل في تخطيط وتوجيه العملية. ويتضمن ذلك تحديد الأهداف المتوخاة من جهود جمع المعلومات وتحليلها، وتحديد نطاقها وحجمها، وتحديد الجهات المعنية التي يجب إشراكها في العملية. كما يتضمن التخطيط والتوجيه أيضاً وضع السياسات والإجراءات اللازمة لجمع المعلومات وتحليلها، بالإضافة إلى تحديد أدوار ومسؤوليات المشاركين في الخطوات المختلفة.

٢- **الجمع:** الخطوة الثانية هي الجمع الفعلي للمعلومات الإلكترونية. ويتضمن ذلك جمع البيانات من مصادر مختلفة (انظر القسم ٣). ويمكن أن تتم عملية الجمع إما يدوياً أو من خلال عمليات آلية. ومن الضروري التأكد من أن البيانات التي يتم جمعها ذات صلة بالموضوع ودقيقة وسليمة من حيث التوقيت.

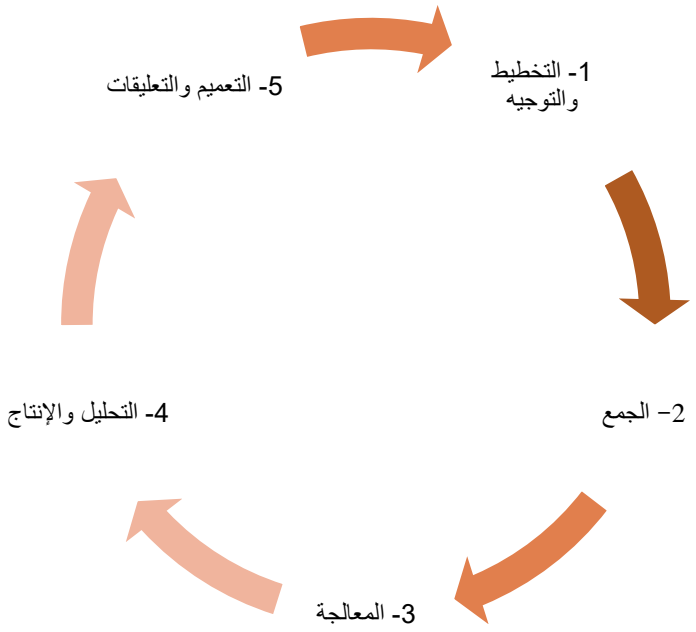
٣- **المعالجة:** الخطوة الثالثة هي معالجة المعلومات التي تم جمعها. ويتضمن ذلك تحويل البيانات التي تم جمعها إلى صيغة قابلة للاستخدام وتحليلها وتحديد ما يظهر فيها من أنماط أو أوجه خلل، مما قد يشير إلى وجود تهديد إلكتروني، على سبيل المثال. ويمكن أن تتضمن هذه الخطوة استخدام أدوات معالجة البيانات والخوارزميات وتقنيات التحليل الأخرى للمساعدة في تحديد التهديدات أو نقاط الضعف الإلكترونية المحتملة مثلاً. وتتضمن المعالجة أيضاً تحديد أهمية المعلومات وإلى أي مدى تُعتبر عاجلة وتحديد أولويات الاستجابة وفقاً لذلك.

٤- **التحليل والإنتاج:** الخطوة الرابعة هي تحليل المعلومات وإعداد التقارير بناءً على البيانات المعالجة. يتضمن ذلك تفسير البيانات، وتحديد الأنماط أو الاتجاهات، والإشارة إلى المخاطر الإلكترونية التي تهدد منظومة الطيران، على سبيل المثال. وقد يؤدي ذلك إلى رفض المعلومات إذا كانت جودة ومستوى التفاصيل فيها غير كافية لتحليلها. ويستخدم المحللون معارفهم وخبراتهم لفهم البيانات وإنتاج تقارير تحليلية تفيد الجمهور المستهدف وتتسم بالدقة وقابلية التنفيذ. وقد تشمل خطوة التحليل والإنتاج أيضاً وضع توصيات للتخفيف من حدّة التهديدات الإلكترونية أو منع وقوعها، على سبيل المثال.

[٣] https://www.first.org/tlp/

٥- **التعميم (تبادل المعلومات الإلكترونية) والآراء والتعليقات:** الخطوة الأخيرة هي تعميم التقارير التحليلية على الجهات المعنية. ويمكن أن يشمل ذلك تبادل المعلومات الإلكترونية مع الجهات المعنية الداخلية، مثل فرق تكنولوجيا المعلومات (IT) وفرق الأمن الإلكتروني و/أو فرق سلامة/أمن الطيران، وكذلك مع الجهات المعنية الخارجية، مثل منظمات الطيران الأخرى أو الوكالات بمختلف الدولة. ويتضمن التعميم ضمان إرسال المعلومات الإلكترونية في الوقت المناسب وبطريقة آمنة، وأن يكون لدى الجهات المعنية السياق والفهم اللازمين للتصرف بناءً عليها. ويساعد التعميم الفعّال على بناء ثقافة تبادل المعلومات الإلكترونية في قطاع الطيران المدني ويمكّن الجهات المعنية من اتخاذ الإجراءات المناسبة التي ربما تُمكّنها مثلاً من الوقاية من التهديدات الإلكترونية أو التخفيف من حدتها.

كما يتم جمع الآراء والتعليقات في هذه الخطوة لتقييم مدى فعالية وأهمية دورة حياة المعلومات الإلكترونية بهدف تحسينها عند تكرار العملية في المستقبل.



الشكل ١- دورة حياة المعلومات التحليلية الإلكترونية

٢ سياسات تبادل المعلومات الإلكترونية (CIShP)

يقدم هذا القسم إرشادات حول كيفية وضع وتنفيذ سياسة لتبادل المعلومات الإلكترونية على المستوى التنظيمي (أي مثلاً بين الجهات المعنية في مجال الطيران).

كما يمكن للدول استخدام هذه الإرشادات لوضع خططها لتبادل المعلومات الإلكترونية. ومع ذلك، تجدر الإشارة إلى أن الخطط الوطنية لتبادل المعلومات الإلكترونية قد تكون شاملة لعدة قطاعات وليست مقتصرةً على الطيران.

٢-١ سياسات تبادل المعلومات الإلكترونية (CIShP)

ينبغي لسياسات تبادل المعلومات الإلكترونية أن تحدد ما يلي:

- سبب تبادل المعلومات الإلكترونية؛
- نطاق التطبيق والسياق العام والقيود (أي مثلاً مصادر المعلومات الإلكترونية والقيود المتعلقة بحقوق الملكية الفكرية وقوانين الخصوصية)؛
- الأعضاء في مجموعة تبادل المعلومات الإلكترونية داخل المؤسسة ومسؤوليات كل منهم؛
- قواعد التوزيع (بما في ذلك التوزيع الإضافي[٤]) للمعلومات الإلكترونية داخل المؤسسة وخارجها، استناداً إلى قواعد تصنيف/تحديد فئات المعلومات ومراعاة المتطلبات التنظيمية والقانونية المطبقة؛
- الإجراءات التنفيذية:
  - جمع المعلومات؛
  - حجب الهوية، إذا لزم الأمر؛
  - التحقق من صحة المحتوى؛
  - التوزيع؛
- دورة مراجعة السياسة ومراقبة الوثائق (أي تسجيل التغييرات الهامة وإجراءات التحقق من الصحة).

وينبغي للمؤسسة أن تعتمد السياسة كجزء من نظام إدارة أمن المعلومات (ISMS)[٥] لديها. وينبغي أن تتم مراجعتها بشكل دوري (سنوياً مثلاً)، بعد أي تغيير ملموس في السياسة، أو عقب أي حادث إلكتروني لاستخلاص الدروس المستفادة.

٢-٢ المتطلبات التنظيمية والتعاقدية[٦]

ينبغي أن تمتثل سياسة تبادل المعلومات الإلكترونية لجميع اللوائح السارية والاتفاقيات القائمة المتعلقة بتبادل المعلومات الإلكترونية مثل:

- اللوائح الوطنية و/أو الإقليمية و/أو الدولية الشاملة لعدة قطاعات.
- اللوائح الوطنية و/أو الإقليمية و/أو الدولية الخاصة بالطيران.

---

[٤] يتناول القسم ٥ في هذه الوثيقة موضوع التبادل الإضافي للمعلومات.

[٥] ISO 27001, chapter A.5.14 Information transfer

[٦] يمكن الاطلاع على مزيد من المعلومات (المتشعبة بين الأقسام) من خلال:
NIST.SP.800-150 – Guide to cyber threat information sharing
ENISA Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches
https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

- الاتفاقات المبرمة مع المراكز الوطنية و/أو الدولية لتبادل المعلومات وتحليلها (ISACs) وفرق الاستجابة لطوارئ أنظمة الكمبيوتر/فرق الاستجابة للحوادث الأمنية الإلكترونية (CERTs/CSIRTs)، (مثل مركز تبادل المعلومات وتحليلها في مجال الطيران، والفريق الأوروبي للاستجابة لطوارئ أنظمة الكمبيوتر في إدارة الحركة الجوية (EATM-CERT)، والفرق الوطنية للاستجابة لطوارئ أنظمة الكمبيوتر/الفرق الوطنية للاستجابة للحوادث الأمنية الإلكترونية (CERTs/CSIRTs) في كل دولة.

٢-٣ الموارد

ينبغي على المؤسسة تحديد الموارد اللازمة لضمان التنفيذ السليم لسياسة تبادل المعلومات الإلكترونية، بما في ذلك ما يلي:

- الموارد البشرية: الاستفادة من فرق الأمن الإلكتروني الحالية مثل فريق مركز العمليات الأمنية (SOC) وتوظيف أشخاص جدد حسب الضرورة؛
- الموارد الفنية: الموقع الإلكتروني والبريد الإلكتروني والهاتف والرسائل النصية بالإضافة إلى منصات التبادل الآمنة و/أو الموثوق بها؛
- الموارد المالية: التكاليف المتعلقة بشراء و/أو تطوير الأنظمة، وتدريب الموارد البشرية، وما إلى ذلك.

٢-٤ التنفيذ

يتضمن تنفيذ سياسة تبادل المعلومات الإلكترونية المراحل التالية:

- تحديد النطاق: تحديد مصادر المعلومات وماهية المعلومات الإلكترونية التي سيتم تبادلها من خلال سياسة تبادل المعلومات الإلكترونية؛
- تحديد الأدوات التي سيتم استخدامها لتبادل المعلومات الإلكترونية؛
- تحديد نقطة الاتصال (POC) في شبكة تبادل المعلومات الإلكترونية وتطوير عمليات لتحديث معلومات نقطة الاتصال؛
- اختبار أنظمة وعمليات تبادل المعلومات الإلكترونية وتعديلها حسب الحاجة؛
- إطلاق نظام لتبادل المعلومات الإلكترونية (بدء التشغيل)؛
- الرصد والمراقبة بصفة مستمرة؛
- المراجعة والتحسين بصفة مستمرة.

٣ إدارة المعلومات الإلكترونية وتبادلها

٣-١ أنواع المعلومات الإلكترونية

من الممكن تبادل المعلومات الإلكترونية التالية.

المعلومات التحليلية الإلكترونية

- **المعلومات التحليلية عن التهديدات الإلكترونية (CTI):** وتشمل المشهد العام للتهديدات الإلكترونية، والمعلومات التحليلية عن العمليات المحبة للمخترقين (الهاكرز)، وما إلى ذلك.

  - **على المستوى الاستراتيجي:** تساعد المعلومات الاستراتيجية المؤسسة على فهم نوع التهديدات الإلكترونية وقدرات ودوافع المهاجمين.
    - تسهل رسم صورة مكتملة عن نوايا وقدرات التهديدات الإلكترونية الخبيثة.
    - تغذي عمليات صنع القرار بالمعلومات و/أو توفر تحذيرات مبكرة.
    - يمكن أن تشمل الاتجاهات (مثل الأهداف، وسلوكيات المهاجمين)، والإحصاءات، والمعلومات المتعلقة بالتهديدات الإلكترونية (مثل التهديدات المستمرة المتقدمة (APTs)، وتقارير الحوادث الإلكترونية، ووثائق السياسات، والورقات البيضاء/الورقات البحثية)، وما إلى ذلك.
    - مثال على المعلومات التحليلية عن التهديدات الإلكترونية على المستوى الاستراتيجي: تقرير شامل عن التهديدات الإلكترونية الناشئة التي تحدق بالبنية التحتية الحيوية في دولة ما، بحيث يحدد مواطن الضعف المحتملة ووسيلة إيصال الهجوم. وعادةً ما يستخدم هذا التقرير صانعو القرار رفيعو المستوى لصياغة سياسات واستراتيجيات الأمن الإلكتروني طويلة الأجل.
  - **على المستوى التشغيلي:**
    - تطرح سياقاً للحوادث الإلكترونية، مما يمكّن المدافعين من تحديد أي مخاطر محتملة.
    - تسمح بتحديد التأثيرات المحتملة للحوادث الإلكترونية على العمليات (مثل الأساليب والتقنيات والإجراءات (TTPs) والدوافع والتأثير والتوقيت).
    - تساعد على تخصيص الموارد وتحديد أولويات المهام.
    - مثال على المعلومات التحليلية عن التهديدات الإلكترونية على المستوى التشغيلي: معلومات عن حملة تصيّد احتيالي جارية تستهدف الطيران. ويتضمن ذلك تفاصيل مثل الأساليب والتقنيات والإجراءات المستخدمة من قبل الجهات الفاعلة في التهديد. وتُعتبر هذه المعلومات ذات قيمة لفرق العمليات الأمنية بهدف الكشف عن التهديدات الإلكترونية الفورية والتصدي لها.
  - **على المستوى التكتيكي:** المعلومات التحليلية التي تستخدمها المؤسسات للمساعدة بشكل استباقي في أن تتبوّأ وضعاً أمنياً يمكّنها من الصمود في وجه الهجمات (مثل مؤشرات الاختراق (IoCs)، والأساليب والتقنيات والإجراءات، ومواطن الضعف).
    - مثال على المعلومات التحليلية عن التهديدات الإلكترونية على المستوى التكتيكي: مؤشرات الاختراق المتعلقة بنوع معين من البرمجيات الخبيثة. يتضمن ذلك عناوين بروتوكول الإنترنت المحددة، وتجزئة الملفات، وأنماط السلوك المرتبطة بالبرمجيات الخبيثة. وتُستخدم هذه المعلومات التكتيكية من قبل محللي الأمن الإلكتروني في الخطوط الأمامية لتحديد التهديدات الإلكترونية والتخفيف من حدّتها في الوقت الفعلي.

- **مؤشرات الاختراق (IoCs):** مؤشرات الاختراق هي على سبيل المثال عناوين بروتوكول الإنترنت الخبيثة، أو عناوين URL خبيثة، أو أسماء النطاقات الخبيثة أو تجزئة الملفات الخبيثة.
  - تبادل هذه المعلومات سيساعد الأطراف المتلقية على حماية أنظمتها/خدماتها بشكل أفضل.
  - عند تبادل مؤشرات الاختراق، لا حاجة للإفصاح عن الجهة التي اكتشفتها.
- **الأساليب والتقنيات والإجراءات (TTPs):** هي سيناريوهات للهجمات والأساليب المفضلة التي يستخدمها المخترقون.[٧]
- **مواطن الضعف:**
  - **كمستخدم لأحد الأصول الإلكترونية:** المعلومات الإلكترونية التي يمكن تبادلها تتعلق في المقام الأول بالأصول الإلكترونية (مثل الأجهزة والبرمجيات والخدمات والبروتوكول والمعايير) التي تم العثور على الثغرة الأمنية فيها. ولن يكون من المفيد تبادل المعلومات المتعلقة بهوية مستخدم هذه الأصول الإلكترونية.
    - يمكن تبادل هذه المعلومات مع الآخرين لمساعدتهم على حماية أنفسهم.
    - ليس هناك حاجة للإفصاح عن هوية من اكتشف الثغرة.
    - فيما يتعلق بالإفصاح المسؤول عن الثغرات، قد يقترح برنامج إدارة الثغرات في المؤسسة عمل "لوحة تكريم" أو عملية مماثلة للإشادة بمساهمات الباحثين في تحديد الثغرات.
  - **كمالك لأحد الأصول الإلكترونية:** ينبغي على مالك الأصول الإلكترونية إطلاع مستخدمي هذه الأصول على مواطن الضعف فيها.
    - ينبغي أيضاً على مالك الأصول الإلكترونية اقتراح تصحيح/إصلاح للثغرات.
    - تتضمن أفضل الممارسات الكشف عن مواطن الضعف هذه كي تطلع عليها فرق الاستجابة للطوارئ أنظمة الكمبيوتر/فرق الاستجابة للطوارئ الأمنية (الوطنية أو القطاعية) وذلك بقصد مساعدتها في الاستجابة لأي حوادث إلكترونية تتعلق بالأصول الإلكترونية المستخدمة.
  - يمكن النظر في الفَرْق بين الثغرات المحتملة والمؤكدة والمستغلة من حيث كيفية التعامل مع تبادل المعلومات المتعلقة بتلك الثغرات.

تقارير الحوادث الإلكترونية

- تحتوي على معلومات عن حادثة إلكترونية تؤثر على المؤسسة.
- ينبغي تضمين المعلومات التالية، قدر الإمكان، في تقارير الحوادث الإلكترونية: الملخص والنوع والتاريخ والوقت المحددين لوقوع الحادث وموقع وقوعه ومدته والتسلسل الزمني (أي تتابع الأحداث) ومؤشرات الاختراق والأساليب والتقنيات والإجراءات والسياق والثغرة (الثغرات) والآثار (على السلامة والأمن والكفاءة والقدرات والأعمال التجارية والمالية والسمعة) والخطورة والدافع والهدف والجهة الفاعلة للتهديد والخدمات والمنظمات المتضررة، وما إلى ذلك.
- كقاعدة عامة، كلما زادت المعلومات المقدمة، كان التقرير أكثر فائدةً من الناحية العملية.

[٧] قامت شركة MITRE ATT&CK بإعداد وتحديث تصنيفاً للأساليب والتقنيات والإجراءات يمكن الاطلاع عليه على الموقع الإلكتروني: https://attack.mitre.org/

التدابير الاحترازية الإلكترونية

- تحتوي على معلومات عن الطرق المستخدمة في الحالات التالية:
  - معالجة مواطن الضعف؛
  - التخفيف من التهديدات الإلكترونية؛
  - الاستجابة للحوادث الإلكترونية والتعافي منها.
- تشمل الأشكال الشائعة لهذه المعلومات برامج التصحيح لمعالجة الثغرات والتحديثات المضادة للفيروسات لوقف الأنشطة الاستغلالية والتوجيهات الرامية إلى تطهير الشبكات من الجهات الفاعلة الخبيثة.

الوعي بالظروف المحيطة

- تحتوي على معلومات تزوّد صانعي القرار بقياس في الوقت الحقيقي لمواطن الضعف المستغلة والتهديدات النشطة والهجمات الإلكترونية التي قد تكون مطلوبة للاستجابة لأي حادث إلكتروني.
- يمكن أن تحتوي أيضاً على معلومات عن أهداف الهجمات وحالة شبكات الكمبيوتر العامة أو الخاصة ذات الأهمية الحرجة.

أفضل الممارسات

- تحتوي على معلومات تتعلق بكيفية تطوير البرمجيات والخدمات وتقديمها، مثل الضوابط الأمنية وممارسات التطوير والاستجابة للحوادث وتصحيح البرمجيات أو مقاييس فعاليتها.

٢-٣ مرسلو المعلومات الإلكترونية ومتلقوها ومصادرها

- يتطلب تبادل المعلومات الإلكترونية مرسلاً ومتلقياً ومصدراً للمعلومات (إذا لم تكن المعلومات صادرة عن المُرسِل).
- يتضمن الجدول أدناه أمثلة على المرسلين والمتلقين ومصادر المعلومات الإلكترونية في الطيران المدني.

المرسلون/المستقبلون	• مستخدمو المجال الجوي (كشركات الطيران والطيران العام ومشغلي نُظُم الطائرات غير المأهولة (UAS)) • – مقدمو خدمات الملاحة الجوية (ANSP) • – مشغلو المطارات • – السلطات (كسلطة الطيران المدني (CAA)) • – مقدمو خدمات الطيران • – المصنّعون • – سلاسل التوريد في مجال الطيران وخارجه • – الجهات الأخرى

المصادر	• المرسلون/المتلقون، كما يرد أعلاه • المركبات الجوية (كنُظُم الطائرات غير المأهولة والطائرات) • جهات المعلومات التحليلية مفتوحة المصدر (OSINT) • جهات إعداد المعلومات التحليلية عن التهديدات الإلكترونية • الجمعيات والمنظمات الدولية (كرابطات شركات الطيران/المطارات/مقدمي خدمات الملاحة الجوية) • مراكز الأمن الإلكتروني في الطيران على المستويات الدولي/الوطني/الإقليمي، وفرق الاستجابة لطوارئ أنظمة الكمبيوتر/المراكز الدولية لتبادل المعلومات وتحليلها (CERTs/ISACs) • الجهات الأخرى

- يتضمن الملحق (أ) الشكل الذي يُوصى به لتدفق الأنواع المختلفة من المعلومات الإلكترونية التي يمكن تبادلها بين مختلف الجهات المعنية في الطيران.

٣-٣ التقييم والتحليل واستخدام بروتوكول الإشارات الضوئية لتصنيف المعلومات الإلكترونية التي يمكن تبادلها كمُرسِل

٣-٣-١ التقييم والتحليل

قبل تبادل المعلومات الإلكترونية، يجب على المُرسِل إجراء تحليل من أجل ما يلي:

- تقييم مدى مصداقية المصدر وموثوقيته (انظر الفقرة ٣-٣-١-١ والملحقين (ب) و(د))
- تحليل مدى معقولية/مقبولية المعلومات (انظر الفقرة ٣-٣-١-٢ والملحقين (ج) و(د))؛
- تحليل مدى أهمية المعلومات بالنسبة للمؤسسة، وأوساط تبادل المعلومات (المنظمة (المنظمات) المتلقية)، ومنظومة الطيران ككل.

وهذه الخطوة بالغة الأهمية في تبادل المعلومات الإلكترونية. فبدونها، تصبح المعلومات مجرد مجموعة من البيانات/الاستنتاجات التي تفتقر إلى سياق.

وعند إجراء التحليل أعلاه، من المهم تذكر ما يلي:

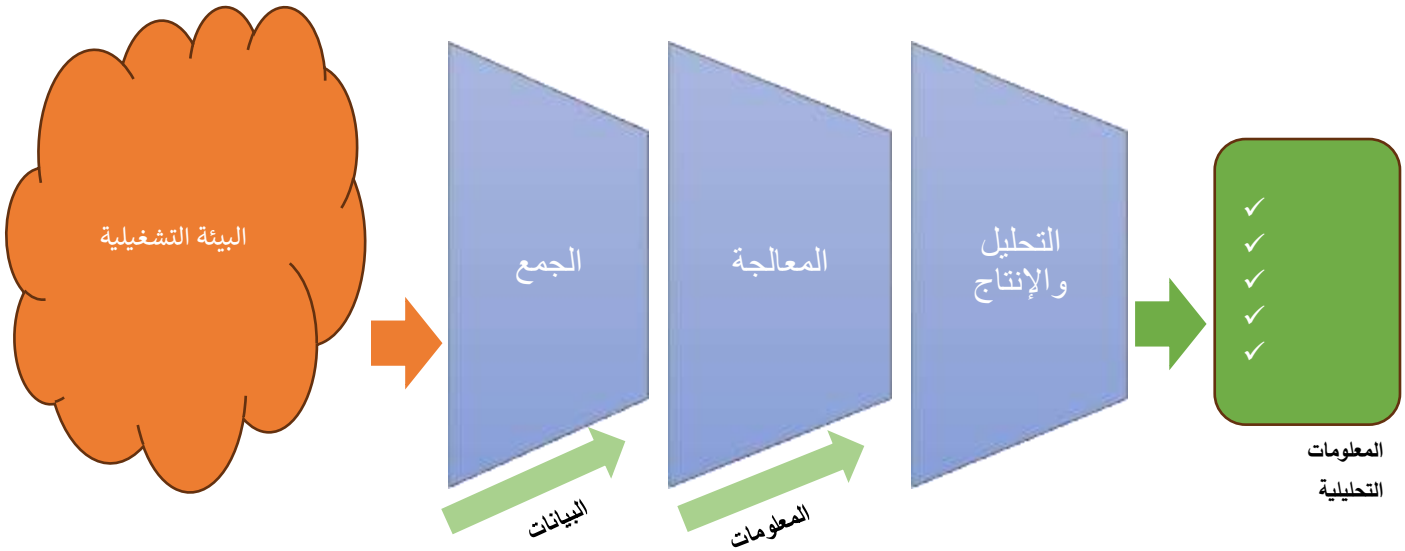
- تتطلب المشاكل التحليلية المختلفة مقاربات مختلفة؛
- ينبغي على المحللين أن يكونوا على دراية بتحيزاتهم الطبيعية، وأن يبذلوا أكبر جهد ممكن للتغلب عليها لإجراء تحليل موضوعي باستخدام الأساليب والأدوات المناسبة.

لتوضيح دور تقييم وتحليل المعلومات الإلكترونية، يوضح الشكلان ٢ و٣ أدناه الفرق بين المعلومات مفتوحة المصدر والمعلومات التحليلية مفتوحة المصدر، حيث يتضح أن قابلية الاستفادة من المعلومات تزداد بشكل كبير مع التحليل وتوفير الضمانات المناسبة قبل تعميمها.

- **المعلومات مفتوحة المصدر (OSINF)** حيث يتم تبادل المعلومات التي يتم جمعها كما هي.

الشكل ٢- المعلومات مفتوحة المصدر

- **المعلومات التحليلية مفتوحة المصدر (OSINT)** حيث تخضع المعلومات بعد جمعها إلى العملية المبينة أدناه.



الشكل ٣- إنتاج المعلومات التحليلية الإلكترونية[٨]

٣-٣-١-١ تقييم مدى مصداقية المصدر وموثوقيته

تقييم مستوى مصداقية وموثوقية مصدر المعلومات/المعلومات التحليلية الإلكترونية أمر بالغ الأهمية لاتخاذ قرارات مستنيرة.

يتضمن الملحق (ب) مثالاً على إطار عام لتحديد المعايير ويقترح نظاماً تقييمياً لقياس مدى مصداقية وموثوقية مصدر المعلومات/المعلومات التحليلية الإلكترونية.

ويمكن تعديل معاملات الترجيح ومقياس منح الدرجات المستخدم في الملحق (ب) وفقاً للمتطلبات المحددة للمؤسسة ومدى تحملها للمخاطر.

ويقدم الملحق (د) مثالاً آخر لنظام قياس الثقة في المعلومات لتقييم كل من موثوقية المصدر ومعقولية المعلومات (انظر الفقرة ٣-٣-١-٢ أدناه) باستخدام طريقة مختلفة: قانون الأميرالية (أو نظام الناتو).

وينبغي على المؤسسات المواظبة على إعادة تقييم درجات الثقة وتحديثها بانتظام مع تطور المشهد العام للتهديدات الإلكترونية ومصادر المعلومات التحليلية المتعلقة بالتهديدات مع مرور الوقت.

[٨] مأخوذة من Joint Publication 2-0, *Joint Intelligence* (2013)

٢-١-٣-٣ تحليل مدى معقولية/مقبولية المعلومات

من الضروري تقييم مستوى معقولية/مقبولية المعلومات/المعلومات التحليلية الإلكترونية.

يتضمن الملحق (ج) مثالاً على إطار لتحديد المعايير ويقترح نظاماً تقييمياً لقياس مدى مصداقية/مقبولية المعلومات/المعلومات التحليلية الإلكترونية.

يمكن تعديل معاملات الترجيح ومقياس منح الدرجات المستخدم في الملحق (ج) وفقاً للمتطلبات المحددة للمؤسسة ومدى تحملها للمخاطر.

وينبغي على المؤسسات المواظبة على إعادة تقييم درجات المصداقية/المقبولية وتحديثها بانتظام مع ظهور معلومات/معلومات تحليلية جديدة عن التهديدات الإلكترونية ومع تطور المشهد العام للتهديدات الإلكترونية مع مرور الوقت.

يقدم الملحق (د) مثالاً آخر لنظام قياس الثقة في المعلومات لتقييم كل من موثوقية المصدر (انظر الفقرة ٣-٣-١-٢ أدناه) ومعقولية المعلومات باستخدام طريقة مختلفة: قانون الأميرالية (أو نظام الناتو).

٢-٣-٣ تصنيف المعلومات بواسطة بروتوكول الإشارات الضوئية [٩] [١٠] (TLP):

١-٢-٣-٣ استخدام بروتوكول الإشارات الضوئية في الطيران

تشمل قاعدة بروتوكول الإشارات الضوئية خمس علامات: الأحمر (RED) والأصفر (AMBER) والأصفر + مقيد (AMBER+STRICT) والأخضر (GREEN) والمتاح (CLEAR).

نظراً لأن علامة **TLP:CLEAR** لا تقيّد تعميم المعلومات المتلقاة بالنسبة لأي شخص ومن خلال أي وسيلة، وبما أن علامة **TLP:RED** تُقصر الكشف عن المعلومات على المتلقي (المتلقين) المحددين دون السماح بأي توزيع آخر على الإطلاق، لا يتطرق هذا القسم إلى هاتين العلامتين. أما العلامات الثلاث التي تتطلب بعض التوضيح حول كيفية استخدامها في سياق الطيران فهي ما يلي:

- **TLP:GREEN**
- **TLP:AMBER**
- **TLP:AMBER+STRICT**

TLP:GREEN	- يمكن تبادل المعلومات التي تحمل العلامة TLP:GREEN داخل أوساط الطيران. - ويجوز لمتلقي المعلومات المصنفة TLP:GREEN توزيعها على أي منظمة في قطاع الطيران (سلطة الطيران المدني ومقدمي خدمات الطيران ومشغلي المطارات ومستخدمي المجال الجوي والمصنعين ومقدمي خدمات الطيران وغيرهم) . - كما يمكن تبادلها مع مؤسسات الأمن الإلكتروني التي لها دور في مجال الطيران (مراكز الأمن الإلكتروني الوطنية، وفرق الاستجابة لطوارئ أنظمة الكمبيوتر/فرق الاستجابة للحوادث

[٩] بروتوكول الإشارات الضوئية (TLP) هو معيار طوّره منتدى فرق الاستجابة للحوادث والأمن (FIRST) لتسهيل تبادل المعلومات مع الجمهور المناسب. تقدم هذه الوثيقة إرشادات بشأن استخدام الإصدار ٢ من قواعد TLP التي يمكن الاطلاع عليها على الرابط التالي: https://www.first.org/tlp/.

[١٠] تحل الإرشادات الواردة في هذه الوثيقة محل "إرشادات بروتوكول الإشارات الضوئية" التي نشرتها الإيكاو في عام ٢٠٢١.

	الأمنية الإلكترونية على المستويات الوطني/الإقليمي/الدولي، ومراكز تبادل المعلومات وتحليلها وغيرها). - ويجوز تبادلها مع المؤسسات غير المعنية بالطيران التي تستخدم تقنيات مماثلة (مثل المعلومات المتعلقة بالتقنيات التشغيلية أو تكنولوجيا المعلومات)، أو المؤسسات التي تواجهها تهديدات إلكترونية مماثلة أو تقدم خدمات للطيران (مثل أنظمة أو خدمات الاتصالات السلكية واللاسلكية، أو أنظمة أو خدمات الطاقة). يمكن أن تكون تلك المنظمات غير المعنية بالطيران جهات فاعلة في قطاعات أخرى (مثل المشغلين والسلطات والمصنعين) أو المنظمات ذات الصلة بالفضاء الإلكتروني (مراكز الأمن الإلكتروني الوطنية، وفرق الاستجابة لطوارئ أنظمة الكمبيوتر/فرق الاستجابة للحوادث الأمنية الإلكترونية في القطاعات الأخرى، ومراكز تبادل المعلومات وتحليلها في القطاعات الأخرى).
TLP:AMBER	- يجوز تبادل المعلومات ذات العلامة TLP:AMBER داخل مؤسسة المتلقي وعملائها، وذلك فقط **بقدر الحاجة إلى المعرفة**. - على الرغم من أن معنى المؤسسة واضح ومباشر، إلا أن معنى "العملاء" الذين لديهم **حاجة إلى المعرفة** في مجال الطيران يجب فهمه على النحو التالي: ○ يجوز لسلطات الطيران المدني تبادل هذا النوع من المعلومات ▪ داخل دولها مع: • الجهات الوطنية المعنية بالطيران؛ • المركز (المراكز) الوطنية للأمن الإلكتروني؛ • فرق الاستجابة لطوارئ أنظمة الكمبيوتر/فرق الاستجابة للحوادث الأمنية الإلكترونية ومراكز تبادل المعلومات وتحليلها بقطاع الطيران في الدولة. ▪ خارج دولها مع: • سلطات الطيران المدني الأخرى؛ • فرق الاستجابة لطوارئ أنظمة الكمبيوتر/فرق الاستجابة للحوادث الأمنية الإلكترونية ومراكز تبادل المعلومات وتحليلها بقطاع الطيران على المستويات الوطنية/الإقليمية/الدولية. ○ يجوز للجهات المعنية في مجال الطيران (كمقدمي خدمات الطيران ومشغلي المطارات ومستخدمي المجال الجوي ومقدمي خدمات الطيران) تبادل هذا النوع من المعلومات مع: ▪ سلطات الطيران المدني الوطنية في دولها؛ ▪ المؤسسات التي تسهل لها تقديم خدماتها؛

	▪ فرق الاستجابة لطوارئ أنظمة الكمبيوتر/فرق الاستجابة للحوادث الأمنية الإلكترونية ومراكز تبادل المعلومات وتحليلها بقطاع الطيران على المستويات الوطنية /الإقليمية/الدولية؛ ▪ عملائها باستثناء الركاب (مثل وكلاء السفر ومنافذ السوق الحرة). ○ يمكن للمُصنّعين تبادل هذا النوع من المعلومات مع: ▪ سلطات الطيران المدني الوطنية؛ ▪ عملائهم (مثل شركات الطيران والمطارات)؛ ▪ فرق الاستجابة لطوارئ أنظمة الكمبيوتر/فرق الاستجابة للحوادث الأمنية الإلكترونية ومراكز تبادل المعلومات وتحليلها بقطاع الطيران على المستويات الوطنية /الإقليمية/الدولية؛ ▪ مقاوليهم من الباطن.
TLP:AMBER+STRICT	- يمكن تبادل المعلومات ذات العلامة TLP:AMBER+STRICT داخل مؤسسة المتلقي، وذلك فقط **بقدر الحاجة إلى المعرفة**.

٣-٣-٢-٢ التصنيف الموصى به بواسطة بروتوكول الإشارات الضوئية لمختلف المعلومات الإلكترونية

يُوصى باستخدام الإرشادات التالية عند تصنيف المعلومات الإلكترونية لأغراض الطيران. وقد تؤدي بعض الاعتبارات إلى الانحراف عن التوصيات الواردة أدناه، بما في ذلك على سبيل المثال لا الحصر:

- قد يتطور التصنيف بواسطة بروتوكول الإشارات الضوئية بمرور الوقت: قد يتم تصنيف المعلومات الإلكترونية في الفئة الأكثر تقييداً عند تبادلها لأول مرة، ثم يتم تخفيض التصنيف بمرور الوقت مع انخفاض المخاطر المرتبطة بالمعلومات بعد الكشف عنها على نطاق أوسع.
- وجهات نظر الدولة مقابل الصناعة بشأن التصنيف: يمكن أن يكون لدى الدولة قواعد مختلفة لتصنيف المعلومات الإلكترونية مقارنةً بالجهات المعنية في مجال الطيران بسبب اعتبارات مختلفة (على سبيل المثال قيود الأمن القومي).
- القيود الوطنية المنطبقة على الصناعة: قد يكون لدى الدولة تصنيف محدد لبعض أنواع المعلومات التي تنطبق على البُنى التحتية الوطنية ذات الأهمية الحيوية (مثل الكشف الأولي عن مؤشرات الاختراق كعناوين بروتوكول الإنترنت المشبوهة).

المعلومات التحليلية الإلكترونية

- **المعلومات التحليلية عن التهديدات الإلكترونية (CTI):**
  - **على المستوى الاستراتيجي:** تعتمد على طبيعة المعلومات التحليلية عن التهديدات الإلكترونية الاستراتيجية وطبيعة الجمهور (مثل مجالس الإدارة، كبار المديرين والرؤساء، محلل المعلومات التحليلية عن التهديدات الإلكترونية، فريق المهام الدفاعية (الفريق الأزرق))
    - **TLP:RED**: معلومات تحليلية محددة وحساسة للغاية عن تهديد إلكتروني محدد يستهدف مؤسسة ما. ويجب أن يكون عدد محدود من صانعي القرار المحددين على علم بهذه المعلومات.

- **TLP:AMBER**: يجب أن تكون الإدارة العليا أو أعضاء مجلس الإدارة أو أعضاء لجنة صنع القرار على دراية بوجود تهديد إلكتروني محدد إما يستهدف المنظمة أو له صلة بالطيران (مثل سلسلة التوريد أو الجهات المعنية المتصلة ببعضها) و/أو له صلة بالبنية التحتية الحيوية بالدولة.
- **TLP:GREEN**: المعلومات التحليلية التي يجب إطلاع المجتمع المحلي عليها لضمان التعريف بها على نطاق واسع والتصرف بناءً عليها (مثل وثائق السياسات العام والورقات البيضاء والاتجاهات والإحصاءات).

▪ **على المستوى التشغيلي:**

- **TLP:RED**: للموظفين التشغيليين والفنيين وموظفي الأمن ممن يتعين عليهم التصرف بناءً على معلومات تحليلية محددة حول تهديد أو حادث إلكتروني محدد يستهدف إحدى الجهات المعنية في مجال الطيران أو البنية التحتية الحيوية بالدولة (مثل سلسلة التوريد الجهات المعنية المتصلة ببعضها).
- **TLP:AMBER**: للموظفين التشغيليين والفنيين وموظفي الأمن ممن يلزم أن يكونوا على دراية بتهديد أو حادث إلكتروني محدد إما يستهدف المؤسسة أو له صلة بالطيران أو البنية التحتية الحيوية بالدولة.
- **TLP:GREEN**: المعلومات التحليلية التي يجب إطلاع المجتمع المحلي عليها لضمان التعريف بها على نطاق واسع والتصرف بناءً عليها.

▪ **على المستوى التكتيكي:**

- **TLP:RED**: لفئات محددة من الموظفين الأمنيين والفنيين ممن يتعين عليهم التصرف حيال تهديد إلكتروني محدد يستهدف المؤسسة أو ممن يلزم أن يكونوا على دراية بحادث إلكتروني مستمر.
- **TLP:AMBER**: للموظفين الأمنيين والفنيين ممن يلزم أن يكونوا على دراية بتهديد إلكتروني أو حادث إلكتروني جارٍ أو موطن من مواطن الضعف يستهدف المؤسسة أو له صلة بالطيران أو بالبنية التحتية الحيوية بالدولة.
- **TLP:GREEN**: المعلومات التحليلية التي يجب إطلاع المجتمع المحلي عليها لضمان التعريف بها على نطاق واسع والتصرف بناءً عليها.

○ **مؤشرات الاختراق:** **TLP:GREEN**

○ **الأساليب والتقنيات والإجراءات:** **TLP:GREEN**

○ **مواطن الضعف:**

▪ موطن ضعف يجري استغلاله: **TLP:RED**

▪ موطن ضعف مؤكد (سواء له إصلاح أم لا): **TLP:AMBER**

▪ موطن ضعف محتمل بلا إصلاح: **TLP:AMBER**

▪ موطن ضعف له إصلاح: **TLP:GREEN**

تقارير الحوادث الإلكترونية

- لا توجد توصية لأن ذلك يعتمد على طبيعة الحادث وسياقه وتوقيته (أي الوقت بين الحادث الإلكتروني وتبادل المعلومات). قد يتم استبعاد المعلومات ذات العلامة **TLP:CLEAR** في المراحل المبكرة، على الرغم من أنها قد تصبح مطلوبة بعد مرور بعض الوقت.

٣-٤ تقييم وتحليل المعلومات كمتلقٍ

يجب على متلقي المعلومات الإلكترونية تحليل المعلومات الواردة للتأكد من كونها تتسم بما يلي:

١- **موثوق بها/مضمونة/ذات جودة:** قد لا يكون مستوى الثقة[١١] في المعلومات الإلكترونية كافياً لاعتبار أن المعلومات يجب أن تؤدي إلى اتخاذ بعض الإجراءات من جانب المتلقي.

٢- **وثيقة الصلة:** مثال على كون المعلومات ذات صلة بالمتلقي هو إذا كان المتلقي ليس بإمكانه التصرف بناءً على المعلومات (كأن لا يقتضي الوضع أن يعرف بهذه المعلومات) في حين أن المعلومات ذات صلة بموظفين آخرين في المؤسسة. فقد يكون ذلك عائقاً إذا كانت المعلومات المتلقاة تحمل العلامة **TLP:RED**. ففي هذه الحالة، يجب على المتلقي أن يتواصل مع المُرسِل إما للحصول على موافقة المُرسِل على إعادة توجيه المعلومات إلى المتلقي (المتلقين) المعنيين من خلال تلقي نسخة من المعلومات ذات تصنيف أدنى، أو تزويد المُرسِل بنقطة اتصال أخرى في المؤسسة لتلقي النسخة ذات العلامة **TLP:RED** من المعلومات.

٣- **تُفضي إلى اتخاذ إجراءات:** قد يحول تصنيف المعلومات دون قيام المتلقي بالتصرف بناءً على المعلومات، الأمر الذي يتطلب مزيداً من النقاش بين المُرسِل والمتلقي للسماح باتخاذ إجراء بناءً على المعلومات الواردة. على سبيل المثال:

- إذا كانت المعلومات تحمل العلامة **TLP:RED** ويتعين على المتلقي التواصل مع آخرين في المؤسسة للتصرف بناءً على تلك المعلومات، لكن الآخرين المعنيين بالأمر لم يتلقوا المعلومات نفسها.
- إذا كانت المعلومات تحمل العلامة **TLP:AMBER+STRICT** ويتعين على المتلقي التواصل مع مؤسسة أخرى للتصرف وفقاً للمحتوى الذي تم تبادله.

ينبغي أن يشمل التحليل أيضاً الأنشطة التالية:

- ينبغي على المتلقي الجمع بين المعلومات الإلكترونية الواردة إليه والمعلومات التحليلية المتاحة (على سبيل المثال ربطها و/أو استكمالها بمعلومات أخرى). فمن شأن ذلك أن سيساعد ذلك على رفع أو خفض مستوى الثقة في تلك المعلومات.
- ينبغي على المتلقي أن يضع المعلومات في سياقها فيما يتعلق بمهام عمله، الأمر الذي من شأنه أن يعالج المسائل المتعلقة بمعنى المعلومات بالنسبة للمتلقي في السياق السياسي و/أو الاستراتيجي و/أو التشغيلي و/أو الفني و/أو من منظور الأمن الإلكتروني.

٣-٥ علاقات الثقة بين الأطراف

الثقة مفهوم ديناميكي متعدد الأوجه، وهو عنصر ضروري للتبادل الآمن للمعلومات الحساسة وإطلاع الآخرين عليها. والثقة ليست مقياساً مطلقاً، بل هي مقياس نسبي يختلف باختلاف السياق والعلاقات والسلوكيات.

ولا شك أن بناء علاقات الثقة بين الطرفين المُرسِل والمتلقي أمر بالغ الأهمية لتبادل المعلومات الإلكترونية بشكل فعّال.

وقد تكون علاقات الثقة مع الشركاء أو الجهات المعنية غير التقليدية مسألة ضرورية أيضاً. ومن المهم تحديد الأطراف الرئيسية لتبادل المعلومات الإلكترونية بشكل استباقي و/أو تفاعلي، ضماناً لتعميم المعلومات الإلكترونية ذات الصلة بالواقع وفي الوقت المناسب.

ومن الممكن بناء علاقات الثقة مع مجموعة متنوعة من الشركاء والجهات المعنية. ومن أمثلة علاقات الثقة ما يلي:

[١١] انظر الفقرتين ٣-٣-١-١ و٣-٣-١-٢، والملحقات (ب) و(ج) و(د).

- داخل قطاع الطيران
  - بين الوكالات الحكومية (على المستوى الوطني و/أو الدولي)
  - من وكالات الدولة إلى هيئات الطيران والعكس
  - فيما بين الهيئات على مستوى الصناعة
  - من الوكالات الحكومية أو هيئات الطيران إلى المنظمات الدولية (مثل الإيكاو) والعكس
- مع الشركاء والجهات المعنية من خارج قطاع الطيران
  - المؤسسات غير الحكومية
  - المؤسسات غير الربحية
  - المنظمات الدولية (مثل وكالات الأمم المتحدة المعنية)
  - المنظمة الدولية للشرطة الجنائية – الإنتربول (ICPO–INTERPOL)

ويستغرق بناء الثقة في العادة وقتاً طويلاً. ويمكن للدول والجهات المعنية إقامة علاقات الثقة ورعايتها وتعزيزها من خلال ما يلي:

- إقامة التحالفات مع الشركاء من ذوي التفكير المماثل.
- الأنشطة المنتظمة: المشاركة في الاجتماعات أو المؤتمرات الدورية.
- الاتفاقات: يورد القسمان التاليان إرشادات حول أنواع الاتفاقات التي يمكن إبرامها لتبادل المعلومات الإلكترونية.

كما ينبغي على الدول والجهات المعنية النظر في الفوائد (انظر القسم ١–١) التي يمكن جنيها من إقامة علاقات الثقة والحفاظ عليها والتكاليف المرتبطة بذلك، من أجل تبرير ضرورة الاستثمار في هذه المساعي واتخاذ قرار بشأنها. وينبغي أن تشمل الاعتبارات ما يلي:

- الوقت: كم من الوقت ينبغي الالتزام بتخصيصه لإقامة علاقة وتطويرها.
- الموارد: بما في ذلك الموارد البشرية والمالية.
- المنافع: ما الذي يحصل عليه كل طرف من العلاقة.
- المسؤوليات: الخسائر المحتملة لكل طرف من العلاقة.
- الاستمرارية: ينبغي أيضاً مراعاة التكلفة الجارية للحفاظ على العلاقة من حيث الوقت والموارد.

كذلك فإن المحافظة على علاقات الثقة تنطوي على أنشطة مثل ما يلي:

- الاجتماعات وجهاً لوجه والاجتماعات الافتراضية: يجب الاتفاق على وتيرة عقد الاجتماعات بين الطرفين. ويُوصى بعقدها حسب الحاجة، وسنوياً على الأقل بالنسبة للاجتماعات وجهاً لوجه، مع مراعاة فئات الموظفين المعنيين (الفئات العليا أو المتوسطة أو الفنية).
- التبادل الاستباقي للمعلومات الإلكترونية: تبادل المعلومات الإلكترونية بشكل متكرر بناءً على الاحتياجات والأولويات. ويمكن أن تشمل هذه المعلومات ما يلي:
  - التغييرات في السياسات والإجراءات مما قد يؤثر على المتلقي (المتلقين).
  - المنتجات: التقارير العاجلة، والتحليل الاستراتيجي، وما إلى ذلك.
  - المعلومات الأولية: شفرة المصدر، والسجلات، إلخ.

- التبادل التفاعلي للمعلومات الإلكترونية: يمكن أن يشمل ذلك تبادل المعلومات المتعلقة بالاستجابة لحادث إلكتروني:
  - أثناء وقوع حادث إلكتروني: تبادل المعلومات في الوقت الفعلي وبشكل متسق أثناء وقوع الحادث.
  - بعد وقوع حادث إلكتروني: تبادل النتائج والأسباب الجذرية والدروس المستفادة، إلخ.

ومن الممكن أن تنتهي علاقات الثقة عندما يتلاشى عنصر الثقة. ومن أمثلة التصرفات التي ربما تؤدي إلى هذه النتيجة ما يلي:

- الإفشاء غير المصرح به للمعلومات السرية: الإفشاء العرضي أو المتعمد للمعلومات السرية لأفراد أو منظمات غير مصرح لهم بالاطلاع على مثل هذه المعلومات والتي قد تكون ذات أهمية إما من ناحية الأمن الوطني أو الملكية الوطنية.
- التبادل المتعمد للمعلومات الحساسة: التبادل المتعمد للمعلومات الأمنية الحساسة أو المعلومات الحساسة المتعلقة بالملكية مع أفراد أو منظمات بقصد كشف مواطن الضعف أو الإضرار بالمصداقية، خاصةً إذا تم ذلك على نطاق عام.

٣-٥-١ الاتفاقات الرسمية

يمكن إضفاء الطابع الرسمي على تبادل المعلومات الإلكترونية بين الأطراف من خلال اتفاقات ثنائية أو متعددة الأطراف، مُلزمة أو غير مُلزمة.

وتشمل هذه الاتفاقات أنواعاً مختلفة من الأطراف. على سبيل المثال، يمكن إبرام اتفاقات بين الدول أو بين الوكالات الحكومية (على سبيل المثال بين سلطة الطيران المدني والوكالة الوطنية للأمن الإلكتروني في الدولة نفسها)، أو بين الوكالات الحكومية في دول مختلفة (على سبيل المثال بين سلطات الطيران المدني في دول مختلفة)، أو بين وكالة حكومية والجهات المعنية في قطاع الطيران بالدولة نفسها، أو بين وكالة حكومية والجهات المعنية في قطاع الطيران في دولة أخرى، و/أو بين مختلف الجهات المعنية في قطاع الطيران.

ويقدم الملحق (هـ) قائمة بالأقسام الموصى بتغطيتها في أي اتفاق رسمي لتبادل المعلومات الإلكترونية لضمان وضوح أدوار ومسؤوليات الأطراف التي تتبادل المعلومات الإلكترونية، مما سينعكس بالإيجاب على مستوى الثقة بين الأطراف بمرور الوقت.

٣-٥-٢ الاتفاقات غير الرسمية

غالباً ما تُستخدم الاتفاقات غير الرسمية عندما تكون الثقة بين الأطراف المتبادِلة قائمةً بالفعل أو ضمنيةً. وينبغي استخدام هذه الأنواع من الاتفاقات بحذر، إذ ليست لها تبعات قانونية على الأطراف الموقعة. ولا ينبغي أن تكون مثل تلك الاتفاقات الآلية الأساسية أو الوحيدة لتبادل المعلومات الإلكترونية.

تتضمن مثل هذه الاتفاقيات معلومات محدودة ضرورية للأطراف كي يتسنى لها تبادل المعلومات، على سبيل المثال:

- الوسائل التقنية التي سيتم استخدامها لتبادل المعلومات؛
- نقاط الاتصال المعنية (بيانات الاتصال بالأفراد والفرق المختصة).

ويجري التشديد على أهمية الاستخدام الصارم والمتسق لتصنيف المعلومات بواسطة علامات بروتوكول الإشارات الضوئية عند تبادل المعلومات الإلكترونية باستخدام الاتفاقات غير الرسمية، من أجل الحفاظ على الثقة القائمة بين الأطراف وتعزيزها.

٤ تنظيم المعلومات الإلكترونية المتبادلة وإيصالها وأرشفتها

٤-١ تنظيم المعلومات الإلكترونية المراد تبادلها

يجب أن يتم تنظيم المعلومات الإلكترونية بناءً على أنواع محددة أو من خلال هيكل محدد من أجل ضمان تبادلها مرفقاً بالسياق المناسب والتفاصيل المفيدة ذات الفائدة العملية.

وفيما يلي مثال على كيفية تنظيم المعلومات الإلكترونية المراد تبادلها:

- العنوان: وصف رفيع المستوى للمعلومات الإلكترونية
- الرقم المرجعي: لمساعدة المُرسِل على تتبع المعلومات
- العلامة في بروتوكول الإشارات الضوئية
- الجوانب الرئيسية، بما في ذلك على سبيل المثال لا الحصر:
  - الفئة (مثل تجسس إلكتروني، جريمة إلكترونية، عملية معلوماتية)
  - النوع (مثل موطن ضعف، روبوت، مراقبة، بيانات شخصية، شبكات تواصل اجتماعي، تسريب بيانات تسجيل الدخول، تصيد احتيالي، هجوم حجب الخدمة الموزّع، برمجيات خبيثة)
  - مستوى التهديد الإلكتروني (على سبيل المثال: حرج، مرتفع، متوسط، منخفض)
  - المجال/القطاع
  - مصداقية وموثوقية مصدر المعلومات (انظر الفقرة ٣-٣-١-١)
- النقاط الرئيسية: قائمة بالنقاط الرئيسية التي تشرح المعلومات
- الملخص
- الإسناد: الجهة (الجهات) الفاعلة للتهديد والتي يُحتمل أن تكون، أو هي بالفعل، الجهة (الجهات) المرتكبة للهجوم
- تقييم الآثار والأهداف والضحايا وما إلى ذلك.
- توصيات بالإجراءات الواجب اتخاذها من قبل المتلقي (المتلقين)
- المعلومات العملية
  - الأصول الإلكترونية المتضررة
  - الخط الزمني
  - مؤشرات الاختراق
  - قواعد الكشف
  - الأساليب والتقنيات والإجراءات
- التدابير الاحترازية
  - التدابير الاحترازية العامة
  - التدابير الاحترازية المحددة
- المراجع

٤-٢ إيصال المعلومات الإلكترونية

يقدم هذا القسم إرشادات حول مزايا وعيوب استخدام الوسائط المختلفة لتبادل المعلومات الإلكترونية.

٤-٢-١ الهاتف

تصلح هذه الوسيلة مع المعلومات ذات العلامة TLP:RED لضمان التواصل المتزامن مع الشخص المقصود بالمعلومات. كما أنها تساعد في توصيل المعلومات الحرجة التي تتطلب استجابة فورية .

وفي حالة استخدام الهاتف لنقل المعلومات الإلكترونية، يوصى باتخاذ الضوابط التي تضمن هوية الطرفين (على سبيل المثال لتجنب المقاطع الصوتية المصنوعة بواسطة الذكاء الاصطناعي).

وبشكل عام، هذه الوسيلة محدودة الاستخدام (إذ تُستخدم في المقام الأول لتبادل المعلومات الإلكترونية ذات الأهمية القصوى و/أو المعلومات الإلكترونية ذات العلامة TLP:RED)، وبالتالي ينبغي النظر فيها بالاقتران مع الوسائط الأخرى لتبادل المعلومات الإلكترونية.

٤-٢-٢ رسائل البريد الإلكتروني بلا مرفقات

يمكن تبادل المعلومات الإلكترونية بواسطة نص عادي في رسالة بالبريد الإلكتروني.

واستخدام هذه الوسيلة لتبادل المعلومات الإلكترونية يعني ما يلي:

- يجب على المتلقي فتح رسالة البريد الإلكتروني وقراءة المعلومات.
- هناك ضرورة أن يقوم محلل المعلومات الإلكترونية بتحليل المحتوى لتقييم مدى ملاءمته وأهميته للمتلقي.
- ستتم معالجة المعلومات يدوياً في البداية.

فيما يلي بعض جوانب القصور عند استخدام رسائل البريد الإلكتروني العادية لتبادل المعلومات الإلكترونية:

- هذه الوسيلة تناسب المحتوى القصير والنصي.
- قد تقوم بعض نُظُم البريد الإلكتروني بحظر الرسالة لأنها قد تحتوي على مؤشرات اختراق، مما قد يؤدي إلى تفعيل ضوابط أمن تكنولوجيا المعلومات.
- من الصعب المواظبة على تحديث قوائم عناوين البريد الإلكتروني. لذا يُوصى باستخدام عناوين البريد الإلكتروني للأفراد والعناوين العامة.
- لا يمكن إرسال المعلومات ذات العلامة TLP:RED إلى عناوين البريد الإلكتروني العامة (مثل groupmailbox@company.com)، ولكن فقط إلى عناوين بريد الأفراد (مثل someone@company.com).
- بعض أنواع عناوين البريد الإلكتروني قد لا يمكن اعتبارها جهات متلقية موثوق بها (مثل عناوين البريد الإلكتروني الخاصة من خلال خدمات استضافة البريد الإلكتروني التجارية مثل yahoo/ Hotmail / gmail / إلخ).
- هناك خطر استغلال البريد الإلكتروني لانتحال شخصية. لذا يُوصى باستخدام طرق المصادقة المناسبة، مثل التوقيع الرقمي على البريد الإلكتروني، للتصدي لهذا الخطر.

٤-٢-٣ البريد الإلكتروني بمرفقات

يمكن تبادل المعلومات الإلكترونية في مستند يُرفق برسالة البريد الإلكتروني. ويمكن تشفير المرفق بكلمة مرور تُرسل إلى المتلقي من خلال وسيلة أخرى موثوق بها (كالرسائل النصية أو تطبيقات المراسلة الآمنة).

واستخدام هذه الوسيلة لتبادل المعلومات الإلكترونية يعني ما يلي:

- يجب على المتلقي فتح رسالة البريد الإلكتروني وقراءة المعلومات.
- هناك ضرورة أن يقوم محلل المعلومات الإلكترونية بتحليل المحتوى لتقييم مدى ملاءمته وأهميته للمتلقي.
- ستتم معالجة المعلومات يدوياً في البداية.

فيما يلي بعض جوانب القصور عند استخدام رسائل البريد الإلكتروني ذات المرفقات لتبادل المعلومات الإلكترونية:

- هناك خطر النقر على مرفق ضار، وبالتالي يجب تعقيم المرفق أولاً.
- تحظر بعض نُظُم البريد الإلكتروني بعض أنواع المرفقات (مثل الملفات المضغوطة كالملفات ذات الامتدادات zip. و rar. و7z).
- قد تقوم بعض نُظُم البريد الإلكتروني بحظر الوصول إلى الوثيقة لأنها قد تحتوي على مؤشرات اختراق، والتي من شأنها أن تؤدي إلى تفعيل ضوابط أمن تكنولوجيا المعلومات.
- قد يمنع حجم المرفق إرساله عبر البريد الإلكتروني.
- من الصعب المواظبة على تحديث قوائم عناوين البريد الإلكتروني. لذا يُوصى باستخدام عناوين البريد الإلكتروني للأفراد والعناوين العامة.
- لا يمكن إرسال المعلومات ذات العلامة TLP:RED إلى عناوين البريد الإلكتروني العامة (مثل groupmailbox@company.com)، ولكن فقط إلى عناوين بريد الأفراد (مثل someone@company.com).

٤-٢-٤ المستودعات الخاصة

يمكن تبادل المعلومات الإلكترونية من خلال منح الوصول إلى مستودع خاص يحتوي على المعلومات المراد تبادلها.

وعند اللجوء إلى هذه الوسيلة، تُرسل إشعارات لإخطار المتلقي (المتلقين) بأن هناك معلومات إلكترونية جديدة متاحة للاطلاع عليها.

ويمكن إرسال مثل هذا الإشعار آلياً بواسطة البريد الإلكتروني أو وسائل أخرى (كالرسائل النصية أو تطبيقات التواصل الآمن).

ويجب تأمين سُبُل الوصول إلى المستودع والحفاظ عليها:

- ينبغي نشر الضوابط/وسائل الحماية الأمنية وفقاً لحساسية المعلومات التي يجري تبادلها من خلال المستودع. ويمكن أن تشمل الضوابط استضافة المستودع (كالاعتماد على خادم خاص/مشترك، والاستضافة السحابية)، والتحكم في سُبُل/الحق في الوصول، وطرق التحقق من المستخدم (مثل تسجيل الدخول الأحادي (SSO)، والمصادقة الثنائية/المتعددة العوامل (2FA/MFA)، وما إلى ذلك).
- ينبغي المواظبة على تحديث قائمة المؤسسات/الأفراد المصرح لهم بالوصول إلى المستودع بشكل مستمر لضمان حداثتها وصحتها.
- يجب منح حقوق الوصول، مثل امتيازات القراءة والكتابة، للحسابات الفردية وتحديثها.
- يجب تسجيل جميع عمليات الوصول والإجراءات التي تتم على المستودع وتحليلها.
- ينبغي فهرسة المعلومات الإلكترونية المنشورة على المستودع بعناية في صورة مجلدات حيث تتفاوت حقوق الوصول إلى المعلومات، الممنوحة إلى مختلف المشاركين. وعلاوة على ذلك، هناك حاجة إلى نقل المعلومات بين المجلدات مع تغير علامات المعلومات (أي من بين علامات بروتوكول الإشارات الضوئية) مع مرور الوقت (على سبيل المثال، قد تكون المعلومات متاحة لجمهور أكبر إذا تم تخفيض علامتها في بروتوكول الإشارات الضوئية). ويمكن أن تصبح هذه عملية معقدة مع تزايد أعداد المستخدمين وزيادة حجم المعلومات المتبادلة عبر المستودع مع مرور الوقت.

٤-٢-٥ التطبيقات

يمكن استخدام تطبيقات برمجيات مختلفة (سواء مفتوحة المصدر أو تجارية) لتبادل المعلومات الإلكترونية (على سبيل المثال MISP وOpenCTI وCyWare وغيرها).

ولا يمكن طرح قائمة عامة بالاعتبارات الخاصة بالتطبيقات بشكل عام، لأن ذلك يعتمد على طبيعة التطبيقات (على سبيل المثال ما إذا كانت مفتوحة المصدر أم تجارية)، ومن المسؤول عن تطوير وتحديث الضوابط الأمنية، وحقوق الوصول، وفهرسة المعلومات (على سبيل المثال يدوياً أم آلياً من خلال القواعد)، وتخزين المعلومات الحساسة (على سبيل المثال الخوادم الآمنة/الخاصة أو العامة)، إلخ. ولذلك يُوصى بتقييم جميع هذه الجوانب، وغيرها حسب الاقتضاء، عند النظر في استخدام تطبيقات تبادل المعلومات الإلكترونية.

ومن بين التطبيقات الموجودة، يقدم الملحق (و) معلومات عن منصة MISP – وهي منصة مفتوحة المصدر لتبادل المعلومات التحليلية عن التهديدات، حيث توفر المنصة ميزات جديرة بالاهتمام من شأنها أن تدعم جهود قطاع الطيران في تبادل المعلومات الإلكترونية.

٤-٣ أرشفة المعلومات الإلكترونية

يجب أرشفة المعلومات الإلكترونية المتبادلة من قبل كل من المُرسِل والمتلقي لأغراض حفظ السجلات ومراقبة الجودة.

وينبغي مراعاة الجوانب التالية عند أرشفة المعلومات:

- اللوائح: يجب مراعاة اللوائح التي قد تنطبق على أرشفة المعلومات (على سبيل المثال، قوانين الخصوصية ومتطلباتها فيما يخص أرشفة أنواع محددة من المعلومات والمدة القصوى المسموح بها لحفظ تلك المعلومات في الأرشيف).
- وسائط التخزين: يعتمد استخدام وسائط التخزين على نوع المعلومات. ويمكن استخدام أنواع مختلفة من الوسائط لأرشفة المعلومات الإلكترونية. على سبيل المثال، يمكن تخزين تقارير الحوادث الإلكترونية في قاعدة بيانات محددة قائمة بذاتها، ويمكن تخزين تقارير المعلومات التحليلية عن التهديدات الإلكترونية كملف على قرص كومبيوتر، إلخ.
- التحكم في الوصول وحقوق الوصول: يجب أن تكون هناك سياسة عامة تُحدد من يجوز له الوصول إلى أي نوع من المعلومات الإلكترونية المؤرشفة. ويتماشى ذلك مع العلامة المسندة للمعلومات في بروتوكول الإشارات الضوئية (فمثلاً العلامة **TLP:AMBER+STRICT** لا تعني كل شخص في المؤسسة، بل فقط أولئك الذين يقتضي الوضع معرفتهم بالأمر).
- إمكانية الوصول محلياً مقابل إمكانية الوصول عن بُعد: قد لا يُسمح بالوصول إلى بعض المعلومات الإلكترونية من خارج المؤسسة (من خلال الشبكات الداخلية على سبيل المثال) ولكن داخلياً فقط. ويشمل ذلك أيضاً تحديد امتيازات كل حق من حقوق الوصول بناءً على أدوار ومسؤوليات الموظفين والتي يمكن استخدامها لأغراض التدقيق/التأكد.
- الضوابط الأمنية/وسائل التأمين: ينبغي نشر مستويات مختلفة من الضوابط الأمنية ووسائل التأمين بحسب نوع المعلومات. على سبيل المثال، يجب تطبيق ضوابط أكثر صرامة لحماية تقارير الحوادث الإلكترونية مقارنةً بتلك المطبقة لحماية الثغرات الأمنية التي تم إصلاحها بالفعل.
- الصلة بالوضع الراهن: قد تصبح بعض المعلومات الإلكترونية قديمةً بسبب التطورات. على سبيل المثال، الثغرات في الأنظمة التي لم تعد تستخدمها المؤسسة، والمعلومات عن تهديدات إلكترونية استراتيجية متعلقة بأحداث جغرافية سياسية لم تعد موجودة، وما إلى ذلك.
- قابلية الاستخدام: يجب تحديد الفئات المختلفة في الأرشيفات، كي يظل من الممكن الاستفادة من المعلومات. على سبيل المثال:
  - "ساخنة": فئة تتضمن البيانات الحديثة التي يتم تخزينها دون ضغط للملفات، مما يسمح بأقصى قدر من الأداء للاسترجاع والمعالجة؛

- "دافئة": فئة تتضمن البيانات المخزنة بضغط خفيف، مما يسمح بأداء جيد جداً لاسترجاعها ومعالجتها، إذا لزم الأمر؛
- "باردة": فئة تتضمن البيانات التي تمت أرشفتها وضغطها بالكامل، والتي يلزم استرجاعها وفك ضغطها يدوياً كي تصبح متاحة.

- المدة: ينبغي النظر في مدة حفظ المعلومات الإلكترونية في الأرشيفات وذلك بحسب على نوع المعلومات. على سبيل المثال، يمكن تحديد قواعد أرشفة تسمح بالاحتفاظ بمؤشرات الاختراق التي لا يزيد عمرها عن [X] سنة. بالإضافة إلى ذلك، ينبغي تنفيذ الإجراءات المتعلقة بحذف المعلومات القديمة كجزء من عمليات إدارة أرشفة المعلومات الإلكترونية.

٥ إعادة إرسال المعلومات الإلكترونية

٥-١ ما الداعي إلى إعادة إرسال المعلومات الإلكترونية

قد يكون من الضروري التوسّع في نقل المعلومات الإلكترونية الواردة من مصدر خارجي لضمان وصول المعلومات إلى أوسع جمهور يحتاج إلى معرفتها. ومع ذلك، ينبغي توخي الحذر قبل التوسّع في نشر هذه المعلومات الإلكترونية.

وكمثال على هذا السيناريو، تتلقى وكالة حكومية معلومات من مصدر خارجي لا يسمح بإعادة إرسال المعلومات إلا مع الكيانات التي أبرم معها المصدر اتفاقاً رسمياً. وفي تقدير الوكالة الحكومية، هناك ضرورة أن تطلع الوكالات الحكومية الأخرى، التي ليست لديها اتفاق رسمي مع الجهة المصدرة للمعلومات، على هذه المعلومات. وفي هذه الحالة، يجب على متلقي المعلومات الاتصال بمنشئ المعلومات وطلب موافقته على إعادة إرسال هذه المعلومات إلى الوكالات الأخرى التي يقتضي الوضع اطلاعها عليها.

ولتقرير ما إذا كان يجب إعادة إرسال المعلومات الإلكترونية ومع من، ينبغي على متلقي المعلومات أن يأخذ بعض العوامل بعين الاعتبار مثل:

- حدود إعادة الإرسال: هل يمكن أو ينبغي إعادة إرسال هذه المعلومات؟ في حالة الشك (أي مثلاً الشك في احتمال إساءة استخدام علامة بروتوكول الإشارات الضوئية)، يجوز لمتلقي المعلومات أن يطلب الإذن من المُرسِل بإعادة إرسال المعلومات.
- الغرض من إعادة إرسال المعلومات ودور المتلقي الإضافي.

ويرتبط الغرض من إعادة إرسال المعلومات الإلكترونية بالإجراء المتوقع من المتلقي اتخاذه:

- للعلم/التوعية: المتلقي الإضافي بحاجة إلى معرفة هذه المعلومات ويجري نقل المعلومات إليه للعلم فقط.
- لاتخاذ إجراء: المتلقي الإضافي بحاجة إلى معرفة هذه المعلومات ويجري نقل المعلومات إليه من أجل إجراء محدد سيقوم به المتلقي. ويمكن أن تشمل مثل هذه الإجراءات ما يلي:
  - تخصيص أو تعبئة الموارد لمعالجة مشكلة معينة.
  - تخصيص أو تعبئة الموارد للتخفيف من تهديد أو ثغرة إلكترونية معينة.
  - تخصيص أو تعبئة الموارد لأغراض المساعدة في الاستجابة.

وقد يشكل دور المتلقي الإضافي عاملاً في تقرير ما إذا كان ينبغي إعادة إرسال المعلومات الإلكترونية. وتشمل الأدوار التي قد تستلزم المعرفة بالمعلومات ما يلي، على سبيل المثال:

- **الخبراء الفنيون:** خبير أو أخصائي يشرف على حماية الشبكات والأنظمة والخدمات والتطبيقات والبنى التحتية لتكنولوجيا المعلومات/التكنولوجيا التشغيلية وما إلى ذلك، من الوصول غير المصرح به.
- **واضع السياسات:** الشخص الذي يقوم بصياغة استراتيجيات وسياسات وإجراءات و/أو عمليات الأمن الإلكتروني في مجال الطيران أو خارجه من المجالات وثيقة الصلة، وذلك كي تنفذها الجهات المعنية في قطاعات الطيران.
- **صانع القرار:** أحد كبار الموظفين ممن يوافقون على تنفيذ استراتيجيات وسياسات وإجراءات و/أو عمليات الأمن الإلكتروني في مجال الطيران أو خارجه من المجالات وثيقة الصلة.
- **المنسق:** خبير أو متخصص في الأمن الإلكتروني مكلّف بإعادة إرسال المعلومات المتبادلة بفعالية إلى الموظفين المختصين.
- **مسؤول سلامة الطيران:** خبير سلامة الطيران الذي يمكنه تحديد التأثير المحتمل على سلامة الطيران و/أو كفاءته و/أو سعته.
- **مسؤول أمن الطيران:** خبير أمن الطيران الذي يمكنه تحديد التأثيرات الأخرى المحتملة على أمن الطيران.

٥-٢ قواعد إعادة إرسال المعلومات الإلكترونية

تتضمن قواعد إعادة إرسال المعلومات الإلكترونية العديد من المجالات التي ينبغي النظر فيها بعناية:

- الجهة التي يُعاد إرسال المعلومات إليها (على سبيل المثال: دولة/جهة معنية في مجال الطيران/جهة معنية خارج قطاع الطيران، أو كيان وطني/دولي).
- دور المتلقي الذي سيُعاد إرسال المعلومات الإلكترونية إليه.
- ما الذي سيُعاد إرساله: المعلومات الإلكترونية الكاملة أو مقتطف منها (على سبيل المثال وثيقة كاملة أم مجرد فقرات محددة).
- تحت أي ظروف سيُعاد إرسال المعلومات: استباقياً أو تفاعلياً.
- وتيرة نقل المعلومات: بشكل روتيني أم حسب الحاجة.
- سبب نقل المعلومات الإلكترونية (على سبيل المثال للعلم أم لاتخاذ إجراء).
- التعامل مع المعلومات الإلكترونية: يجب أن تبقى جميع التصنيفات والتحذيرات الأصلية موجودة على قنوات الاتصال المستخدمة (أي قنوات الاتصال السرية وغير السرية).
- لا يمكن تغيير علامة بروتوكول الإشارات الضوئية المسندة للمعلومات الإلكترونية عند إعادة إرسالها.

٥-٣ وسائل ووسائط إعادة إرسال المعلومات الإلكترونية

ينبغي أن تكون الوسائل/الوسائط المستخدمة لإعادة إرسال المعلومات الإلكترونية آمنة وبسيطة، حسب الاقتضاء.

المعلومات المادية: المعلومات التي يتم توفيرها في نسخة مطبوعة. ينبغي تغليف المعلومات بشكل سليم (في مجلد مثلاً) وتأمينها (مثلاً في حاوية تُغلق بسحاب أو قفل) أثناء نقلها إلى موقع الاجتماع وقبل تقديم النسخة (النسخ) المطبوعة. وأي تذكير أو محاذير بشأن أسلوب التعامل مع المعلومات ينبغي تدوينها إما على المعلومات نفسها أو على ورقة غلاف (فمثلاً عادةً ما تُدرج محاذير التعامل مع المعلومات الأمنية الحساسة[١٢] في ورقة غلاف تسرد التعليمات).

المعلومات الإلكترونية: نفس وسائل تبادل المعلومات الإلكترونية التي وردت في القسم ٤-٢ تنطبق أيضاً على إعادة إرسال المعلومات. ومع ذلك، ينبغي مراعاة أن المتلقي المقصود، الذي يُعاد إرسال المعلومات الإلكترونية إليه، قد لا تكون لديه إمكانية الوصول إلى بعض الوسائل الإلكترونية المتاحة للمُرسِل (كقائمة بعناوين البريد الإلكتروني الآمنة، وإمكانية الوصول إلى البوابة/المستودع الذي توجد فيه المعلومات).

وهناك قواعد إضافية للتعامل مع المعلومات السرية والتي تختلف بحسب الدولة أو المؤسسة. وينبغي اتباع هذه القواعد بدقة وفقاً للقواعد والإجراءات المعمول بها.

— — — — — — — —

[١٢] تتضمن الإرشادات المتعلقة بالتعامل مع معلومات أمن الطيران الحساسة في القسم ٢-٣ من "دليل أمن الطيران" الصادر عن الإيكاو (Doc 8973 – مقيدة التوزيع) معلومات مفيدة يمكن استخدامها في سياق تبادل المعلومات الإلكترونية.

الملحق (أ)

المعلومات الإلكترونية الموصى بتبادلها في الطيران وفقاً لنوع المعلومات

المعلومات التحليلية الإلكترونية

- **المعلومات التحليلية عن التهديدات الإلكترونية:**
  - **على المستوى الاستراتيجي:**
    - من الوكالات الحكومية (المركز الوطني للأمن الإلكتروني وسلطة الطيران المدني وغيرها) إلى الجهات المعنية في مجال الطيران بالدولة
    - من المركز الوطني للأمن الإلكتروني إلى فرق الاستجابة لطوارئ أنظمة الكمبيوتر/مراكز تبادل المعلومات وتحليلها
    - من فرق الاستجابة لطوارئ أنظمة الكمبيوتر/مراكز تبادل المعلومات وتحليلها إلى الجهات المعنية في مجال الطيران
    - بين مراكز الأمن الإلكتروني الوطنية الموثوق بها
    - بين الدول الموثوق بها
  - **على المستوى التشغيلي**
    - من الجهات المعنية في مجال الطيران إلى الجهات المعنية في مجال الطيران
    - من فرق الاستجابة لطوارئ أنظمة الكمبيوتر/مراكز تبادل المعلومات وتحليلها إلى الجهات المعنية في مجال الطيران
    - من الجهات المعنية في مجال الطيران إلى الوكالات الحكومية (المركز الوطني للأمن الإلكتروني وسلطة الطيران المدني وغيرها) بالدولة
  - **على المستوى التكتيكي:**
    - من الجهات المعنية في مجال الطيران إلى الجهات المعنية في مجال الطيران
    - من فرق الاستجابة لطوارئ أنظمة الكمبيوتر/مراكز تبادل المعلومات وتحليلها إلى الجهات المعنية في مجال الطيران
    - من المركز الوطني للأمن الإلكتروني إلى فرق الاستجابة لطوارئ أنظمة الكمبيوتر/مراكز تبادل المعلومات وتحليلها
    - من المركز الوطني للأمن الإلكتروني إلى الجهات المعنية في مجال الطيران بالدولة
    - من الجهات المعنية في مجال الطيران إلى الوكالات الحكومية (المركز الوطني للأمن الإلكتروني وسلطة الطيران المدني وغيرها)

- **مؤشرات الاختراق:**
  - من الجهات المعنية في مجال الطيران إلى الجهات المعنية في مجال الطيران
  - من فرق الاستجابة لطوارئ أنظمة الكمبيوتر/مراكز تبادل المعلومات وتحليلها إلى الجهات المعنية في مجال الطيران
  - من المركز الوطني للأمن الإلكتروني إلى فرق الاستجابة لطوارئ أنظمة الكمبيوتر/مراكز تبادل المعلومات وتحليلها
  - من المركز الوطني للأمن الإلكتروني إلى الجهات المعنية في مجال الطيران بالدولة
  - من الجهات المعنية في مجال الطيران إلى المركز الوطني للأمن الإلكتروني بالدولة

- **الأساليب والتقنيات والإجراءات:**
  - من الجهات المعنية في مجال الطيران إلى الجهات المعنية في مجال الطيران
  - من فرق الاستجابة لطوارئ أنظمة الكمبيوتر/مراكز تبادل المعلومات وتحليلها إلى الجهات المعنية في مجال الطيران
  - من المركز الوطني للأمن الإلكتروني إلى فرق الاستجابة لطوارئ أنظمة الكمبيوتر/مراكز تبادل المعلومات وتحليلها
  - من المركز الوطني للأمن الإلكتروني إلى الجهات المعنية في مجال الطيران بالدولة
  - من الجهات المعنية في مجال الطيران إلى المركز الوطني للأمن الإلكتروني بالدولة

- **مواطن الضعف**
  - من الجهات المعنية في مجال الطيران إلى الجهات المعنية في مجال الطيران
  - من الجهات المعنية في مجال الطيران إلى مقدمي سلاسل التوريد المتعاملين معها
  - من الباحثين إلى فرق الاستجابة لطوارئ أنظمة الكمبيوتر/مراكز تبادل المعلومات وتحليلها في مجال الطيران
  - من الباحثين إلى الوكالات الحكومية (المركز الوطني للأمن الإلكتروني، سلطة الطيران وما إلى ذلك)
  - من الباحثين إلى الجهات المعنية في مجال الطيران
  - من الباحثين إلى سلاسل التوريد
  - من فرق الاستجابة لطوارئ أنظمة الكمبيوتر/مراكز تبادل المعلومات وتحليلها إلى الجهات المعنية في مجال الطيران
  - من المركز الوطني للأمن الإلكتروني إلى فرق الاستجابة لطوارئ أنظمة الكمبيوتر/مراكز تبادل المعلومات وتحليلها في مجال الطيران
  - من المركز الوطني للأمن الإلكتروني إلى الجهات المعنية في مجال الطيران بالدولة
  - من الجهات المعنية في مجال الطيران إلى الوكالات الحكومية المختصة (المركز الوطني للأمن الإلكتروني وسلطة الطيران المدني وغيرها) بالدولة

تقارير الحوادث الإلكترونية

- التقارير الإلزامية عن الحوادث الإلكترونية (من خلال القوانين و/أو اللوائح الوطنية المعمول بها):
  - من الجهات المعنية في مجال الطيران إلى الوكالات الحكومية المختصة (المركز الوطني للأمن الإلكتروني، سلطة الطيران المدني، إلخ) (فيما يخص حوادث سلامة و/أو أمن الطيران)
  - من الجهات المعنية في مجال الطيران إلى سلطات إنفاذ القانون (فيما يخص حوادث محددة تتعلق بالجرائم الإلكترونية كالاحتيال أو قوانين محددة كقوانين الخصوصية)
  - من الدولة إلى الإيكاو (فيما يخص الحوادث الإلكترونية المتعلقة بأعمال التدخل غير المشروع)

- التقارير الطوعية عن الحوادث الإلكترونية:
  - من الجهات المعنية في مجال الطيران إلى المركز الوطني للأمن الإلكتروني
  - من الجهات المعنية في مجال الطيران إلى الجهات المعنية في مجال الطيران (خاصةً إذا كانت هناك تعاملات فيما بينها)
  - من الجهات المعنية في مجال الطيران إلى فرق الاستجابة لطوارئ أنظمة الكمبيوتر/مراكز تبادل المعلومات وتحليلها في مجال الطيران

— — — — — — — —

الملحق (ب)

مثال على إطار عام لتقييم وتصنيف مصداقية وموثوقية مصدر للمعلومات/المعلومات التحليلية الإلكترونية

١- السمعة وسجل الأداء:

- قيّم تاريخ المصدر وسمعته في أوساط الأمن الإلكتروني.
- ابحث عن نجاحاته السابقة ومساهماته وتعاونه مع مؤسسات القطاع.
- قيّم أداءه السابق في توفير معلومات/معلومات تحليلية دقيقة وفي الوقت المناسب عن التهديدات الإلكترونية.

٢- المصداقية والخبرة:

- قيّم مؤهلات وشهادات وخبرات الأفراد أو فرق العمل المسؤولة عن المصدر.
- انظر في خبراتهم تحديداً في مجال المعلومات/المعلومات التحليلية عن التهديدات الإلكترونية.

٣- مصادر البيانات وطرق جمعها:

- افحص ما يطبقه المصدر من طرق جمع البيانات ومصادرها.
- حدّد ما إذا كان المصدر لديه إمكانية الوصول إلى مصادر بيانات متنوعة وموثوق بها.
- قيّم دقة عمليات جمع البيانات التي يطبقها المصدر.

٤- تبادل البيانات والتعاون:

- حدد ما إذا كان المصدر يتبادل المعلومات/المعلومات التحليلية عن التهديدات الإلكترونية مع مؤسسات موثوق بها أو مع نظرائه في القطاع.
- التعاون مع كيانات الأمن الإلكتروني الأخرى يمكن أن يعزز المصداقية.

٥- الشفافية:

- قيّم مستوى الشفافية في تقارير المصدر ومنهجياته.
- قم بتقييم ما إذا كان المصدر يكشف عن مصادر بياناته وأساليبه التحليلية ووتيرة تحديث البيانات لديه.

٦- حسن التوقيت والدقة:

- قيّم قدرة المصدر على توفير معلومات/معلومات تحليلية دقيقة وفي الوقت المناسب عن التهديدات الإلكترونية.
- انظر في أداء المصدر على مر السنوات من حيث التنبؤ بالتهديدات الإلكترونية واكتشافها.

٧- التحليل والسياق:

- حلّل درجة عمق ومستوى جودة تحليل المصدر للتهديدات الإلكترونية.
- قيّم قدرة المصدر على توفير السياق حول التهديدات الإلكترونية، بما في ذلك الإسناد والتأثيرات المحتملة.

٨- التوافق مع معايير الصناعة:

- حدّد ما إذا كان المصدر يتبع معايير الصناعة وأفضل الممارسات في مجال المعلومات/المعلومات التحليلية عن التهديدات الإلكترونية، على سبيل المثال الالتزام بأطر العمل مثل STIX/TAXII وتنسيقات البيانات المشتركة.

٩- الامتثال القانوني والأخلاقي:

- تأكد من امتثال المصدر للقواعد القانونية والأخلاقية فيما يتعلق بجمع البيانات وتبادلها.

ولقياس مستوى الثقة في مصدر المعلومات/المعلومات التحليلية الإلكترونية، يمكن استخدام نظام لمنح الدرجات يستند إلى المعايير المذكورة أعلاه.

وفيما يلي مثال على نظام تقييم.

١- حدد مستوى أرجحية كل معيار بناءً على أهميته بالنسبة للاحتياجات المحددة للمؤسسة وملف المخاطر التي تواجهها.

٢- قيّم المصدر على مقياس (على سبيل المثال ١-٥) من حيث كل معيار، بحيث تكون الدرجة ٥ هي أعلى مستوى من الثقة.

٣- احسب الدرجة الكلية للثقة من خلال جمع الدرجات المرجّحة لكل معيار. وتشير الدرجة الأعلى إلى كون المصدر أكثر موثوقيةً.

فيما يلي مثال مبسط لكيفية حساب الدرجة الكلية للثقة:

- السمعة وسجل الأداء: ٤/٥
- المصداقية والخبرة: ٥/٥
- مصادر البيانات وطرق جمعها: ٣/٥
- تبادل البيانات والتعاون: ٤/٥
- الشفافية: ٤/٥
- حسن التوقيت والدقة: ٤/٥
- التحليل والسياق: ٥/٥
- التوافق مع معايير الصناعة: ٤/٥
- الامتثال القانوني والأخلاقي: ٥/٥

يمكن أن تكون الدرجة الكلية لموثوقية المصدر:

(٠,١*٤) + (٠,١٥*٥) + (٠,١*٣) + (٠,١*٤) + (٠,١*٤) + (٠,١*٤) + (٠,١٥*٥) + (٠,١*٤) + (٠,١*٥) = **٤,٣٠**

— — — — — — — —

الملحق (ج)

مثال على إطار عام لتقييم مدى معقولية/مقبولية المعلومات/المعلومات التحليلية الإلكترونية

١- التوثيق من مصادر متعددة:

- قيّم ما إذا كانت المعلومات/المعلومات التحليلية عن التهديدات الإلكترونية مدعومة من مصادر مستقلة متعددة، فمثلاً قيام مصادر متعددة بالإبلاغ عن نفس المعلومات يزيد من معقولية المعلومات.

٢- الاتساق مع التهديدات والتكتيكات المعروفة:

- حدّد ما إذا كانت المعلومات/المعلومات التحليلية عن التهديدات الإلكترونية تتوافق مع التهديدات الإلكترونية المعروفة وتقنيات وتكتيكات الهجوم، فعدم الاتساق مثلاً ربما يشير إلى مستوى أقل من المعقولية.

٣- التفاصيل الفنية والأدلة:

- افحص وجود تفاصيل فنية وأدلة تدعم المعلومات/المعلومات التحليلية عن التهديدات الإلكترونية، فالأدلة الفنية القوية مثلاً تزيد من مستوى المعقولية.

٤- الإسناد والدافع:

- قيّم إسناد التهديد الإلكتروني إلى جهات أو مجموعات محددة.
- انظر في دوافع هذه الجهات الفاعلة وما إذا كانت تتماشى مع التهديد الإلكتروني المبلغ عنه.

٥- التوقيت والسياق:

- حلّل توقيت التهديد الإلكتروني وسياقه ضمن المشهد العام للأمن الإلكتروني.
- انظر فيما إذا كان التهديد الإلكتروني يتماشى مع الأحداث أو الاتجاهات الحالية.

٦- الدقة التاريخية:

- تقيّم دقة المصدر في الإبلاغ عن التهديدات الإلكترونية على مر السنين، فوجود سجل ثابت من الإبلاغ الدقيق مثلاً يزيد من درجة المعقولية.

٧- التحقق من صحة المعلومات بمراجعة الأقران ومجموعات الثقة:

- حدّد ما إذا كان قد تم التحقق من صحة المعلومات/المعلومات التحليلية المتعلقة بالتهديدات الإلكترونية أو المصادقة عليها من قبل أقران موثوق بهم أو مجموعات موثوقة بها في هذا المجال، فمصادقة الأقران مثلاً على صحة المعلومات يعزز من معقوليتها.

٨- الإشارات التحذيرية وأوجه الخلل:

- ابحث عن الإشارات التحذيرية أو أوجه الخلل أو العناصر المريبة في المعلومات/المعلومات التحليلية عن التهديد الإلكتروني؛ ويمكن أن تؤدي معالجة هذه المسائل وشرحها إلى تحسين مستوى المعقولية.

ولقياس مستوى المعقولية/المقبولية في المعلومات/المعلومات التحليلية الإلكترونية، يمكن استخدام نظام لمنح الدرجات يستند إلى المعايير المذكورة أعلاه.

وفيما يلي مثال لنظام تقييم.

١- حدد مستوى أرجحية كل معيار بناءً على أهميته وصلته بتقييم المخاطر الإلكترونية الذي تجريه المؤسسة.
٢- قيّم معقولية التهديد على مقياس (على سبيل المثال ١-٥) من حيث كل معيار، بحيث تكون الدرجة ٥ هي أعلى مستوى من المعقولية.
٣- احسب الدرجة الكلية للمعقولية من خلال جمع الدرجات المرجّحة لكل معيار. وتشير الدرجة الأعلى إلى كون التقرير التحليلي عن التهديد أكثر معقوليةً.

فيما يلي مثال مبسط لكيفية حساب الدرجة الكلية للمعقولية/المصداقية:

- التوثيق من مصادر متعددة: ٤/٥
- الاتساق مع التهديدات والتكتيكات المعروفة: ٣/٥
- التفاصيل الفنية والأدلة: ٥/٥
- الإسناد والدافع: ٤/٥
- التوقيت والسياق: ٤/٥
- الدقة التاريخية: ٤/٥
- التحقق من صحة الأقران ومجموعات الثقة: ٤/٥
- الإشارات التحذيرية وحالات الخلل ٣/٥

يمكن أن تكون درجة الكلية للمعقولية/المصداقية:

(٠,١٥*٤)+(٠,١٥*٣)+(٠,١٥*٥)+(٠,١*٤)+(٠,١٥*٤)+(٠,١*٤)+ (٠,١*٤)+(٠,١*٣)=٣,٩٠

— — — — — — — —

الملحق (د)

مثال على نظام الثقة بالمعلومات الإلكترونية

يصف هذا الملحق كود الأميرالية[١٣] كمثال آخر لطريقة تقييم عناصر مجمّعة من المعلومات التحليلية.

يمكن استخدام هذا المقياس عند تبادل المعلومات لتقييم موثوقية المصدر ومعقولية المعلومات. تعتمد الطريقة على ترميز مكوّن من رمزين (حرف ورقم)، حيث يقيّم الحرف موثوقية المصدر ويعكس الرقم مستوى الثقة التقديري في المعلومات.

موثوقية المصدر

يتم تقييم موثوقية المصدر بناءً على تقييم فني لقدرته، أو في حالة المصادر البشرية للمعلومات التحليلية، على أساس أدائه على مر السنين. ويستخدم الترميز حرفاً أبجدياً من (أ) إلى (و) لتقييم درجة موثوقية المصدر على النحو التالي.

رمز الموثوقية	الموثوقية	الشرح
أ	موثوق به تماماً	لا يوجد شك في الصدق أو الجدارة بالثقة أو الكفاءة؛ لديه تاريخ من الموثوقية الكاملة.
ب	موثوق به عادةً	شك بسيط في المصداقية أو الجدارة بالثقة أو الكفاءة؛ لديه تاريخ من المعلومات الصحيحة في معظم الأوقات.
ج	موثوق به إلى حد ما	شكوك حول المصداقية أو الجدارة بالثقة أو الكفاءة؛ لكن لديه تاريخ من تقديم معلومات صحيحة في الماضي.
د	غير موثوق به عادةً	شك كبير في المصداقية أو الجدارة بالثقة أو الكفاءة، لكنه قدم معلومات صحيحة في الماضي.
هـ	موثوق به	يفتقر إلى الموثوقية والجدارة بالثقة والكفاءة؛ تاريخ من المعلومات غير الصحيحة.
و	لا يمكن تقييم درجة الموثوقية	لا يوجد أساس لتقييم موثوقية المصدر.

[١٣] يمكن الاطلاع على تفاصيل هذه الطريقة في الصفحتين ٥٩–٦٠ من Joint Doctrine Publication 2-00, Intelligence, Counter-intelligence and Security Support to Joint Operations (الإصدار الرابع)، الذي يمكن الاطلاع عليه علي:
https://www.gov.uk/government/publications/jdp-2-00-understanding-and-intelligence-support-to-joint-operations

معقولية المعلومات

يتم تقييم معقولية عنصر ما من المعلومات بناءً على احتمالية ومستويات توثيق صحته من مصادر أخرى. يستخدم الترميز أرقاماً من ١ إلى ٦ لتحديد درجة معقولية المصدر على النحو التالي.

درجة المعقولية	المعقولية	الشرح
١	مؤكد من قبل مصادر أخرى	مؤكد من قبل مصادر مستقلة أخرى؛ منطقي في حد ذاته؛ متوافق مع معلومات أخرى حول الموضوع.
٢	من المرجح أن يكون صحيحاً	غير مؤكد؛ منطقي في حد ذاته؛ متوافق مع معلومات أخرى عن الموضوع.
٣	من المحتمل أن يكون صحيحاً	غير مؤكد؛ منطقي في حد ذاته بدرجة معقولة؛ يتوافق مع بعض المعلومات الأخرى حول الموضوع.
٤	مشكوك فيه	غير مؤكد؛ ممكن ولكن غير منطقي؛ لا توجد معلومات أخرى عن الموضوع.
٥	غير مرجح	غير مؤكد؛ غير منطقي في حد ذاته؛ يتعارض مع معلومات أخرى عن الموضوع.
٦	لا يمكن الحكم على الصحة	لا يوجد أساس لتقييم صحة المعلومات.

ويمكن الجمع بين الجداول أعلاه والجدول التالي.

موثوقية المصدر	معقولية المعلومات الإلكترونية
أ) موثوق به تماماً	١- مؤكد من قبل مصادر أخرى
ب) موثوق به عادةً	٢- من المرجح أن يكون صحيحاً
ج) موثوق به إلى حد ما	٣- من المحتمل أن يكون صحيحاً
د) غير موثوق به عادةً	٤- مشكوك فيه
هـ) موثوق به	٥ -غير مرجح
و) لا يمكن تقييم درجة الموثوقية	٦- لا يمكن الحكم على الصحة

هذان مثالان على تصنيفات المعلومات الإلكترونية المتبادلة:

- C4 ويُقصد به: مصدر موثوق به إلى حد ما ومعلومات مشكوك فيها.
- A1 ويُقصد به: مصدر موثوق به تماماً ومعلومات مؤكدة من مصادر أخرى.

وعلى الرغم من أن التقييم يسمح بالتقدير الشخصي، يتيح التصنيف أداةً مفيدةً تساعد متلقي المعلومات الإلكترونية في إجراء تقييمه وتحليله الخاص للمعلومات الإلكترونية .

— — — — — — — —

الملحق (هـ)

النموذج الموصى به لاتفاق رسمي لتبادل المعلومات الإلكترونية

ينبغي أن يتضمن الاتفاق الرسمي لتبادل المعلومات الإلكترونية الأقسام التالية:

- ✓ الديباجة التي تتضمن أسماء الأطراف ووصف لها.
- ✓ التعاريف والمختصرات.
- ✓ النطاق: يصف نطاق الوثيقة ويشير إلى الملحق ١ الذي يوضح نوع المعلومات الإلكترونية التي سيتم تبادلها.
- ✓ حقوق والتزامات متلقي المعلومات (المتلقي).
- ✓ مصادر المعلومات: من سيقدم أي معلومات إلى من واستناداً إلى أي مصادر، وما إذا كان مصدر المعلومات يلزم الكشف عنه.
- ✓ القيود المفروضة على ماهية المعلومات التي يمكن تبادلها ومع من، مع مراعاة القوانين السارية، وحقوق الملكية الفكرية، والمعلومات التجارية السرية، وتعريف علامات بروتوكول الإشارات الضوئية، وما إلى ذلك.
- ✓ شكل المعلومات المتبادلة وتواترها.
- ✓ وسائل نقل المعلومات (مثل الرسائل والهاتف والرسائل النصية والبريد الإلكتروني والمستودع، وما إلى ذلك)، بما في ذلك حماية وضمان سرية وسلامة وتوافر المعلومات المنقولة رقمياً.
- ✓ متطلبات الجودة: يصف الإجراءات التي يجب أن يقوم بها المُرسِل قبل إرسال المعلومات. كما يصف أيضاً وسائل ضمان سلامة وجودة المعلومات التي يتم تبادلها، بما في ذلك على سبيل المثال حجب الهوية و/أو التعقيم.
- ✓ التخزين وحفظ السجلات: يصف سياسات وإجراءات أرشفة المعلومات المتبادلة. كما يصف الحد الأدنى لمدة أرشفة المعلومات المرسلة/المتلقاة لأغراض مراقبة جودة الاتفاق والعلاقة بين الأطراف.
- ✓ التكلفة: يحدد الطرف الذي يتحمل تكلفة تبادل المعلومات. ويُوصى بأن يتحمل كل طرف التكلفة الخاصة به المتعلقة بتنفيذ الاتفاق.
- ✓ النُظُم الإدارية وإجراءات إدارة التغيير في الاتفاق.
- ✓ المراسلات والإشعارات المتعلقة بالاتفاق.
- ✓ المسؤولية القانونية: حيث يتم وصف التزامات الأطراف. ويُوصى بإبراء الطرف المُرسِل من أي مسؤولية تتعلق بالمعلومات المتبادلة.
- ✓ معالجة البيانات الشخصية: يصف كيفية معالجة البيانات الشخصية، بما في ذلك القوانين واللوائح المعمول بها.
- ✓ تسوية المنازعات: كيف وبموجب أي قوانين ستتم معالجة المنازعات المتعلقة بالاتفاق. ويُوصى بأن تحاول الأطراف حل النزاعات ودياً أولاً، ثم إذا لم تنجح عن طريق الوساطة في ولاية قضائية يُتفق عليها.
- ✓ الاتفاق بأكمله وتعديلاته: حيث يتم وصف أسبقية مختلف أجزاء الاتفاقية.
- ✓ تاريخ بدء نفاذ الاتفاق ومدته وإجراءات تجديده وإنهائه.
- ✓ الاعتماد: توقيعات الأفراد المفوضين عن كل طرف.
- ✓ الملاحق:
  - الملحق ١ – المعلومات التي سيتم تقديمها: يصف نوع المعلومات التي سيرسلها كل طرف.
  - الملحق ٢: تعريف علامات بروتوكول الإشارات الضوئية، بما في ذلك الإشارة إلى قاعدة FIRST بشأن بروتوكول الإشارات الضوئية.

— — — — — — — —

الملحق (و)

MISP – المنصة مفتوحة المصدر للمعلومات التحليلية عن التهديدات وتبادلها

MISP [١٤]هي منصة لتبادل وتخزين والربط بين مؤشرات الاختراقات (IoCs) التي تؤدي إلى الهجمات الإلكترونية الموجّهة، بالإضافة إلى المعلومات التحليلية عن التهديدات الإلكترونية مثل المعلومات عن الجهات الفاعلة للتهديدات، ومعلومات عن الاحتيال المالي، وما إلى ذلك .

وهي عبارة عن منصة مجانية مفتوحة المصدر تتيح تبادل المعلومات التحليلية عن التهديدات الإلكترونية، تسمح للمؤسسات بإنشاء مجتمعات لتبادل المعلومات مثل معلومات التهديدات الإلكترونية والمؤشرات ومعلومات عن الجهات الفاعلة للتهديدات أو أي نوع من التهديدات الإلكترونية التي يمكن إدراجها في المنصة.

ويستفيد مستخدمو منصة MISP من المعرفة التعاونية حول البرمجيات الخبيثة أو التهديدات الإلكترونية الموجودة. وتُستخدم منصة MISP من خلال إنشاء "مجتمعات" للمستخدمين، بحيث يجري تبادل المعلومات داخل مجتمع المستخدمين. والهدف من هذه المنصة القائمة على الثقة هو المساعدة في تحسين التدابير المضادة المستخدمة ضد الهجمات الإلكترونية الموجّهة وتنفيذ الإجراءات الوقائية والكشف.

ويُوصى بأن تنظر الدول والجهات المعنية في مجال الطيران في استخدام منصة MISP، أو أي منصة مماثلة، كوسيلة/طريقة لتبادل المعلومات الإلكترونية حيث أن المنصة تتيح ما يلي:

- الاستخدام الآلي للمعلومات الواردة من أجل تحديث أنظمة الأمن المختلفة، مثل مراكز إدارة المعلومات الأمنية والأحداث/مراكز العمليات الأمنية (SIEM/SOC)، وجدران الحماية، وبرامج مكافحة الفيروسات، وأنظمة كشف ومنع التطفل/أنظمة منع التطفل (IDPS/IPS)؛
- تبادل المعلومات الإلكترونية بسرعة لأن الوقت قد يكون عاملاً حاسماً في حالة تبادل المعلومات المتعلقة بالاستجابة الجارية لحادث إلكتروني ما؛
- تحديث المعلومات الإلكترونية المتعلقة بالحادث الإلكتروني بمعلومات إضافية ذات صلة بالمسألة عند توفرها؛
- تبادل المعلومات عن جميع أنواع العلامات في بروتوكول الإشارات الضوئية عبر منصة MISP. ومع ذلك، لا يتم تبادل المعلومات التي تحمل العلامة TLP:RED على منصة MISP إلا عندما يتألف مجتمع المستخدمين من عدد محدود من الأشخاص الذين يوافقون على تبادل هذه المعلومات. وبشكل عام، لا يتم تبادل المعلومات التي تحمل العلامة TLP:RED على منصة MISP، وإنما من خلال وسائل بديلة (كالهاتف والرسائل النصية والبريد الإلكتروني).

—انتهى —

[١٤] لمزيد من المعلومات عن منصة MISP: https://www.circl.lu/services/misp-malware-information-sharing-platform/