منتدى الأفرقة المعنية بالأمن والتصدي للحوادث (FIRST.Org)

إطار خدمات أفرقة التصدي للحوادث الأمنية (SIRT)

الإصدار 1.0

إطار خدمات أفرقة التصدي للحوادث الأمنية (SIRT)

مقدمة

فيما يلي قائمة الخدمات التي يمكن لمنظمة لفريق من أفرقة التصدي للحوادث الأمنية أن تنظر في تنفيذها لتلبية احتياجات الجهات التي تخدمها، والآليات اللازمة لمعالجة الثغرات في القدرة على القيام بذلك. وتهدف هذه القائمة لإيضاح الخدمات التقليدية التي تقوم بها أفرقة التصدي للحوادث الأمنية فضلاً عن الخدمات التي ظهرت مؤخراً والتي تضطلع بها الأفرقة والمؤسسات القائمة فيما تتطور هذه الخدمات. وتضم هذه الوثيقة قائمة الخدمات التي ينبغي أن تشكل إطار خدمات أفرقة التصدي للحوادث الأمنية.

وتنقسم كل خدمة أدناه إلى الوظائف الأساسية والوظائف الفرعية التي تدعم أداء أفرقة التصدي للحوادث الأمنية في تلك الخدمة لدعم مهمتها الأوسع نطاقاً. وإذ تمثّل العديد من الوظائف والوظائف الفرعية هنا على أنها متفردة، يرجى الانتباه إلى أنها تُستخدم لتفعيل تقديم خدمات و/أو وظائف متعددة، ويمكن أن يعتمد بعضها على البعض الآخر. وعلى الرغم من أن هذه الوثيقة تعترف بوجود تلك العلاقات، فهي لا تسعى إلى تحديد هذه العلاقات البينية في هذه المرحلة.

ولاحقاً، ستجمَّع الخدمات وفق تشابهها في مجال خدمات. وفي البداية، ستركز هذه الورقة على ثلاثة أنواع من أفرقة التصدي للحوادث: فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) الوطني؛ وفريق التصدي للحوادث الأمنية الحاسوبية القطاعي (البنية التحتية الحرجة)؛ وفريق التصدي للحوادث الأمنية الحاسوبية المؤسسي (التنظيمي). وستضيف نسخة متابعة من إطار الخدمات نوعين إضافيين أيضاً: أفرقة التصدي لحوادث أمن المنتجات (PSIRT)؛ والتصدي الإقليمية/متعددة الأطراف للحوادث. وستوفر وثائق مصاحبة مستقبلية أمثلة نموذجية لكل نوع ومجالات خدمة/خدمات/وظائف التي ترى عادة في بناء برنامج أساسي. وستُنشر أيضاً وثيقة إضافية تحدد المهام والمهام الفرعية وكذلك الإجراءات اللازمة لكل وظيفة فرعية بغية تطوير وحدات تدريبية. ويجري كذلك تنسيق مستويات النضج مع العديد من الأطراف الأخرى لضمان العمل من أجل توافق الآراء على الصعيد العالمي.

الغرض

يحدد إطار خدمات فريق التصدي للحوادث الأمنية الحاسوبية مجموعة من الخدمات والوظائف التي تنفذها أفرقة التصدي للحوادث الأمنية الحاسوبية لخدمة الجهات التي تخدمها. والغرض منه هو تسهيل التشغيل البيني لفريق التصدي للحوادث الأمنية الحاسوبية وأنشطة تنمية القدرات العالمية والتعليم والتدريب، من خلال استخدام المصطلحات المقبولة والنهج المتبع لدى المجتمع العالمي في ما يؤديه فريق التصدي للحوادث الأمنية الحاسوبية.

السجل الزمني

استُخدمت قائمة خدمات فريق التصدي للطوارئ الحاسوبية (CERT)/مركز تنسيق فريق التصدي للحوادث الأمنية الحاسوبية (CC CSIRT) في كثير من الحالات لتكون بمثابة وصف متسق وقابل للمقارنة لأفرقة التصدي للحوادث الأمنية الحاسوبية وخدماتها المقابلة. وفي التقييمات الأخيرة لقوائم خدمات فريق التصدي للحوادث الأمنية الحاسوبية القائمة، تقرر أن قائمة خدمات فريق التصدي للطوارئ الحاسوبية/مركز التنسيق قد تجاوزها الزمن رغم استخدامها على نطاق واسع وتكيفها، إذ تنقصها مكونات رئيسية تمثل مهمة أفرقة التصدي للحوادث الأمنية الحاسوبية في العصر الحديث. وأدرك منتدى أفرقة الأمن والتصدي للحوادث (FIRST) المهتم في تمكين تطوير وإنضاج أفرقة التصدي للحوادث الأمنية الحاسوبية على الصعيد العالمي، بأن ذلك كان شطراً أساسياً في تأطير وضع برنامج تعليمي شامل لفريق التصدي للحوادث الأمنية الحاسوبية. ونظراً للامتداد الجغرافي والوظيفي لأعضاء منتدى FIRST، تقرر أن المجتمع الذي يضمه هو مصدر مناسب لإيضاح وتمثيل الخدمات التي تقدمها أفرقة التصدي للحوادث الأمنية الحاسوبية بصورة قطعية. وتقرر أيضاً أن الحاجة تدعو لانتهاج نهج مماثل في خدمات فريق التصدي لحوادث أمن المنتجات، وأن يُدرَج ذلك النهج في إصدار لاحق لإطار الخدمات هذا.

التعاريف

نعرّف استخدام بعض المصطلحات على النحو الذي تُستخدم فيه ضمن هذه الوثيقة؛ علماً بأن مصطلحات مثل مجالات الخدمة والخدمات والوظائف تحدد *ماذا* يجري على مستويات مختلفة من التفاصيل، في حين أن المهام والإجراءات تحدد كيف يجرى ذلك على مستويات مختلفة من التفاصيل. ويجري نشر المهام والإجراءات في وثيقة مرفقة، يمكن وسيتم تحديثها بتواتر أكبر:

- **مجال الخدمة** - خدمات مجموعة ذات صلة بجانب مشترَك. وهي تساعد على تنظيم الخدمات وفق تصنيف إجمالي تسهيلاً للفهم. (وسيجري تطوير هذا المجال في الإصدار 2.0).

- **الخدمة** - مجموعة إجراءات متماسكة يمكن تمييزها تسعى إلى نتيجة محددة نيابةً عن الجهات التي يخدمها فريق التصدي للحوادث. وهي قائمة الوظائف المستخدمة لتنفيذ الخدمة.

- **الوظيفة** - وسيلة لتحقيق هدف أو مهمة لخدمة محددة. وهي قائمة المهام التي يمكن القيام بها كجزء من الوظيفة.

- **المهام** - قائمة الإجراءات التي يجب تنفيذها لإنجاز المهمة

- **الإجراءات** - قائمة بكيفية القيام بشيء ما على مستويات مختلفة من التفاصيل/النضج

- **القدرة** – نشاط قابل للقياس يمكن القيام به كجزء من أدوار منظمة ومسؤولياتها. ولأغراض إطار خدمات أفرقة التصدي للحوادث الأمنية، يمكن أن تعرَّف القدرات كالخدمات الأوسع، أو كالوظائف المطلوبة أو الوظائف الفرعية أو المهام أو الإجراءات.

- **السعة** - عدد العمليات أو الوقائع المتزامنة لقدرة خاصة يمكن أن تنفذها المنظمة قبل أن تتعرض لنوع ما من استنفاد الموارد.

- **النضج** - مدى فعالية تنفيذ منظمة لقدرة معينة ضمن مهام وسلطات المنظمة. وهو مستوى الكفاءة المتحققة سواء في الإجراءات أو المهام أو في مجموع الوظائف أو الخدمات.

أنواع أفرقة التصدي للحوادث

- **الفريق الوطني للتصدي للحوادث الأمنية الحاسوبية (CSIRT)** - يشير الفريق الوطني للتصدي للحوادث الأمنية الحاسوبية إلى كيان تشكله هيئة وطنية ليقوم بالتنسيق على المستوى الوطني للتصدي لحوادث الأمن السيبراني. وتشمل الجهات التي يخدمها الفريق عموماً جميع الإدارات والوكالات الحكومية، وهيئات إنفاذ القانون والمجتمع المدني. وهو أيضاً، بشكل عام، السلطة التي تتفاعل مع أفرقة التصدي للحوادث الأمنية الحاسوبية الوطنية في البلدان الأخرى، وكذلك مع الجهات الفاعلة الإقليمية والدولية.

فريق التصدي للحوادث الأمنية الحاسوبية القطاعي/المعني بالبنية التحتية الحرجة - هو الفريق المسؤول عن مراقبة حوادث الأمن السيبراني المتعلقة بقطاع معين (مثل الطاقة والاتصالات والتمويل)، وعن إدارتها والتصدي لها.

الفريق المؤسسي (التنظيمي) للتصدي للحوادث الأمنية الحاسوبية - يشير الفريق المؤسسي للتصدي للحوادث الأمنية الحاسوبية إلى الفريق المسؤول عن مراقبة حوادث الأمن السيبراني التي تؤثر على البنى التحتية والخدمات الداخلية لتكنولوجيا المعلومات والاتصالات في منظمة محددة، وعن إدارتها والتعامل معها.

فريق التصدي الإقليمي/متعدد الأطراف للحوادث الأمنية الحاسوبية - يشير فريق التصدي **الإقليمي/متعدد الأطراف** للحوادث الأمنية الحاسوبية إلى فريق أو نفر تضم عضويته ممثلين عن دوائر مختلفة ويتولى المسؤولية عن مراقبة حوادث الأمن السيبراني المتصلة بمنطقة معينة أو عدد من المنظمات، وعن إدارة هذه الحوادث والتصدي لها.

فريق التصدي لحوادث أمن المنتجات (PSIRT) - فريق التصدي لحوادث أمن المنتجات هو فريق داخل كيان تجاري (منفذ بيع عادة) يدير تلقي المعلومات بشأن الثغرات الأمنية المتعلقة بمنتجات أو خدمات تتعاطى بها المنظمة تجارياً، ويدير التحقيق فيها والإبلاغ عنها داخلياً وللعموم.

الخدمة 1 إدارة الحوادث

الوظيفة 1.1 **التعامل مع الحوادث:** الخدمات المتعلقة بإدارة الحدث السيبراني، وتشمل تنبيه الجهات المخدَّمة وتنسيق الأنشطة المرتبطة بالتصدي لحادثة والتخفيف من ضررها والتعافي منها. ويعتمد التعامل مع الحوادث على تحليل الأنشطة المعرَّفة في فقرة "التحليل".

الوظيفة الفرعية 1.1.1 **جمع المعلومات**: الخدمات المتعلقة بتلقف المعلومات ذات الصلة بالأحداث والحوادث، وتصنيفها وتخزينها، وهي تشمل ما يلي:

- **جمع التقارير عن الحوادث**: جمع التقارير بشأن الأحداث والحوادث الضارة أو المشبوهة من الجهات المخدَّمة وأطراف ثالثة (مثل أفرقة أمنية أخرى أو معلومات استخباراتية تجارية)، بالأشكال اليدوية أو المؤتمتة أو القابلة للقراءة الآلية على السواء.
- **جمع البيانات الرقمية**: جمع وتصنيف البيانات الرقمية التي يمكن أن تكون مفيدة في فهم نشاط الحادثة (مثل صور القرص الحاسوبي، والملفات، وسجلات/تدفقات شبكة)، دون ضمان هذه الفائدة المرجوة.
- **أنواع البيانات الأخرى (غير الرقمية)**: جمع وتصنيف البيانات غير الرقمية (صحائف تسجيل الدخول المادية، والرسوم البيانية للمعمارية، ونماذج الأعمال التجارية، وبيانات تقييم الموقع، والسياسات المتبعة، وأطر المخاطر في المؤسسة، وما إلى ذلك).
- **جمع الصنائع**: العمليات التجارية والتقنية المستخدمة لتلقف الصنائع التي يُعتقد أنها بقايا نشاط مُنَاوِئ، وتصنيفها وتخزينها وتعقبها.
- **جمع الأدلة**: أعمال جمع المعلومات والبيانات لإمكانية استخدامها في أنشطة إنفاذ القانون، وهي تتضمن في كثير من الأحيان التقاط بيانات شرحية بشأن مصدر المعلومات وأسلوب جمعها ومالكها وحائزها.

الوظيفة الفرعية 2.1.1 **التصدي**: الخدمات ذات الصلة بالتخفيف من تأثير حادثة والعمل على استعادة وظائف مصالح الأعمال لدى الجهة المخدَّمة.

- **الاحتواء**: وقف الضرر المباشر والحد من مدى نشاط ضار من خلال إجراءات تكتيكية على المدى القصير (على سبيل المثال، عرقلة الحركة أو اصطفاؤها)؛ ويمكن أيضاً أن ينطوي على استعادة التحكم في الأنظمة.
- **التخفيف**: منع المزيد من الضرر من خلال الاجتثاث، أو تنفيذ عمل التفافي، أو تنفيذ استراتيجيات احتواء أكثر تعمقاً وشمولاً.
- **الإصلاح**: تنفيذ التغييرات اللازمة فيما يطاله الضرر ضمن ميدان أو بنية تحتية أو شبكة، لتدارك هذا النوع من النشاط ومنع تكراره. ويشمل ذلك تعزيز التموضع التنظيمي الدفاعي والاستعداد التشغيلي بتغيرات سياساتية والمزيد من التدريب والتعليم.
- **الاسترداد**: استعادة سلامة أنظمة متضررة وإرجاع البيانات والأنظمة والشبكات المتضررة إلى حالة تشغيلية غير متردية.

الوظيفة الفرعية 3.1.1 **التنسيق**: نشاط تبادل المعلومات والتحليل المتروي الداخلي والخارجي على حد سواء لفريق التصدي للحوادث الأمنية الحاسوبية. ويحدث ذلك في المقام الأول عندما يعتمد فريق التصدي للحوادث الأمنية الحاسوبية على الخبرات والموارد الخارجة عن سيطرته المباشرة لتفعيل الإجراءات اللازمة للتخفيف من ضرر حادثة. ومن خلال تقديم التنسيق الثنائي أو متعدد الأطراف، يشارك فريق التصدي للحوادث الأمنية الحاسوبية في تبادل المعلومات لتمكين تلك الموارد القادرة على اتخاذ الإجراءات اللازمة من القيام بذلك أو لمساعدة الآخرين في كشف أنشطة الخصوم الجارية أو الحماية منها أو تداركها.

الوظيفة الفرعية 4.1.1 **تتبع الحوادث**: توثيق المعلومات بشأن الإجراءات المتخذة لحل حادثة، بما في ذلك المعلومات الهامة التي جمُعت، والتحليل الذي جرى وخطوات التدارك والتخفيف المتخذة، والاختتام والحل.

الوظيفة 2.1 **إدارة الثغرة الأمنية والتشكيلة والأصول**: الخدمات ذات الصلة بفهم الثغرات الأمنية وتداركها، وبإشكالات التشكيلة وجرد الأصول.

الوظيفة الفرعية 1.2.1**البحث الساعي لاكتشاف الثغرة الأمنية**: تحديد الثغرات الأمنية الجديدة من خلال البحث والتجريب (أي اختبار البرمجيات العشوائي والهندسة العكسية).

الوظيفة الفرعية 2.2.1**الإبلاغ عن ثغرة أمنية**: الأعمال والعمليات التقنية المستخدمة لتلقف التقارير عن الثغرات الأمنية وتصنيفها وتخزينها وتعقبها.

الوظيفة الفرعية 3.2.1**التنسيق بشأن الثغرات الأمنية**: إخطار المنظمات المناسبة بوجود ثغرة أمنية كي تقوم بإصلاحات وتطوق التأثيرات المحتملة لاستغلالها.

الوظيفة الفرعية 4.2.1**تدارك السبب الجذري لثغرة أمنية**: تنفيذ الإجراءات التصحيحية الرسمية اللازمة لتصحيح ثغرة أمنية تم تحديدها. وعادةً ما يقوم بائع المنتَج بذلك.

الخدمة 2 تحليل

الوظيفة 1.2 **تحليل حادثة**: الخدمات المتعلقة بتحديد وتشخيص المعلومات بشأن أحداث أو حوادث مثل مجال التطبيق أو الأطراف المتضررة أو الأنظمة المعنية والأطر الزمنية (الاكتشاف، الواقعة، الإبلاغ) والحالة (مستمرة أم مكتملة).

[ملاحظة: يجري مزيد من التحليل المتعمق لحادثة من خلال مهام تحليل أخرى أكثر تركيزاً، مثل تحليل الصنائع، أو سوء التشكيلة، أو الثغرة الأمنية، أو الشبكة، أو المعلومات الحاسوبية القضائية.]

الوظيفة الفرعية 1.1.2**التحقق من حادثة**: التحقق القاطع من أن الحادثة المبلَّغ عنها قد وقعت بالفعل وكان له تأثير ما على الأنظمة المعنية.

الغرض: تقديم دليل تقني على أن الحدث هو حادثة أمنية، أو خطأ في الشبكة أو في العتاد، وتحديد التداعيات الأمنية المحتملة والضرر الذي تتعرض له سرية أصول المعلومات و/أو تيسرها و/أو سلامتها.

***النتيجة**: تحديد ما إذا كان الحدث المبلَّغ عنه هو في الواقع حادثة تستدعي التعامل معها أو ما إذا كان يمكن أن يسجَّل البلاغ في الأنظمة ذات الصلة ويُغلق دون اتخاذ مزيد من الإجراءات. والوقوف على حيثيات الأحداث التي حملت الجهة المخدَّمة على الاعتقاد بأن حادثة أمنية قد وقعت بالفعل وتحديد ما إذا كانت هناك نوايا خبيثة أو إذا كان هناك سبب مختلف - مثل سوء التشكيلة أو عطل في العتاد.*

الوظيفة الفرعية 2.1.2**تحليل التأثير**: تحديد وتشخيص التأثير على وظيفة الأعمال التي تدعمها الأنظمة المعنية.

الغرض: تحديد حجم الحادثة ونطاقها بما يشمل الأجزاء المتضررة من البنية التحتية والخدمات والبيانات، والدائرة أو المنظمة. ويمكن انتهاج النهج العام للتدارك على أساس هذا التحليل.

***النتيجة**: تحديد الضرر (المحتمل) الذي أوقعته أو قد توقعه حادثة. وعدم الاكتفاء بتحديد الجوانب التقنية، بل إدراج أي تغطية إعلامية كذلك، وأي فقدان للثقة أو المصداقية، وأي ضرر للسمعة.*

الوظيفة الفرعية 3.1.2**الدروس المستفادة**: إجراء استعراض بعد التنفيذ لتحديد التحسينات على العمليات والسياسات والإجراءات والموارد والأدوات للمساعدة في التخفيف من وطأة الحادثة ومنع أي خرق في المستقبل.

الغرض: تحديد ما جرى على غير ما يرام، وتنفيذ تدابير وقائية، وتبادل الدروس المستفادة لأمن المجتمع المعني من خلال المنشورات والعروض.

***النتيجة**: مجموعة من التوصيات التي يتعين أخذها بعين الاعتبار كتعديلات محتملة لأنظمة المعلومات والعمليات والإجراءات ضمن الدوائر ذات الصلة في المنظمة المتضررة.*

الوظيفة 2.2 **تحليل الصنائع**: الخدمات ذات الصلة بفهم قدرات ومآرب الصنائع (كملفات البرمجيات الخبيثة والبرمجيات المستغِلة والبريد الطفيلي والتشكيلة) وفهم سبل إيصالها وكشفها وتحييدها.

الغرض: *كجزء من عملية التعامل مع حادثة، يمكن أن تصادَف الصنائع الرقمية في الأنظمة المتضررة بها أو في مواقع توزيع البرمجيات الخبيثة. وقد تكون الصنائع من مخلفات هجوم دخيل، مثل البرامج النصية والملفات والصور وملفات التشكيلة والأدوات ومخرجات أداة، وسجلات، وما إلى ذلك. ويجري تحليل الصنائع لمعرفة كيف استخدمها دخيل، من أجل الدخول مثلاً إلى أنظمة منظمة وشبكاتها، أو لتحديد ما فعله الدخيل ذات مرة في النظام. ويسعى تحليل الصنائع للتعرف على كيفية عمل الصنيعة من تلقاء نفسها أو بالاشتراك مع غيرها من الصنائع. ويمكن تحقيق ذلك من خلال أنواع مختلفة من الأنشطة بما في ذلك: تحليل السطح، والهندسة العكسية، وتحليل وقت التشغيل، والتحليل المقارن. ويقدم كل نشاط مزيداً من المعلومات عن الصنائع. وتشمل أساليب التحليل، على سبيل المثال لا الحصر، تحديد نوع وخصائص الصنائع بالمقارنة مع الصنائع المعروفة، ورصد تنفيذ الصنيعة في بيئة وقت التشغيل، وتفكيك الصنائع الاثنينية وتفسيرها. ومن خلال العمل على تحليل الصنيعة (الصنائع)، يحاول المحلل إعادة بناء ما فعله الدخيل وتحديده، وذلك لتقييم الأضرار، ووضع حلول للتخفيف من أفاعيل الصنائع، وتقديم معلومات للجهات المخدَّمة وغيرها من الباحثين.*

النتيجة: *فهم طبيعة الصنيعة الرقمية المنتشَلة إلى جانب علاقتها مع غيرها من الصنائع والهجمات والثغرات الأمنية المستغَلة. وتحديد الحلول للتخفيف من وطأة الصنيعة (الصنائع) المحلَّلة من خلال فهم التكتيكات والتقنيات والإجراءات التي يلجأ إليها المتسللون لاختراق أنظمة وشبكات وتنفيذ الأنشطة الخبيثة.*

الوظيفة الفرعية 1.2.2 **تحليل السطح:** تحديد وتشخيص المعلومات الأساسية والبيانات الشرحية عن الصنائع (كنوع الملف، وخرج السلاسل، والاختزالات التجفيرية، وحجم الملف، واسم الملف)؛ إلى جانب استعراض أي معلومات من مصادر عامة أو خاصة عن الصنائع.

الغرض: *كخطوة أولى في جمع المعلومات الأساسية، يقارن تحليل السطح المعلومات التي جُمعت من الصنيعة مع الصنائع العامة والخاصة الأخرى و/أو مستودع تواقيع. وتُجمع كل المعلومات المعروفة (أي بشأن الضرر المحتمل، والخواص الوظيفية، والتخفيف من الضرر) ويجري تحليلها. وقد يلزم مزيد من التحليل حسب الهدف من التحليلات التي تجرى.*

النتيجة: *تحديد خصائص و/أو توقيع الصنيعة الرقمية وأي معلومات معروفة سابقاً عن الصنيعة بما في ذلك مدى الخبث الذي تنطوي عليه وتأثيرها والتخفيف منه.[1] (ويمكن استخدام هذه المعلومات لتحديد الخطوات التالية.)*

الوظيفة الفرعية 2.2.2 **الهندسة العكسية:** تحليل متعمق ساكن لصنيعة لتحديد خواصها الوظيفية الكاملة، بغض النظر عن البيئة التي يمكن تنفَّذ ضمنها.

الغرض: *توفير تحليل أعمق لصنائع البرمجيات الخبيثة يشمل تحديد الإجراءات الخفية وأوامر الشروع بالتنفيذ. وتسمح الهندسة العكسية للمحلل بسبر أغوار ما تتكون به البرمجيات الخبيثة من برنامج أو نص البرمجي أو شفرة متجاوزاً أي تعتيم وتجميع (للاثنينيات)، إما بكشف النقاب عن أي شفرة مصدرية أو بتفكيك السلاسل الاثنينية إلى لغة التجميع وتفسيرها. وبكشف لغة الآلة كلها تنكشف الوظائف والإجراءات الخبيثة التي يمكن أن تؤديها. والهندسة العكسية هي تحليل أعمق يجرى عندما لا يقدم تحليل السطح ووقت التشغيل المعلومات الكاملة اللازمة.*

النتيجة: *تُستخرج كامل الخواص الوظيفية من الصنيعة الرقمية لفهم كيف تعمل، وكيف تشغَّل، وكيف تُطلق، ونقاط ضعف النظام ذات الصلة التي يمكن استغلالها، وتأثير الصنيعة الكامل،*

وأضرارها المحتملة، وبالتالي توضع الحلول للتخفيف من وطأة الصنيعة، وإذا كان ذلك مناسباً، لإنشاء توقيع جديد لها من أجل المقارنة مع عينات أخرى.

الوظيفة الفرعية 3.2.2 **تحليل وقت التشغيل:** فهم قدرات الصنيعة عن طريق الرصد أثناء تشغيل العينة في بيئة حقيقية أو جرت مضاهاتها (على سبيل المثال، فصل البرامج، وبيئة افتراضية، وعتاد أو برمجيات المضاهاة).

الغرض: *تقديم أفكار مستنيرة عن تشغيل الصنيعة. فاستخدام بيئة محاكاة يلتقط التغييرات الطارئة على المضيف وحركة الشبكة ومخرجات التنفيذ. وتقوم الفرضية الأساسية على محاولة رؤية الصنيعة في طور التشغيل في أقرب حالة ممكنة إلى الواقع.*

النتيجة: *تكوين أفكار إضافية عن تشغيل الصنيعة الرقمية من خلال رصد سلوكها أثناء التنفيذ للوقوف على التغييرات في نظام المضيف المتضرر، وغيرها من تفاعلات النظام وحركة الشبكة الناتجة لتحسين فهم تضرر النظام وتأثره، وإنشاء توقيع (تواقيع) الصنيعة الجديدة، وتحديد خطوات التخفيف من وطأتها. (ملاحظة: لا تظهر كل الخواص الوظيفية من تحليل وقت التشغيل نظراً لأن أقسام شفرة الصنيعة قد لا تُشغَّل كلها. فلا يتيح وقت التشغيل للمحلل إلا رؤية ما تفعله البرمجيات الخبيثة في وضع الاختبار وليس ما هي قادرة تماماً على القيام به.)*

الوظيفة الفرعية 4.2.2 **التحليل المقارن:** يركز هذا التحليل على تحديد الخواص الوظيفية أو المآرب المشتركة، بما في ذلك تحليل عائلة من الصنائع المصنَّفة.

الغرض: *استكشاف علاقة الصنيعة مع غيرها من الصنائع. ويمكنها تحديد أوجه التشابه في الشفرة أو طريقة العمل وفي الأهداف والمآرب والمؤلفين. ويمكن استخدام أوجه التشابه هذه لاستقراء نطاق هجوم (أي هل هناك هدف أكبر؟ وهل استُخدمت شفرة مشابهة من قبل، وما إلى ذلك). ويمكن أن تشمل تقنيات التحليل المقارن مقارنات تطابق تام أو مقارنات تشابه شفرة. ويقدم التحليل المقارن رؤية أوسع لكيفية استخدام الصنيعة أو الإصدارات المماثلة لها وكيف تغيرت بمرور الوقت، مما يساعد على فهم تقييم البرمجيات الخبيثة أو أنواع أخرى خبيثة من الصنائع.*

النتيجة: *استقراء أي قواسم مشتركة أو علاقات مع صنائع أخرى، من أجل تحديد الاتجاهات أو أوجه التشابه التي قد تقدم المزيد من الأفكار أو الفهم للخواص الوظيفية للصنيعة الرقمية ولتأثيرها والتخفيف منه.*

الوظيفة 3.2 **تحليل الوسائط:** الخدمات التي تنطوي على تحليل البيانات ذات الصلة بالأنظمة والشبكات والتخزين الرقمي والوسائط القابلة للاقتلاع من أجل فهم أفضل لكيفية منع وقوع حوادث مماثلة أو ذات صلة و/أو كشفها و/أو التخفيف منها. ويمكن أن توفر هذه الخدمات معلومات للاستعراض القانوني أو الحاسوبي القضائي أو استعراض الامتثال أو غيرها من استعراضات السجلات الزمنية للمعلومات.

الغرض: *جمع وتحليل الأدلة من وسائط مثل محركات الأقراص الصلبة أو الأجهزة المتنقلة أو التخزين القابل للاقتلاع أو التخزين السحابي، أو غيرها من الأنساق بما في ذلك الأنساق الورقية أو الفيديوية. وإذا كانت نتائج التحليل ستُعرض في سياق قانوني أو سياق الامتثال، يتعين جمع المعلومات بطريقة سليمة من الناحية الحاسوبية القضائية بما يحفظ سلامة الأدلة وسلسلة إيداعها. إذ يمكن أن تتضمن الأدلة صنائع مثل مخلفات البرمجيات الخبيثة، وتغيُّر حالة الملفات والسجلات، وغيرها من مكونات النظام؛ ومعلومات مستقاة من اعتراض حركة الشبكة أو ملفات السجل أخرى، ومعلومات في الذاكرة. وتجدر الإشارة إلى أن تحليل الوسائط يبحث عن أدلة تنبئ بما جرى، ويعزو هذا النشاط اختيارياً إلى جهة معينة. وهو يختلف عن*

تحليل الصنيعة الذي يسعى لفهم صنيعة واحدة وعلاقاتها. بيد أن تقنيات تحليل الصنيعة يمكن أن تُستخدم كجزء من تقنيات وأساليب تحليل الوسائط. ويمكن اللجوء أيضاً إلى هذه الخدمات بمعزل عن حادثة سيبرانية كجزء من قضية موارد بشرية أو تحقيق قانوني أو تنظيمي آخر.

***النتيجة**: إن الحصيلة الحالية 1) تبين أصول معلومات الجرد (أي الملكية الفكرية أو غيرها من المعلومات الحساسة التي يُعثر عليها)؛ 2) توفر تسلسلاً زمنياً للأحداث قد يظهر الإضافات والتعديلات والحذوفات التي أجريت لأي أصول وسائط تنطوي عليها الحادثة، إلى جانب من أو ما هو الذي يقوم بتلك الأنشطة، إن أمكن، وكيف تترابط كل خيوط الأدلة معاً لشرح مدى هذه الحادثة وتأثيرها.*

الوظيفة 4.2 **تحليل الثغرة الأمنية/الاستغلال**: الخدمات المقدمة للتوصل إلى فهم أعمق للثغرات الأمنية التي كانت عاملاً في حادثة سيبرانية.

الوظيفة الفرعية 1.4.2 **التحليل التقني للثغرة الأمنية (البرمجيات الضارة) /الاستغلال**: فهم نقطة (نقاط) الضعف المستغَلة لإيقاع حادثة والحيلة المناوئة المستخدمة للاستفادة من ذلك الضعف.

الغرض: إعلام الجهة المخدَّمة بأي ثغرات أمنية معروفة (نقاط الدخول الشائعة للمهاجمين)، وبالتالي يمكن أن تبقى الأنظمة مواكِبة لآخر المستجدات ومراقبَة ضد الاستغلال، على نحو يقلل من أي أثر سلبي إلى أدنى حد.

***النتيجة**: الاستيعاب التام لثغرة أمنية والطريقة التي ستتمكن بها الجهات الخبيثة من استخدام هذه الثغرة الأمنية لتنفيذ تسللها/استغلالها للأنظمة.*

الوظيفة الفرعية 2.4.2 **تحليل السبب الجذري**: فهم "تصميم" أو "تنفيذ" الخلل الذي سمح بوقوع الهجوم.

الغرض: تحديد السبب الجذري ونقطة الاختراق، بما يساعد على القضاء على المشكلة بشكل كامل.

***النتيجة**: الاستيعاب المحكم للظروف التي تسمح بوجود ثغرة أمنية تمكِّن المهاجم من استغلالها.*

الوظيفة الفرعية 3.4.2**تحليل التدارك**: فهم الخطوات اللازمة لإصلاح الخلل الأساسي الذي مكَّن الهجوم، ومنع هذا النوع من الهجمات في المستقبل.

الغرض: التعرف على المشكلة التي مكَّنت الاختراق، وتلافي الثغرة الأمنية ببرمجية تصحيحية، وتغيير الإجراءات أو التصميم، واستعراض طرف ثالث للتدارك، وتحديد أي ثغرات أمنية جديدة أدخلت في ثنايا خطوات التدارك

***النتيجة**: وضع خطة لتحسين العمليات والبنية التحتية والتصاميم لقطع الطريق على ناقل الهجوم المحدد ومنع هذا الهجوم في المستقبل.*

الوظيفة الفرعية 4.4.2 **تحليل التخفيف من الوطأة**: تحليل لتحديد وسائل للتخفيف من المخاطر (منعها) الناجمة عن هجمة أو ثغرة أمنية دون أن يقتضي ذلك حكماً تدارك الخلل الأساسي الذي أحضرها.

الخدمة 3 أمن المعلومات

الوظيفة 1.3 **تقييم المخاطر/الامتثال**: الخدمات المتعلقة بتقييم المخاطر أو بأنشطة تقييم الامتثال. وقد يشمل ذلك إجراء التقييم الفعلي، من أجل تقديم الدعم لتقدير نتائج التقييم. وعادة ما يجرى لدعم متطلب امتثال
(على سبيل المثال، ISO 27XXX، COBIT).

الغرض: تحسين تبيُّن الفرص والتهديدات، وتحسين الضوابط، وتحسين الوقاية من الخسارة وإدارة الحوادث بالتضافر مع أمن المعلومات وغيرها من الوظائف ذات الصلة.

***النتيجة*: عملية متسقة لتقييم وإدارة المخاطر المحدقة بالمعلومات وتطبيقها على الأصول والبيانات الرئيسية ؛ ومدخلات لتقييم المخاطر؛ والاختيار من خيارات معالجة المخاطر ذات الصلة بما يشمل إدارة الحوادث والأدلة الحاسوبية القضائية عند الاقتضاء.**

الوظيفة الفرعية 1.1.3 **جرد الأصول/البيانات الحرجة**: تحديد الأصول والبيانات الأساسية التي لا غنى عنها لاستكمال مهمة المنظمة. وقد لا تعود ملكية هذه الأصول ليس بالضرورة إلى المنظمة (ومثال ذلك، مقدِّم خدمة سحابية أو مجموعة بيانات خارجية). ويشمل ذلك تحديد مواقعها، ومالكها، ومستوى حساسية معلوماتها، ووظيفة مهمتها، ووضعها/مستواها الراهن.

الغرض: المواظبة على تحديد تلك الأصول والبيانات التي قد تكون إدارة حوادثها مطلوبة لتمكين المنظمة من إنجاز مهمتها، إلى جانب خطوط الأعمال ذات الصلة.

***النتيجة*: جرد للمخزون محدَّث بانتظام، وقائمة أو قاعدة بيانات للأصول والبيانات الرئيسية كي تستخدمها المنظمة في تقييم المخاطر.**

الوظيفة الفرعية 2.1.3 **تحديد معيار التقييم**: اكتساب المديرين التنفيذيين لسياسة (سياسات) بشأن المخاطر التي تتعرض لها المنظمة ومعايير معدَّدة/محددة لتقييم مستوى/حالة الأمن. واقتراح معايير للتقييم أو المقارنة المرجعية كي ينظر فيها مدراء المخاطر المؤسسية وكبار مسؤولي أمن المعلومات. ويمكن أن تشمل المعايير، على سبيل المثال لا الحصر، Basel II وCOBIT وITIL ومعيار إصدار الشهادات والاعتماد.

الغرض: مساعدة في اختيار منهجية معتمدة لتقييم المخاطر التي تتعرض لها المعلومات للاستخدام ضمن المنظمة ولتقديم مدخلات تساهم في تقييم المخاطر وإدارتها على المستوى التنظيمي الأوسع.

***النتيجة*: منهجية مختارة لتقييم المخاطر التي تتعرض لها المعلومات معدة للاستخدام في جميع أقسام المنظمة؛ ودعم على مستوى المديرين وتبنيهم لما يقع عليه الاختيار؛ وسياسات تنظيمية تجيز استخدام منهجية تقييم المخاطر المختارة حسب الاقتضاء؛ وتدابير ونماذج ومخرجات متفق عليها؛ وعملية وإجراءات متفق عليها لتقييم المخاطر التي تتعرض لها المعلومات؛ وآليات متفق عليها لدمج نتائج تقييم المخاطر التي تتعرض لها المعلومات ضمن إدارة المخاطر على المستوى التنظيمي وصنع القرار.**

الوظيفة الفرعية 3.1.3 **تنفيذ التقييم**: يساعد في إجراء استعراضات والمشاركة في عمليات التقييم لضمان تلبية/معالجة المتطلبات من حيث المخاطر والأمن.

الغرض: إنجاز تقييم المخاطر التي تتعرض لها المعلومات عن الأصول أو البيانات الرئيسية المختارة، وذلك باستخدام المنهجية المعتمدة، بأكبر قدر ممكن من الدقة.

__النتيجة__: إنجاز تقييم المخاطر التي تتعرض لها المعلومات عن الأصول أو البيانات الرئيسية المختارة.

الوظيفة الفرعية 4.1.3 **النتائج والتوصيات**: إعداد وتقديم النتائج والتقارير و/أو التوصيات (على سبيل المثال، كتابة التقارير، واستخدام المهام في نشر المعلومات).

الغرض: المساعدة في التوثيق الكامل لنتائج تقييم المخاطر المنجز وتعداد الإجراءات الواجب اتخاذها والتوصيات التي يتعين أخذها بعين الاعتبار نتيجة للتقييم.

__النتيجة__: تقرير مخوَّل موقَّع يورد تفاصيل الأصول أو البيانات الحرجة، وعملية تقييم المخاطر المتبعة، والبيانات المستخدمة في تقييم المخاطر، والنتائج والتوصيات والإجراءات والخطط والجداول الزمنية المعدة للتوزيع.

الوظيفة الفرعية 5.1.3**التتبع**: مساعدة كبير مسؤولي أمن المعلومات (CISO) و/أو المسؤول عن إدارة المخاطر في تتبع حالة التقييمات والتنفيذ اللاحق للتوصيات.

الغرض: التأكد من اتباع جميع الخطط والإجراءات والتوصيات وإنجازها ضمن الجداول الزمنية الموثقة.

__النتيجة__: استعراض منتظم للخطط والجداول الزمنية؛ وقائمة الإجراءات المكتملة؛ ومراجعات للجداول الزمنية إن لم تُنجَز الإجراءات في الوقت المحدد؛ وتقرير عن التقدم المحرَّز قياساً بالخطط والجداول الزمنية.

الوظيفة الفرعية 6.1.3**الاختبار:** اختبار نشط للامتثال لمقتضيات مستويات المخاطر. ويمكن أن يشمل اختبار الانتشار، والبحث عن الثغرات الأمنية وتقييمها، واختبار التطبيق وتدقيقه والتحقق منه، وما إلى ذلك.

الغرض: اختبار ما إذا كان ما اختير من معالجة (معالجات) للمخاطر صالح للغرض المنشود، وما إذا كان ينفَّذ على الوجه الصحيح، ويخفف من المخاطر على النحو المتوقع.

__النتيجة__: خطة اختبار موثقة مشفوعة بالنتائج المتوقعة؛ والاختبارات والنتائج الموثقة؛ ومقارنة مع النتائج المتوقعة؛ والإجراءات والجداول الزمنية اللازمة لتصحيح أي انحرافات عن التوقعات.

الوظيفة 2.3 **إدارة البرمجيات التصحيحية**: الخدمات التي تساعد الجهة المخدَّمة بالقدرات اللازمة لإدارة تحديد هوية المخزون، وإدارة الأنظمة التي يتعين تزويدها بالبرمجيات التصحيحية، وإدارة نشر تركيب البرمجيات التصحيحية والتحقق منها.

الغرض: المساعدة في تحديد هوية البرمجيات التصحيحية وتحصيلها وتركيبها والتحقق منها لمنتجات وأنظمة، وتقديم تقييم لفائدة البرمجيات التصحيحية وتأثيرها من منظور إدارة الحوادث.

__النتيجة__: الوعي والفهم التنظيمي للبرمجيات التصحيحية المطلوبة؛ وتطبيق مقدمي الخدمة لفهم البرمجيات التصحيحية؛ وفهم تأثير البرمجيات التصحيحية على المخاطر التي تتعرض لها المعلومات؛ وفهم هذا التأثير على إدارة الحوادث.

الوظيفة 3.3 **إدارة سياسات التشغيل**: خدمات تقوم بإعداد مفهوم تنظيمي للتشغيلات ولغيرها من السياسات وبصيانته وإضفاء الطابع المؤسسي عليه.

الغرض: العمل كمستشار موثوق لجهة مخدَّمة أو لنوع من أنواع الأعمال التجارية بشأن استمرارية الأعمال وإعادتها إلى نصابها إثر وقوع كوارث من خلال إسداء المشورة المحايدة القائمة على الواقع، مع الأخذ بعين الاعتبار الفرصة أو المشكلة قيد المناقشة، والبيئة التي قد تُستخدم فيها المشورة وأي قيود تسري على الموارد.

***النتيجة**: قرارات الأعمال التي تتضمن استمرارية الأعمال وإعادتها إلى نصابها إثر وقوع كوارث؛ وإدارة الحوادث المعتبَرة بمثابة مستشار موثوق؛ وإشراك أعضاء فريق إدارة الحوادث في قرارات الأعمال متى وحيثما كان ذلك مناسباً.*

الوظيفة 4.3 **تحليل المخاطر/المشورة بشأن استمرارية الأعمال وإعادتها إلى نصابها إثر وقوع كوارث**: الخدمات المقدمة إلى الجهة المخدّمة ذات الصلة بانشطة تجاوز العثرات التنظيمية على أساس المخاطر المحددة. ويمكن أن يشمل ذلك مجموعة من أنشطة إدارة المخاطر، من إجراء التقييم الفعلي إلى تقديم الدعم التحليلي في التقدير والتخفيف من نتائج التقييم.

الغرض: العمل كمستشار موثوق بشأن أمن المعلومات وإدارة الحوادث لجهة مخدَّمة أو لنوع من أنواع الأعمال التجارية من خلال إسداء المشورة المحايدة القائمة على الواقع، مع الأخذ بعين الاعتبار الفرصة أو المشكلة قيد المناقشة، والبيئة التي قد تُستخدم فيها المشورة وأي قيود تسري على الموارد.

***النتيجة**: قرارات الأعمال التي تتضمن أمن المعلومات وإدارة الحوادث؛ وإدارة الحوادث المعتبَرة بمثابة مستشار موثوق؛ وإشراك أعضاء فريق إدارة الحوادث في قرارات الأعمال متى وحيثما كان ذلك مناسباً.*

الوظيفة 5.3 **المشورة الأمنية**: خدمات تقدم المشورة لجهة مخدَّمة أو لنوع من أنواع الأعمال التجارية بشأن تنفيذ وتطبيق العمليات أو الوظائف الأمنية ذات الصلة.

الخدمة 4 الوعي الظرفي

الغرض: الوعي الظرفي هو مجموعة من الأنشطة التي توعي منظمة ببيئتها التشغيلية. ويشمل الوعي الظرفي تحديد العناصر الحرجة التي قد تؤثر على مهمة المؤسسة، ومراقبة تلك العناصر، واستخدام هذه المعرفة لتزويد صنع القرار وغيره من الإجراءات بالمعلومات.

***النتيجة**: التوعية الضرورية بالأحداث والأنشطة، داخل المنظمة وحولها، التي قد تؤثر على قدرة المنظمة على العمل في الوقت المناسب وبطريقة آمنة.*

الوظيفة 1.4 **عمليات الاستشعار/القياس**: الخدمات التي تركز على تطوير ونشر وتشغيل الأنظمة ومنهجيات التحليل لتحديد الأنشطة التي يتعين التحقيق فيها.

الغرض: إنشاء البنية التحتية لجمع المعلومات، والعمليات اللازمة للتوعية الظرفية في المنظمة.

***النتيجة**: بنية تحتية تشغيلية (أي أجهزة استشعار) لجمع المعلومات تقدم معلومات عن الوعي الظرفي.*

الوظيفة الفرعية 1.1.4 **وضع المتطلبات**: فهم احتياجات الجهة المخدَّمة وضمان الحصول على التخويل الذي يمكن لفريق التصدي للحوادث الأمنية الحاسوبية أن يعمل بموجبه.

الغرض: تحدد عملية وضع المتطلبات احتياجات الوعي الظرفي للمنظمة ثم تحدد ما يقابل تلك المتطلبات من أنواع المعلومات اللازمة لتحقيق تلك الأهداف.

***النتيجة**: فهم مستوى الوعي اللازم للمنظمة والجهات التي تخدِّمها من منظور المعلومات. وبالإضافة إلى ذلك، التأكد من أن لدى المنظمة جميع السياسات اللازمة والموافقات القانونية لجمع المعلومات.*

الوظيفة الفرعية 2.1.4 **تحديد البيانات اللازمة**: تحديد البيانات اللازمة للإيفاء بالمتطلبات.

الغرض: تتنوع أشكال أجهزة الاستشعار بين الأنظمة المؤتمتة والبشر. وتستخدم مصادر المعلومات (البيانات) هذه لبناء صورة الوعي الظرفي للمنظمة. وتحدد عملية "تحديد اللازمة البيانات" ما يقابل متطلبات الوعي الظرفي من مصادر المعلومات (أي أجهزة الاستشعار) المحتملة.

***النتيجة**: تحديد البيانات اللازمة لدعم متطلبات الوعي الظرفي للمنظمة. وقد تكون بعض مصادر البيانات موجودة بالفعل في حين قد يحتاج البعض الآخر منها إلى أن يهندَس و/أو يحصَّل.*

الوظيفة الفرعية 3.1.4 **أساليب تحصيل البيانات**: تحديد الأساليب والأدوات والتقنيات والتكنولوجيات المستخدمة لجمع البيانات اللازمة.

الغرض: تحدد هذه العملية أساليب جمع ومعالجة وتخزين المعلومات (البيانات) التي تُجمع.

***النتيجة**: تحديد تفاصيل محددة بشأن الكيفية التي ستُجمع بها المعلومات وتخزَّن وتعالَج وتصطفى.*

الوظيفة الفرعية 4.1.4**إدارة الاستشعار**: الصيانة والتحسين المستمر لأداء أجهزة الاستشعار نسبةً إلى متطلبات محددة.

الغرض: صيانة أجهزة الاستشعار ومراقبتها لضمان سلامة الخواص الوظيفية ودقتها.

***النتيجة**: تنفيذ إدارة جهاز الاستشعار وبرنامج استدامة دورة حياته.*

الوظيفة الفرعية 5.1.4**إدارة النتائج**: فرز المعلومات والقياسات المستمدة من أجهزة الاستشعار ونشرها. وعادةً ما تقدَّم عبر لوحة بيان كي تشاهَد من مختلف المستويات داخل منظمة.

الوظيفة 2.4 **الصَهر/الارتباط**: الخدمات التي تجري تحليل وإدراج مصادر بيانات متعددة. وهي تغذّى بالمعلومات، بغض النظر عن المصدر، وتدمجها في مشهد شامل للوضع (الوعي الظرفي).

الغرض: تحديد علاقات جديدة بين الحوادث والمؤشرات والجهات الفاعلة تسمح بالتخفيف من وطأة حادثة أمنية أو التصدي لها على نحو أفضل.

***النتيجة**: تمكين عملية متسقة كي تستفيد المنظمة من المعلومات عن تهديدات جديدة، ودمجها مع المعلومات المتاحة ضمن المخزن الحالي لمعارف المنظمة. وستتمثل النتيجة النهائية لهذه العملية في مجموعة محسنة من المعلومات التي تمكن فريق التصدي للحوادث الأمنية الحاسوبية من اتخاذ القرارات بطريقة أكثر كفاءة ودقة.*

الوظيفة الفرعية 1.2.4**تحديد خوارزميات الصَهر**: تحديد الأساليب أو التقنيات (الخوارزميات) أو التكنولوجيات المستخدمة لتحليل (صَهر) المعلومات.

الغرض: كجزء من التعامل مع حادثة، من المهم أن يبقى فريق التصدي للحوادث الأمنية الحاسوبية على اطلاع تشغيلي جيد على المعلومات الواردة من مصادر مختلفة. فيسمح الصَهر بإدارة المعلومات بطريقة تتيح لفريق التصدي للحوادث الأمنية الحاسوبية أن يأخذ المعلومات الجديدة في الاعتبار بسرعة فور تلقيها، وأن يضع هذه المعلومات في سياقها تماماً فيجعلها صالحة للاستعمال أثناء عملية التعامل مع الحادثة.

***النتيجة**: إعداد عملية داخلية تسمح بتلقف معلومات جديدة، وتقييمها في سياق المعلومات الموجودة، وبالاستغلال الناجح للمعلومات الناتجة المتاحة لفريق التصدي للحوادث الأمنية الحاسوبية، في سياق حادثة.*

الوظيفة الفرعية 2.2.4**تحليل الصَهر**: تحليل (صَهر) موارد البيانات باستخدام البيانات الموجودة في نظام إدارة المعارف لتحديد القواسم المشتركة والعلاقات بين البيانات.

الغرض: كجزء من التعامل مع حادثة، سيتعين على فريق التصدي للحوادث الأمنية الحاسوبية أن يواكب في فهمه باستمرار التهديد الذي تشكله حادثة معينة للمنظمة. ومن أجل القيام بذلك، يتعين أن يكون على علم بآخر مستجدات الحادثة نفسها وتطور التكتيكات والتقنيات والإجراءات التي يلجأ إليها الخصم. وسيحتاج إلى جمع المعلومات باستمرار، وتقييمها قياساً بالمعلومات الموجودة. وستستفيد الوظيفة الفرعية 2.2.4 من خوارزميات الصَهر المختارة في الوظيفة الفرعية 1.2.4 لإجراء تحليل المعلومات عن التهديدات المحصَّلة من مصادر خارجية.

***النتيجة**: فهم تأثير المعلومات عن تهديدات جديدة التي جُمعت قياساً بالحوادث القائمة، وكذلك إعداد المنظمة جيداً لأي تغييرات في بروتوكول نقل النصوص (TTP) للخصم، أو تمكينها من تحديث تقنيات التخفيف والتصدي باستمرار كي تتعامل مع الحوادث ذات الصلة على نحو أفضل.*

الوظيفة 3.4 **إعداد المعلومات الاستخباراتية الأمنية والإشراف عليها**: الخدمات المقدمة لجهات مخدَّمة داخلية أو خارجية بغية إعداد مصادر معلومات استخباراتية أمنية تعود لطرف ثالث والإشراف عليها. ويمكن تعريف المعلومات الاستخباراتية الأمنية على أنها معلومات عن الأمن والتهديدات وتقدم إما معلومات استخباراتية تشغيلية أو معلومات استخباراتية عن التهديدات. ويمكن أن تشمل الخدمات، على سبيل المثال لا الحصر، تحليل المعلومات الاستخباراتية الأمنية وإعدادها وتوزيعها وإدارتها؛ بما في هذه المعلومات من مؤشرات عن التهديدات، ومنطق كشف التهديد مثل قواعد مكافحة البرمجيات الضارة والتواقيع، وتكتيكات الخصم وتقنياته وإجراءاته. وتعتمد هذه الخدمات على أنشطة تبادل المعلومات، المعرَّفة في الفقرة 6.5، المعنونة "التوعية/التواصل".

الغرض: تُعتبر المعلومات الواردة من جهات خارجية بالغة الأهمية للحصول على مستوى كاف من الوعي الظرفي. ويحتاج فريق التصدي للحوادث الأمنية الحاسوبية إلى كمية كبيرة من المعلومات عالية الجودة ذات الصلة بما يقوم بتشغيله، ولكن ما يلزم من تكلفة وعبء عمل للحصول عليها يوجب أن تركز الجهود على مجموعة مختارة من المصادر.

***النتيجة**: يستوعب نظام إدارة البيانات مصادر متعددة لبيانات عالية الجودة تغطي جميع المجالات ذات الصلة بما يقوم فريق التصدي للحوادث الأمنية الحاسوبية بتشغيله - من خلال عمليات مؤتمتة بالكامل في المقام الأول (الوظيفة 4.4). وثمة نتيجة أخرى أيضاً في عمليات كشف الشذوذ والتغيرات في اتجاهات تدفقات معلومات المحصَّلة من مصادر خارجية.*

الوظيفة الفرعية 1.3.4 **تحديد المصدر والجرد**: التحديد المستمر لمصادر المعلومات وصيانتها ودمجها في عمليات إدارة وتحليل المعارف.

الغرض: الحصول على معلومات ذات صلة عالية الجودة من مصادر خارجية لأداء التصدي الفعالة للحوادث والرفع الاستباقي للوعي الظرفي (والتأهب الأمني في المنظمة، بشكل عام). وتكمل مصادر خارجية البيانات التي جُمعت داخلياً: تقارير عن الحوادث (الوظيفة 1.1)، وتقارير عن الثغرات الأمنية (الوظيفة 2.1) ومخرجات أجهزة الاستشعار التي يديرها فريق التصدي للحوادث الأمنية الحاسوبية (الوظيفة 1.4).

***النتيجة**: الحصول على معلومات أمنية ذات صلة عالية الجودة ، من مصادر داخلية و/أو خارجية و/أو مفتوحة المصدر و/أو تجارية. وتخزَّن كل المعلومات التي جُمعت في نظام إدارة البيانات (الوظيفة 4.4).*

الوظيفة الفرعية 2.3.4 **جمع وتصنيف محتوى المصدر**: تحصيل مواد مصادر المعلومات عن التهديدات. وقد تكون هذه المصادر داخلية و/أو خارجية و/أو مفتوحة المصدر و/أو مقدَّمة لقاء رسوم خدمة، على حد سواء.

الغرض: تقييم جودة المعلومات التي جُمعت. ورصد التغيرات في خصائص (بما في ذلك كمية) البيانات التي حُصِّلت من مصادر خارجية لكشف الحالات الشاذة و/أو الاتجاهات الجديدة.

__النتيجة__: التوثيق الحاوي على تصنيفات جودة المصادر. ومعالجة مؤتمتة أو شبه مؤتمتة للتغييرات الكبيرة في الخصائص العامة للمعلومات المحصَّلة من مصادر خارجية.

الوظيفة 4.4 **إدارة البيانات والمعارف**: الخدمات المقدمة للجهات المخدَّمة دعماً للالتقاط البيانات وإعدادها والتشارك فيها على نحو فعّال باستخدام المعارف التنظيمية لتشمل ترميز البيانات (من قبيل، STIX ، TAXII، IODEF، TLP) وقواعد بيانات المؤشر، ودليل البرمجيات الخبيثة/الثغرات الأمنية.

الغرض: تتطلب الجهات المخدَّمة بيانات ومعارف عن الأمن السيبراني بمستوى الجودة وحسن التوقيت المناسبين لاحتياجاتها. وتتكون بيانات الأمن السيبراني من المعلومات المهيأة لكي تعالجها أنظمة لدعم أتمتة الأمن. وتتكون معارف الأمن السيبراني من المعلومات المهيأة لمحللي/مشغلي الأمن السيبراني البشريين. وبالإضافة إلى ذلك، فإن خدمات فريق التصدي للحوادث الأمنية الحاسوبية ووظائفه الأخرى تتطلب بيانات ومعارف الأمن السيبراني كمدخلات. والأفضل أن تدار هذه المعلومات كمورد عام لفريق التصدي للحوادث الأمنية الحاسوبية نظراً إلى أن معظم المعلومات يعاد استخدامها في العديد من الخدمات والوظائف.

__النتيجة__: تقديم بيانات ومعارف الأمن السيبراني بالجودة المطلوبة إلى الجهات المخدَّمة في الوقت المناسب. ويمكن بسهولة للخدمات والوظائف الأخرى لدى فريق التصدي للحوادث الأمنية الحاسوبية أن تحصل على البيانات والمعلومات التي تتطلبها من مصدر واحد ضمن فريق التصدي للحوادث الأمنية الحاسوبية.

- **إدارة تمثيل البيانات**: تقييس كيفية تمثيل البيانات وتبادلها (من قبيل، STIX ، TAXII، IODEF، RID، وما إلى ذلك)
- **إدارة تخزين البيانات**: تصميم أنظمة إدارة التخزين وتنفيذها وصيانتها.
- **هضم البيانات**: العمليات والأنظمة المستخدمة لإدخال المعلومات والتحقق من صحتها وتخزينها.
- **استخراج البيانات**: العمليات والسياسات والأساليب التقنية لاستخراج المعلومات.
- **تقييم الأدوات**: تقييم ودمج الأدوات المستخدمة لإدارة البيانات وتحليلها، والتعاون بشأنها.

الوظيفة 5.4 **المقاييس التنظيمية**: الخدمات التي تركز على تحديد تحقق أهداف الأداء التنظيمي وعلى إرسائه وجمع معطياته وتحليله، إلى جانب قياس الفعالية التنظيمية.

الغرض: تجهد أفرقة التصدي للحوادث الأمنية الحاسوبية ومنظمات إدارة الحوادث اليوم لتحديد مدى نجاحها في الإيفاء بمهمتها المتمثلة بإدارة حوادث الأمن السيبراني. وإذ تصبح الأفرقة أكثر نضجاً من حيث طول العمر التشغيلي، تتساءل "ما مدى جودة ما نقوم به حقاً؟". فتبحث عن سبل لتقييم عملياتها ليس لتحديد نقاط القوة والضعف في العمليات والتقنيات والأساليب فحسب، بل أيضا لقياس أنفسها بالمقارنة مع أفرقة أخرى مماثلة. وتبحث عن الأدلة والمقاييس الكمية لإظهار ما إذا كانت فعالة في منع الأحداث والحوادث السيبرانية وكشفها وتحليلها والتصدي لها. وتركز هذه الوظيفة على تحديد ماهية الأسئلة (المعلومات) التي تحتاج إلى إجابة من الإدارة وأفرقة التصدي للحوادث الأمنية الحاسوبية وأصحاب المصلحة، من بين جهات أخرى، لتقييم عملياتها وبيان القيمة؛ وتركز على إنشاء آليات لجمع القياسات لتوفير المقاييس المطلوبة، ثم جمع النتائج وتحليلها وعرضها.

__النتيجة__: تقديم ما يلزم من التوعية والأدلة التجريبية لبيان مدى جودة إيفاء منظمة إدارة الحوادث بمهمتها وتنفيذها لها، مع تحديد الثغرات التي يتعين تحسينها. وتُستخدم هذه المعلومات لتسهيل اتخاذ القرارات، وتحسين الأداء والمساءلة.

الخدمة 5 التوعية/التواصل

الوظيفة 1.5 **الاحتكام إلى سياسة الأمن السيبراني**: الخدمات التي تدعم وضع سياسة الأمن السيبراني واعتمادها لتشكيل بيئة إيجابية لفريق التصدي للحوادث الأمنية الحاسوبية والجهة التي يخدِّمها، وغيرها من أصحاب المصلحة، من خلال تقديم مشورة الخبراء بشأن هذا الموضوع ليكون صناع القرار على بينة من الأمر.

الوظيفة الفرعية 1.1.5 على الصعيد الداخلي

- **الاستشارات السياساتية والقانونية**: إبلاغ مدخلات الآثار السياساتية والقانونية المتعلقة بالسلطات التنظيمية والمخدَّمة وبولاياتها.
- **سياسة التأليف**: وضع سياسة بدلالة صلتها أو تأثيرها بعمليات وسلطات المنظمات أو الجهات المخدَّمة.

الوظيفة الفرعية 2.1.5 على الصعيد الخارجي

- **تقديم مدخلات مستقاة من السياسة المتبعة**: تقديم المشورة بشأن قضايا السياسة التقنية والأمنية التي قد تؤثر على المنظمة والجهة التي تخدِّمها أو الشركاء الآخرين.
- **التأثير على السياسة المتبعة**: تقديم المعلومات الموثوقة أو الخبرة في الموضوع لتوجيه مراجعة السياسات أو اللوائح أو القوانين. ويمكن أن يشمل ذلك، على سبيل المثال لا الحصر، الإدلاء بشهادات أمام الهيئات التشريعية أو العلمية أو غيرها؛ وكتابة أوراق عرض موقف أو أوراق بيضاء أو مقالات أو مدونات على شبكة الإنترنت أو وسائل الإعلام الاجتماعي؛ ولقاءات مع أصحاب المصلحة، وما إلى ذلك.
- **إعداد المعايير أو الممارسات الفضلى**: المساهمة في جهود الصناعة، وجهود منظمات وضع المعايير أو الممارسات الفضلى العالمية والإقليمية والوطنية (IETF، ISO، FIRST) لتمكين تطبيع العمليات/الممارسات الفضلى كي يتحقق أقصى قدر من التوافق أو قابلية التشغيل البيني أو السلامة أو إمكانية التكرار أو الجودة.

الوظيفة 2.5 **إدارة العلاقات**: الخدمات التي تركز على إنشاء العلاقات والحفاظ عليها للمنظمة.

الوظيفة الفرعية 1.2.5 **إدارة العلاقات بين النظراء**: تطوير العلاقات والحفاظ عليها مع المنظمات التي قد تكون قادرة على تمكين تنفيذ مهمة فريق التصدي للحوادث الأمنية الحاسوبية. ويمكن أن يشمل ذلك ضمان قابلية التشغيل البيني أو تعزيز التعاون بين المنظمات أو على امتدادها.

الوظيفة الفرعية 2.2.5 **إدارة العلاقة مع الجهة المخدَّمة**: تطوير وتنفيذ الممارسات والاستراتيجيات والتكنولوجيات المستخدمة لتحديد هوية الجهات المخدَّمة والجهات صاحبة المصلحة وتمييزها وفهمها وإدارتها ومتابعتها وتقييمها.

الوظيفة الفرعية 3.2.5 **إدارة الاتصالات**: إدارة القوائم المستخدمة لتوزيع الإعلانات والتنبيهات والتحذيرات ومصادر التغذية بالبيانات، والمطبوعات أو المعلومات الأخرى المتشارَك فيها.

الوظيفة الفرعية 4.2.5 **إدارة الاتصالات الآمنة**: إدارة آليات الاتصال الآمنة المستخدمة للبريد الإلكتروني أو الإنترنت أو الرسائل الفورية أو الاتصالات الصوتية.

الوظيفة الفرعية 5.2.5 **المؤتمرات/ورش عمل**: تتيح الفرص لفريق التصدي للحوادث الأمنية الحاسوبية والجهة التي يخدمها لقضاء بعض الوقت معاً لمناقشة التهديدات والتحديات التي تعترضهما، وتعزيز علاقات الثقة، وتبادل الاتصالات، والتشارك في الممارسات الفضلى أو الدروس المستفادة.

الوظيفة الفرعية 6.2.5 **التعامل/العلاقات مع أصحاب المصلحة**: يشمل ذلك التنسيق مع القطاع/المنظمات المتخصصة، والحفاظ على العلاقة مع جهات الاتصال الرسمية للاتصال

مع أصحاب المصلحة الداخليين والخارجيين على حد سواء. والتعامل مع المستويات القيادية داخل المنظمة للتثقيف بشأن مهمة المنظمة وضمان فهم الوعي الأمني.

الوظيفة 3.5 **التوعية الأمنية**: الخدمات التي تعمل ضمن الجهة المخدَّمة لتعزيز الفهم الجماعي للتهديدات التي تواجهها والإجراءات التي يمكن اتخاذها للحد من الخطر الذي تشكله هذه التهديدات.

الوظيفة 4.5 **ترويج العلامة التجارية/التسويق**: الخدمات التي تضمن أن أصحاب المصلحة والجهات المخدَّمة على علم بوجود فريق التصدي للحوادث الأمنية الحاسوبية وبالقدرات المتوفرة من خلاله، وكذلك بالكيفية التي ينبغي أن تتفاعل بها مع فريق التصدي للحوادث الأمنية الحاسوبية للإبلاغ عن احتياجاتها.

الوظيفة 5.5 **تبادل المعلومات، والمنشورات**: الخدمات التي تركز على الاتصالات واسعة النطاق، بما في ذلك التبليغات التي تبلِّغها المنظمة إلى الجهة التي تخدمها لدعم العمليات. ومن الأمثلة على ذلك، ترميزات التدريب، والأحداث، والسياسات والإجراءات التنظيمية.

الوظيفة الفرعية 1.5.5 **إعلانات الخدمة العامة**: نشر المعلومات المتعلقة بالأمن لتعزيز الوعي الأمني وتنفيذ الممارسات الأمنية التنظيمية أو المخدَّمة أو القطاعية أو العمومية.

الوظيفة الفرعية 2.5.5 **نشر المعلومات**:

- **جمع المتطلبات**: تحديد ماهية المعلومات المطلوب نشرها، ولمن، وبأي طريقة وإطار زمني (تحديد مجال التطبيق). ملاحظة: قد يكون النشر لفئة محدودة أو قد تُنشر منشورات أكثر تعمقاً لفئات شريكة.
- **الإعداد**: تحديد نسق منتجات المعلومات والغرض منها للإيفاء بالمتطلبات.
- **التأليف**: التقاط المعلومات بدقة بحيث تفهمها الفئة (الفئات) المقصودة بسهولة (على سبيل المثال، عرض نتائج الأنشطة المتعلقة بالمعلومات الحاسوبية القضائية والحادثة والثغرة الأمنية وإدارة البرمجيات الخبيثة).
- **الاستعراض**: استعراض المنشور توخياً للوضوح والدقة، وسلامة النحو والإملاء، والحساسية، والتقيد بقواعد الإفصاح عن المعلومات، والحصول على الموافقة النهائية.
- **التوزيع**: إيصال المعلومات إلى الفئة المستهدفة عبر القنوات اللازمة والمناسبة.

الخدمة 6 بناء القدرات

الغرض: يجب أن يكون بناء القدرات دوماً في صلب القوام المتين للتعامل مع حادثة وعملية ونهج التصدي لها. فبناء القدرات هو محور مجمل الأداء والفعالية للمنظمة. وتحتاج المنظمات إلى مزيد من التروي في فهم أي من القدرات تؤثر حقاً في فريق التصدي للحوادث الأمنية الحاسوبية لديها وفي أداء الأعمال بشكل عام، وإلى مواءمة البرامج التدريبية وفقاً لذلك. وفي استطلاع ماكينزي (McKinsey)، أشارت ما يقرب من 60% من المستطلَعين إلى أن بناء القدرات التنظيمية هو أحد أهم ثلاث أولويات لمنظماتهم. ولكن عندما حان الوقت لتناول ما تمس الحاجة إليه، ركز أقل من 30% منهم فقط في برامجهم التدريبية على بناء القدرات التي تضيف القيمة الأكبر وما يلزم لتحقيق الأداء الأمثل.

ويمكن أن تعرَّف قدرة كأي شيء تُحسن منظمة فعله فيدفع بعجلة نتائج الأعمال الهادفة. وتحتاج المنظمات إلى القدرات الأكثر حسماً لمجمل أداء الأعمال وأداء الفريق، وإلى فهم نتائج ما يدعوها إلى التركيز على القدرات التي اختارتها. وليس للثقافة دور في القدرات التي توليها المنظمة الأولوية وتقدِّمها. وفي حين أن الإدارة على المستوى الأعلى تشارك عادة في رسم معالم قدرات المنظمة، فإن أنجح هذه الإدارات مَن واءم القدرات على المستوى التنظيمي مع تلك اللازمة والمطلوبة على مستوى وحدة الأعمال أو الفريق.

***النتيجة**: فهم خطة وتوثيقها وتنفيذها والقدرة على استخدام وقياس نتائج وعلاقات مختلف فرص بناء القدرات، على مستوى جهوزية عضو الفريق الفردي وعلى مستوى الجهوزية التنظيمي العام كليهما. وتحديد وممارسة نهج منتظم يصبح جزءاً من تخطيط القوى العاملة بشكل عام.*

الوظيفة 1.6 **التدريب والتعليم**: يُستدل من المقدرة مستوى معين من القدرات بمستوى معين من النضج. وبالتالي، فإن القدرات هي اللبنة الأساسية لخدمات فريق التصدي للحوادث الأمنية الحاسوبية. ويوفر بناء القدرات التدريب والتعليم للجهة المخدَّمة من فريق التصدي للحوادث الأمنية الحاسوبية (والتي قد تشمل موظفي المنظمة، عدا البنود الوظيفية مثل تدريب الموارد البشرية للفريق) بشأن مواضيع تتعلق بالأمن السيبراني وضمان المعلومات والتصدي للحوادث.

الغرض: عادة ما يكون برنامج التدريب والتعليم الخطوة الأولى نحو تحديد كيان بناء القدرات ووضعه موضع التنفيذ. ويمكن القيام بذلك من خلال أنواع مختلفة من الأنشطة تشمل التدريب والتعليم، والمعارف المطلوبة الموثقة، والمهارات والقدرات المطلوبة، والمواد التعليمية والتدريبية المتقدمة، والمحتوى المسلَّم، والإرشاد، والتطوير المهني وتطوير المهارات، وتقديم التمارين والمختبرات. وسيساهم كل من هذه الأنشطة بشكل جماعي في بناء قدرات المنظمة والفريق.

***النتيجة**: فهم مشهد برنامج التدريب والتعليم وكذلك علاقته بدعم بناء قدرات فريق التصدي للحوادث الأمنية الحاسوبية. والوصول إلى وضع يمكِّن من فهم وتوثيق أنواع نتائج الفريق والمنظمة، فضلاً عن مؤشرات الأداء الرئيسية، للتمكن من فهم التقدم المحرز.*

الوظيفة الفرعية 1.1.6 **جمع المتطلبات من حيث المعارف والمهارات والقدرات**: جمع الاحتياجات من حيث معارف ومهارات وقدرات وكفاءة الجهة المخدَّمة في ما يتعلق بتحديد ما ينبغي تقديمه من تدريب وتعليم.

الغرض: تقييم ماهية احتياجات فريق التصدي للحوادث الأمنية الحاسوبية وتحديدها وتوثيقها على الوجه الصحيح، من حيث المعارف والمهارات والقدرات المطلوبة، كي يصبح أعضاء الفريق مقتدرين وعلى أهبة الاستعداد.

***النتيجة**: تحديد خصائص المعارف والمهارات والقدرات اللازمة والعملية التي تمكِّن فريق التصدي للحوادث الأمنية الحاسوبية من الإيفاء باحتياجات الأعمال كفريق لا يشق له غبار. وسيساعد ذلك في تحديد المستوى الذي يعمل فيه الفريق، وكذلك المجالات التي يمكن أن يتحسن فيها، إن وُجدت.*

الوظيفة الفرعية 2.1.6 **إعداد مواد التعليم والتدريب**: بناء أو الحصول على محتوى المواد التعليمية والتدريبية مثل العروض والمحاضرات والبيانات العملية، والمحاكاة، وما إلى ذلك.

الغرض: يلجأ فريق التصدي للحوادث الأمنية الحاسوبية إلى إعداد مواد التعليم والتدريب للمساعدة في إبقاء المستخدمين على علم بالتغيرات السريعة في المشهد العام والتهديدات، وفي إبقاء الفريق مواكباً لها؛ ولتسهيل الاتصالات بين فريق التصدي للحوادث الأمنية الحاسوبية والجهات التي يخدِّمها.

***النتيجة**: مواد تعليم وتدريب ذات جودة كافية لفريق التصدي للحوادث الأمنية الحاسوبية؛ وتلبية احتياجات البيئة سريعة التغير لفريق التصدي للحوادث الأمنية الحاسوبية، والاستفادة من تقنيات ومنصات عرض متنوعة وفعالة.*

الوظيفة الفرعية 3.1.6 **إيصال المحتوى**: نقل المعارف والمحتوى إلى "الطلاب". ويمكن أن يحدث ذلك عن طريق وسائل مختلفة، مثل التدريب القائم على الحاسوب/عبر الإنترنت، أو بقيادة مدرب، أو افتراضياً، أو في مؤتمرات أو عروض أو مختبر، وما إلى ذلك.

الغرض: إن وجود عملية رسمية لإيصال المحتوى ستساعد الفريق في تحديد نهج شفاف بشأن أفضل سبيل يستطيع فيه أعضاء فريق التصدي للحوادث الأمنية الحاسوبية تلقي تدريباتهم.

***النتيجة**: إطار لإيصال المحتوى يستخدم جميع الأساليب المتاحة للعرض، والتعلم التقني، والمهارات والعمليات غير التقنية، وذلك باستخدام جميع النُهج البديلة، بما في ذلك التدريب العملي في مختبرات والتدريب القائم على الحاسوب والتدريب الشخصي، وما إلى ذلك.*

الوظيفة الفرعية 4.1.6 **الإرشاد**: التعلم من الموظفين ذوي الخبرة من خلال علاقة قائمة يمكن أن تنطوي على زيارات ميدانية، وتناوب (تبادل)، وملازمة، والأساس المنطقي للنقاش في اتخاذ قرارات وإجراءات محددة.

الغرض: عادة ما يكون برنامج التدريب والتعليم الخطوة الأولى نحو تحديد كيان بناء القدرات ووضعه موضع التنفيذ. ويمكن أن يساعد على توفير آلية رسمية وكذلك غير رسمية للمرشد كي يُطلع من يتلقى الإرشاد على التعليم وتنمية المهارات والرؤى، والخبرات الحياتية والمهنية، خارج علاقة التبعية الرسمية وهيكل الفريق.

***النتيجة**: تعزز قدرة فريق التصدي للحوادث الأمنية الحاسوبية على الاحتفاظ بالأعضاء والحصول على ولائهم وثقتهم، وتعزز مجمل قدرته على اتخاذ القرارات السليمة.*

الوظيفة الفرعية 5.1.6 **التطوير المهني**: مساعدة الموظفين في التخطيط بنجاح وبشكل مناسب لتطوير حياتهم المهنية. ويمكن أن يشمل ذلك حضور المؤتمرات والتدريب المتقدم، وأنشطة التدريب

على مهارات مختلفة، وما إلى ذلك.

الغرض: يلجأ فريق التصدي للحوادث الأمنية الحاسوبية إلى التطوير المهني لتعزيز عملية مستمرة تسعى للحصول على جديد المعارف والمهارات والقدرات التي تتعلق بمهنة الأمن والمسؤوليات التي تنفرد بها وبيئة الفريق الإجمالية.

***النتيجة**: اشتقاق خصائص التطوير المهني وبالتالي لا يكتسب الفريق الثقة فحسب، بل المعارف والمهارات والقدرات اللازمة أيضاً التي تنقل مباشرة إلى التطبيق العملي، ويجري تحديثها على أساس أدوار واحتياجات العمل.*

الوظيفة الفرعية 6.1.6 **تطوير المهارات**: تقديم التدريب لموظفي المنظمة على الأدوات والعمليات والإجراءات اللازمة لوظائف العمليات اليومية.

الغرض: بعد التعرف على المهارات المناسبة، يحتاج فريق التصدي للحوادث الأمنية الحاسوبية إلى الالتزام بسلسلة من الإجراءات التي من شأنها تحديد قدرتهم على الارتقاء إلى الجهوزية.

***النتيجة**: تطوير وتدريب الموظفين وتزويدهم بالمهارات التقنية وغير التقنية اللازمة، وبفهم العملية. واستعداد أعضاء فريق التصدي للحوادث الأمنية الحاسوبية لمواجهة التحديات التشغيلية اليومية، ولدعم الفريق وعملائه على السواء.*

الوظيفة الفرعية 7.1.6 **إجراء تمارين**: تنفيذ اختبار لجهوزية "طلاب" الجهة المخدَّمة لفحص قدرتهم على تطبيق التدريب وأداء وظائف العمل أو المهمة. ويمكن أن يتخذ ذلك شكل بيئات افتراضية، أو محاكاة، أو اختبارات ميدانية، أو تقليد، أو سيناريوهات وهمية، أو توليفة مما ذُكر.

الغرض: من خلال إجراء تدريبات/تمارين ستزداد ثقة فريق التصدي للحوادث الأمنية الحاسوبية لدى المنظمة في صحة خطته وقدرته على التنفيذ.

***النتيجة**: قيام فريق جاهز قدر الإمكان، وضمان العمليات الرئيسية للمعارف والمهارات والقدرات (KSA) وتنفيذ جميع الأعمال بنجاح معاً. وسيساعد ذلك في تحديد المستوى الذي يعمل فيه الفريق، وكذلك المجالات التي يمكن أن يتحسن فيها، إن وُجدت.*

الوظيفة 2.6 **تنظيم تمارين**: الخدمات التي تقدمها المنظمة للجهات المخدَّمة والتي تدعم تصميم وتنفيذ وتقييم التمارين السيبرانية الساعية إلى تدريب و/أو تقييم قدرات فرادى الجهات المخدَّمة والجهات المخدَّمة ككل. ويمكن استخدام هذه الأنواع من التمارين من أجل:

- **سياسات وإجراءات الاختبار**: يقيّم الفريق ما إذا كانت هناك سياسات وإجراءات كافية للتصدي للحدث. وبوجه عام، يتخذ ذلك شكل تمرين نظري أو تمرين محاكاة.
- **اختبار الجهوزية العملية**: يقيّم الفريق ما إذا كان الأشخاص المناسبين في مكانهم الصحيح للتصدي للحدث، وما إذا كانت الإجراءات بشكل تنفَّذ على الوجه الصحيح. وينطوي ذلك عادة على إجراءات التمرُّن.

الغرض: تجرى تمارين لتحسين فعالية وكفاءة خدمات الأمن السيبراني ووظائفه. وتتناول هذه الوظيفة وما يرتبط بها من وظائف فرعية احتياجات المنظمة وكذلك احتياجات الجهات التي تخدمها. وبعبارة أدق، من خلال محاكاة أحداث/حوادث الأمن السيبراني، يمكن استخدام التمارين لهدف واحد أو عدة أهداف:

- بيان عملي: توضيح خدمات الأمن السيبراني ووظائفه، فضلاً عن الثغرات الأمنية والتهديدات والمخاطر، من أجل رفع مستوى الوعي.
- تدريب: إرشاد الموظفين بشأن الأدوات والتقنيات والإجراءات الجديدة.
- تمرين: إتاحة الفرصة للموظفين لاستخدام الأدوات والتقنيات والإجراءات التي سبق أن تدربوا عليها. ويلزم التمرين للمهارات القابلة للتراجع ويساعد على تحسين الكفاءة والحفاظ عليها.
- تقييم: تحليل وفهم مستوى فعالية وكفاءة خدمات الأمن السيبراني ووظائفه.
- إشهاد: تحديد ما إذا كان مستوى معين من الفعالية و/أو الكفاءة يمكن أن يتحقق لخدمات الأمن السيبراني ووظائفه.

***النتيجة**: ستتحسن فعالية وكفاءة الخدمات الأمن السيبراني ووظائفه مباشرة، وستتحدد الدروس المستفادة لمزيد من التحسينات. وحسب الهدف المحدد (الأهداف المحددة) من التمرين، يمكن أيضاً أن يُعرض لأصحاب المصلحة بيان عملي للأمن السيبراني، ويمكن تدريب الموظفين، ويمكن تقييم كفاءة وفعالية الخدمات والوظائف و/أو الشهادة بذلك. ويمكن كذلك تحديد الدروس المستفادة لتحسين التمارين في المستقبل.*

1.2.6 **المتطلبات**: فهم القصد من التمرين، وعلى وجه التحديد، أهداف جميع المشاركين، لضمان أن يشمل التطوير هذه الرغبات.

الغرض: إن الغرض من المشاركة في التمارين هو تحسين فعالية وكفاءة خدمات الأمن السيبراني ووظائفه. ويمكن أن تتخذ المشاركة أحد الأشكال التالية:

- مراقب: يراقب الموظفون سير التمرين، دون أن يكونوا في عداد جمهوره المستهدف فلا تتحدى أحداث التمرين قدراتهم ولا يقيَّم أداؤهم. ويمكن للمراقبة دون المشاركة المباشرة أن تساعد على تحسين فعالية وكفاءة خدمات فريق التصدي للحوادث الأمنية الحاسوبية ووظائفه إلى حد ما. ويمكن أن تساعد أيضاً في تنظيم التمارين في المستقبل.
- جمهور التمرين: يشارك الموظفون في التمرين بوصفهم الجمهور المستهدف، فتتحدى أحداث التمرين قدراتهم ويمكن أن يقيَّم أداؤهم كذلك.

وحسب طرائق التمرين، يمكن للموظفين أن ينتقلوا إلى موقع التمرين أو أن يشاركوا عن بعد من مكاتبهم الاعتيادية أو من موقع آخر مناسب. وكذلك، يمكن للتمرين أن يوفر بيئة محددة أو يمكن للمشاركين أن يشاركوا من بيئة تمرينهم الخاصة أو بيئة العمل المعتادة.

***النتيجة**: تحسن في فعالية وكفاءة خدمات الأمن السيبراني ووظائفه، فضلاً عن تحديد الدروس المستفادة لمزيد من التحسينات. وحسب الهدف المحدد (الأهداف المحددة) من*

التمرين، يمكن أيضاً تقديم بيان عملي بالأمن السيبراني لأصحاب المصلحة، ويمكن تدريب الموظفين، ويمكن تقييم كفاءة وفعالية الخدمات والوظائف و/أو الشهادة على ذلك. ويمكن كذلك تحديد الدروس المستفادة لتحسين التمارين المستقبلية.

الوظيفة الفرعية 2.2.6 **إعداد السيناريو والبيئة**: وضع سيناريوهات التمرين في دعم أهداف الجهة المخدَّمة.

الغرض: إن الغرض من تنظيم التمارين هو إتاحة الفرصة للجمهور المستهدف لتحسين كفاءة وفعالية الخدمات والوظائف من خلال التعامل مع محاكاة أحداث/حوادث الأمن السيبراني.

***النتيجة**: حسَّن الجمهور المستهدف المحدد كفاءة وفعالية الخدمات والوظائف وحدد الدروس المستفادة لمزيد من التحسينات به. وحُددت أيضاً الدروس المستفادة لتحسين التمارين المستقبلية.*

الوظيفة الفرعية 3.2.6 **المشاركة في تمرين**: يمكن أن يكون للمنظمة مستويات مختلفة من المشاركة في تمرين بحكم مستوى نضجها.

- **التقييم**: تقييم نتائج تمرين، والتماس الملاحظات التقييمية بشأنه، وتحديد الدروس المستفادة على أساس مراقبة التمرين.
- **المراقبة**: مراقبة تمرين طرف ثالث.
- **التنسيق**: تنسيق التمرين.
- **المشاركة**: المشاركة في تمرين سيبراني. فيتاح للمشارك اختيار مستوى المشاركة وينتفع من نتائج التمرين (بجعل طرف ثالث يقيم مشاركته، مثلاً).

الوظيفة الفرعية 4.2.6 **تحديد الدروس المستفادة**: وضع تقرير ما بعد العمل، والذي يتضمن الدروس المستفادة أو النتائج/أفضل الممارسات المستقاة من التمرين.

الوظيفة 3.6 **أنظمة وأدوات لدعم الجهة المخدَّمة**: خدمات تركز على مجالات التوصية والتطوير والتزويد والتحصيل الخاصة بالأدوات والخدمات ذات الصلة بالأمن السيبراني للجهة المخدَّمة. وترتبط جميع هذه الأنظمة والأدوات بفريق التصدي للحوادث الأمنية الحاسوبية/الأمن وليس بتكنولوجيا المعلومات العامة؛ ويمكن أن تشمل هذه الأنظمة المراسلات/بوابات التنبيه.

***النتيجة**: يمتلك فريق التصدي للحوادث الأمنية الحاسوبية عمليات وأنظمة في مكانها الصحيح لتحديد متطلبات الجهة المخدَّمة وقدراتها ويحصِّل أو يهيئ أو يطور منصات لدعم هذه المتطلبات.*

الوظيفة 4.6 **دعم الخدمات المقدَّمة إلى أصحاب المصلحة**: خدمات تركز على القدرات التقنية التي يقدمها فريق التصدي للحوادث الأمنية الحاسوبية للمساعدة في بناء القدرات والسعة، وإنضاج الخدمات التي يقدمها فريق التصدي للحوادث الأمنية الحاسوبية إلى أصحاب المصلحة. ومفاد ذلك إنضاج مستويات الخدمة.

الغرض: خلال عملية بناء وتعزيز قدرات الجهة التي يخدمها فريق التصدي للحوادث الأمنية الحاسوبية، يولى اهتمام خاص بتقديم المساعدة بشأن تصميم وحيازة وإدارة وتشغيل وصيانة البنية التحتية للجهة المخدَّمة.

***النتيجة**: تطوير نهج منتظم لتقييم احتياجات البنية التحتية، وتحديد متطلباتها، وتصميم مخططها، وحيازتها، والتحقق من التزامها بالمعايير، وصيانتها، وتحديثها، وإجراء التدريب لتشغيلي عليها، وإخضاعها للتدقيق الداخلي والخارجي.*

الوظيفة الفرعية 1.4.6 **تصميم وهندسة البنية التحتية**: المساعدة في تصميم وهندسة البنية التحتية لدعم متطلبات الجهة المخدَّمة.

الغرض: توفر فهماً للخطوط العريضة لمنهجية تصميم، ومعرفة بالمعايير والأعراف ذات الصلة؛ وتسلط الضوء على أفضل الممارسات في مجال تصميم وهندسة البنية التحتية، بناءً على تقييم شامل للاحتياجات وتحليل لمتطلبات الجهة المخدَّمة.

***النتيجة**: الخبرة العملية في تطوير ومقارنة نُهج تصميم البنية التحتية والبدائل، بناءً على الممارسات الدولية الفضلى وبتضمين المعايير والأعراف ذات الصلة.*

الوظيفة الفرعية 2.4.6 **شراء البنية التحتية**: مساعدة في شراء البنى التحتية، سواء كانت مساعدة في وضع استحقاق إطار المخاطر أو الحد الأدنى من المتطلبات والمعايير الأمنية في نص العقد (من قبيل تطلُّب الامتثال لمعيار معين كمنح شهادة للمنتج).

الغرض: تكوين فكرة عن الاختصاصات المتعلقة بشراء البنية التحتية، في ضوء المتطلبات المؤسسية والتقنية والتشغيلية.

***النتيجة**: فهم عملية شراء البنية التحتية، مع مراعاة المعايير والأعراف ذات الصلة، ومراعاة التدابير التقنية المختلفة وإجراءات التعاقد التي ينبغي اتباعها.*

الوظيفة الفرعية 3.4.6 **تقييم أدوات البنية التحتية**: تقييم أدوات نيابة عن الجهة المخدَّمة.

الغرض: تقديم الدعم في تقييم الخواص الوظيفية للأدوات المختلفة ومطابقتها للمعايير المرعية، بما في ذلك معدات العتاد والبرمجيات والتطبيقات المخصصة.

***النتيجة**: تحليل أداء الأدوات وكذلك امتثالها للمعايير والأعراف والمرجعية المحددة مسبقاً.*

الوظيفة الفرعية 4.4.6 **توفير الموارد البنية التحتية**: المساعدة في الحصول على موارد البنية التحتية اللازمة. (أي باعة العتاد ومقدمي الخدمات، وما إلى ذلك).

الغرض: تسليط الضوء على العوامل الرئيسية لتحقيق النجاح في الحصول على موارد البنية التحتية، وتطوير آليات لإقامة علاقات مستدامة وفعالة مع مقدمي وباعة الحلول على أساس وضوح المسؤولية والمساءلة.

***النتيجة**: اشتقاق مؤشرات الأداء الرئيسية (KPIs) لتوفير موارد البنية التحتية، مع اتفاقات مستوى الخدمة المناسبة (SLAs) التي يمكن أن تكفل كفاءة وفعالية الحصول على موارد البنية التحتية.*

الخدمة 7 البحث/التطوير

الوظيفة 1.7 **تطوير منهجيات اكتشاف ثغرة أمنية وتحليلها وتداركها وتحليل سببها الجذري**: الخدمات التي تساعد على تعريف وتحديد قدرات جديدة وتحسين المنهجيات لأداء الخدمات ذات الصلة بثغرات أمنية، أو تنسيق ممارسات منظمات أخرى أو ممارسات تجارية يمكنها أن تثبت الجدارة نفسها.

الغرض: تعمل بعض المنظمات من خلال الحصول على معلومات عن ثغرات أمنية من مصادر خارجية حصراً، ولكن هناك منظمات تحتاج إلى، أو ترغب في، الحصول على قدرات ذاتية لاكتشاف الثغرات الأمنية وتحليلها. وتهدف هذه الوظيفة إلى تحديد كيف يمكن لمنظمة أن تخطط لوظائف بحوث الثغرات الأمنية هذه.

***النتيجة**: عند الضرورة، تحديد المنهجيات التي يمكن أن تستخدمها المنظمة لفهم الثغرات الأمنية على نحو أفضل.*

الوظيفة 2.7 **تطوير عمليات جمع/صهر/ترابط المعلومات الاستخباراتية الأمنية**: الخدمات التي تعرّف وتحدد قدرات جديدة، وتحسن منهجيات القيام بتحليل المعلومات وتبادل الخدمات ذات الصلة من حيث علاقتها بالمعلومات الاستخباراتية التشغيلية وعن التهديدات.

الغرض: يقتضي النجاح أي تتمكن وظيفة معلومات استخباراتية أمنية من جمع المعلومات، وكذلك تبادل المعلومات ذات الصلة مع أطراف ثالثة. ويعتمد جمع المعلومات غالباً على العلاقات الإنسانية بين أطراف متشاركة فيتفعل مستوى من الثقة الكافية لتمكين تبادل المعلومات الحساسة. ويجب أن يكون المحلل قادراً على تطوير هذه العلاقات، وتحديد المجموعات المناسبة من المعلومات التي يتعين التشارك فيها، وتحديد البروتوكولات الأكثر ملاءمة للتبادل المؤتمت، وإدارة العلاقات، والقيام بتحقيقات مشتركة، وتقييم فعالية مصدر المعلومات.

***النتيجة**: من مصادر خارجية والتي تصف التهديدات المحدقة بأصول أمن المعلومات. وتمتلك المنظمة القدرة الذاتية على إعداد مصادر جديدة وشركاء تبادل.*

الوظيفة 3.7 **تطوير الأدوات**: خدمات تطور وتحدد قدرات جديدة، وتنشر نُهُج التعامل مع أدوات جديدة وأتمتة تنفيذ العمليات المتعلقة بفريق التصدي للحوادث الأمنية الحاسوبية.

***النتيجة**: أدوات طورها فريق التصدي للحوادث الأمنية الحاسوبية للمساعدة في أتمتة المهام المتعلقة به، وهي أدوات قابلة للتوسعة أو التقليص، ويمكن الاعتماد عليها، وتسفر عن نتائج حتمية، ولا تضعف التأهب الأمني لفريق التصدي للحوادث الأمنية الحاسوبية الذي يستخدمها. وهي تحرر موارد المحلل للقيام بمهام غير اعتيادية.*

الموارد الداعمة

https://www.first.org - **FIRST**

http://www.cert.org - **CERT/CC**

https://stix.mitre.org - **STIX/TAXII**

https://www.us-cert.gov/tlp - **TLP**

https://www.ietf.org - **IETF**

- ISO/IEC 27035
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44379

مسرد المصطلحات

اختبار تطبيق - تحقيق يجرى لتزويد أصحاب المصلحة بمعلومات عن جودة المنتج أو الخدمة تحت الاختبار.

بازل الثانية (Basel II) – الاتفاق الثاني من اتفاقات بازل، وهو عبارة عن توصيات بشأن القوانين واللوائح المصرفية الصادرة عن لجنة بازل للإشراف المصرفي.

القدرة - نشاط قابل للقياس يمكن القيام به كجزء من أدوار المنظمة ومسؤولياتها. ولأغراض إطار خدمات فريق التصدي للحوادث الأمنية الحاسوبية، يمكن أن تعرَّف القدرات إما على أنها الخدمات الأوسع، أو على أنها ما يُستلزم من الوظائف أو الوظائف الفرعية أو المهام.

السعة - عدد الوقائع المتزامنة لقدرة معينة يمكن أن تنفذها المنظمة قبل حصول شكل من أشكال استنفاد الموارد.

CERT/CC - مركز تنسيق فريق التصدي للحوادث الأمنية الحاسوبية.

CISO - كبير مسؤولي أمن المعلومات.

سحابة - بيئة الحوسبة الموزعة التي تسمح بتشغيل برمجيات تطبيق باستخدام الأجهزة الممكَّنة بالإنترنت.

COBIT - أهداف مراقبة المعلومات والتكنولوجيا المتصلة بها

الاختزال التجفيري - وظيفة اختزال يُعتبر عكسُها مستحيلاً عملياً، أي تستحيل إعادة إنشاء بيانات المدخلات من قيمتها المختزلة وحدها.

CSIRT - فريق التصدي للحوادث الأمنية الحاسوبية.

مجموعة بيانات خارجية - مجموعة من البيانات عائدة لطرف ثالث.

FIRST - منتدى أفرقة الأمن والتصدي للحوادث.

وظيفة - وسيلة لتحقيق غرض أو مهمة لخدمة محددة.

اختبار البرمجيات العشوائي - تقنية اختبار برمجيات، كثيراً ما تكون مؤتمتة أو شبه مؤتمتة، وتنطوي على تقديم بيانات غير صالحة أو غير متوقعة أو عشوائية لمدخلات برنامج حاسوبي.

مضاهي العتاد/البرمجيات - العتاد أو البرمجيات التي تمكن نظاماً حاسوبياً (يسمى المضيف) من التصرف مثل نظام حاسوبي آخر (يسمى الضيف). ويُستخدم عادةً لتمكين النظام المضيف من تشغيل البرمجيات أو استخدام الأجهزة الطرفية المصممة لنظام الضيف.

IEC - اللجنة الكهرتقنية الدولية.

IETF - فريق مهام هندسة الإنترنت.

IODEF - نسق تبادل وصف الكائن المتعلق بالحادث، وهو تمثيل للبيانات يوفر إطاراً لتبادل المعلومات، المتبادلة عادة بين أفرقة التصدي للحوادث الأمنية الحاسوبية، عن حوادث أمن الحاسوب.

ISO - المنظمة الدولية للتوحيد القياسي.

سلسلة ISO/IEC 27000 (ISO27k) - معايير أمن المعلومات التي تقدم توصيات بالممارسات الفضلى في إدارة أمن المعلومات والمخاطر والضوابط التي ينطوي عليها ضمن سياق نظام شامل لإدارة أمن المعلومات (ISMS)، وتماثل في تصميمها أنظمة إدارة ضمان الجودة (سلسلة the ISO 9000) وحماية البيئة (سلسلة ISO 14000).

ITIL - مكتبة البنية التحتية لتكنولوجيا المعلومات، وهي مجموعة من ممارسات إدارة خدمة تكنولوجيا المعلومات (ITSM) التي تركز على مواءمة خدمات تكنولوجيا المعلومات مع احتياجات مصالح الأعمال.

النضج - مدى الفعالية التي تنفذ بها منظمة قدرة معينة ضمن مهمة المنظمة وسلطاتها.

المصدر المفتوح - نموذج تطوير يروج لنفاذ الجميع دون ترخيص إلى تصميم أو مخطط منتَج، وإعادة توزيع ذلك التصميم أو المخطط على الجميع، بما في ذلك التحسينات اللاحقة التي يدخلها أي شخص عليه.

اختبار الاختراق - هجوم على نظام حاسوبي بقصد إيجاد الثغرات الأمنية فيه، ويُحتمل أن ينفذ إليه وإلى خواصه الوظيفية وبياناته.

الهندسة العكسية - عملية استخراج المعارف أو معلومات التصميم من أي شيء من صنع الإنسان، وإعادة إنتاجها، أو إعادة إنتاج أي شيء بناء على المعلومات المستخرجة.

RID - الدفاع المشترك بين الشبكات في الوقت الفعلي، وهو وسيلة الاتصال بين الشبكات لتسهيل الإعلام بوقوع حادثة والتعامل مع البيانات، في حين تُدمج آليات الكشف والتتبع وتحديد المصدر والتخفيف، للخروج بحل كامل للتعامل مع الحادثة.

فصل البرامج - آلية أمنية لفصل البرامج قيد التشغيل.

الخدمة - فعل المساعدة أو القيام بعمل نيابة عن الجهة المخدَّمة أو من أجلها.

STIX - التعبير المنظم عن معلومات بشأن التهديدات، هو جهد تعاوني مدفوع باعتبارات المجتمعات المحلية في تعريف وتطوير لغة موحدة لتمثيل معلومات منظمة بشأن التهديدات السيبرانية.

مخرجات سلاسل – تتابع حروف ناتج إما كثابت حرفي أو كمتغير من نوع ما.

TAXII - التبادل المؤتمت الموثوق لمعلومات المؤشر، وهو مجموعة من الخدمات والرسائل المتبادلة التي تمكِّن، عند تنفيذها، تبادل معلومات عن التهديدات السيبرانية كافية للتدخل على امتداد المنظمة وحدود المنتج/الخدمة..

TLP - بروتوكول إشارة المرور. وهو يُستخدم لضمان إطلاع الجمهور الصحيح على المعلومات الحساسة.

البيئة الافتراضية - مضاهاة نظام حاسوبي معين.

التفتيش الشامل عن الثغرات الأمنية وتقييمها - تقنية أمنية تُستخدم لتحديد الثغرات الأمنية في نظام حاسوبي.

ملحق - هيكل الخدمة

كما ذكر في الفقرات السابقة، يشمل هيكل الخدمة المعتمد في هذا الإطار التعرُّف على ثلاث طبقات (مجالات الخدمة، والخدمة، والوظائف) تحدد "الماهية" وطبقتين إضافيتين (المهام والإجراءات) تحدد "الكيفية".

وبعبارات بسيطة، يتمثل الهيكل العام على النحو التالي: