Version 2.1

TLP:WHITE

نوفمبر 2019

إطار خدمات فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT)

الإصدار 2.1

إشعار: تصف هذه الوثيقة ما يعتقد منتدى أفرقة الأمن والتصدي للحوادث (FIRST.Org) بأنها أفضل الممارسات. وترد هذه الأوصاف لأغراض إعلامية حصراً. ولا يتحمل منتدى FIRST.Org المسؤولية عن أي أضرار تُتكبد أياً كان طابعها جراء استخدام هذه المعلومات أو فيما يتعلق باستخدامها.

جدول المحتويات

الصفحة

إطار خدمات فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT)

1 الغرض

يرد إطار خدمات فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) في وثيقة إجمالية تصف بطريقة مهيكلة مجموعة من خدمات الأمن السيبراني والوظائف المرتبطة بها التي يمكن تقدمها أفرقة التصدي للحوادث الأمنية الحاسوبية والأفرقة الأخرى التي تقدم خدمات متعلقة بإدارة الحوادث. وقد وضع هذا الإطار خبراء معروفون لدى مجتمع منتدى أفرقة الأمن والتصدي للحوادث (FIRST) بدعم قوي من مجتمع أفرقة المهام لدى فريق التصدي للحوادث الأمنية الحاسوبية (TF-CSIRT)، والاتحاد الدولي للاتصالات (ITU).

وتتمثل مهمة إطار خدمات فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) والغرض من هذا الإطار في تسهيل إنشاء عمليات CSIRT وتحسينها، خاصةً في دعم الأفرقة التي تعمل على اختيار أو توسيع أو تحسين مجموعة خدماتها. والخدمات الموضحة هي تلك الخدمات المحتملة التي يمكن أن يقدمها فريق CSIRT. ولا يُتوقع من أي فريق CSIRT تقديم جميع الخدمات الموصوفة. وسيحتاج كل فريق إلى اختيار الخدمات التي تدعم مهمته والجهات التي يخدمها، على النحو الموضح في تفويضه.

ويسعى الإطار إلى مساعدة الأفرقة من خلال تحديد وتعريف الفئات الأساسية للخدمات ومكوناتها الفرعية. ويتضمن ذلك عنواناً ووصفاً لكل خدمة، وخدمة فرعية، ووظيفة، ووظيفة فرعية اختيارية – حسب الاقتضاء. وهذا الوثيقة هي نقطة انطلاق لتقديم إطار خدمة متسق يحدد مجموعة معيارية من المصطلحات والتعاريف التي ستُستخدم عبر المجتمع المحلي؛ علماً بأن هذه الوثيقة لا تشرح كيفية إنشاء أو تحسين فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) أو فريق مناظر له. فهذا النوع من المعلومات متاح في وثائق أخرى، بعضها مدرج في الملحق 1 كموارد داعمة.

ولا يقدم إطار خدمات فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) أي مقترحات أو توصيات بشأن قدرة أو سعة أو نضج أو جودة أي نوع معين من أفرقة CSIRT. وهذه المواضيع مهمة للقيمة التي يقدمها أي فريق CSIRT إلى الجهات التي يخدمها، ولكنها لم تُدرَج في وثيقة الإطار هذه عن قصد. وأيضاً، لا ينظر هذا الإطار إلى التنفيذ أو يقترح طريقة محددة لتنفيذ أي خدمة معينة. ومن المهم أن يُفهم أن تنفيذ هذه الخدمات ممكن بعدة طرق مختلفة، مع الاستمرار في ضمان تلبية التوقعات المعقولة من الجهات التي يخدمها الفريق ومن أصحاب المصلحة.

2 مقدمة وخلفية

إن فريق التصدي للحوادث الأمنية الحاسوبية هو وحدة تنظيمية (يمكن أن تكون افتراضية) أو قدرة تقدم وفقاً لمهمتها خدمات ودعم لجهة مخدَّمة محددة لمنع الحوادث الأمنية الحاسوبية وكشفها والتعامل معها والتصدي لها.

ويمتلك فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) ذو النشر السليم تفويضاً واضحاً ونموذجاً للإدارة وإطاراً مخصصاً للخدمات، وتكنولوجيات وعمليات لتقديم خدمات محددة وقياسها وتحسينها باستمرار.

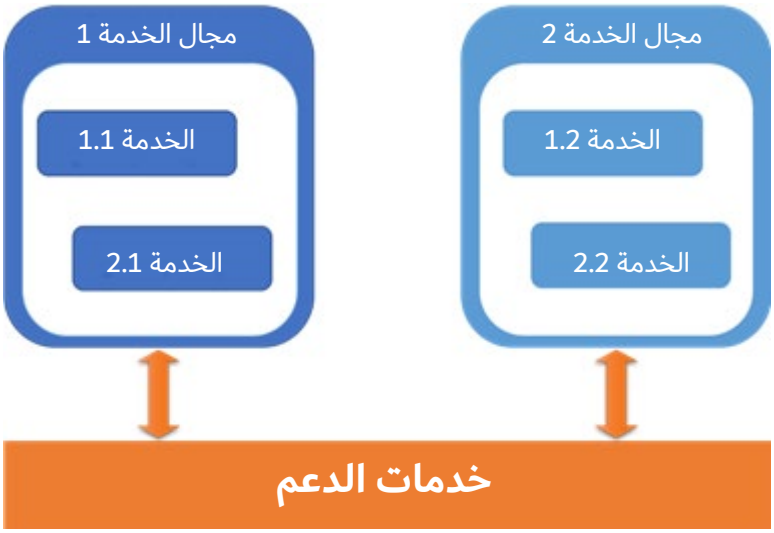
وقد طورت كيانات متنوعة في مجتمع أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) قوائم أو أطر خدمة خاصة بها على مر السنين. مع تغير التكنولوجيا والأدوات والعمليات، شعر هذا المجتمع بنقص مواضيع وأنشطة من القوائم الحالية. وأدرك منتدى أفرقة الأمن والتصدي للحوادث (FIRST) المهتم في تمكين تطوير وإنضاج أفرقة التصدي للحوادث الأمنية الحاسوبية على الصعيد العالمي، بأن ذلك كان شطراً أساسياً في وضع لغة مشتركة لجميع هذه الأفرقة وللكيانات الأخرى المتعاونة معها. 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. وبناءً على هذا الفهم، أُطلق نهج يشكل المجتمع قاطرته لتطوير إطار محسّن لخدمات CSIRT، ونُشر إصداره الأولي في عام 2017.

ومنذ ذلك الحين، اتبُع نهج مشابه لتطوير إطار خدمات أفرقة التصدي لحوادث أمن المنتجات (PSIRT) اعترافاً بالعديد من الجوانب التشغيلية التي تتطلب مجموعة مختلفة من الخدمات والأنشطة المقابلة. ويمكن الاطلاع على جميع أطر الخدمات في الموقع الإلكتروني لمنتدى أفرقة الأمن والتصدي للحوادث (FIRST).[1]

[1] https://www.first.org/standards/frameworks/csirts بشأن المواد ذات الصلة بأفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT).

وهذه نسخة محسنة من الإصدار الثاني من إطار خدمات أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT). واستناداً إلى ملاحظات تقييمية من العديد من الخبراء بشأن الإصدار الأول، أُعيدت هيكلة هذه الطبعة ووُسعت عند الضرورة. وعلى وجه الخصوص، أزيلت الأنشطة الداخلية لأنها لا تشكل عروض خدمة للجهات التي تخدمها. ويمكن تنظيم الأنشطة الداخلية والخارجية التي تدعم دورة الحياة الكاملة لأي عرض خدمة ضمن خدمات ووظائف مثل الخدمات المخصصة لتقديمها إلى الجهات المخدَّمة. وتُعرف هذه الخدمات والوظائف في الغالب باسم خدمات الدعم. ومن الأمثلة على ذلك، أنشطة إدارية مثل إدارة الموظفين والتوظيف، وتعويضات السفر، أو تنظيم الأحداث التدريبية.[2]

وحسب عِلمنا، تتعدد الطرق المختلفة لتقديم خدمات الدعم هذه، ومعظمها يعتمد على المنظمة التي تستضيف فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) أو عروض الخدمات ذات الصلة. فعلى سبيل المثال، يلزم توظيف وإدارة الموظفين بالتأكيد لدعم فريق CSIRT، ولكن ذلك يُعتبر مهمة دعم نمطية في المنظمة وليس شأناً خاصاً بأفرقة CSIRT.



وعلى الرغم من أن الخدمات والوظائف الداخلية تشكل قوام تمكين أي فريق أو وحدة تنظيمية من إنجاز المهمة المنوطة بهما، فإن خدمات الدعم هذه تعتبر خارج مجال التطبيق ولا يُتوسع في تفاصيلها أو بحثها ضمن أطر خدمات منتدى أفرقة الأمن والتصدي للحوادث (FIRST).

ونظراً لأن أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) ستظل تواجه التحديات المتغيرة باستمرار لتأمين الجهات التي تخدمها ضد التهديدات الناشئة الجديدة، سيجري استعراض الخدمات التي يغطيها هذا الإطار، والتدقيق فيها وتوسيعها وتعديلها حسب الحاجة في الإصدارات المستقبلية.[3]

3 الفرق بين فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) وفريق الاستجابة لحوادث أمن المنتجات (PSIRT)

إن الاختلافات الرئيسية بين فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) في منظمة وأفرقة أمنية أخرى ممثَلة في نفس المنظمة، مثل PSIRT، تتجلى في التركيز على الجهات المخدَّمة وكذلك على الخدمات المقدَمة. وبوجه عام، يمثل التركيز على المنتجات الفرق الرئيسي بين فريق PSIRT وأي فريق أمني آخر، بما في ذلك على سبيل المثال لا الحصر، أفرقة CSIRT داخل المنظمة.

2 راجع المرجع [Kossakowski 2001] للاطلاع على بحث بشأن خدمات الدعم الداخلي وعلاقتها بالخدمات الأخرى.

3 أنشئ فريق المصالح الخاصة (SIG) في منتدى فرق الأمن والتصدي للحوادث (FIRST) لتوجيه "تطوير إطار عمل فرق CSIRT".

وداخل المنظمة، يركز فريق CSIRT المؤسسي على أمن الأنظمة والشبكات الحاسوبية التي تشكل البنية التحتية للمنظمة. وإذا تعددت الأفرقة الأمنية، وأفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT)، داخل منظمة كبيرة، يمكن أن يعمل أحدها كمنسق ونقطة اتصال واحدة مع الأطراف الخارجية. وتسمى هذه الأفرقة بأفرقة CSIRT التنسيقية.

وتؤسَس أفرقة CSIRT التنسيقية هذه أيضاً ككيانات مستقلة تخدم مجموعة محددة من الأفراد و/أو المنظمات المعروفة باسم الجهات المخدَّمة. وتشترك المنظمات التي تنتمي إلى جهة مخدَّمة معينة في بعض الخصائص المشتركة (مثل كونها جزءاً من شبكة بحث وطنية أو انتمائها إلى بلد معين). ويتصرف فريق CSIRT التنسيقي كنقطة اتصال واحدة للمجموعة بأكملها ويركز على مجمل الجوانب الأمنية لهذه المنظمات.

واليوم، أنشئت أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) الوطنية كنوع مميز من فريق CSIRT التنسيقي لتسهيل وتنسيق أنشطة أفرقة CSIRT الموجودة في دولة معينة أو تقديم خدمات محدودة لجميع المواطنين، وقطاعات محددة من كيانات البنية التحتية الحيوية وما إلى ذلك في هذه الدولة.

وفي حين أن هناك اختلافات مهمة بين أي فريق تصدي للحوادث الأمنية الحاسوبية (CSIRT) وفريق استجابة لحوادث أمن المنتجات (PSIRT)، فمن المهم إدراك أن هناك تآزراً أيضاً بين الكيانين. والنقطة المهمة التي تُستنتج هي أن أفرقة CSIRT وأفرقة PSIRT لا تعمل بمعزل عن بعضها البعض، فعلى سبيل المثال، تحذر العديد من أفرقة CSIRT الجهات المخدَّمة بشأن الثغرات الأمنية. وتكاد تعتمد مثل هذه التحذيرات دائماً على المعلومات التي تقدمها الأفرقة الموردة للاستجابة لحوادث أمن المنتجات.

4 هيكل إطار خدمات فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT)

يستند إطار خدمات فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) إلى علاقات أربعة عناصر رئيسية:

مجالات الخدمة ← الخدمات ← الوظائف ← الوظائف الفرعية

وتعرَّف هذه العناصر على النحو التالي:

مجالات الخدمة

خدمات مجموعة مجالات الخدمة ذات صلة بجانب مشترَك. وهي تساعد على تنظيم الخدمات وفق تصنيف إجمالي تسهيلاً للفهم والتواصل. ومن شأن توصيف كل مجال خدمة أن يتضمن حقل "الوصف" الذي يتكون من نص سردي عام إجمالي يصف مجال الخدمة وقائمة الخدمات ضمن مجال الخدمة.

الخدمات

الخدمة هي مجموعة إجراءات متماسكة يمكن تمييزها تسعى إلى نتيجة محددة. ويمكن أن تكون هذه النتائج متوقَعة أو مطلوبة من الجهات المخدَّمة أو متأتية نيابة عن أصحاب المصلحة في كيان ما أو من أجلهم.

وتوصَّف الخدمة بالصيغة النموذجية التالية:

- حقل "الوصف" الذي يصف طبيعة الخدمة.
- حقل "الغرض" الذي يصف الغرض من الخدمة.
- حقل "النتائج" الذي يصف أي نتائج قابلة للقياس من الخدمة.

الوظائف

الوظيفة هي نشاط أو مجموعة من الأنشطة وتهدف إلى تحقيق الغرض من خدمة معينة. ويمكن التشارك في أي وظيفة واستخدامها في سياق العديد من الخدمات.

وتوصف الوظيفة بالصيغة النموذجية التالية:

- حقل "الوصف" الذي يصف الوظيفة.
- حقل "الغرض" الذي يصف القصد من الوظيفة.
- حقل "النتائج" الذي يصف أي نتائج قابلة للقياس من الوظيفة.
- قائمة الوظائف الفرعية التي يمكن القيام بها كجزء من الوظيفة.

الوظائف الفرعية

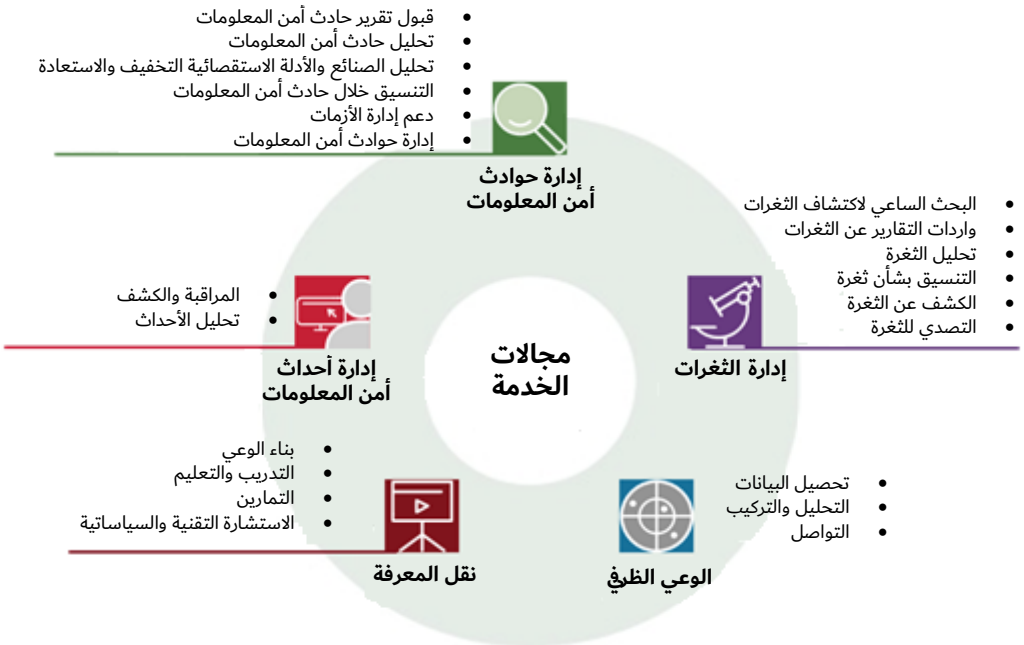
الوظيفة الفرعية هي نشاط أو مجموعة أنشطة وتهدف إلى تحقيق الغرض من وظيفة معينة. ويمكن التشارك في أي وظيفة فرعية واستخدامها في سياق العديد من الوظائف، و/أو الخدمات. ويمكن تنفيذ الوظائف الفرعية بشكل اختياري أو مطلوب لأي من هذه الوظائف، و/أو الخدمات.

وتوصف الوظيفة الفرعية أيضاً بالصيغة النموذجية التالية:

- حقل "الوصف" الذي يصف الوظيفة الفرعية.
- حقل "الغرض" الذي يصف القصد من الوظيفة الفرعية.
- حقل "النتائج" الذي يصف أي نتائج قابلة للقياس من الوظيفة الفرعية.

ولغرض إطار عمل خدمات فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT)، لا يرد وصف الوظائف الفرعية بشكل كامل. ولا يرد سوى توصيف موجز لكل وظيفة فرعية.

ويعرض الشكل أدناه (في الصفحة التالية) مجالات وخدمات إطار عمل خدمات فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT)، ويرد في التذييل 4 جدول كامل بمجالات الخدمة والخدمات والوظائف.



5 مجال الخدمة: إدارة أحداث أمن المعلومات

تهدف إدارة أحداث أمن المعلومات إلى التعرف على حوادث أمن المعلومات بناءً على تلازم وتحليل الأحداث الأمنية من خلال مجموعة واسعة من الأحداث ومصادر البيانات السياقية. وفي المنظمات الكبيرة، يخصَّص مجال الخدمة هذا كلياً أو جزئياً في بعض الأحيان لمركز العمليات الأمنية (SOC) الذي يمكن أن يؤدي أيضاً إدارة من المستوى الأول أو حتى من المستوى الثاني لحوادث أمن المعلومات مثل بدء عمليات التخفيف أو تعديل ضوابط الأمن. ونظراً لأن أي خدمة من خدمات إدارة حوادث أمن

المعلومات تعتمد على بيانات مؤهلة ودقيقة عن أحداث أمن المعلومات، فإن سطح التماس بين مركز العمليات الأمنية والفريق المكلف بالتصدي للحوادث الأمنية الحاسوبية (CSIRT) أمر بالغ الأهمية.[4]

وتُعتبر الخدمات التالية بمثابة عروض في مجال الخدمة هذا:

- المراقبة والكشف.
- تحليل الأحداث.

1.5 خدمة: المراقبة والكشف

الغرض: تنفيذ معالجة مؤتمتة ومستمرة لمجموعة متنوعة من مصادر أحداث أمن المعلومات والبيانات السياقية من أجل تحديد حوادث أمن المعلومات المحتملة، مثل الهجمات، والتسللات، وخرق البيانات، أو انتهاكات سياسة الأمن.

الوصف: استناداً إلى السجلات أو بيانات NetFlow أو تنبيهات نظام كشف التسلل (IDS) أو شبكات الاستشعار أو مصادر خارجية أو غيرها من بيانات أحداث أمن المعلومات المتاحة، تطبَّق مجموعة من الأساليب تتراوح بين المنطق البسيط أو قواعد مطابقة الأنماط وبين تطبيق النماذج الإحصائية أو التعلم الآلي لتحديد حوادث أمن المعلومات المحتملة. ويمكن أن يتضمن ذلك كمية هائلة من البيانات ويتطلب للمعالجة، ولكن ليس بالضرورة، أدوات متخصصة مثل معلومات الأمن وإدارة الأحداث (SIEM) أو منصات البيانات الضخمة. ويتمثل أحد الأهداف الهامة للتحسين المستمر في التقليل إلى أدنى حد من كمية الإنذارات الكاذبة التي تحتاج إلى تحليل كجزء من خدمة التحليل.

النتيجة: تتحدد حوادث أمن المعلومات المحتملة لتحليلها كجزء من خدمة التحليل.

وتعتبر الوظائف التالية جزءاً من تنفيذ هذه الخدمة:

- إدارة السجل وأجهزة الاستشعار.
- إدارة حالات استخدام الكشف.
- إدارة البيانات السياقية.

1.1.5 وظيفة: إدارة السجل وأجهزة الاستشعار

الغرض: إدارة مصادر السجل وأجهزة الاستشعار.

الوصف: تحتاج أجهزة الاستشعار ومصادر السجل إلى إدارة تشغيلية طوال دورة حياتها. ويجب نشرها وإلحاقها وإيقاف تشغيلها. ويجب تحديد حالات الانقطاع وجودة/نطاق البيانات ومشاكل التشكيلة وحلها. وتحتاج أجهزة الاستشعار التي لها شكل ما من أشكال التشكيلة مثل تعاريف الأنماط إلى الحفاظ على تشكيلتها حتى تظل فعالة. ويمكن أن تتضمن أجهزة الاستشعار أيضاً خدمات الكشف الخارجية أو مصادر استعلامات المصادر المفتوحة (OSINT)، إذا كانت تشكل أساس حالات استخدام الكشف.

النتيجة: يتوفر تدفق موثوق لأحداث أمن المعلومات ذات الصلة كمدخلات لحالات استخدام الكشف.

2.1.5 وظيفة: كشف إدارة حالات الاستخدام

الغرض: إدارة مجموعة حالات استخدام الكشف خلال دورة حياتها بأكملها.

الوصف: طُورت نُهج كشف جديدة واختُبرت وحُسنت، وأُلحقت في النهاية في حالة استخدام الكشف في الإنتاج. وتدعو الحاجة لإعداد الفرز والتأهيل والتلازم للمحللين، في شكل خطط التشغيل وإجراءات التشغيل المعيارية (SOP) على سبيل المثال. وتدعو الحاجة لتحسين حالات الاستخدام التي لا تحسن أداءً، أي ذات نسبة الفائدة إلى الجهد غير المؤاتية، أو إعادة تعريفها أو التخلي عنها. وينبغي توسيع مجموعة حالات استخدام الكشف بطريقة موجهة نحو المخاطر وبالتنسيق مع الضوابط الوقائية.

النتيجة: أُعدت مجموعة حالات استخدام الكشف الفعال ذات الصلة بالجهات المخدَّمة.

[4] على الرغم من أن إطار الخدمات هذا لا يهدف إلى تعريف إطار خدمات مركز العمليات الأمنية (SOC)، فمن المؤكد أن تُرتقب فائدة الخدمات من حدث أمن المعلومات ومجالات إدارة الحوادث أيضاً وقابليتها للتطبيق مباشرة أثناء تعريف خدمات مركز العمليات الأمنية.

3.1.5 وظيفة: إدارة البيانات السياقية

الغرض: إدارة مصادر البيانات السياقية للكشف والإغناء.

الوصف: تدعو الحاجة لإدارة مختلف مصادر البيانات السياقية التي تشارك في الكشف والإغناء طوال دورة حياتها. ويمكن أن تكون هذه المصادر سطوحاً بينية مباشرة لبرمجة تطبيقات إلى، أو صادرات من، أنظمة تكنولوجيا المعلومات الأخرى مثل قاعدة بيانات إدارة التشكيلة (CMDB) أو إدارة الهوية والنفاذ (IAM) أو أنظمة استعلامات عن التهديدات أو مجموعات بيانات منفصلة تماماً تتعين إدارتها يدوياً. وسيكون ذلك هو الحال بالنسبة لقوائم المؤشرات وقوائم المراقبة والقوائم البيضاء لإلغاء التأكيدات الخاطئة.

النتيجة: تتوفر بيانات سياقية محدثة للكشف والإغناء معاً.

2.5 خدمة: تحليل الأحداث

الغرض: فرز ما يُكشف من حوادث أمن المعلومات المحتملة وتأهيلها كحوادث أمن المعلومات للتصعيد إلى مجال خدمة إدارة حوادث أمن المعلومات أو كإنذارات كاذبة.

الوصف: يجب فرز تدفق حوادث أمن المعلومات المكتشفة وأن يؤهَل كل واحد منها كحادث أمن معلومات (تأكيد صحيح) أو كإنذار كاذب (تأكيد كاذب) باستخدام التحليل اليدوي، و/أو المؤتمت. ويمكن أن يتطلب ذلك جمع معلومات إضافية يدوياً أو آلياً، حسب حالة استخدام الكشف. وينبغي إيلاء الأولوية لتحليل أخطر حوادث أمن المعلومات لضمان الرد على أهمها في الوقت المناسب. ويتيح التأهيل المهيكَل لحوادث أمن المعلومات المكشوفة استمرار التحسين الفعال بطريقة موجهة من خلال تحديد حالات استخدام الكشف أو مصادر البيانات أو العمليات ذات مشاكل الجودة.

النتيجة: تتوفر حوادث أمن المعلومات المؤهلة والمتلازمة كمدخلات لمجال خدمة إدارة حوادث أمن المعلومات، وتؤهَل التأكيدات الخاطئة للتحسين المستمر.

وتُعتبر الوظائف التالية جزءاً من تنفيذ هذه الخدمة:

- التلازم.
- التأهيل.

1.2.5 وظيفة: التلازم

الغرض: تحديد الأحداث المتعلقة مباشرة بحوادث أمنية أخرى محتملة أو جارية.

الوصف: تجمَّع معاً حوادث أمن المعلومات المحتملة المتعلقة بنفس الأصول (من قبيل الأنظمة، الخدمات، العملاء) أو الهويات (من قبيل المستخدمين)، أو التي ترتبط بشكل مباشر بحوادث أمن المعلومات المحتملة الأخرى وتصعَّد كحادث أمن معلومات واحد لتفادي ازدواجية الجهود. وتخصَص لحادث أمن المعلومات هذا حوادث أمن المعلومات المحتملة الجديدة ذات الصلة المباشرة بحوادث أمن المعلومات الجارية بدلاً من فتح حادث أمن معلومات منفصل جديد.

النتيجة: يجرى تجميع حوادث أمن المعلومات المحتملة ذات الصلة للتأهل أو التحديث المشترك في حادث أمن معلومات قائم سبق أن عالجه مجال خدمة إدارة حوادث أمن المعلومات.

2.2.5 وظيفة: التأهيل

الغرض: فرز وتأهيل حوادث أمن المعلومات المحتملة المكتشفة من أجل تحديد التأكيدات الصحيحة وتصنيفها وتحديد أولوياتها.

الوصف: يلزم فرز حوادث أمن المعلومات المحتملة وتصنيف كل منها على أنه حادث أمن معلومات (تأكيد صحيح) أو كإنذار كاذب (تأكيد كاذب). ونظراً لأن المحللين يمكنهم تحليل عدد محدود من حوادث أمن المعلومات المحتملة، ولتجنب الإرهاق الناجم عن التنبيهات، تشكل الأتمتة مفتاح الحل. وتسهل الأدوات الناضجة الفرز الفعال من خلال إغناء معلومات السياق، وتخصيص درجات المخاطر استناداً إلى حراجة الأصول والهويات المتأثرة، و/أو تحديد أحداث أمن المعلومات ذات الصلة تلقائياً. وينبغي تحديد وأتمتة الحالات المتكررة التي تمكن أتمتتها. وينبغي تحليل حوادث أمن المعلومات المحتملة ذات الخطورة

الأعلى قبل الحوادث الأقل خطورة. وبالإضافة إلى التأهيل كتأكيدات صحيحة أو خاطئة، يعد التأهيل الأكثر تفصيلاً دخلاً مهماً لتواصل تحسين حالات استخدام الكشف بالإضافة إلى إدارة مصادر السجلات وأجهزة الاستشعار ومصادر البيانات السياقية. ويمكن أيضاً أن يدعم التأهيل الأكثر تفصيلاً تحديد مؤشرات أداء رئيسية ذات جودة أعلى لقياس مدى نجاح مجال الخدمة هذا.

النتيجة: تتوفر حوادث أمن المعلومات المحتملة المؤهلة للتعامل معها كجزء من مجال خدمة إدارة حوادث أمن المعلومات.

6 مجال الخدمة: إدارة حوادث أمن المعلومات

يقع مجال الخدمة هذا في صميم أي فريق تصدي للحوادث الأمنية الحاسوبية (CSIRT)، ويتكون من الخدمات الحيوية في مساعدة الجهات المخدَّمة أثناء هجوم أو حادث. ويجب إعداد أفرقة CSIRT لتقدم المساعدة والدعم. ومن خلال فرادة هذا الوضع والخبرة، لا تقتصر قدرتها على جمع وتقييم تقارير حوادث أمن المعلومات، بل يمكنها أيضاً تحليل البيانات ذات الصلة وإجراء تحليل تقني مفصل للحادث نفسه ولأي صنائع مستخدمة.

ومن هذا التحليل، تمكن التوصية بالتخفيف وخطوات التعافي من حادث، وستُدعم الجهات المخدَّمة في تطبيق التوصيات. ويتطلب ذلك أيضاً جهداً تنسيقياً مع الكيانات الخارجية مثل الأقران من أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) أو خبراء الأمن أو الموردين أو أفرقة التصدي لحوادث أمن المنتجات (PSIRT) لمعالجة جميع الجوانب وتقليل عدد الهجمات الناجحة لاحقاً.

والخبرة الخاصة التي يمكن أن تقدمها أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) حاسمة أيضاً في التصدي لأزمات (أمن المعلومات). وفي حين أن فريق CSIRT لن يتعامل مع إدارة الأزمات في العديد من الحالات، فهو يمكنه دعم أي نشاط من هذا القبيل. على سبيل المثال، يمكن لإتاحة جهات الاتصال التي يتواصل معها أن تحسن إلى حد كبير تطبيق خطوات التخفيف المطلوبة أو آليات حماية أفضل.

وتطبيق المعارف والبنية التحتية المتاحة لدعم جهاتها المخدَّمة هو المفتاح لتحسين إدارة حوادث أمن المعلومات إجمالاً.

وتُعتبر الخدمات التالية عروض محتملة لمجال الخدمة هذا:

- قبول تقرير حادث أمن المعلومات.
- تحليل حوادث أمن المعلومات.
- تحليل الصنائع والأدلة الاستقصائية.
- التخفيف والاستعادة.
- التنسيق خلال حادث أمن المعلومات.
- دعم إدارة الأزمات.

1.6 خدمة: قبول تقرير حادث أمن المعلومات

الغرض: تلقي ومعالجة التقارير الخاصة بحوادث أمن المعلومات المحتملة من الجهات المخدَّمة أو من خدمات إدارة أحداث أمن المعلومات أو جهات خارجية.

الوصف: تتمثل أهم مهمة تناط بفريق تصدي للحوادث الأمنية الحاسوبية (CSIRT) في قبول التقارير بشأن أحداث أمن المعلومات وحوادث أمن المعلومات المحتملة التي تؤثر على الشبكات أو الأجهزة أو المكونات أو المستخدمين أو المنظمات أو البنية التحتية – المشار إليها باسم "الهدف" – ضمن الجهة المخدَّمة. وينبغي أن يتوقع فريق CSIRT إمكانية الإبلاغ عن حوادث أمن المعلومات المحتملة من مصادر مختلفة بأنساق مختلفة، يدوياً وتلقائياً على السواء.

ولتمكين الجهات المخدَّمة من الإبلاغ عن حوادث أمن المعلومات بشكل أكثر فاعلية، ينبغي لفريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) تقديم آلية واحدة أو أكثر بالإضافة إلى إرشادات أو تعليمات بشأن ماهية وكيفية الإبلاغ بشكل آمن عن حوادث أمن المعلومات. ويمكن أن تتضمن آليات الإبلاغ بريداً إلكترونياً أو موقعاً إلكترونياً أو استمارة مخصصة أو بوابة إلكترونية للإبلاغ عن حوادث أمن المعلومات أو أساليب أخرى مناسبة لتمكين تقديم التقارير على نحو سليم وآمن. وإذا لم تُدرَج إرشادات

إعداد التقارير، كجزء من استمارة الإبلاغ نفسها عن حوادث أمن المعلومات، فينبغي تقديمها في توثيق منفصل أو عبر صفحة إلكترونية، وينبغي أن تسرد المعلومات المحددة المرغوب إدراجها في التقرير.

ونظراً للعدد الكبير المحتمل لحوادث أمن المعلومات التي تصعَّد تلقائياً وتُكشف عبر خدمة إدارة أحداث أمن المعلومات، يجب التخطيط لذلك قبل اعتماد هذه السطوح البينية أو إجازة استخدامها للجهات المخدَّمة.[5]

النتيجة: يُستلم تقرير حوادث أمن المعلومات ويُستوعب كل تقرير بشكل احترافي ومتسق بالإضافة إلى التحقق الأولي منه والتصنيف الأولي له.

وتُعتبر الوظائف التالية جزءاً من تنفيذ هذه الخدمة:

- استلام تقرير حادث أمن المعلومات.
- فرز حوادث أمن المعلومات ومعالجتها.

1.1.6 وظيفة: استلام تقرير حادث أمن المعلومات

الغرض: قبول أو استلام معلومات بشأن حادث أمن معلومات، كما تبلِّغ عنه الجهات المخدَّمة أو الأطراف الثالثة.

الوصف: يتطلب الاستخدام الفعال لتقارير حوادث أمن المعلومات آليات وعمليات لاستلام التقارير من الجهات المخدَّمة، وأصحاب المصلحة، والأطراف الثالثة (من قبيل المكتشفين، والباحثين، ومراكز تبادل وتحليل المعلومات (ISAC)، وأفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) الأخرى). ويمكن أن تتضمن تقارير حوادث أمن المعلومات الأجهزة/الشبكات/المستخدمين/المنظمات المتأثرة، والظروف التي سبق تحديدها مثل الثغرات المستغلة، والتأثير على كل من المستوى التقني ومستوى الأعمال، والإجراءات التي اتُخذت لبدء خطوات الإصلاح، و/أو التخفيف وربما الحل. وفي بعض الأحيان، يمكن أن ترد معلومات حوادث أمن المعلومات بشكل مشترك كجزء من المدخلات إلى الخدمات الأخرى، ومعظمها من واردات تقارير عن ثغرات (ومثال ذلك، إذا أُبلغ عن حادثة أمن معلومات تحدَدت أثناء تحليل تقرير عن ثغرة). ويمكن أو لا يمكن الإشعار باستلام التقارير المقدمة تلقائياً في انتظار المزيد من خيارات السطوح البينية والبروتوكولات المنفذة.

النتيجة: تتعامل الجهات المخدَّمة أو الأطراف الثالثة مع تقارير حوادث أمن المعلومات بشكل مناسب، بما في ذلك بدء توثيق أو تتبع التقارير.

وتُعتبر الوظائف الفرعية التالية جزءاً من هذه الوظيفة:

- مراقبة قنوات الاتصالات بانتظام والتحقق مما إذا كانت الوسائل المعلن عنها للاتصال بفريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) جاهزة للعمل ويمكن تقديم التقارير.
- إبلاغ الإشعار الأولي بالاستلام لمقدم تقرير حادث أمن المعلومات، وطلب معلومات إضافية إذا لزم الأمر، وتهيئة التوقعات مع مقدم التقرير.

2.1.6 وظيفة: فرز ومعالجة حوادث أمن المعلومات

الغرض: في البداية استعراض حادث أمن المعلومات المبلغ عنه وتصنيفه وتحديد أولويته ومعالجته.

الوصف: تُستعرض تقارير حوادث أمن المعلومات وتُفرز لتشكيل فهم أولي لحادث أمن المعلومات المعني. ومن المهم بشكل خاص ما إذا كان له تأثير أمن معلومات حقيقي على الهدف ويمكن أن يؤدي (أو يكون قد أدى بالفعل) إلى إلحاق الضرر بكتمان وتوفر وسلامة، و/أو أصالة أصول المعلومات أو الأصول الأخرى. وحسب مقدار التفاصيل وجودة المعلومات المقدمة في التقرير الأولي، يمكن أن يتضح أو لا يتضح ما إذا كان قد وقع حادث أمن معلومات حقيقي أو إذا كان هناك سبب مختلف – مثل سوء التشكيلة أو عطل في العتاد. وستتحدد الخطوة التالية على أساس التقييم الأولي (من قبيل معالجة التقرير لمواصلة تحليله؛ أو طلب معلومات إضافية من الجهة المبلِّغة أو مصادر أخرى؛ أو البت في أن التقرير لا يحتاج إلى أي إجراء آخر أو أنه إنذار كاذب).

[5] هناك العديد من أوجه التشابه على النحو المتوقع لجميع الخدمات المتعلقة باستيعاب المعلومات والبيانات. لذلك يشيع الجمع بين هذه الخدمات من عدة مجالات خدمات مقدمة في خدمة/وظيفة واحدة. ونظراً لأن ذلك ليس إلزامياً ولعدم وجود توليفة محددة من مجالات الخدمة، فقد اخترنا إبقاء هذه الخدمات منفصلة في إطار خدمات فرق CSIRT، على الرغم من أن كل فريق حر في اختيار أفضل نموذج تنظيمي لإعداده الخاص.

ويمكن أن تنشأ الهجمات من ضمن الجهات التي يخدمها فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) أو يمكن أن تستهدف هذه الجهات أو أن لا تتأثر هذه الجهات إلا بآثار جانبية. وإذا لم يقدم فريق CSIRT خدمات إدارة أمن المعلومات للأهداف المحددة، تنبغي إعادة توجيه التقرير بشكل آمن إلى مجموعة خارجية للتعامل معه، مثل المنظمة (المنظمات) أو فريق (فرق) CSIRT المتأثرة.

وما لم يكن هناك سبب لرفض تقرير حادث أمن المعلومات أو إذا أُعيد تسيير التقرير إلى كيان آخر مسؤول عن معالجته، ينبغي أن يمرَر التقرير إلى خدمة تحليل الثغرات لمواصلة استعراضه وتحليله والتعامل معه.

النتيجة: يمكن تحديد ما إذا كانت المسألة المبلغ عنها هي بالفعل حادثة أمن معلومات تحتاج لمعالجة من فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) أو لتمريرها إلى كيان ذي صلة.

وتُعتبر الوظائف الفرعية التالية جزءاً من تنفيذ هذه الخدمة:

- معالجة التقارير والبيانات المقدمة بما في ذلك الصنائع أو المواد بمعزل عن بعضها البعض لحماية سلامة بيئة العمل وتجنب الهجمات الناجحة على فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) بهذه الوسائل.
- تحديث الإشعار باستلام التقارير من خلال تقديم بعض الملاحظات التقييمية بشأن الخطوات الإضافية بناءً على نتائج التصنيف أو تحديد الأولويات المتاحة.
- دمج المعلومات الجديدة بشأن حوادث أمن المعلومات التي سبق التعامل معها في البيانات المتاحة للسماح باتساق التحليل والمعالجة.

2.6 خدمة: تحليل حوادث أمن المعلومات

الغرض: تحليل وفهم حادث أمن المعلومات المؤكد.

الوصف: تتكون هذه الخدمة من وظائف لاكتساب فهم لحادث أمن المعلومات وتأثيره الفعلي والمحتمل لتحديد المشاكل أو الثغرات أو نقاط الضعف الأساسية (الأسباب الجذرية) التي سمحت بنجاح الهجوم أو الاختراق أو الاستغلال.

وكثيراً ما يكون التحليل التفصيلي معقداً ويستغرق وقتاً طويلاً. ويتمثل الهدف في تحديد وتشخيص حادث أمن المعلومات بأكبر قدر من التفاصيل على النحو المطلوب أو المبرر بالفهم الحالي لتأثيره. ويمكن أن تتميز حوادث أمن المعلومات بالنطاق أو الكيانات المتأثرة أو الأدوات المستخدمة أو الهجمات المنفذة أو الجداول الزمنية، وما إلى ذلك. ويمكن أن تستمر هذه الخدمة بالتوازي مع تنفيذ خدمة ووظيفة التنسيق خلال حادث أمن المعلومات أو اتخاذ إجراءات التخفيف/الاسترداد.

ويمكن أن يستخدم فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) معلومات أخرى وتحليلاً خاصاً به (انظر أدناه للاطلاع على بعض الخيارات) أو المعارف المتاحة من المورِّدين وأفرقة أمن المنتجات أو الباحثين الأمنيين لتحسين فهم ما حدث أفضل والخطوات التي يجب اتخاذها لتدارك الخسائر أو الأضرار.

النتيجة: زيادة المعارف بشأن التفاصيل الرئيسية لحادث أمن المعلومات (مثل الوصف والتأثير والنطاق والهجمات/الاستغلال والعلاجات).

وتُعتبر الوظائف التالية جزءاً من تنفيذ هذه الخدمة:

- فرز حوادث أمن المعلومات (تحديد الأولويات والفهرسة).
- جمع المعلومات.
- تنسيق تحليل مفصل.
- تحليل الأسباب الجذرية لحادث أمن المعلومات.
- التلازم بين الحوادث.

1.2.6 وظيفة: فرز حوادث أمن المعلومات (تحديد الأولويات والفهرسة)

الغرض: تصنيف حادث أمن المعلومات، وتحديد أولوياته، وإنشاء تقييم أولي له.

الوصف: تبدأ خدمة تحليل حوادث أمن المعلومات باستعراض المعلومات المتاحة لتصنيف حادث أمن المعلومات، وتحديد أولوياته، وتقييم تأثير حادثة أمن المعلومات على الأنظمة المعنية ذات الصلة بولاية فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT). ولعل توثيق بعض هذه المعلومات يرد أثناء عملية فرز ومعالجة تقرير حادث أمن المعلومات (من خدمة واردات تقرير حادث أمن المعلومات) إذا أُبلغت إحدى الجهات المخدَّمة أو طرف ثالث عن حادث أمن المعلومات إلى فريق CSIRT.

وفي حال عدم الانتهاء من الفرز المسبق بالفعل، يمكن إسناد حادث أمن المعلومات إلى خبير في الموضوع يمكنه تقديم تأكيد تقني بأن له بعض التأثير على الأنظمة المعنية وأنه على صلة بولاية فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) (أي له تأثير أمني محتمل على الشبكات أو الأنظمة يمكن أن يؤدي إلى الإضرار بكتمان أو توفر أو سلامة أصول المعلومات في مجال يخص فريق CSIRT وفقاً لولايته).

النتيجة: يصنَّف سجل المعلومات الخاص بحادث أمن المعلومات وتحدَد أولوياته ويحدَّث.

2.2.6 وظيفة: جمع المعلومات

الغرض: أخذ المعلومات المتعلقة بحادث أمن المعلومات وجميع أحداث أمن المعلومات التي تعتبر جزءاً منه وفهرسة هذه المعلومات وتخزينها وتتبعها.

الوصف: تمكين جمع كل المعلومات القيمة للحصول على أفضل فهم للسياق، بحيث يمكن تقييم أصل ومحتوى المعلومات بشكل مناسب ووسمها لاستخدامها في أي معالجة أخرى.

وأثناء جمع المعلومات، يجب قبول ما اتُفق عليه من سياسات تبادل البيانات وحدود البيانات التي يمكن استخدامها في أي سياق أو أي شكل من أشكال المعالجة والالتزام بها. ويجب أيضاً أن تضمن آليات وإجراءات جمع المعلومات استخدام الوسم والإسناد إلى مصادر بشكل سليم للتحقق لاحقاً من منشأها وكذلك مدى ملاءمتها أو صحتها.

النتيجة: تتوفر معلومات مهيكلة بشأن ما جُمع من البيانات الرقمية وغير الرقمية أو البيانات الشرحية، مع معلومات التتبع ونقاط التحكم في سلامة كل من المعالجة والتخزين. وحسبما إذا كانت النتائج ستُستخدم في التحليل (غير الرسمي) المستقبلي أو أنشطة إنفاذ القانون، تختلف المتطلبات فيما يتعلق بإنشاء سلسلة وصاية رسمية يمكن الدفاع عنها في المحكمة في مرحلة لاحقة.

وتُعتبر الوظائف الفرعية التالية جزءاً من تنفيذ هذه الوظيفة:

- تقييم مصادر المعلومات التي تقدم البيانات والمعلومات والاستيقان منها.
- جمع التقارير بشأن الأحداث الضارة أو المشبوهة، و/أو أحداث أمن المعلومات، و/أو تقارير حوادث أمن المعلومات من الجهات المخدَّمة وأطراف ثالثة (مثل أفرقة أمنية أخرى أو معلومات استخبارية تجارية)، بالأشكال اليدوية أو المؤتمتة أو القابلة للقراءة الآلية على السواء.
- جمع وفهرسة البيانات الرقمية التي يمكن أن تكون مفيدة في فهم نشاط الحادثة (مثل صور القرص الحاسوبي، والملفات ذات البيانات الشرحية أو المجاميع التحققية، وخصائص معمارية الشبكة، وسجلات)، دون ضمان هذه الفائدة المرجوة؛ وهذا يشمل على سبيل المثال لا الحصر الصنائع التي يعتقد أنها بقايا نشاط عدائي.
- جمع وفهرسة البيانات غير الرقمية (صحائف تسجيل الدخول المادية، والرسوم البيانية للمعمارية، ونماذج الأعمال التجارية، وبيانات تقييم الموقع، والسياسات المتبعة، وأطر المخاطر في المنظمة).
- جمع وفهرسة البيانات الشرحية فيما يتعلق بمصدر المعلومات، وأسلوب جمعها، والأشخاص الذين تعاملوا مع البيانات أو الكائنات، ومالكها، ومعلومات الوصاية؛ خاصة لأنها يمكن أن تُعتبر دليلاً في تحليل استقصائي أو أنشطة إنفاذ القانون لاحقاً.

3.2.6 وظيفة: تنسيق التحليل التفصيلي

الغرض: بدء وتتبع أي تحليل تقني آخر فيما يتعلق بحادث أمن المعلومات.

الوصف: نظراً لإمكانية تطلُّب تحليل تقني أكثر تفصيلاً يمكن تنفيذ هذا التحليل بواسطة خبراء آخرين (داخل أو خارج المنظمة المضيفة أو فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT)) أو أطراف ثالثة أخرى (مثل مقدم خدمة متخصص في هذا التحليل). ويتطلب ذلك بدء وتتبع هذه الأنشطة حتى التسليم الناجح للتحليل المطلوب.

النتيجة: تَوفر قائمة تحليل يُنتظر استكماله – ومن وجهة نظر معالج الحوادث الذي ينسق التصدي لأي حادث أمن معلومات معين – يجري بالاستعانة بمصادر خارجية.

4.2.6 وظيفة: تحليل السبب الجذري لحادث أمن المعلومات

الغرض: تحديد السبب الجذري لحادث أمن المعلومات، وتحديد الظروف التي سمحت بوجود الثغرات المستغلة أو التي سمحت بنجاح الاستغلال (بما في ذلك سلوك المستخدم على سبيل المثال لا الحصر).

الوصف: تتضمن هذه الوظيفة العملية والإجراءات المطلوبة لفهم ما يوجد في المعمارية أو الاستخدام أو التنفيذ من عيب (عيوب) كان سبباً أو عرّض الأنظمة والشبكات والمستخدمين والمنظمات وما إليها لذلك النوع من الهجوم أو الاستغلال أو الاختراق كالذي شُن ضد أهداف حادث أمن المعلومات. وهي معنية أيضاً بالظروف التي يمكن فيها للمهاجم اختراق المزيد من الأنظمة بناءً على النفاذ الأولي للحصول على مزيد من النفاذ.

وحسب طبيعة حادث أمن المعلومات، يمكن أن يصعب على فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) أداء هذه الوظيفة على أكمل وجه. وفي العديد من المواقف، يمكن أن تنفَّذ هذه الوظيفة على أفضل وجه بواسطة الهدف المتأثر نفسه، خاصة في سياق تنسيق أفرقة CSIRT عندما لا تتوفر معرفة تقنية تفصيلية بشأن الأنظمة أو الشبكات المخترَقة.

النتيجة: يُفهم حادث أمن المعلومات والطريقة التي تمكنت بها الجهات الخبيثة في البداية من النفاذ ومواصلة استخدامه كي يتاح تحديد أساليب التدارك أو التخفيف لتقليل مخاطر التعرض أو الاستغلال إلى أدنى حد في المستقبل من خلال القضاء على الأسباب الجذرية.

5.2.6 وظيفة: التلازم بين الحوادث

الغرض: تمكين استخدام جميع المعلومات المتاحة للحصول على أفضل فهم للسياق واكتشاف العلاقات المتبادلة التي، بخلاف ذلك، لن يُتعرف عليها أو يُتصرف تجاهها.

الوصف: تتضمن هذه الوظيفة تلازم المعلومات المتاحة بشأن حوادث أمن المعلومات المتعددة لتحديد العلاقات المتبادلة، أو الاتجاهات، أو عوامل التخفيف المطبقة في حوادث أمن المعلومات التي سبق أن أُغلقت ملفاتها لتحسين التصدي لحوادث أمن المعلومات التي يُتعامل معها حالياً.

النتيجة: تُفهم الصورة الأكبر من حيث الوعي الظرفي بناءً على معرفة تفصيلية بأوجه التشابه والعلاقات المتبادلة المؤكدة أو المشتبه بها في حوادث أمن المعلومات المستقلة.

3.6 خدمة: تحليل الصنائع والأدلة الاستقصائية

الغرض: تحليل واكتساب فهم للصنائع المتعلقة بحادث أمن معلومات مؤكد، مع الأخذ في الاعتبار الحاجة إلى الحفاظ على الأدلة الاستقصائية.

الوصف: الخدمات المتعلقة بفهم قدرات ومقاصد صنائع (كالبرمجيات الضارة، وعمليات الاستغلال، ومفرغات الذاكرة غير المستدامة أو نُسخ القرص، وشفرات التطبيقات، والسجلات، والوثائق)، وآليات تسليمها، وانتشارها، وكشفها، والتخفيف منها، ونزع سلاحها أو تحييدها. وينطبق ذلك على أي أنساق ومصادر: العتاد والبرمجيات الثابتة والذاكرة والبرمجيات وما إلى ذلك. ويجب الحفاظ على أي صنائع أو أدلة وجمعها دون أي تعديل، والاحتفاظ بها في معزل عن أي شيء آخر. ونظراً لأن بعض الصنائع والبيانات يمكن أن تصبح دليلاً في سياق أنشطة إنفاذ القانون، يمكن أن تسري لوائح أو متطلبات محددة.

وحتى بدون الاحتفاظ بسلسلة الوصاية، تتضمن هذه الخدمة عادةً مهام معقدة وتستغرق وقتاً طويلاً، وتتطلب خبرة، وإعداد بيئات تحليل مخصصة ومراقبتها – مع أو بدون نفاذ خارجي من شبكات سلكية أو لاسلكية معيارية (مثل تنفيذ أنشطة استقصائية في غرفة مغلقة أو غرفة فاراداي) وتسجيل الأنشطة والالتزام بالإجراءات.

وكجزء من عملية التعامل مع حوادث أمن المعلومات، يمكن أن تصادَف الصنائع الرقمية في الأنظمة المتضررة بها أو في مواقع توزيع البرمجيات الخبيثة. وقد تكون الصنائع من مخلفات هجوم دخيل، مثل الملفات القابلة للتنفيذ والبرامج النصية والملفات والصور وملفات التشكيلة والأدوات ومخرجات أداة، وسجلات ومقاطع الشفرة الحية أو الهامدة، وما إلى ذلك.

ويجرى التحليل لمعرفة بعض أو كل المعلومات المدرجة أدناه، والتي لا تعتبر قائمة كاملة:

- السياق المطلوب من الصنيعة لتشغيل وأداء المهام المقصودة، سواء كانت ضارة أم لا.
- كيفية استخدام الصنائع للهجوم: أي الصنائع التي جرى رفعها أو تحميلها أو نسخها أو تنفيذها أو إنشاؤها في بيئات أو مكونات المنظمة.
- ما هي الأنظمة التي أُشركت محلياً وعن بُعد لدعم التوزيع والإجراءات.
- الوقوف على ما قام به الدخيل ذات مرة للنفاذ إلى النظام أو الشبكة أو المنظمة أو البنية التحتية: من الجمع السلبي للبيانات، إلى المسح النشط للبيانات وإرسالها لأغراض التسلل إلى الخارج، أو جمع طلبات إجراءات جديدة، أو تحديث نفسه أو التحرك على المستوى نفسه داخل شبكة (محلية) مخترقة.
- ما فعله مستخدم أو عملية مستخدم أو نظام مستخدم بمجرد اختراق حساب المستخدم أو جهاز المستخدم.
- ما هو السلوك الذي يميز الصنائع أو الأنظمة المخترقة، سواء بأسلوب مستقل، أو بالاشتراك مع الصنائع أو المكونات، المتصلة بشبكة محلية أو الإنترنت، أو في أي توليفة.
- كيف تنشئ الصنائع أو الأنظمة المخترقة التوصيلية بالهدف (من قبيل مسار التسلل أو الهدف الأولي أو تقنيات التهرب من الكشف).
- ما هي معمارية الاتصالات المستخدمة (من نظير إلى نظير، القيادة والتحكم، كلتاهما).
- ما هي إجراءات الجهات المهددة، وما هي رقعة انتشارها عبر الشبكة والأنظمة.
- كيف تهرب المتسللون أو الصنائع من الكشف (حتى على مدى فترات طويلة يمكن أن تتضمن إعادة التشغيل أو إعادة التهيئة).

ويمكن تحقيق ذلك من خلال أنواع مختلفة من الأنشطة بما في ذلك:

- تحليل الوسائط أو السطح.
- الهندسة العكسية.
- تحليل وقت التشغيل أو تحليل دينامي.
- التحليل 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 أو بيئة حية، وتفكيك الصنائع الإثنينية وتفسيرها.

ومن خلال العمل على تحليل الصنيعة (الصنائع)، يحاول المحلل إعادة بناء ما فعله الدخيل وتحديده، وذلك لكشف الثغرة المستغَلة وتقييم الأضرار، ووضع حلول للتخفيف من أفاعيل الصنائع، وتقديم معلومات للجهات المخدَّمة وغيرها من الباحثين.

النتيجة: تُفهم طبيعة الصنائع الرقمية المنتشَلة والأدلة الاستقصائية التي جرى تحليلها إلى جانب العلاقة بالصنائع الأخرى أو الكائنات أو المكونات الداخلية أو الخارجية، والهجمات على الأطر والأدوات والثغرات المستغلة. وتُفهم افتراضات العمل أو الإثباتات على ما فعله منفذ التهديد وكيف تصرفت الصنائع. وهذه المعارف حرجة لتقييم الخسائر والأضرار والتأثيرات على الأعمال وما إلى ذلك، ولوضع استراتيجيات الاحتواء والتخفيف أو التعافي. وتُفهم التكتيكات والتقنيات والإجراءات المستخدمة من المهاجمين أو المتسللين لاختراق الأنظمة و/أو المستخدمين و/أو الشبكات و/أو المنظمات و/أو البنى التحتية. وهذا يشمل تلك التكتيكات والتقنيات والإجراءات المستخدمة للانتشار أو التسلل إلى الخارج أو تحديث أو تعديل أو تمويه سلوكهم أو بياناتهم أو حذف آثار أنشطتهم تلقائياً أو تنفيذ أنشطة ضارة إضافية.

وفيما يلي قائمة الوظائف التي تعتبر جزءاً من تنفيذ هذه الخدمة:

- تحليل الوسائط أو السطح.
- الهندسة العكسية.
- تحليل وقت التشغيل أو تحليل دينامي.

- التحليل المقارن.

1.3.6 وظيفة: تحليل الوسائط أو السطح

الغرض: مقارنة المعلومات التي جُمعت من الصنيعة مع غيرها من الصنائع العامة والخاصة، و/أو مستودعات التواقيع.

الوصف: تتضمن هذه الوظيفة تحديد وتوصيف المعلومات الأساسية والبيانات الشرحية بشأن الصنائع، بما في ذلك على سبيل المثال لا الحصر أنواع الملفات، ومخرجات السلسلة، واختزالات التجفير، والشهادات، ومقاسات الملفات، وأسماء الملفات/الدليل. ونظراً لأن جميع المعلومات المتاحة يتواصل جمعها وتحليلها، فيمكن استخدامها لاستعراض أي مستودعات معلومات ذات مصدر عام/مفتوح أو خاص/مغلق لمعرفة المزيد عن الصنيعة أو سلوكها، حيث يمكن استخدام هذه المعلومات لتحديد الخطوات التالية.

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.

2.3.6 وظيفة: الهندسة العكسية

الغرض: إجراء تحليل متعمق ساكن لصنيعة لتحديد خواصها الوظيفية الكاملة، بغض النظر عن البيئة التي يمكن تنفّذ ضمنها.

الوصف: تقديم 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 (للإثنينيات)، إما بكشف النقاب عن أي شفرة مصدرية أو بتفكيك السلاسل الإثنينية إلى لغة التجميع وتفسيرها. وإذ يكشف المحلل 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، بغية وضع الحلول للتخفيف من وطأة الصنيعة، وإذا كان ذلك مناسباً، لإنشاء توقيع جديد لها من أجل المقارنة مع عينات أخرى.

وتُعتبر الوظائف الفرعية التالية جزءاً من تنفيذ هذه الوظيفة:

- التحليل الساكن.
- الهندسة العكسية للشفرة.
- تحليل السلوك المحتمل ووصفه.
- تصميم توقيع محتمل.

3.3.6 وظيفة: تحليل وقت التشغيل أو تحليل دينامي

الغرض: تقديم فكرة مستنيرة عن تشغيل الصنيعة.

الوصف: تنطوي هذه الوظيفة على فهم قدرات الصنيعة عن طريق الرصد أثناء تشغيل العينة في بيئة حقيقية أو جرت مضاهاتها (من قبيل فصل البرامج، وبيئة افتراضية، وعتاد أو برمجيات المضاهاة).

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.

وتُعتبر الوظائف الفرعية التالية جزءاً من تنفيذ هذه الوظيفة:

- إعداد بيئة تحليل (حية/مقيدة/مغلقة، مضاهاة/محاكاة).
- إعداد أجهزة جمع و/أو أجهزة استشعار و/أو مسابير.
- جمع بيانات السلوك الأولية والبيانات الشرحية.
- سبر الصنيعة عدة مرات في سياقات مختلفة.
- إجراء تحليل للأنظمة و/أو سلوك الشبكة، على المديين القصير والطويل معاً.
- استخلاص الخلاصات من خلال تقييم جميع النتائج والبيانات التي جُمعت، ومقارنة النتائج المختلفة والبحث في قواعد المعارف المتاحة عن النتائج التقنية الحالية التي تطابق المُكْتَشَفَات.

4.3.6 وظيفة: التحليل المقارن

الغرض: إجراء تحليل يركز على تحديد الخواص الوظيفية أو المآرب المشتركة، بما في ذلك تحليل عائلة من الصنائع المفهرسة.

الوصف: تتضمن هذه الوظيفة 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 (من قبيل هل هناك هدف أكبر؟ وهل استُخدمت شفرة مشابهة من قبل).

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.

وتُعتبر الوظائف الفرعية التالية جزءاً من تنفيذ هذه الوظيفة:

- تحديد خط الأساس للخصائص والسلوكيات المرصودة.
- البحث عن نفس الخصائص أو خصائص مماثلة في المستودعات/قواعد المعارف المتاحة.
- تحديث المستودعات/قواعد المعارف المتاحة فيما يتعلق بالأعراض والسلوكيات، و/أو التوقيعات المرصودة حديثاً أو التي لم تكن معروفة من قبل والتي يمكن استخدامها لفهرسة الصنائع التي تناولها البحث.

4.6 خدمة: التخفيف والاستعادة

الغرض: احتواء حادث أمن المعلومات قدر الإمكان للحد من عدد الضحايا، وتقليل الخسائر والتعافي من الضرر، وتجنب المزيد من الهجمات والمزيد من الخسائر بإزالة الثغرات أو نقاط الضعف المستغلة، وتحسين مجمل الأمن السيبراني.

الوصف: بمجرد تأكيد التحليل لحادث أمن معلومات محتمل ووضع استراتيجية تصدي، يجب تحويل ذلك إلى خطة تصدي. وحتى قبل وضع اللمسات الأخيرة على خطة التصدي، يمكن اتخاذ تدابير مخصصة. وتتضمن هذه الخدمة أيضاً بدء وتتبع جميع الأنشطة التي تنفَّذ إلى أن يمكن اعتبار ملف حادث أمن المعلومات مغلقاً أو تتاح معلومات جديدة تتطلب مزيداً من التحليل ويمكن منذئذ أن تغير أيضاً استراتيجية وخطة التصدي.

النتيجة: تخفَف تداعيات حادث أمن المعلومات ويحسَّن وضع الأمن السيبراني. وتستعاد سلامة الأنظمة التي تأثرت بالهجوم أو الأنشطة الأساسية للمهاجم، بالإضافة إلى صلاحية خدمة الشبكة والأنظمة المخترقة. وتستعاد البيانات في حال فقدان البيانات، إن أمكن.

وتُعتبر الوظائف التالية جزءاً من تنفيذ هذه الخدمة:

- وضع خطة التصدي.
- تدابير مخصصة واحتواء مخصص.

- استعادة الأنظمة.
- دعم كيانات أمن المعلومات الأخرى.

وفي حالة فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) التنسيقي، لن تقدَّم جميع الوظائف. في حين أن "دعم كيانات أمن المعلومات الأخرى" هو نشاط تقدمه هذه الفرق، إلا أنه يساعد في بعض الأحيان أيضاً في "وضع خطة تصدي".

1.4.6 وظيفة: وضع خطة التصدي

الغرض: تحديد وتنفيذ خطة لاستعادة سلامة الأنظمة المتأثرة وإعادة البيانات والأنظمة والشبكات المتأثرة إلى حالة تشغيلية غير متردية، وإعادة الخدمات المتأثرة إلى الأداء الوظيفي الكامل دون إعادة إنشاء سياق تمكين المشكلة الأمنية الأصلية لكيلا يُستغل مرة أخرى.

الوصف: بدون فهم كامل للتأثير على الأعمال ومتطلباتها للتخفيف والاستعادة، لن يقدَّم تصد ذو مغزى. ونظراً لوجود تضارب في المصالح – يتمثل في تتبع الهجوم للحصول على مزيد من المعلومات الاستخبارية مقابل احتواء الهجوم لتجنب المزيد من الخسائر – تقتضي الضرورة أخذ جميع المصالح في الاعتبار ووضع خطة تصد معقولة لمعالجة الوقائع المعروفة وتقديم النتيجة المرجوة ضمن الإطار الزمني المطلوب.

وكحال جميع الخطط، يجب أن تؤخذ في الاعتبار الحاجة إلى استعراض نتائج التحليل الجديدة كلما توفرت نتائج جديدة. وفي الواقع، ستحتاج خطة التصدي عادة إلى تغيير للاستمرار في تقديم التوجيه والإرشاد. ولكن بدون مثل هذه الخطة – وما لم تتولَّ التصدي مجموعة تنظيمية واحدة صغيرة ذات متطلبات قليلة من سطوح البينية خارجية أو كيانات أخرى – قد لا تنفَّذ الأنشطة بفعالية أو كفاءة بسبب نقص التنسيق.

النتيجة: خطة تصد متفق عليها تفي بمتطلبات الأعمال إذا حظيت بمساعدة ما هو متاح من الموارد والدعم، وهي ستنفَّذ بعدئذ. وستقدم خدمةُ "التنسيق" التتبع والتنسيق بواسطة فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT).

- تحديد أثر حادث أمن المعلومات على مصالح الأعمال.
- تحديد متطلبات الأعمال والإطار الزمني للتعافي الناجح.
- تحديد عمليات ومعايير القرار (إن لم تكن محددة أصلاً بالسياسات).
- تحديد الكائنات التي ستستعاد: البيئات والأنظمة والتطبيقات والأنظمة والوظائف الشاملة لعدة قطاعات، وما إلى ذلك.
- تحديد الدعم والإجراءات المطلوبة من الكيانات الداخلية والخارجية.
- تحديد خطة تصد تقدم تصدياً ذا مغزى ضمن ما يرجى من متطلبات الأعمال والإطار الزمني بناءً على الموارد المتاحة والنطاق التقني للإجراءات المطلوبة.

2.4.6 وظيفة: التدابير المخصصة والاحتواء المخصص

الغرض: تنفيذ التدابير التي تضمن عدم تواصل انتشار حادث أمن المعلومات، أي بقاءه محصوراً في المتأثر حالياً من نظام، و/أو المستخدمين، و/أو الميادين لضمان عدم تكبد خسائر أخرى (بما في ذلك تسرب الوثائق أو التغييرات في قواعد البيانات أو البيانات، وما إلى ذلك).

الوصف: يتمثل التحدي المباشر عند وقوع حادث أمن معلومات في منعه من الانتشار. فعندما تُخترق الأنظمة أو تنشط البرمجيات الضارة على أنظمة المستخدم النهائي، يُتكبد المزيد من خسائر البيانات والمزيد من الخروقات. وعادةً ما يكون الهدف الرئيسي للهجمات هو النفاذ إلى بيانات وأنظمة محددة، بما في ذلك الهجمات (ومنها على سبيل المثال لا الحصر التحركات على المستوى نفسه) على منظمات أخرى داخل وخارج المنظمة التي تتعرض لحادث أمن معلومات. ويتطلب إيقاف أي أنشطة ضارة، أو على الأقل الحد من نطاقها أو من المزيد من الخسائر، إجراءات قصيرة المدى مثل حظر أو اصطفاء الحركة وإزالة النفاذ إلى خدمات أو أنظمة معينة، ويمكن أن يؤدي أيضاً إلى قطع التوصيل بأنظمة حرجة.

وسيسمح منع المزيد من النفاذ إلى بيانات الأدلة التي يحتمل أن تكون حرجة بإجراء تحليل كامل لهذه الأدلة. وكذلك سيؤدي منع المزيد من النفاذ إلى الأنظمة والشبكات الأخرى إلى الحد من التعرض للمساءلة نتيجة الأضرار التي تصيب المنظمات الأخرى.

ويمكن أن ينطوي كف الضرر الفوري والحد من مدى النشاط الضار من خلال الإجراءات التكتيكية قصيرة المدى (من قبيل حظر أو اصطفاء الحركة) على استعادة السيطرة على الأنظمة. فطالما ملك المهاجمون أو البرمجيات الضارة النشطة نفاذاً جاهزاً إلى المزيد من الأنظمة أو الشبكات، ستتعذر العودة إلى التشغيل العادي.

النتيجة: استعادة السيطرة على الأنظمة والشبكات المعنية. وحظر نفاذ المهاجمين والبرمجيات الضارة إلى البيانات والأنظمة والشبكات لتجنب المزيد من الهجمات، و/أو الأنظمة والبيانات المخترقة.

ويمكن أن نشكل الوظائف الفرعية التالية جزءاً من تنفيذ هذه الوظيفة:

- حجب النفاذ مؤقتاً عن المستخدمين/الأنظمة/الخدمات/الشبكات.
- فصل الأنظمة أو الشبكات مؤقتاً عن الشبكات أو الوصلات الفقرية.
- تعطيل الخدمات مؤقتاً.
- مطالبة المستخدمين بتغيير كلمات المرور أو بيانات اعتماد التجفير الخاصة بهم.
- ترصُّد علامات التسلل ومؤشرات الاختراق.
- التحقق من عدم تأثر جميع المستخدمين/الأنظمة/الخدمات/الشبكات.

3.4.6 وظيفة: استعادة النظام

الغرض: تنفيذ التغييرات اللازمة فيما يطاله الضرر ضمن ميدان أو بنية تحتية أو شبكة، لتدارك هذا النوع من النشاط ومنع تكراره.

الوصف: استعادة سلامة أنظمة متضررة وإرجاع البيانات والأنظمة والشبكات المتضررة إلى حالة تشغيلية غير متردية وإعادة الخدمات المتأثرة إلى الأداء الوظيفي الكامل. ونظراً لأن واقع الأعمال يتطلب عادةً عودة الأنظمة إلى التشغيل العادي في أقرب وقت ممكن، ثمة خطر يتمثل في عدم إزالة جميع وسائل النفاذ غير المجاز بنجاح. لذلك، ما لم تكن نتائج التحليل متاحة بالفعل، تجب مراقبة وإدارة الأنظمة المرتجعة بعناية. وخاصة إذا لم يكن من الممكن (بعد) إزالة الثغرات ونقاط الضعف المحددة، تدعو الحاجة إلى تطبيق آليات محسنة للحماية والكشف لتجنب نفس حوادث أمن المعلومات أو أنواع مماثلة لها.

النتيجة: تطبَّق تدابير لإعادة الأنظمة والخدمات إلى الأداء الوظيفي الكامل وكذلك السعة الكاملة. وتطبَّق إجراءات لإغلاق أيما يُكشف من ثغرات أو نقاط ضعف تساهم في حادث أمن المعلومات الأصلي. وتحسَّن تدابير الكشف والرد على النحو الموصى به في خطة التحليل والتصدي.

ويمكن أن نشكل الوظائف الفرعية التالية جزءاً من تنفيذ هذه الوظيفة:

- استعادة بيانات المستخدم/النظام من وسائط النسخ الاحتياطي الموثوقة.
- استعادة التشكيلات من وسائط النسخ الاحتياطي الموثوقة أو المحتوى المعاد إنشاؤه.
- تمكين الخدمات المعطلة وإعادة إنشاء النفاذ للمستخدمين/الأنظمة/الشبكات.
- إجراء اختبارات وظيفية للتحقق من سعة وقدرة الأنظمة/الخدمات/الشبكات على مستوى البنية التحتية والتطبيق معاً.

4.4.6 وظيفة: دعم كيانات أمن المعلومات الأخرى

الغرض: تمكين الجهات المخدَّمة من أداء الأنشطة الإدارية والتقنية المطلوبة من أجل التخفيف بنجاح من وطأة حادث أمن المعلومات والتعافي منه.

الوصف: يمكن أن يقدم فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) مساعدة مباشرة (في الموقع) لمساعدة الجهات المخدَّمة على التعافي من الخسائر وإزالة الثغرات الأمنية. ويمكن أن يشكل ذلك امتداداً مباشراً لتقديم خدمات التحليل في الموقع (انظر أعلاه). ومن ناحية أخرى، يمكن أن يختار فريق CSIRT دعم موظفي الجهات المخدَّمة المتصدين لحادث أمن المعلومات بتفسيرات وتوصيات أكثر تفصيلاً، وما إلى ذلك.

النتيجة: يُحسَّن تصدي الجهات المخدَّمة ويسرَّع التعافي. وبالإضافة إلى مجموعة المعارف المتاحة، يمكن تعزيز فعالية وكفاءة الأنشطة ذات الصلة في المستقبل. فضلاً عن ذلك، فهي تساعد على دعم تلك الكيانات داخل الجهات المخدَّمة التي تفتقر إلى المعارف التقنية التفصيلية لتنفيذ الإجراءات اللازمة للتصدي.

5.6 خدمة: التنسيق خلال حادث أمن المعلومات

الغرض: ضمان إرسال التبليغات في الوقت المناسب وتوزيع المعلومات بدقة؛ والحفاظ على تدفق المعلومات وتتبع حالة أنشطة الكيانات التي كُلفت بالمشاركة أو طُلبت منها المشاركة في التصدي لحادث أمن المعلومات؛ والتأكد من تنفيذ خطة التصدي وإدارة الانحرافات الناتجة عن كل من التأخيرات أو المعلومات الجديدة وفقاً لذلك.

الوصف: إن تلقي التبليغ والبقاء على اطلاع بشأن التفاصيل والأنشطة الجارية فيما يتعلق بحادث أمن المعلومات أمر بالغ الأهمية لجميع أصحاب المصلحة والمنظمات المعنية. ونظراً لأن بعض الأنشطة المطلوبة للنجاح في التخفيف والاسترداد يمكن أن تنطوي على موافقة الإدارة، فإن ذلك يتطلب وظائف تصعيد وتبليغ مناسبة توضع قبل أن يتسنى التعامل مع أي حادث أمن معلومات بفعالية وكفاءة. وإذ يقوم فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) بتحليل جميع المعلومات عند توفرها، يضمن التنسيق وصول التبليغات والمعلومات إلى نقاط الاتصال الصحيحة، وتتبُّع ردودها والتأكد من أن جميع الأطراف المنفذة للأنشطة تقدم تقارير جوابية تغذي الوعي الظرفي الدقيق إلى حين اعتبار ملف حادث أمن المعلومات مغلقاً ولا يتطلب المزيد من التنسيق.

وينبغي أن تتاح سبل لأصحاب المصلحة لإرسال الأسئلة، والتحقق من حالة حوادث أمن المعلومات، وإبلاغ المشاكل إلى فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT). وللتعامل مع أصحاب المصلحة الداخليين، ينبغي لفريق CSIRT تقديم قنوات اتصالات للإعلان عن حالة تدارك حوادث أمن المعلومات. وللتعامل مع أصحاب المصلحة الخارجيين، ينبغي لفريق CSIRT الحفاظ على قنوات اتصالات مع أفرقة CSIRT ومجتمعات CSIRT الأخرى التي يمكن أن تقدم توصيات أو دعماً تقنياً.

النتيجة: ينسَّق التصدي بنجاح بناءً على كيانات مطلعة تساهم في التصدي لحادث أمن المعلومات.

وتُعتبر الوظائف التالية جزءاً من تنفيذ هذه الخدمة:

- الاتصالات.
- توزيع التبليغات.
- توزيع المعلومات ذات الصلة.
- تنسيق الأنشطة.
- الإبلاغ.
- الاتصالات عبر وسائل الإعلام.

1.5.6 وظيفة: الاتصالات

الغرض: التعامل بفعالية مع أصحاب المصلحة وإنشاء قنوات اتصال متعددة مناسبة تقدم الكتمان المطلوب.

الوصف: يجب أن يقدم فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) أدق التفسيرات لجمهوره عند صياغة الاتصالات وإصدارها. وفي المقابل، يجب أيضاً تجهيز فريق CSIRT لتلقي التعليقات والتقارير والتعليقات والأسئلة الواردة من مجموعة متنوعة من المصادر بناءً على اتصالاته الخاصة.

ويمكن أن تتطلب سياسة الأمن وسياسة تناقل المعلومات معالجة المعلومات بطريقة صارمة. ويجب أن يتمكن فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) من تناقل المعلومات مع أصحاب المصلحة بطريقة موثوقة وآمنة ومنعزلة، سواء خارجياً أو داخلياً.

ويجب إعداد اتفاقات عدم الكشف مقدماً قدر الإمكان، وإعداد موارد الاتصالات وفقاً لذلك. واستطراداً، يمكن كذلك استخدام مفهوم "المعلومات الخاضعة للحظر". وبالتالي، يجب أيضاً وضع سياسة استبقاء لضمان التعامل مع البيانات المستخدمة لصياغة المعلومات، ومع المعلومات نفسها، وتناقلها والاحتفاظ بها على الوجه الصحيح استناداً إلى قيود – مثل الوقت – إلى أن تُرفع هذه القيود أو تُنشر المعلومات علناً.

يمكن لقنوات الاتصالات أن تتخذ أشكالاً متعددة حسب احتياجات أصحاب المصلحة والجهات المخدَّمة. ويجب وسم جميع المعلومات المرسلة وفقاً لسياسة تناقل المعلومات. ويمكن استخدام بروتوكول إشارات المرور.

النتيجة: تتوفر جميع قنوات الاتصالات وفقاً لمتطلبات الأمن لدى جميع الأطراف المستقبِلة والمرسِلة.

وتُعتبر الوظائف الفرعية التالية جزءاً من تنفيذ هذه الوظيفة:

- تقديم قنوات اتصال داخلية.
- تقديم قنوات اتصال خارجية.

2.5.6 وظيفة: توزيع التبليغات

الغرض: تنبيه الكيانات المتأثرة بحادث أمن المعلومات أو تلك التي يمكن أن تساهم في التصدي له وتزويد تلك الكيانات بالمعلومات المطلوبة لفهم دورها في التعامل معه وأي توقعات يمكن أن تكون موجودة فيما يتعلق بتعاونها ودعمها.

الوصف: تمس حادثة أمنية العديد من الكيانات الداخلية، وكيانات خارجية محتملة، وربما الأنظمة والشبكات. ونظراً لأن أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) تشكل نقطة مركزية لتلقي تقارير عن حوادث أمن المعلومات المحتملة، فإنها تعمل أيضاً كمحور لتبليغ جهات الاتصال المجازة عنها. ولا يقدم التبليغ عادةً التفاصيل التقنية المناسبة فحسب، بل أيضاً معلومات بشأن التصدي المتوقع ونقطة الاتصال بشأن أي متابعة.

النتيجة: تتوفر معلومات بشأن حادث أمن المعلومات للكيانات المطلوب منها إما المشاركة في التصدي له أو أخذ العلم به.

6.5.3 وظيفة: توزيع المعلومات ذات الصلة

الغرض: الاستمرار في التواصل مع الكيانات المحددة وتقديم تدفق مناسب من المعلومات المتاحة لتمكين تلك الكيانات من الاستفادة من الأفكار والدروس المستفادة المتاحة، وتطبيق الاستجابات المحسنة أو اتخاذ تدابير مخصصة جديدة.

الوصف: مع توالي فصول التصدي لحادث أمن المعلومات، يتيسر المزيد من نتائج التحليل والتقارير من خبراء أمنيين آخرين محتملين، أو أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT)، أو الضحايا.

ويمكن التماس العون من تمرير بعض المعلومات والدروس المستفادة إلى مجال خدمة نقل المعارف (إذا كانت مدعومة) لتحسين التدريب والوثائق التقنية وكذلك للمساعدة في خلق الوعي المناسب، خاصة إذا تحدَد جديد الهجمات أو اتجاهات الحوادث.

النتيجة: توزَّع المعلومات المتاحة إما على أولئك المسؤولين عن المشاركة في التصدي أو من يطلبون البقاء على علم بالتقدم الحاصل والوضع الراهن.

4.5.6 وظيفة: تنسيق الأنشطة

الغرض: تتبع حالة جميع الاتصالات والأنشطة.

الوصف: تقتضي الضرورة تتبع حالة جميع الاتصالات والأنشطة لأن العديد من الكيانات يُحتمل أن تشارك في التصدي لحادث أمن معلومات. ويشمل ذلك الإجراءات التي يطلبها فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) أو طلبات الاطلاع على المزيد من المعلومات بالإضافة إلى طلبات التحليل التقني للصنائع أو الاطلاع على مؤشرات الاختراق والمعلومات بشأن الضحايا الآخرين، وما إلى ذلك. 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 حادث. ولكنه يحدث أيضاً داخل المنظمات الكبيرة التي ينسق فيها فريق CSIRT الداخلي أنشطة التخفيف والاستعادة.

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 المهاجمين الجارية أو الحماية منها أو تداركها، وللمساعدة في إغلاق ملف حادث أمن المعلومات.

النتيجة: إذكاء الوعي الظرفي بالحالة الراهنة لجميع الأنشطة وحالة الكيانات التي تشارك في التصدي.

5.5.6 وظيفة: الإبلاغ

الغرض: التأكد من حصول جميع الكيانات المشاركة في مصالح الأعمال على معلومات بشأن حالة الأنشطة الحالية بحيث تستند القرارات الأخرى بشأن الخطوات التالية التي يجب اتخاذها إلى أفضل معرفة متاحة بالظروف.

الوصف: تقديم معلومات موجزة وواقعية عن الوضع الحالي للأنشطة المطلوبة أو المنفذة رداً على حادث أمن المعلومات. وبدلاً من انتظار سحب هذه المعلومات كجزء من عمل منسق مستمر على النحو المطلوب لأي تصد ناجح، تعد التقارير المقدَمة في الوقت المناسب حاسمة لتمكين التنسيق الفعال.

النتيجة: إطلاع أصحاب المصلحة الداخليين على نطاق الأنشطة الحالية والإجراءات المنجزة بالفعل والإجراءات المنتظَر اتخاذها. ويبلَّغ عن الأثر المقدَر للتأخيرات والتوصيات والإجراءات المطلوبة، مما يمكّن من فهم التأثير الإجمالي فيما يتعلق باستراتيجية التصدي المختارة والخطة الموضوعة.

6.5.6 وظيفة: الاتصالات عبر وسائل الإعلام

الغرض: التفاعل مع وسائل الإعلام (العامة) كي تتمكن من تقديم معلومات واقعية وسهلة الفهم بشأن الأحداث الجارية ودرءاً لانتشار الشائعات والمعلومات المضللة.

الوصف: لا يتيسر التواصل مع وسائل الإعلام في كثير من الحالات. وبينما تحاول أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) عادةً تجنب مثل هذا الاتصال، من المهم إدراك أن وسائل الإعلام يمكن أن تساعد في التخفيف من أنواع معينة من الهجمات المستمرة والواسعة النطاق التي تتسبب في حوادث أمن المعلومات. لذا تقتضي الضرورة شرح ما الذي يسبب حوادث أمن المعلومات وشرح التأثير على المستخدمين، و/أو المنظمات. وفي بعض الحالات، يمكن أن يختار فريق CSIRT تقديم هذه المعلومات فعلاً بطريقة نشر مناسبة للجمهور، ولكن ذلك يتطلب بالتأكيد مهارات معينة داخل فريق CSIRT لا يسهل توفرها في الغالب. وعلى أي حال، إذا تواصل فريق CSIRT مع وسائل الإعلام، يجب أن يحرص على تبسيط المشاكل التقنية قدر الإمكان وحذف جميع المعلومات المكتومة.

النتيجة: إعداد معلومات واقعية تقدم ملخصاً واضحاً لحادث أمن المعلومات الجاري بما في ذلك الخطوات التي يتعين على الضحايا المحتملين اتخاذها أو تحديد استراتيجية التصدي المختارة للتعافي من حادث أمن المعلومات.

6.6 خدمة: دعم إدارة الأزمات

الغرض: تقديم الخبرة وجهات الاتصال لخبراء الأمن الآخرين، وأفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT)، ومجتمعات CSIRT للمساعدة في تخفيف الأزمة.

الوصف: على الرغم من أن حوادث أمن المعلومات اليوم نادراً ما تشكل أزمة للمنظمات أو أزمة وطنية، إلا أنها تنطوي على إمكانية فعل ذلك. ولكن التصدي لأزمة عادة ما يرتبط بحالة طوارئ تهدد حسن حال البشر والمجتمع ككل، أو تهدد على الأقل وجود منظمة. ومن الثابت في إدارة الأزمات أن دوراً رفيع المستوى سيتولى مسؤولية الأزمة، وبالتالي يتغير تسلسل القيادة المعتاد طوال فترة الطوارئ.

ونظراً لأن الأنظمة والشبكات يمكن أن تساهم في حالات الطوارئ أو يُطلب منها أن تكون متاحة للتصدي لحالة متأزمة، فإن فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) سيكون عادةً مورداً مهماً لإدارة مثل هذه المواقف وتقديم خبرة قيِّمة وأيضاً الخدمات والشبكات القائمة لنقاط الاتصال.

النتيجة: يمكن لفريق إدارة الأزمات استخدام موارد فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) لمعالجة جوانب الأمن السيبراني للأزمة الحالية. وفي الوقت نفسه، يمكن استخدام موارد الاتصالات الخاصة بفريق CSIRT للتواصل مع الجهات المخدَّمة والأطراف الخارجية طلباً لإجراءات دعم أو مساعدة محددة. ويمكن استخدامه أيضاً للتواصل بطريقة موثوقة مع الجهات المخدَّمة، باستخدام وسائل الاتصال المعمول بها والشبكات الموثوقة.

وتُعتبر الوظائف التالية جزءاً من تنفيذ هذه الخدمة:

- توزيع المعلومات على الجهات المخدَّمة.
- الإبلاغ عن حالة أمن المعلومات.

- إبلاغ القرارات الاستراتيجية.

1.6.6 وظيفة: توزيع المعلومات على الجهات المخدَّمة

الغرض: تقديم موارد اتصالات قائمة للمساعدة في التصدي لأزمة.

الوصف: مع تقدم التصدي لأزمة، يجب توزيع المعلومات ونشرها. ونظراً لأن فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) قد أنشأ هذه الموارد لأغراضه الخاصة، يمكن أن ترى إدارة الأزمة أن من المناسب أو الضروري استخدام هذه الموارد.

النتيجة: توزَّع المعلومات المتاحة على الجهات المخدَّمة، بالاستفادة من علاقات الثقة القائمة التي تساعد على طمأنة المستفيدين من دقة المعلومات المنشورة.

2.6.6 وظيفة: الإبلاغ عن حالة أمن المعلومات

الغرض: التأكد من أن لدى فريق إدارة الأزمات نظرة عامة كاملة على حوادث أمن المعلومات الحالية والثغرات المعروفة لينظر في ذلك كجزء من مجمل أولوياته واستراتيجياته.

الوصف: تتضمن الوظيفة تقديم معلومات موجزة وواقعية بشأن الوضع الحالي للأمن السيبراني ضمن الجهات المخدَّمة. ونظراً لأن الأزمة يمكن أن تُستخدم لشن هجمات أخرى أو يمكن أن تكون الهجمات التي تشَن جزءاً من مجمل الأنشطة التي تؤدي إلى هذه الأزمة، من المهم جداً لفريق إدارة الأزمات أن يسعى إلى التوعية الكاملة بظروفها.

ويمكن لفريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) إذكاء مثل هذا الوعي الظرفي في خدماته ولدى الجهات التي يخدمها. ويمكن طلب ذلك أو توقعه بالسياسات المعيارية في وقت الأزمات. وعلى أي حال، ونظراً لأن إدارة الأزمات لا تنجح إلا بناءً على تدفق المعلومات المعمول به حيث يعتمد على تنسيق الموارد لمعالجة أكثر جوانب الأزمة حراجةً، يجب أن يكون الإبلاغ دقيقاً وفي الوقت المناسب.

ونظراً لأن حوادث أمن المعلومات الجارية ستتطلب موارد للتعامل معها، يجب اتخاذ قرار إما بوقف التصدي طوال مدة الحادث (وتخصيص الموارد المتاحة الآن لمجالات أخرى) أو بمواصلة العمل. ولا يمكن اتخاذ قرارات معقولة إلا بناءً على أفضل معرفة متاحة بالظروف.

النتيجة: إطلاع فريق إدارة الأزمات على نطاق الأنشطة الحالية والإجراءات المنجزة بالفعل والإجراءات المنتظَر اتخاذها. ويبلَّغ عن الأثر المقدَر للتأخيرات والتوصيات والإجراءات المطلوبة، مما يمكِّن من فهم التأثير الإجمالي فيما يتعلق بالاستراتيجية المختارة لمعالجة الأزمة الحالية.

3.6.6 وظيفة: القرارات الاستراتيجية

الغرض: إبلاغ الكيانات الأخرى في الوقت المناسب عن تأثير الأزمة على حوادث أمن المعلومات المفتوح ملفها حالياً.

الوصف: إبلاغ الكيانات الأخرى في الوقت المناسب بشأن التأثير الذي تسببه الأزمة على حوادث أمن المعلومات المفتوح ملفها حالياً على نحو يقدم فهماً واضحاً للدعم الذي يمكن أن يقدمه أيضاً فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) طوال فترة الأزمة، ويتأكد من فهم الكيانات لما يُتوقع. ويتأكد أيضاً من إيقاف الأطراف الأخرى لدعمها أو تفاعلها مع فريق CSIRT عندما تعتقد بأن الأزمة تستفحل.

ونظراً لأن فريق إدارة الأزمات يمكن أن يقرر تأجيل التصدي لحادث أمن معلومات فعلي بسبب أزمة، تدعو الحاجة إلى إبلاغ هذه القرارات إلى جميع الكيانات المطلعة والمشاركة حالياً. وذلك لتجنب سوء الفهم والإشكالات الأخرى التي يمكن أن تؤدي أيضاً إلى فقدان الثقة في فريق CSIRT، و/أو المنظمة المضيفة.

النتيجة: معلومات تأثير الأزمة على تشغيل فريق CSIRT توزَّع على الجهات المخدَّمة والكيانات الأخرى المشاركة في التصدي لحوادث أمن المعلومات المفتوح ملفها. ويرد وصف واضح لتوقعات فريق CSIRT تجاه هذه الكيانات ويُضمن الإبلاغ بوضوح عن احتياجات فريق CSIRT من المعلومات.

7 مجال الخدمة: إدارة الثغرات

يتضمن مجال خدمة إدارة الثغرات الخدمات المتعلقة باكتشاف وتحليل ومعالجة الثغرات الأمنية الجديدة أو التي أُبلغ عنها في أنظمة المعلومات. ويتضمن مجال خدمة إدارة الثغرات أيضاً الخدمات المتعلقة بكشف الثغرات المعروفة والتصدي لها منعاً لاستغلالها. لذلك، يشمل مجال الخدمة هذا الخدمات المتعلقة بالثغرات الجديدة والمعروفة على السواء.

وعلى الرغم من استخدام مصطلح "إدارة الثغرات" أحياناً للإشارة إلى مجرد عملية منع استغلال الثغرات المعروفة (مثل "البحث والترقيع")، ففي هذا الإطار لخدمات فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT)، تعتبر هذه الأنشطة وظائف ووظائف فرعية ضمن خدمة تسمى التصدي للثغرات وهي ليست إلا خدمة واحدة يمكن أن يقدمها فريق CSIRT. وبالنسبة للعديد من أفرقة CSIRT، تقع مسؤولية وظائف التصدي للثغرات على عاتق الأدوار الأخرى التي تبحث عن الثغرات الأمنية وتتداركها.

وتُعتبر الخدمات التالية بمثابة عروض في مجال الخدمة هذا:

- البحث الساعي لاكتشاف الثغرات.
- التقارير الواردة عن الثغرات.
- تحليل الثغرات.
- التنسيق بشأن الثغرات.
- الكشف عن الثغرات.
- التصدي للثغرات.

وسيقدم عدد قليل من أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) كل هذه الخدمات، بل إنها ستكتفي بدلاً من ذلك بتقديم ما يقع من هذه الخدمات في مجال مسؤوليتها. فعلى سبيل المثال، يمكن أن يقصر فريق CSIRT خدماته على التعرف على ثغرة جديدة من المصادر العامة (البحث الساعي لاكتشاف الثغرات) أو من أطراف ثالثة (التقارير الواردة عن الثغرات) ثم يصدر مشورة أمنية إلى الجهات التي يخدمها (الكشف عن الثغرات) عند الحاجة، دون المشاركة بالضرورة في أي جهود تنسيقية مع موردي المنتجات أو الآخرين الذين يطورون حلاً (التنسيق بشأن الثغرات)، أو يشاركون في نشر تصليح مباشرةً (التصدي للثغرات).

1.7 خدمة: البحث الساعي لاكتشاف الثغرات

الغرض: العثور على ثغرات جديدة (غير معروفة سابقاً) أو العلم بها أو البحث عنها؛ ويمكن اكتشاف الثغرات على يد الأعضاء في مجال خدمة إدارة الثغرات أو من خلال أنشطة فريق CSIRT الأخرى ذات الصلة.

الوصف: يعد اكتشاف ثغرة أمنية جديدة خطوة أولى ضرورية تبدأ مجمل دورة حياة إدارة الثغرات. وتتضمن هذه الخدمة تلك الوظائف والأنشطة التي يمكن أن ينشط بها فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) من خلال أبحاثه الخاصة أو خدمات أخرى لاكتشاف ثغرة جديدة. ويرد لاحقاً، في خدمة التقارير الواردة عن الثغرات، وصف الوظائف والأنشطة المتعلقة بالاستلام السلبي لمعلومات عن ثغرات جديدة من شخص آخر. وفي بعض الأحيان، يمكن أن يكتشف فريق CSIRT ثغرة جديدة خلال أنشطة أخرى، ومثال ذلك أثناء تحليل تقرير حادث أو التحقيق فيه. وثمة وسيلة أخرى تتمثل بالعلم بثغرة جديدة من خلال قراءة المصادر العامة (من قبيل المواقع الإلكترونية والقوائم البريدية[6]) أو مصادر خارجية أخرى (مثل الخدمات ذات الرسوم الإضافية والاشتراكات)، أو من خلال البحث بنشاط عن الثغرات عبر البحث المتعمد (من خلال الفحص العشوائي أو الهندسة العكسية على سبيل المثال). وينبغي توثيق هذه الاكتشافات وإدخالها في عمليات معالجة الثغرات في المنظمة، بغض النظر عن كيفية اكتشاف فريق CSIRT للثغرة أو معرفته بها.

النتيجة: تؤدي هذه الخدمة إلى تزايد اكتشاف الثغرات المحتملة التي لم يبلَّغ عنها مباشرة إلى فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT).

---

6 يمكن اعتبار المعلومات عن الثغرات الجديدة التي ترد عبر البريد الإلكتروني نشاطاً يندرج إما في خدمة اكتشاف الثغرات، أو وظيفة اكتشاف الثغرات من المصادر العامة، أو خدمة التقارير الواردة عن الثغرات، أو وظيفة تلقي تقرير عن الثغرات، حسب العمليات الداخلية لفريق CSIRT أو مدى اتساع نطاق توزيع المعلومات عن الثغرات.

وتُعتبر الوظائف التالية جزءاً من تنفيذ هذه الخدمة:

- اكتشاف ثغرة عند التصدي لحادث.
- اكتشاف ثغرة من مصدر عام.
- البحث عن الثغرات.

ويمكن أن تكون هذه الوظائف عبارة عن خدمات (أو وظائف) يؤديها آخرون (مثل الباحثين أو الموردين أو أفرقة التصدي لحوادث أمن المنتجات (PSIRT) أو المتخصصين الخارجيين) بدلاً من فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT).

1.1.7 وظيفة: اكتشاف ثغرة عند التصدي لحادث

الغرض: التعرف على ثغرة أمنية استُغلت كجزء من حادث أمني.

الوصف: أثناء تحليل حادث أمني، يمكن اكتشاف معلومات تشير إلى أن المهاجم استغل ثغرة. ولعل الحادث وقع من خلال استغلال ثغرة معروفة لم ترقَّع أو يخفَّف ضررها سابقاً؛ أو لعله وقع بسبب ثغرة جديدة (قبل الإعلان عنها).

ويمكن استلام بعض معلومات عن هذه الثغرة على أنها من مخرجات إحدى خدمات مجال خدمة إدارة حوادث أمن المعلومات إذا استُغلت ثغرة أمنية كجزء من حادث. ويمكن بعد ذلك تمرير المعلومات إلى وظيفة فرز الثغرات أو خدمة تحليل الثغرات، حسب الاقتضاء.

النتيجة: تمرَر إلى مجال خدمة إدارة الثغرات معلومات بشأن ثغرة أمنية يُشتبه في استغلالها كجزء من حادث أمني.

2.1.7 وظيفة: اكتشاف ثغرة من مصدر عام

الغرض: التعرف على ثغرة أمنية جديدة من قراءة مصادر عامة أو مصادر أخرى تابعة لأطراف ثالثة.

الوصف: يمكن أن يتعرف فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) في البداية على ثغرة جديدة من مصادر عامة مختلفة تعلن عن مثل هذه المعلومات. ويمكن أن تتضمن المصادر إعلانات الموردين، ومواقع إلكترونية أمنية، وقوائم بريدية، وقواعد بيانات الثغرات، ومؤتمرات أمنية، ووسائل التواصل الاجتماعي، وما إلى ذلك. ويمكن أن تتعرف هذه الوظيفة أيضاً على ثغرات جديدة من خلال مصادر أخرى تابعة لأطراف ثالثة قد لا تكون مفتوحة تماماً للعموم، من خلال الاشتراكات المدفوعة أو الخدمات ذات الرسوم الإضافية مثلاً حيث ينحصر تناقل المعلومات ضمن مجموعة محدودة. ويمكن أن تُسند إلى موظفين مسؤولية أداء هذه الوظيفة وجمع المعلومات لتنظيمها بغية مواصلة استعراضها وتناقلها. ويمكن أيضاً تلقي معلومات مماثلة عن ثغرات من خدمات مجال خدمة الوعي الظرفي.

النتيجة: تحدَد ثغرات جديدة كُشف عنها من خلال مصادر عامة أو مصادر خارجية أخرى.

3.1.7 وظيفة: البحث عن الثغرات

الغرض: اكتشاف ثغرات جديدة أو البحث عنها من خلال الأنشطة المتعمدة أو البحوث.

الوصف: تتضمن هذه الوظيفة اكتشاف ثغرات جديدة نتيجة لأنشطة محددة يقوم بها فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT)، مثل اختبار الأنظمة أو البرمجيات التي تستخدم الفحص العشوائي (fuzzing)، أو من خلال الهندسة العكسية للبرمجيات الضارة.

ويمكن أن تتلقى هذه الوظيفة أيضاً مدخلات من خدمة (خدمات) مجال خدمة إدارة حوادث أمن المعلومات أو مجال خدمة الوعي الظرفي التي من شأنها أن تباشر بهذه الوظيفة للبحث عن الثغرات المشتبه فيها.

ويمكن أن يصبح اكتشاف ثغرة جديدة نتيجة لوظيفة البحث عن الثغرة هذه مدخلاً لخدمة التصدي للحوادث، ووظيفة كشف الثغرات الأمنية (انظر الوظائف الفرعية لفحص الثغرات واختبار تغلغل الثغرات).

النتيجة: تتحدد الثغرات الجديدة من خلال البحث.

2.7 خدمة: التقارير الواردة عن الثغرات

الغرض: تلقي ومعالجة معلومات عن ثغرات أبلغت عنها جهات مخدَّمة أو أطراف ثالثة.

الوصف: يمكن للتقارير أو الأسئلة التي ترسلها جهات يخدمها فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) أو أطراف ثالثة أخرى أن تكون أحد المصادر الأساسية للمعلومات عن الثغرات. وينبغي أن يتوقع فريق CSIRT إمكانية الإبلاغ عن الثغرات من هذه المصادر المتنوعة، وأن يقدم آلية وعملية وتوجيهات لإعداد تقارير عن الثغرات. ويمكن أن تتضمن البنية التحتية لتقديم التقارير بريداً إلكترونياً أو استمارة على شبكة الإنترنت للإبلاغ عن الثغرات. ولا تبلِّغ الجهات المخدَّمة أو الأطراف الثالثة فريقَ CSIRT مباشرة بجميع الثغرات من خلال القنوات القائمة. وينبغي أن تتضمن الإرشادات الداعمة مبادئ توجيهية لإعداد التقارير ومعلومات الاتصال وأي سياسات بشأن الكشف عن المعلومات.

ولتمكين الجهات المخدَّمة من الإبلاغ عن الثغرات بمزيد من الفعالية، ينبغي لفريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) تقديم آلية واحدة أو أكثر بالإضافة إلى إرشادات أو تعليمات بشأن ماهية وكيفية الإبلاغ عن الثغرات بشكل آمن. ويمكن أن تتضمن آليات الإبلاغ بريداً إلكترونياً أو موقعاً إلكترونياً أو استمارة مخصصة أو بوابة إلكترونية للإبلاغ عن الثغرات أو أساليب أخرى مناسبة لتمكين تقديم التقارير على نحو سليم وآمن. وإذا لم تُدرَج إرشادات إعداد التقارير، كجزء من استمارة الإبلاغ نفسها عن حوادث أمن المعلومات، فينبغي تقديمها في توثيق منفصل أو عبر صفحة إلكترونية، وينبغي أن تسرد المعلومات المحددة المرغوب إدراجها في التقرير.

النتيجة: يُتلقى تقرير الثغرات بواردات مهنية ومتسقة في كل تقرير بالإضافة إلى التحقق الأولي منه وتصنيفه الأولي.

وتُعتبر الوظائف التالية جزءاً من تنفيذ هذه الخدمة:

- تلقي تقارير عن ثغرات.
- فرز التقارير عن ثغرات ومعالجتها.

1.2.7 وظيفة: تلقي تقارير عن ثغرات

الغرض: قبول أو تلقي معلومات بشأن ثغرة، كما تُبلغ عنها الجهات المخدَّمة أو الأطراف الثالثة.

الوصف: تتطلب الواردات الفعالة للتقارير عن الثغرات آليات وعمليات لاستلام التقارير من الجهات المخدَّمة وأصحاب المصلحة والأطراف الثالثة (أي المكتشفين، أو الباحثين، أو أفرقة التصدي لحوادث أمن المنتجات (PSIRT)، أو أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) الأخرى أو منسقي الثغرات ومن إلى ذلك). ويمكن أن تتضمن المعلومات عن الثغرات الأجهزة المتأثرة، والظروف اللازمة لاستغلال الثغرات، والتأثير (مثل تصعيد الامتيازات، والنفاذ إلى البيانات، وما إلى ذلك)، بالإضافة إلى الإجراءات المتخذة لحل الثغرات، وخطوات التدارك و/أو التخفيف، والحل. وفي بعض الأحيان، يمكن أن ترد معلومات الثغرات بشكل مشترك كجزء من المدخلات إلى خدمات أخرى، وعلى الأخص واردات تقرير حادث أمن المعلومات (من قبيل إذا أُبلغ عن استغلال ثغرة كجزء من تقرير الحادث).

النتيجة: يُتعامل مع تقارير عن الثغرات من الجهات المخدَّمة أو الأطراف الثالثة بشكل مناسب، بما في ذلك بدء توثيق أو تتبع التقارير.

وتُعتبر الوظائف الفرعية التالية جزءاً من تنفيذ هذه الوظيفة:

- مراقبة قنوات الاتصالات بانتظام والتحقق مما إذا كانت الوسائل المعلن عنها للاتصال بفريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) جاهزة للعمل ويمكن تقديم التقارير.
- إرسال إشعار أولي باستلام التقرير لمقدم تقرير عن ثغرة، وطلب معلومات إضافية إذا لزم الأمر، وتهيئة التوقعات مع مقدم التقرير.

2.2.7 وظيفة: فرز التقارير عن ثغرات ومعالجتها

الغرض: استعراض التقرير عن ثغرة وتصنيفه وترتيب أولوياته ومعالجته في البداية.

الوصف: تُستعرض التقارير عن الثغرات وتُفرز للتوصل إلى فهم أولي للثغرة المعنية وتحديد ما يجب القيام به بعد ذلك (من قبيل معالجة الثغرة لمواصلة التحليل، وطلب معلومات إضافية من الجهة المبلِّغة أو مصادر أخرى، والبت في أن الثغرة لا تحتاج

إلى مزيد من الإجراءات). وحسب مقدار التفاصيل وجودة المعلومات المقدمة في التقرير عن الثغرات، يمكن أن يتضح أو لا يتضح ما إذا كانت هناك ثغرة جديدة.

وما لم يكن هناك سبب لرفض تقرير عن ثغرة، ينبغي إرسال التقرير إلى خدمة تحليل الثغرات لمواصلة استعراضه وتحليله والتعامل معه. وإذا لم يقدم فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) خدمة تحليل الثغرات، تنبغي إعادة توجيه التقرير بشكل آمن إلى مجموعة خارجية للتعامل معه، مثل المورد (الموردين) المتأثرين أو فريق (فرق) الاستجابة لحوادث أمن المنتجات (PSIRT) أو منسق بشأن الثغرة.

النتيجة: تتحدد المعلومات المتاحة للوقوف على ما يجب القيام به بعد ذلك.

وتُعتبر الوظائف الفرعية التالية جزءاً من تنفيذ هذه الوظيفة:

- معالجة التقارير والبيانات المقدمة بما في ذلك الصنائع أو المواد بمعزل عن بعضها البعض لحماية سلامة بيئة العمل وتجنب الهجمات الناجحة على فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) بهذه الوسائل.
- تحديث الإشعار باستلام التقارير من خلال تقديم بعض الملاحظات التقييمية بشأن الخطوات الإضافية بناءً على نتائج الفهرسة أو تحديد الأولويات المتاحة.
- دمج المعلومات الجديدة بشأن ثغرة يُتعامل معها بالفعل في البيانات المتاحة للسماح باتساق التحليل والمعالجة.

3.7 خدمة: تحليل الثغرات

الغرض: تحليل الثغرات المؤكدة وفهمها.

الوصف: تتكون خدمة تحليل الثغرات الأمنية من وظائف تهدف إلى اكتساب فهم للثغرة وتأثيرها المحتمل، وتحديد الإشكال أو الخلل الأساسي (السبب الجذري) الذي يسمح باستغلال الثغرة، وتحديد واحدة أو أكثر من استراتيجيات العلاج أو التخفيف لمنع استغلال الثغرة أو التقليل منه إلى أدنى حد.

ويمكن أن تستمر خدمة ووظائف تحليل الثغرات بالتوازي أثناء تنفيذ خدمة ووظائف التنسيق بشأن الثغرات مع مشاركين آخرين في عملية الكشف المنسق عن الثغرات (CVD).[7]

.**النتيجة:** زيادة المعارف بالتفاصيل الرئيسية للثغرة (من قبيل الوصف، والتأثير، والحل).

وتُعتبر الوظائف الفرعية التالية جزءاً من تنفيذ هذه الوظيفة:

- فرز الثغرات (التحقق والفهرسة).
- تحليل السبب الجذري للثغرة.
- إعداد تدارك الثغرة.

1.3.7 وظيفة: فرز الثغرات (التحقق والفهرسة)

الغرض: فهرسة الثغرة، وتحديد أولويتها، وإجراء تقييم أولي لها.

الوصف: تبدأ خدمة تحليل الثغرات باستعراض المعلومات المتاحة من أجل فهرسة الثغرة وتحديد أولويتها وتقييم ما إذا كان لها بعض التأثير على الأنظمة المعنية وما إذا كانت ذات صلة بولاية فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT). ولعل توثيق بعض من ذلك يرد أثناء وظيفة فرز ومعالجة تقرير عن الثغرة (من خدمة واردات تقرير عن الثغرة) إذا أُبلغت إحدى الجهات المخدَّمة أو طرف ثالث عن الثغرة إلى فريق CSIRT.

وفي حال عدم الانتهاء من الفرز المسبق بالفعل، يمكن إسناد الثغرة إلى خبير في الموضوع يمكنه تقديم تأكيد تقني بأن له بعض التأثير على الأنظمة المعنية وأنه على صلة بولاية فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) (أي له تأثير أمني محتمل

[7] انظر مجالات خدمة التنسيق بشأن الثغرات والكشف عن الثغرات للاطلاع على معلومات ذات صلة بالكشف المنسق عن الثغرات (CVD).

على الشبكات أو الأنظمة يمكن أن يؤدي إلى الإضرار بكتمان أو توفر أو سلامة أصول المعلومات في مجال يخص فريق CSIRT وفقاً لولايته).

النتيجة: يصنَّف سجل المعلومات الخاص بالثغرة وتحدَد أولوياته ويحدَّث.

2.3.7 وظيفة: تحليل السبب الجذري للثغرة

الغرض: فهم عيب التصميم أو التنفيذ الذي يتسبب بوجود الثغرة أو يكشف النقاب عنها.

الوصف: الهدف من هذا التحليل هو تحديد السبب الجذري للثغرة، وتحديد الظروف التي تسمح بوجود ثغرة، وفي أي ظروف يمكن للمهاجم أن يستغل الثغرة. ويمكن أن يسعى هذا التحليل أيضاً لفهم نقطة (نقاط) الضعف المغتنَمة للتسبب في حادث ما، والصنائع العدائية المستخدمة في اغتنام نقطة الضعف تلك. وحسب طبيعة الثغرة، يمكن أن يصعب على فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) أداء هذه الوظيفة على أكمل وجه. وفي بعض الحالات، يمكن لمكتشف الثغرة أو المبلِّغ عنها أن يقوم بهذه الوظيفة. وفي العديد من المواقف، يكون أفضل من يقوم بهذه الوظيفة مورِّد المنتج أو مطور البرمجيات أو النظام المتأثر أو فريق الاستجابة لحوادث أمن المنتجات (PSIRT) الخاص به. ويمكن: أيضاً وجود ثغرة في أكثر من منتج، وفي هذه الحالة قد تدعو الحاجة إلى تحليلات متعددة للبرمجيات أو الأنظمة المتأثرة، مما يتطلب التنسيق مع العديد من الموردين أو أفرقة PSIRT أو أصحاب المصلحة.

النتيجة: يُستخدم فهم الثغرة والطريقة التي سيتمكن بها الفاعلون الضارون من استخدام هذه الثغرة لتحديد أساليب التدارك أو التخفيف لتقليل خطر التعرض أو الاستغلال إلى أدنى حد.

3.3.7 وظيفة: إعداد تدارك الثغرة

الغرض: وضع الخطوات اللازمة لإصلاح (تدارك) الثغرة الأمنية أو التخفيف (التقليل) من استغلال آثار الثغرة.

الوصف: ستحدد هذه الوظيفة في الحالة المثالية تداركاً أو إصلاحاً لثغرة. وإن لم يتوفر ترقيع تصحيحي أو إصلاح لدى المورِّد في الوقت المناسب، يمكن أن يوصى بحل مؤقت للمشكلة أو التفاف عليها، يسمى التخفيف، مثل تعطيل البرمجيات المتأثرة أو إجراء تغييرات في التشكيلة، لتقليل الآثار السلبية المحتملة للثغرة إلى أدنى حد؛ علماً بأن التطبيق أو النشر الفعلي للتدارك (الترقيع التصحيحي) أو التخفيف (حل التفافي) هو وظيفة لخدمة منفصلة، تسمى التصدي للثغرة في هذا الإطار.

وكجزء من خدمة تحليل الثغرات وإعداد تداركها، يمكن أن تتضمن هذه الوظيفة اختيارياً وظائف فرعية أو أنشطة أخرى، مثل التحقق من تغيير إجراء أو تصميم، أو استعراض طرف ثالث للتدارك، أو تحديد أي ثغرات جديدة أُدخلت في خطوات التدارك. وينبغي توثيق الثغرات التي لم تُتدارك أو تخفَف كمخاطر مقبولة.

وكثيراً ما ستتلقى هذه الوظيفة معلومات أو مدخلات من مورِّد (مورِّدي) المنتج المتأثر، كجزء أحياناً من التقرير أو الإعلان الأولي الذي تتعامل معه خدمات أو وظائف أخرى.

النتيجة: توضع خطة لتغيير (ترقيع) شفرة البرمجيات، أو تنفيذ حل التفافي، أو لتحسين العمليات، و/أو البنى التحتية، و/أو التصاميم من أجل إغلاق ناقل الهجوم المحدد ومنع استغلال الثغرة.

وتُعتبر الوظائف الفرعية التالية جزءاً من هذه الوظيفة:

- إعداد تدارك/ترقيع الثغرة.
- إعداد التخفيف من الثغرة.

وتنفِّذ هذه الوظيفة عادةً كيانات أخرى (من قبيل مورِّدي المنتجات، أو أفرقة التصدي لحوادث أمن المنتجات (PSIRT)).

4.7 خدمة: التنسيق بشأن الثغرات

الغرض: تبادل المعلومات وتنسيق الأنشطة مع المشاركين المنخرطين في عملية الكشف المنسق عن الثغرات (CVD).

الوصف: تتضمن معالجة معظم الثغرات التبليغ والعمل البيني وتنسيق تبادل المعلومات ذات الصلة مع أطراف متعددة بما فيها الباحثون/المبلغون عن الثغرات أو مَن يتأثر بها من المورِّدين أو المطورين أو أفرقة التصدي لحوادث أمن المنتجات

(PSIRT) أو غيرهم من الخبراء الموثوقين (مثل الباحثين، وأفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) والمنسقين بشأن الثغرات) الذين يمكنهم العمل معاً لتحليل الثغرة وإصلاحها.

النتيجة: تناقل المعلومات مع المشاركين في عملية الكشف المنسق عن الثغرات (CVD) الذين يمكنهم المساعدة في تقديم المعلومات لتدارك/تخفيف الثغرة بفعالية وفي الوقت المناسب.

وتُعتبر الوظائف الفرعية التالية جزءاً من تنفيذ هذه الوظيفة:

- الإبلاغ/إعداد التقارير عن الثغرات.
- التنسيق بشأن الثغرات مع أصحاب المصلحة.

1.4.7 وظيفة: الإبلاغ/إعداد التقارير عن الثغرات

الغرض: مستهل تناقل أو إبلاغ معلومات عن ثغرة جديدة مع الآخرين الذين سيشاركون في عملية الكشف المنسق عن الثغرات (CVD).

الوصف: تتضمن معالجة معظم الثغرات التبليغ والعمل البيني وتنسيق تبادل المعلومات ذات الصلة مع أطراف متعددة بما فيها الباحثون/المبلغون عن الثغرات أو مَن يتأثر بها من المورِّدين أو المطورين أو أفرقة التصدي لحوادث أمن المنتجات (PSIRT) أو غيرهم من الخبراء الموثوقين (مثل الباحثين، وأفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) والمنسقين بشأن الثغرات) الذين يمكنهم العمل معاً لتحليل الثغرة وإصلاحها.

النتيجة: إبلاغ المورِّدين (أو المشاركين الآخرين في عملية الكشف المنسق عن الثغرات (CVD)) بشأن الثغرة بحيث يمكنهم العمل على تطوير حل متدارك أو تخفيفي.

2.4.7 وظيفة: التنسيق بشأن الثغرات مع أصحاب المصلحة

الغرض: إجراء تنسيق متابعة وتناقل معلومات بين مختلف أصحاب المصلحة والمشاركين المنخرطين في جهود الكشف المنسق عن الثغرات.

الوصف: تنسيق تبادل المعلومات بين المكتشفين/الباحثين، المورِّدين، وأفرقة التصدي لحوادث أمن المنتجات (PSIRT)، وأي مشاركين آخرين في جهود الكشف المنسق عن الثغرات (CVD) لتحليل الثغرات وإصلاحها، والتحضير للكشف عن الثغرات. وينبغي أن يشمل هذا التنسيق أيضاً موافقة المشاركين على توقيت ومزامنة الكشف.

النتيجة: تُتناقل المعلومات عن الثغرات بمزيد من الفعالية، وفي الوقت المناسب، وبشكل مسؤول بين المشاركين الذين يمكنهم تطوير أو إعلان حل متدارك/تخفيفي.

وتُعتبر الوظائف الفرعية التالية جزءاً من هذه الوظيفة:

- إعداد منشورات عن الثغرات.

5.7 خدمة: الكشف عن الثغرات

الغرض: نشر معلومات عن الثغرات المعروفة للجهات المخدَّمة بحيث يمكنها التصرف بناءً على تلك المعلومات لمنع الثغرات المعروفة واكتشافها وتداركها/تخفيفها.

الوصف: إعلام الجهة المخدَّمة بأي ثغرات أمنية معروفة (نقاط الدخول الشائعة للمهاجمين)، وبالتالي يمكن أن تبقى الأنظمة مواكِبة لآخر المستجدات ومراقبَة ضد الاستغلال. ويمكن أن تتضمن أساليب الكشف نشر المعلومات عبر قنوات اتصالات متعددة (مثل موقع إلكتروني أو البريد الإلكتروني أو وسائل التواصل الاجتماعي) أو قاعدة بيانات الثغرات أو وسائط أخرى. وكثيراً ما تقدَّم هذه الخدمة، وليس دائماً، بعد التنسيق بشأن الثغرات.

النتيجة: يمكن للجهات المخدَّمة المستنيرة تجنب الاستغلال المحتمل للثغرات المعروفة قبل الاستغلال ويمكنها كشف الثغرات الموجودة بالفعل وتخفيفها.

وتُعتبر الوظائف التالية جزءاً من تنفيذ هذه الخدمة:

- إدارة سياسة الكشف عن الثغرات وبنيته التحتية.
- الإعلان/الاتصالات/النشر بشأن الثغرات.
- الملاحظات التقييمية بشأن الكشف عن الثغرات بعد تداركها.

1.5.7 وظيفة: إدارة سياسة الكشف عن الثغرات وبنيته التحتية

الغرض: وضع وإدارة سياسة تقدم إطاراً وتحدد التوقعات بشأن كيفية تعامل فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) مع الثغرات والكشف عنها، وبشأن الآلية (الآليات) المستخدمة للكشف عن الثغرات.

الوصف: ينبغي لأفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) التي تتعامل مع تقارير الثغرات أن تحدد سياسة الكشف عن الثغرات الخاصة بها وأن تتيح هذه السياسة للجهات المخدَّمة وأصحاب المصلحة والمشاركين في عملية الكشف المنسق عن الثغرات (CVD)، ويفضل نشرها على الموقع الإلكتروني لفريق CSIRT. وستقدم سياسة الكشف عن الثغرات الشفافية لأصحاب المصلحة وستساعد على الترويج لسياسات الكشف المناسبة. ويمكن أن تتراوح السياسات بين عدم الكشف، حيث لا يكُشف عن معلومات عن ثغرات، مروراً بالكشف المحدود، حيث لا تقدَّم إلا بعض المعلومات، وبين الكشف الكامل، حيث يكُشف عن جميع المعلومات، والتي يمكن أن تشمل عمليات الاستغلال ذات الجدوى التجريبية. وينبغي أن تتضمن سياسة الكشف عوامل مثل نطاق السياسة المرعية، وإحالات إلى أي آليات ومبادئ توجيهية للإبلاغ، والأطر الزمنية والآليات المتوقعة للكشف عن الثغرات.

النتيجة: زيادة الثقة والتعاون والتحكم في الكشف وتحسين العلاقات والتنسيق مع المشاركين في عملية الكشف المنسق عن الثغرات (CVD).

2.5.7 وظيفة: الإعلان/الاتصالات/النشر بشأن الثغرات

الغرض: تقديم معلومات للجهات المخدَّمة (أو لعامة الناس) بشأن ثغرة جديدة، كي تتمكن من كشف الثغرة أو تداركها أو تخفيفها ومنع استغلالها في المستقبل.

الوصف: الكشف عن معلومات عن الثغرات لجهات مخدَّمة محددة. ويمكن إجراء الكشف من خلال أي أو كل الآليات المحددة في سياسة الكشف عن الثغرات. ويمكن أن تختلف آليات النشر حسب احتياجات أو توقعات الجمهور المستهدف. ويمكن أن تجري الاتصالات في شكل إعلان أو مشورة أمنية توزَّع عبر البريد الإلكتروني أو الرسائل النصية، أو نشرة منشورة في موقع إلكتروني أو قناة تواصل اجتماعي، أو بأشكال وقنوات اتصالات أخرى حسب الاقتضاء. وينبغي أن يتبع المحتوى المراد تضمينه في الكشف نسقاً محدداً يمكن أن يتضمن عادةً معلومات مثل نظرة عامة أو وصف ومعرّف الثغرة الفريد وتأثيرها وشدتها أو الدرجة حسب نظام تحديد درجات الثغرات الشائعة (CVSS) والحل (التدارك أو التخفيف) والمراجع أو المواد الداعمة.

النتيجة: منع الثغرة وكشفها وتداركها/تخفيفها من خلال تقديم معلومات فعالة وعالية الجودة في الوقت المناسب للجهات المخدَّمة (أو العامة).

3.5.7 وظيفة: الملاحظات التقييمية بشأن الكشف عن الثغرات بعد تداركها

الغرض: تلقي أسئلة أو تقارير من جهات مخدَّمة بشأن الكشف عن الثغرات أو وثيقة عن الثغرات والرد عليها.

الوصف: بعد الكشف عن ثغرة جديدة، يمكن أن تتوقع أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) تلقي اتصالات متابعة في شكل أسئلة من بعض الجهات المخدَّمة بشأن وثيقة عن الثغرة. ويمكن أن تبين الأسئلةُ الحاجة إلى توضيح أو مراجعة أو تعديل آلية الكشف عن الثغرات، إذا لزم الأمر. ويمكن أن تكون المعلومات الواردة من الجهات المخدَّمة مجرد إشعار باستلام وثيقة الثغرة، أو يمكن أن تبلغ الجهة المخدَّمة عن مشكلة أو صعوبة في تنفيذ التدارك/التخفيف المقترح. وإذا تبين أن الثغرة قد استُغلت بالفعل، يمكن أن تقوم الجهات المخدَّمة بالإبلاغ عن الحوادث المكتشفة حديثاً نتيجة الكشف عن الثغرة. وينبغي أن تصب هذه التقارير في مجرى وظائف خدمة الإبلاغ عن الحوادث لدى فريق CSIRT.

النتيجة: يُرد على أي أسئلة أو طلبات مساعدة في الوقت المناسب بعد الكشف عن الثغرات.

6.7 خدمة: التصدي للثغرات[8]

الغرض: السعي بنشاط للحصول على معلومات عن الثغرات المعروفة والتصرف بناءً على تلك المعلومات لمنع هذه الثغرات واكتشافها وتداركها/تخفيفها.

الوصف: يُقصد من الوظائف الواردة في هذه الخدمة تحديد ما إذا كانت الثغرة المكتشفة موجودة في أنظمة الجهة المخدَّمة، غالباً من خلال الفعل المتعمد للبحث عن وجود هذه الثغرات. ويمكن أن تتضمن الخدمة أيضاً إجراءات المتابعة لتدارك أو تخفيف الثغرة من خلال نشر الرُقع التصحيحية أو استراتيجيات التفافية.

النتيجة: التصرف بناءً على المعلومات لكشف وجود ثغرة، وتدارك/تخفيف ثغرة كُشف عنها، ومنع استغلال الثغرة.

وتُعتبر الوظائف التالية جزءاً من تنفيذ هذه الخدمة:

- كشف/البحث عن الثغرات.
- تدارك الثغرات.

وعادةً ما تنفَّذ خدمة التصدي للثغرات ووظائفها ذات الصلة على يد مجموعات متخصصة أخرى داخل المنظمة، غير فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT). ويُستبعد أيضاً أن يقدم فريق CSIRT تنسيقي هذه الخدمة.

1.6.7 وظيفة: كشف/البحث عن الثغرات

الغرض: الانخراط بنشاط في البحث عن وجود ثغرات معروفة في الأنظمة المنشورة.

الوصف: الهدف من هذه الوظيفة هو اكتشاف أي ثغرات لم يسبق أن رُقعت أو خُففت قبل استغلالها أو التأثير على الشبكة أو الأجهزة. ويمكن بدء هذه الوظيفة رداً على إعلان عن ثغرة جديدة، أو يمكن تحقيقها كجزء من المسح المجدول دورياً للبحث عن الثغرات المعروفة. وللقيام بكشف الثغرات بشكل فعال، يستفاد من جرد الأنظمة. لأن مثل هذا الجرد يمكن الاستعلام منه للحصول على معلومات عن إصدارات البرمجيات يمكن أن تمكّن المنظمة من تقييم الانتشار المحتمل لثغرة أُبلغ عنها حديثاً في بنيتها التحتية.

يمكن أن تتلقى هذه الوظيفة مدخلات، أو أن تشغَّل بإيعاز، من خدمات ووظائف أخرى.

النتيجة: تكُشف الثغرات من خلال العمليات الرسمية أو الأدوات المصممة للتعرف عليها.

وتُعتبر الوظائف الفرعية التالية جزءاً من هذه الوظيفة:

- البحث عن/مطاردة الثغرات.
- تقييمات أمن/اختبار تغلغل الثغرات.

وعادة ما تنفَّذ هذه الوظيفة على يد كيانات أخرى (من قبيل خدمة تكنولوجيا المعلومات، مركز العمليات الأمنية (SOC)، الاختصاصيين الخارجيين، مالكي النظام).

2.6.7 وظيفة: تدارك الثغرات

الغرض: تدارك الثغرات أو تخفيفها لمنع استغلالها، وذلك عادةً من خلال تطبيق الرُقع التصحيحية التي يقدمها المورِّد أو الحلول الأخرى في الوقت المناسب.

الوصف: يُقصد من تدارك الثغرات حل مشكلة الثغرة أو إزالتها. وبالنسبة إلى ثغرات البرمجيات، يحدث ذلك عادةً من خلال نشر الحلول التي يقدمها المورِّد وتثبيتها في شكل تحديثات أو رُقع تصحيحية برمجية. وعندما لا تكون الرُقع التصحيحية المعتمدة متاحة أو يتعذر نشرها، يمكن أن يطبَّق تخفيف بديل أو حل التفافي كإجراء مضاد لمنع استغلال الثغرة. وكثيراً ما تأتي هذه الوظيفة إثر تعرف مؤكد على ثغرة نتيجة لوظيفة كشف/البحث عن/مطاردة الثغرات.

---

8 على الرغم من أن وظيفة كشف الثغرات ووظائفها الفرعية يُشار إليها أحياناً باسم "إدارة الثغرات"، فإن هذا الإطار لخدمات فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) يشير بدلاً من ذلك إلى هذه الخدمات كجزء من خدمة التصدي للثغرات، وهي تعد جزءاً من مجال الخدمة الأكبر المسمى إدارة الثغرات في هذا الإطار.

النتيجة: منع التعرض لتهديد باستغلال ثغرة أو تقليله.

وتُعتبر الوظائف الفرعية التالية جزءاً من هذه الوظيفة:

- تدارك الثغرات (إدارة الرُقع التصحيحية).
- تخفيف الثغرات.

وعادة ما تنفَّذ هذه الوظيفة على يد جهات أخرى غير فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) (من قبيل خدمة تكنولوجيا المعلومات، مركز العمليات الأمنية (SOC)، الاختصاصيين الخارجيين، مالكي النظام).

8 مجال الخدمة: الوعي الظرفي

يشمل الوعي الظرفي القدرة على تحديد ومعالجة وفهم وإبلاغ العناصر الحرجة لما يحدث في مجال مسؤولية فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) وحوله، والتي يمكن أن تؤثر على تشغيل أو مهمة الجهات التي يخدمها هذا الفريق. ويتضمن الوعي الظرفي إدراك الحالة الراهنة، وتحديد أو توقع التغييرات المحتملة لتلك الحالة. ويشمل مجال الخدمة هذا تحديد كيفية جمع المعلومات ذات الصلة من مجالات مختلفة، وكيفية تكامل تلك المعلومات، وكيفية نشرها في الوقت المناسب لمساعدة الجهات المخدَّمة على اتخاذ قرارات أكثر استنارة. يمكن أن تنشئ بعض المنظمات فريقاً منفصلاً لإذكاء الوعي الظرفي، وفي منظمات أخرى، يقوم فريق CSIRT بهذه الوظيفة بناءً على رؤيته، وفهمه للسياق، وقدراته التقنية، ونفاذه إلى الأصول، وصلاته الخارجية، ومهمته المعنية بمنع الحوادث. ولا يركز الوعي الظرفي على مجرد التصدي للحوادث، فهو يقدم خدمة تضمن توفر البيانات والتحليل والإجراءات إلى خدمات أخرى مثل إدارة أحداث الأمن وإدارة الحوادث ونقل المعارف. وهو يضمن أيضاً تكامل المعلومات الواردة من مجالات الخدمات الأخرى معاً على الوجه الصحيح وتسليمها إلى الجهات المخدَّمة المناسبة في الوقت المناسب.

وتُعتبر الخدمات التالية بمثابة عروض في مجال الخدمة هذا:

- تحصيل البيانات.
- التحليل والتركيب.
- الاتصالات.

1.8 الخدمة: تحصيل البيانات

الغرض: جمع البيانات التي ستساعد على زيادة الحضور المرئي لما يحدث من أنشطة داخلية وخارجية والتي يمكن أن تؤثر على الوضع الأمني للجهة المخدَّمة.

الوصف: طلب وجمع وتحديد وتلبية متطلبات الجهات المخدَّمة من المعلومات لتحقيق الوعي بالأنشطة الداخلية والخارجية الهامة ذات الصلة. وتتضمن هذه الخدمة، الخدمات اللوجستية الخاصة بجمع المعلومات ذات الصلة بما في ذلك أخبار الأحداث الجارية، والجدولة الزمنية للأحداث المستقبلية، والتقارير والخلاصات، واصطفاء المعلومات التي جُمعت، وتنظيم المعلومات لاستخدامها في تحليل الحوادث، والوقاية، والكشف، أو الأنشطة الأخرى (مثل التخطيط أو متابعة الاتجاهات) وتخزينها لاستخدامها لاحقاً وتحسين "قابلية البحث فيها"، وأكثر من ذلك. وستُستخدم البيانات التي جُمعت لتحديد التدابير الوقائية اللازمة وللمساعدة في اتخاذ قرارات مستنيرة بشأن إدارة الحوادث وأنشطة ضمان المعلومات. وبدون تصور أساسي للعناصر البيئية المهمة، تزداد مخاطر أن ترسم الخدمات الأخرى صورة غير صحيحة عن الأوضاع. وستحتاج أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) إلى وضع سياسة وإجراءات في هذا الصدد، ويمكن أن تستخدم تكنولوجيا خاصة بجمع المعلومات وتفحصها.

النتيجة:

تَنتج عن هذه الخدمة الصنائع التالية:

- مجموعة من متطلبات جمع البيانات تحدد احتياجات الوعي الظرفي، ثم ترسم خارطة ارتباطات تلك المتطلبات بأنواع المعلومات التي ستُجمع من أجل تحقيق تلك الأهداف.

- معلومات بشأن الوضع الحالي والمتوقع لأصول وأنشطة الجهة المخدَّمة.
- معلومات بشأن الأحداث أو الاتجاهات الخارجية تقدم أفكاراً مستنيرة عن محيط الجهة المخدَّمة وبيئتها الحالية، بما في ذلك جديد التكنولوجيات والأساليب والممارسات والمخاطر والتهديدات.
- معلومات ذات نسق سليم جاهزة لأنشطة التحليل والكشف.

وتُعتبر الوظائف التالية جزءاً من تنفيذ هذه الخدمة:

- تجميع السياسات واستخلاصها والتوجه وفقها.
- رسم خارطة ارتباطات الأصول مع الوظائف والأدوار والإجراءات والمخاطر الرئيسية.
- جمع المعلومات.
- معالجة البيانات وإعدادها.

1.1.8 وظيفة: تجميع السياسات واستخلاصها والتوجه وفقها

الغرض: تحديد السياق الذي ينبغي أن تلتزم به الجهات المخدَّمة وأصولها لمعرفة ما ينبغي أن يحدث في البنية التحتية.

الوصف: يؤسس جمع وتجميع السياسات واستخلاصها أساس النشاط الطبيعي المقبول. وتتمثل النتيجة النهائية في سياق يحدد كيف يفترض أن تعمل الجهات المخدَّمة وبنيتها التحتية في ظل ظروف مقبولة. وبالنسبة لأفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) في المنظمات، يتضمن السياق فهم السياسات والخطط المقبولة للمنظمات وظروف التشغيل العادية والمخاطر المقبولة والمفاضلات. ويضع الفهم والسياق الأساس الذي يمكن من خلاله تقييم الرصدات.

النتيجة: تُفهم الرصدات المقبولة التي تحدث لدى الجهات المخدَّمة. ويركز هذا الفهم على التغييرات أو التأثيرات على البنية التحتية والأصول.

2.1.8 وظيفة: رسم خارطة ارتباطات الأصول مع الوظائف والأدوار والإجراءات والمخاطر الرئيسية

الغرض: تقديم المعارف بشأن الأصول القائمة والملكية وخطوط الأساس، ويدعم النشاط المتوقع وظائف التحليل التي تحدد الرصدات الظرفية الشاذة.

الوصف: تحتاج أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) إلى فهم حالة الأمن السيبراني الراهنة لجهة مخدَّمة، وتشكيل فهم جيد لماهية الأمن المقبول. ويمكن أن تحتاج إلى معرفة ما يلي:

- المستخدمون المشروعون للأنظمة والأجهزة الداخلية والعامة.
- الأجهزة المجازة ومجالات استخدامها.
- العمليات والتطبيقات المعتمدة، وأين يُسمح بها، وكيف تخدم الجهات المخدَّمة.

وتساعد هذه المعلومات في تحديد أولويات الأصول التي يحتمل تعرضها للخطر، والتي يمكن أن تقدم سياقاً لأنشطة إدارة الحوادث. وكلما زادت دقة المعلومات المتاحة لفريق التصدي للحوادث الأمنية الحاسوبية (CSIRT)، سهل استنتاج مشاكل الأمن والقيام بشيء حيالها. ويمكن أن تعني المعلومات الدقيقة نفاذ فريق CSIRT إلى سياسات الأمن المعمول بها، وضوابط النفاذ الحالية، وتحديث جرد العتاد والبرمجيات، والرسوم البيانية التفصيلية للشبكة.

النتيجة:

تَنتج عن هذه الوظيفة القوائم التالية:

- قائمة بالوظائف الرئيسية والأصول التي تدعمها؛ ويمكن أن تدعم بعض الأصول وظائف متعددة
- قائمة بالأدوار التي تؤدي كل وظيفة ودورها الرقمي المكافئ على الأصل
- قائمة بالإجراءات المسموح بها عموماً لكل دور
- قائمة بالمخاطر الرئيسية التي تواجه الأصول والوظائف.

وستتطور هذه القوائم حسب التغييرات الظرفية.

3.1.8 وظيفة: جمع المعلومات

الغرض: جمع المعلومات لدعم خدمة التحليل والتفسير، و/أو الخدمات الأخرى التي يقدمها فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT).

الوصف: تتجاوز أنشطة جمع المعلومات والبيانات الخلاصات التي تقدم معلومات مؤتمتة. ويتضمن جمع المعلومات تحديد مصادر مفيدة مثل الأنشطة الخارجية ذات الصلة بالمعلومات بما في ذلك الأخبار من الجهات المخدَّمة الأخرى، ومصادر وسائل الإعلام، وغيرها من أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) أو المنظمات الأمنية، والأنشطة الداخلية (مثل التغييرات في المنظمة)، والتطورات التكنولوجية، والأحداث الخارجية، والأحداث السياسية، والاتجاهات الهجومية، والاتجاهات الدفاعية، والمؤتمرات، والتدريب المتاح، وأكثر من ذلك.

وتدعم وظيفة جمع البيانات خدمات أخرى مثل إدارة أحداث الأمن وإدارة الحوادث ونقل المعارف. وهي تدعم أيضاً الوظائف والأنشطة ضمن هذه الخدمات مثل التحليل والتنبؤ والتصدي وتخفيف المخاطر. ويمكن أن تكشف المعلومات التي جُمعت حديثاً أن الهجوم على جهة مخدَّمة مرجح أكثر من ذي قبل. ويمكن أن تكشف الأحداث الخارجية معلومات تحدد مخاطر جديدة للأصول لفترة من الوقت أو إنها تتطلب أنشطة كشف مشددة. وإجمالاً تساعد هذه المعلومات في تقديم معلومات تستدعي إجراءات مضادة للمساعدة في اتخاذ القرار والتعامل مع الحوادث.

النتيجة: جمع البيانات ومجموعات البيانات وإنتاجها لتقديم سياق تشغيلي أو بيئي يمكن أن تستخدمه الخدمات والوظائف الأخرى، بما في ذلك التحليل، لإنشاء صورة ظرفية للجهات المخدَّمة، أو التعرف على المنبهات، أو التخطيط للتخفيف من مجالات المخاطر المتزايدة على الأصول ودعم البنى التحتية.

4.1.8 وظيفة: معالجة البيانات وإعدادها

الغرض: إنشاء مجموعة بيانات موثوقة ومتسقة ومواكبة للمستجدات يمكنها دعم أنشطة فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) ومتطلبات خدمة التحليل.

الوصف: تشتمل معالجة البيانات وإعدادها على تحويل ومعالجة وتقييس مجموعة من البيانات والتحقق من صحتها. وتدعو الحاجة إلى التحقق من صحة مصادر بيانات الأمن السيبراني في كثير من الأحيان بسبب وجود عدد كبير من التأكيدات الخاطئة. وعادةً ما تأتي البيانات ذات الصلة بأنساق مختلفة، ويجب دمج البيانات الجديدة مع البيانات السابقة قبل أن يتسنى إجراء تحليل كامل. ويمكن أن تحتاج بعض أنواع البيانات (مثل المقالات الإخبارية) إلى التحليل أو المعالجة كجزء من عملية التحضير. ومن الأمثلة على ذلك، استخراج معلومات الأمن ذات الصلة من مقال إخباري (مثل الأسماء والتواريخ والأماكن والمعلومات التقنية ونقاط الضعف وأسماء النظام) ومقارنتها بالبيانات الداخلية لاستشفاف التأثيرات المحتملة.

وتتطلب بعض أساليب التحليل تخزين البيانات بنفس النسق، أو أن يكون للملفات نفس عدد السجلات. وتتعدد خطوات المعالجة التي يمكن أن ينطوي عليها إعداد البيانات. وتجرى زيادة البيانات (تسمى الإغناء أيضاً) بإدراج المعلومات الأخرى المتاحة ذات الصلة بجزء معين من البيانات من مصادر داخلية وخارجية أخرى. فعلى سبيل المثال، يمكن أن تقوم الأفرقة بجمع معلومات تتعلق بعناوين بروتوكول الإنترنت (عناوين IP) مثل معرفات النظام المستقلة، أو الرموز الدليلية للبلدان، أو بيانات تحديد الموقع الجغرافي. وللحصول على معلومات الأصول الداخلية، يمكن للأفرقة إغناء بيانات جرد الأصول بأسماء مالكي الأصول، وأدوارهم، وأذوناتهم تجاه الأصول الأخرى، ومواقع عملهم الفعلية بمرور الوقت، وأكثر من ذلك.

النتيجة: البيانات متاحة وجاهزة للاستخدام من جانب خدمات أو وظائف أخرى.

2.8 خدمة: التحليل والتركيب

الغرض: تقييم متى لا يتطابق الموقف مع التوقعات (من قبيل عندما يمكن أن توشك أصول معينة على مواجهة حدث ضار).

الوصف: عملية استخدام البيانات الحالية والسجل الزمني وتقنيات التحليل لتحديد ما يحدث ويمكن أن يؤثر على أصول الجهات المخدَّمة والموقف الأمني، وكثيراً ما تجرى بتحديد إجابة على سؤال أو اختبار حدس. ويمكن أن يكشف التحليل متى لا تتطابق الأحداث مع السلوك المتوقع المعتاد، أو يمكن أن يكشف عن معلومات بشأن ظروف الأحداث أو السلوكيات أو طبيعتها أو منشأها. ويمكن أن يكشف التحليل التداعيات على المواقف الحالية والمستقبلية. فعلى سبيل المثال: يمكن أن يقوم النظام بتسجيل دخول معرف المستخدم بنجاح إلى النظام، لكن النظام لا يبين ما إذا كان مستخدم مشروع هو الفاعل في هذا الحدث.

وتدعو الحاجة إلى إدراج مصادر جديدة (مثل مقابلات مع المستخدم) في التحليل لتزويد الفريق بصورة أدق لتحديد مشروعية الحدث. ويمكن استخدام مجموعة متنوعة من التقنيات لتحليل وتفسير البيانات التي جُمعت وتأثيرها على الجهات المخدَّمة.

النتيجة: إنتاج مجموعة من الاستنتاجات بشأن الأحداث التاريخية والحالية، و/أو الأحداث المستقبلية المحتملة ضمن جهة مخدَّمة. يمكن أن تتضمن أيضاً توصيات بشأن قرارات معينة تواجهها الجهة المخدَّمة. وينبغي دعم التحليل بأدلة مثل بيانات الرصد التي جُمعت من أجهزة الاستشعار ومصادر أخرى وتفسير المحللين لهذه الأدلة من خلال مجموعة متنوعة من الأساليب. ويمكن أن يشمل التحليل أيضاً الجهات المخدَّمة التي يجب إخبارها بالنتائج، وما يجب إخبارها به.

وتُعتبر الوظائف التالية جزءاً من تنفيذ هذه الخدمة:

- التوقع والاستدلال.
- كشف الأحداث (من خلال التنبيه و/أو المطاردة).
- التأثير الظرفي.

1.2.8 وظيفة: التوقع والاستدلال

الغرض: تحليل المعلومات التي جُمعت أثناء تحصيل البيانات بقصد تحديد صور الوضع الحالي أو التنبؤ بها في المستقبل.

الوصف: عملية استنتاج حالة الموقف الراهنة ووضع تنبؤات بشأن الصور المرجحة على المدى القريب استناداً إلى حالة وديناميات البيانات التي جُمعت. وفي بعض الأحيان يمكن أن تُظهر البيانات مشكلة أمنية بسرعة.

النتيجة: تحديث الصورة الظرفية إلى جانب معرفة متى ستتغير الصورة الظرفية وكيف يمكن أن تتغير.

2.2.8 وظيفة: كشف الأحداث (من خلال التنبيه و/أو المطاردة)

الغرض: تحديد تفاصيل الصورة الظرفية الحالية وتأكيدها للجهات المخدَّمة.

الوصف: البحث المنهجي، والموجه في كثير من الأحيان، عن نشاط شاذ داخل وخارج حدود الشبكة بناءً على المعلومات والاتجاهات الخارجية والداخلية. وذلك لمساعدة الجهات المخدَّمة في تحليل بياناتها المأخوذة من أجهزة الاستشعار والمصادر الأخرى لاستخلاص استنتاجات بشأن بيئتها ووضعها. فعلى سبيل المثال، إذا أرسل مستشعر مكافحة الفيروسات تنبيهاً بشأن ملف مريب، يمكن أن يحلل الفريق تشكيلة النظام وتشكيلة المستشعر والملف الذي جرى تنبيهه ونشاط المستخدم في ذلك الوقت وغير ذلك، لاستخلاص استنتاج بشأن شدة الرصد. يمكن أن تتلقى هذه الوظيفة مدخلات مهمة من مجال خدمة إدارة أحداث الأمن. ويمكن تناقل الرصدات من أجهزة الاستشعار التي تُستخدم لكشف الأحداث بين خدمات متعددة.

وتحتاج أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) أيضاً إلى تحديد الصورة الظرفية الحالية بناءً على معلومات محددة عن التهديدات. ويمكن أحياناً أن يُطلق على هذا النشاط اسم "مطاردة التهديدات". وعادة، يتضمن البحث عن التهديدات إما إعداد البيئة لكشف نشاط تهديد معين، أو البحث عن نشاط تهديد معين يمكن أن يكون موجوداً بالفعل.

النتيجة: تحديث الصورة الظرفية بناء على كشف الأحداث في الجهات المخدَّمة.

3.2.8 وظيفة: دعم قرار إدارة حوادث أمن المعلومات

الغرض: تحديد رؤى مستنيرة جديدة خلال الحوادث يمكن أن تساعد في الحد من الضرر أو التخفيف من المخاطر المستقبلية أو تحديد نقطة ضعف أنشئت حديثاً.

الوصف: يساعد إجراء تحليل لأدلة محددة في تحديد أفكار مستنيرة لدعم حل الحوادث. وفي بعض الأحيان، يمكن أن تركز أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) على تحليلها الظرفي لدعم نتيجة محددة مرجوة مثل حل الحوادث. ويمكن لردود معينة على حادث ما أن تؤثر على الصورة الظرفية بشكل مختلف، ويمكن أن يطلب المتصدون تحليل لخيارات (من قبيل التأثير، أو التكلفة، أو خطر التعطل). ويمكن أن تتغير احتياجات اتخاذ القرار لدى الجهات المخدَّمة مع تطور صورتها الظرفية، ويمكن أن يبدأ فريق CSIRT عمليات تحليل جديدة لمساعدتها. ويرتبط هذا النشاط بمجال خدمة إدارة الحوادث. وتُدعم وظائف إدارة الحوادث بالوعي الظرفي ويمكن أن تتغير الصورة الظرفية بناءً على أنشطة إدارة الحوادث.

النتيجة: تعزيز الوعي الظرفي لوظائف إدارة الحوادث بناءً على الرصدات الجديدة. وتحديث الصورة الظرفية القائم على أنشطة إدارة الحوادث.

4.2.8 وظيفة: التأثير الظرفي

الغرض: تحديد الأثر المحتمل المتوقع لرصد معين أو رصد ممكن لصورة ظرفية.

الوصف: تحدد هذه الوظيفة تأثير التوقع أو الاستدلال على الوضع الحالي أو المستقبلي القريب الأجل. ويمكن أن يشمل التأثير زيادة أو تقليل مخاطر معينة مثل خسارة بيانات، أو توقف النظام، أو التأثيرات على كتمان البيانات/توافرها/تكاملها.

النتيجة: إنتاج تحليل للأثر الممكن المرجح لاستدلال أو توقع على الموقف.

3.8 خدمة: الاتصالات

الغرض: إبلاغ الجهات المخدَّمة أو غيرها في مجتمع الأمن بالتغييرات في المخاطر التي تهدد الصورة الظرفية.

الوصف: يجب إبلاغ المعارف المكتسبة من الوعي الظرفي إلى الجهات المخدَّمة. وهذا سيسمح لها بالتفاعل مع الرصدات واتخاذ الإجراءات التي ستحسن المواقف الدفاعية، من قبيل الحد من مخاطر الطرف الثالث من خلال تحسين البيئة الأمنية لدى بعض الموردين ذوي المخاطر العالية.

النتيجة: تسليم معلومات ظرفية دقيقة تستدعي إجراءات مضادة في الوقت المناسب إلى الجهات المخدَّمة حتى تتمكن من فهم ماضيها بشكل أفضل وتحسين صورتها الظرفية الحالية والمستقبلية.

وتُعتبر الوظائف التالية جزءاً من تنفيذ هذه الخدمة:

- الاتصالات الداخلية والخارجية.
- إعداد التقارير والتوصيات.
- التنفيذ.
- النشر/التكامل/تناقل المعلومات.
- إدارة تناقل المعلومات.

1.3.8 وظيفة: الاتصالات الداخلية والخارجية

الغرض: إبلاغ الجهات المخدَّمة (وغيرها) بالصورة الظرفية الحالية وكيف يمكن أن تتغير.

الوصف: بمجرد اكتمال نتائج التحليل والتأويل، يمكن استخدامها لتحسين عملية صنع القرار عبر عمليات الاتصالات الداخلية والخارجية على السواء. وتوزَّع معلومات محددة بناءً على من يحتاج إلى معرفتها. وتشمل الاتصالات أسلوب التسليم والمحتوى الجاري تسليمه. يمكن أن ينقل فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) معلومات جديدة ويفسر كيف ستغير الصورة الظرفية. ومثال ذلك الإبلاغ عن التغيير المتوقع أن تحدثه تقنية خبيثة جديدة رُصدت خلال حادث في عضو من أعضاء جهة مخدَّمة. ويمكن أن يتضمن أيضاً معلومات عن الاتجاه السائد مثل المصادر الأكثر فائدة لبيانات الإغناء والخطوات التي يمكن للجهات المخدَّمة استخدامها لتحسين وعيها الظرفي.

النتيجة: الجهات المخدَّمة أفضل اطلاعاً وعلى استعداد لاتخاذ إجراءات أو اتخاذ قرارات ستحسن أمنها أو وضعها.

2.3.8 وظيفة: إعداد التقارير والتوصيات

الغرض: إنشاء نتائج أو صنائع أو اكتشافات تبلِّغ المعلومات المهمة المكتشفة أو التي أنشئت أثناء التحليل إلى المتابعين بأسلوب ونسق سيفهمونهما.

الوصف: ينبغي أن تبين التقارير والتوصيات بوضوح الخيارات والإجراءات التي تواجهها الجهات المخدَّمة، وتشمل تحليل التبعات المتوقعة لكل خيار أو إجراء. وينبغي أن يتضمن الإبلاغ عن اكتشافات قائمة الأدلة التي تدعم التحليل والتوصية (إذا قُدمت توصية). وينبغي شرح الأساليب المستخدمة لإنشاء الاكتشافات بوضوح للجمهور حتى يتمكنوا أيضاً من الحكم على الادعاءات

المقدمة. ويمكن أن ينشئ فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) تقارير بشأن حدث واحد، أو سلسلة من الأحداث، أو الاتجاهات، أو الأنماط، أو الأحداث الممكنة، أو أكثر من ذلك لدعم احتياجات الجهات التي يخدمها في فهم الصورة الظرفية.

النتيجة: تحسَّن القدرة على تقديم تقارير دقيقة وكاملة في الوقت المناسب عن الصورة الظرفية، و/أو الأدلة التي تدعم الاستنتاجات، و/أو التوصيات بشأن مسارات العمل الممكنة ومؤثراتها المحتملة على الجهات المخدَّمة.

3.3.8 وظيفة: التنفيذ

الغرض: تكييف بيئة الجهات المخدَّمة على أساس الاتصالات لتكون أكثر استعداداً للتغيرات في الصورة الظرفية أو للتفاعل معها.

الوصف: في بعض الحالات، يمكن أن يقوم فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) أيضاً بإجراء التعديلات الموصى بها على أجزاء من البنية التحتية الأمنية، من قبيل تغيير قواعد جدار الحماية في مصيدة جاذبة معينة بناءً على تحليل ظرفي.

النتيجة: تنفِّذ الجهات المخدَّمة مسار العمل أو تنفِّذ تغيير في البنية التحتية بناءً على الاتصالات المستلمة التي تحتوي على التحليل، و/أو التوقعات، و/أو التوصيات.

4.3.8 وظيفة: النشر/التكامل/تناقل المعلومات

الغرض: تجميع المعلومات وتقييمها وإعدادها ثم تناقلها مع الجهات المخدَّمة ومع غيرها من خارج الجهات المخدَّمة.

الوصف:

ويمكن أن تتضمن هذه الوظيفة الوظائف الفرعية التالية:

- استخدام نتائج خدمة التحليل في التخطيط الداخلي والخارجي وعمليات صنع القرار.
- تحديد الأهداف الصحيحة لتلقي المعلومات.
- إتاحة نتائج التحليل.
- ضمان نجاح التسليم.
- التتبع والتبليغ بشأن تناقل المعلومات.
- إرسال المعلومات ذات الصلة إلى خدمة نقل المعارف لمواصلة الاستخدام والنشر.

النتيجة: تُستخدم مخرجات تحليل الوعي الظرفي كمدخلات (داخلياً وبين الجهات المخدَّمة) في عمليات اتخاذ القرار الرئيسية، من قبيل مطاردة التهديدات، وتحليل الحوادث، والحل. وتُنشر المخرجات كجزء من التعامل مع الحوادث أو كشفها. ويمكن للمعلومات والبيانات الواردة من الوعي الظرفي أن تشكل أيضاً أفضل الممارسات والتقارير ومواد التدريب والتوعية عبر مجال خدمة نقل المعارف.

5.3.8 وظيفة: إدارة تناقل المعلومات

الغرض: التأكد من أن نقل المعلومات ناجح وقابل للاستخدام.

الوصف:

ويمكن أن تتضمن هذه الوظيفة الوظائف الفرعية التالية:

- تقديم المعلومات لمجموعات أخرى.
- إنساق المعلومات للنقل.
- تتبع عملية النقل ونتائجها.

النتيجة: التأكيد على تناقل المعلومات المناسبة، وبمجرد نقلها، يتلقاها الشركاء والجهات المخدَّمة وأعضاء المجتمع الآخرون. وتقدَّم تقارير عن نشاط تناقل المعلومات.

6.3.8 وظيفة: الملاحظات التقييمية

الغرض: تحسين جودة وتوقيت ودقة وصلة البيانات التي ترد من مصادر داخلية وخارجية.

الوصف: تتضمن هذه الوظيفة تقديم وتلقي الملاحظات التقييمية بشأن المعلومات المقدمة والمستلمة والمستخدمة من جانب الجهات المخدَّمة أو مقدمي الخدمات الآخرين أو أصحاب المصلحة الآخرين. فتجيب على أسئلة من قبيل هل وردت المعلومات بدقة، وفي الوقت المناسب، وكانت قابلة للتطبيق، واستراتيجية، وجديدة/حديثة، وما إلى ذلك؟ وهل كانت مساعدة في حل التحقيق؟ وهل أدت إلى رؤية جديدة؟ ويمكن أن يعني ذلك تقديم معلومات أيضاً إلى فريق CSIRT آخر (كمصدر خارجي) بشأن فائدة التوقيعات أو تغييرات فيها، واكتشافات المصائد الجاذبة، ومؤشرات الخرق (IOC)، والتحذيرات، ومعلومات التهديد، والتخفيف، وما إلى ذلك. ويمكن أيضاً تنفيذ هذا النشاط من خلال مجال خدمة نقل المعارف. وإذا كان الأمر كذلك، فيجب الرد بإرسال النتائج إلى مجال خدمة الوعي الظرفي.

النتيجة: تقدَّم الرصدات والملاحظات التقييمية إلى المصادر الداخلية والخارجية من أجل تحسين دقة المعلومات الواردة وأوانها ونوعيتها وفائدتها.

9 مجال الخدمة: نقل المعارف

نظراً لطبيعة خدمات أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT)، فإنها في وضع فريد لجمع البيانات ذات الصلة، وإجراء تحليل مفصل، وتحديد التهديدات والاتجاهات والمخاطر، بالإضافة إلى إنشاء أفضل الممارسات التشغيلية الحالية لمساعدة المنظمات على كشف الحوادث الأمنية ومنعها والتصدي لها. ونقل هذه المعارف إلى الجهات التي تخدمها هذه الأفرقة هو مفتاح تحسين الأمن السيبراني بمجمله.

وتُعتبر الخدمات التالية بمثابة عروض في مجال الخدمة هذا:

- التوعية.
- التدريب والتعليم.
- التمارين.
- المشورة التقنية والسياساتية.

1.9 خدمة: التوعية

الغرض: تعزيز مجمل الوضع الأمني للجهات المخدَّمة ومساعدة أعضائها على كشف الحوادث ومنعها والتعافي منها، ضمان إعداد الجهات المخدَّمة وتعليمها بشكل أفضل.

الوصف: تتضمن هذه الخدمة العمل مع الجهات المخدَّمة والخبراء والشركاء الموثوقين من أجل تعزيز الفهم الجماعي للتهديدات والإجراءات التي يمكن اتخاذها لمنع أو تخفيف المخاطر التي تشكلها هذه التهديدات.

النتيجة: تزويد الجهات المخدَّمة بالوعي اللازم بشأن ما يلي:

- الأحداث والأنشطة والاتجاهات التي يمكن أن تؤثر على قدرتها على العمل في الوقت المناسب وبطريقة آمنة.
- الخطوات التي يجب اتخاذها لكشف التهديدات والأنشطة الضارة ومنعها والتخفيف من حدتها.
- أفضل الممارسات الأمنية والتشغيلية.

وتُعتبر الوظائف التالية جزءاً من تنفيذ هذه الخدمة:

- البحوث وتجميع المعلومات.
- إعداد التقارير والمواد التوعوية.
- نشر المعلومات.
- مد الجسور.

1.1.9 وظيفة: البحوث وتجميع المعلومات

الغرض: تجميع وتصنيف وترتيب أولويات المعلومات التي يمكن نشرها للجهات المخدَّمة من أجل تحسين الوضع الأمني ومنع المخاطر وتخفيفها.

الوصف: تتضمن هذه الوظيفة إجراء البحوث وتجميع المعلومات ذات الصلة بمواد وتقارير التوعية، بما في ذلك من نتائج الخدمات/الوظائف الأخرى، خاصةً من مجالات خدمات إدارة الأحداث الأمنية وإدارة الحوادث والوعي الظرفي.

النتيجة: تجميع معلومات بشأن الاتجاهات ذات الصلة والحوادث المستمرة وأفضل الممارسات، ويمكن استخدامها لإعداد التقارير والمواد التوعوية لمختلف المتابعين.

2.1.9 وظيفة: إعداد التقارير والمواد التوعوية

الغرض: استخدام المعلومات المجمعة والبحث فيها على أنها ذات صلة لإنتاج مواد في وسائط مختلفة بهدف النفاذ إلى متابعين متنوعين أو تقديم محتوى معيَّن بأفضل طريقة ممكنة.

الوصف: تتضمن هذه الوظيفة إعداد مواد لمختلف المتابعين (الطاقم التقني والإدارة والمستخدمين النهائيين ومن إلى ذلك) وبأنساق مختلفة، مثل العروض ومقاطع الفيديو القصيرة والرسوم المتحركة والكتيبات والتحليل التقني وتقارير الاتجاهات والتقارير السنوية.

النتيجة: قيام أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) بإعداد تقارير ومواد توعوية بالجودة الكافية لتلبية احتياجات الجهات المخدَّمة باستخدام تقنيات ومنصات إيصال متنوعة وفعالة.

3.1.9 وظيفة: نشر المعلومات

الغرض: نشر المعلومات المتعلقة بالأمن لتحسين الوعي وتنفيذ الأعراف الأمنية.

الوصف: تتضمن هذه الوظيفة تنفيذ عملية نشر المعلومات التي يمكن أن تساعد فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) على تقديم تقاريره ومواده التوعوية إلى الجهات التي يخدمها على أفضل وجه وفق خصائص مختلف المتابعين والمحتوى.

النتيجة: ينفَّذ إطار نشر المعلومات لتمكين الجهات التي يخدمها فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) من النفاذ إلى المعلومات ذات الصلة في الوقت المناسب بأساليب مختلفة، ومنها البث الصوتي الرقمي (podcast) والمدونات المدرجة عبر شبكة الإنترنت وعبر وسائل التواصل الاجتماعي ومقاطع الفيديو والنشرات الصحفية والإعلانات والحملات والتقارير العامة وما إلى ذلك.

4.1.9 وظيفة: مد الجسور

الغرض: تطوير وإدامة العلاقات مع الخبراء أو المنظمات التي يمكن أن تساعد فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) أو أن تشارك تنفيذ مهمته.

الوصف: تتضمن هذه الوظيفة بناء شراكات، وتعزيز التعاون، وإشراك أصحاب المصلحة الرئيسيين، داخلياً أو خارجياً بالنسبة للجهات المخدَّمة، بهدف: نشر الوعي وأفضل الممارسات؛ ومساعدة الجهات المخدَّمة وأصحاب المصلحة الخارجيين على فهم الخدمات والمزايا التي يمكن أن يقدمها فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT)؛ ومساعدة فريق CSIRT على فهم احتياجات الجهات المخدَّمة بشكل أفضل؛ وتمكين إنجاز مهمة فريق CSIRT.

النتيجة: تنفَّذ أنشطة مد الجسور النشطة والمتسقة التي يمكن أن تشمل، على سبيل المثال لا الحصر، الاجتماع مع أصحاب المصلحة الرئيسيين، والمشاركة في الاجتماعات القطاعية، وتقديم العروض في المؤتمرات، وتنظيم المؤتمرات.

2.9 خدمة: التدريب والتعليم

الغرض: تقديم التدريب والتعليم إلى الجهات التي يخدمها فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) (والتي يمكن أن تشمل موظفي المنظمة، وفريق CSIRT) بشأن المواضيع المتعلقة بالأمن السيبراني وضمان المعلومات وإدارة الحوادث.

الوصف: يمكن لبرنامج التدريب والتعليم أن يساعد فريق CSIRT على إقامة علاقات وتحسين مجمل وضع الأمن السيبراني للجهات المخدَّمة، بما في ذلك القدرة على منع وقوع الحوادث مستقبلاً. يمكن لمثل هذا البرنامج تحقيق ما يلي:

- المساعدة في إدامة وعي المستخدم.
- مساعدة الجهات المخدَّمة على فهم متغيرات المشهد والتهديدات.
- تسهيل تبادل المعلومات بين فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) والجهات المخدَّمة.
- تدريب الجهات المخدَّمة على الأدوات والعمليات والإجراءات المتعلقة بالأمن وإدارة الحوادث.

ويمكن القيام بذلك من خلال أنواع مختلفة من الأنشطة تشمل توثيق المعارف والمهارات والقدرات (KSA) المطلوبة، وتطوير المواد التعليمية والتدريبية، والمحتوى المسلَّم، والإرشاد، والتطوير المهني وتطوير المهارات. وسيساهم كل من هذه الأنشطة بشكل جماعي في بناء قدرات الجهات المخدَّمة والفريق.

النتيجة: يقدَّم برنامج تدريب وتعليم متسق يمكّن الجهات التي يخدمها فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) من الحصول على ما يلي بشكل مناسب:

- أساليب كشف التهديدات أو منعها أو التصدي لها.
- أدوات وممارسات للمساعدة في حماية الأصول الهامة.
- فهم لعمليات إدارة الحوادث وكيفية الحصول على المساعدة.

وتُعتبر الوظائف التالية جزءاً من تنفيذ هذه الخدمة:

- جمع متطلبات المعارف والمهارات والقدرات.
- إعداد مواد التعليم والتدريب.
- إيصال المحتوى.
- الإرشاد.
- التطوير المهني لطاقم فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT).

1.2.9 وظيفة: جمع متطلبات المعارف والمهارات والقدرات

الغرض: تقييم وتحديد وتوثيق احتياجات الجهات المخدَّمة بشكل صحيح فيما يتعلق بالمعارف والمهارات والقدرات المطلوبة، لإعداد مواد التدريب والتعليم المناسبة وتحسين مستوى مهارتها.

الوصف: تنطوي هذه الوظيفة على جمع الاحتياجات من حيث معارف ومهارات وقدرات وكفاءة الجهة المخدَّمة فيما يتعلق بتحديد ما ينبغي تقديمه من تدريب وتعليم.

النتيجة: تشخيص وتوثيق احتياجات الجهات المخدَّمة من المعارف والمهارات والقدرات لاستخدامها كأساس لإعداد مواد التعليم والتدريب ذات الصلة.

2.2.9 وظيفة: إعداد مواد التعليم والتدريب

الغرض: استخدام احتياجات الجهات المخدَّمة من المعارف والمهارات والقدرات كأساس لإعداد مواد التعليم والتلقين والتدريب المناسبة لأساليب الإيصال المحددة على أنها الأفضل للوصول إلى مختلف المتابعين أو لإيصال محتوى معين.

الوصف: تنطوي هذه الوظيفة على بناء أو تحصيل محتوى المواد التعليمية والتدريبية مثل العروض والمحاضرات والبيانات العملية، والمحاكاة وتسجيلات الفيديو والكتب والكتيبات، وما إلى ذلك.

النتيجة: يلجأ فريق التصدي للحوادث الأمنية الحاسوبية إلى إعداد مواد التعليم والتدريب باستخدام تقنيات ومنصات عرض متنوعة وفعالة ذات جودة مناسبة وتفي باحتياجات الجهات التي يخدِّمها.

3.2.9 وظيفة: إيصال المحتوى

الغرض: تطوير عملية رسمية لإيصال المحتوى يمكن أن تساعد فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) في إيصال المحتوى على أفضل وجه إلى الجهات التي يخدِّمها ، بناءً على خصائص مختلف المتابعين والمحتوى.

الوصف: تتضمن هذه الوظيفة نقل المعارف والمحتوى إلى "الطلاب". ويمكن أن يحدث ذلك بأساليب مختلفة، مثل التدريب القائم على الحاسوب/عبر الإنترنت (CBT/WBT)، بقيادة مدرس، أو بشكل افتراضي، أو عبر المؤتمرات، أو العروض، أو المختبرات، أو مسابقات التقاط العلم (CTF) للأمن السيبراني، أو الكتب، أو تسجيلات الفيديو عبر الإنترنت، وما إلى ذلك.

النتيجة: تصميم إطار إيصال المحتوى لمساعدة الجهات المخدَّمة على تعلم المهارات والعمليات التقنية والميسرة، باستخدام جميع المناهج البديلة، بما في ذلك الكتب والكتيبات وتسجيلات الفيديو عبر الإنترنت والعروض والمختبرات العملية، ومسابقات التقاط العلم (CTF) للأمن السيبراني، والتدريب القائم على الحاسوب/عبر الإنترنت (CBT/WBT)، وحضور التدريب شخصياً، وما إلى ذلك. وينتج عن ذلك أعضاء لدى الجهات المخدَّمة يفهمون المحتوى المقدَّم.

4.2.9 وظيفة: الإرشاد

الغرض: تطوير برنامج لطاقم فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) أو أعضاء لدى الجهات المخدَّمة أو الشركاء الخارجيين الموثوقين للتعلم من الموظفين ذوي الخبرة من خلال علاقة قائمة.

الوصف: يمكن أن يساعد برنامج الإرشاد على تقديم 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. ويمكن أن ينطوي ذلك على زيارات ميدانية، وتناوب (تبادل)، وملازمة، ومناقشة الأساس المنطقي في اتخاذ قرارات وإجراءات محددة.

النتيجة: تعزيز قدرة فريق التصدي للحوادث الأمنية الحاسوبية على الاحتفاظ بالأعضاء والحصول على ولائهم وثقتهم، وتعزيز مجمل قدرته على اتخاذ القرارات السليمة. وتحسين الجهات المخدَّمة لمستويات المهارة ولعلاقتها مع فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) الخاص بها. وتحسين سعة وقدرة الجهات المخدَّمة وأعضاء فريق CSIRT، بما في ذلك تطوير العلاقات الموثوقة.

5.2.9 وظيفة: التطوير المهني لطاقم فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT)

الغرض: مساعدة الموظفين في التخطيط بنجاح وبشكل مناسب لتطوير حياتهم المهنية.

الوصف: بعد التعرف على المهارات المناسبة، 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. ويمكن أن يشمل ذلك حضور المؤتمرات والتدريب المتقدم، وأنشطة التدريب على مهارات مختلفة، وما إلى ذلك.

النتيجة: تطوير وتدريب تيسر الموظفين المطورين والمدربين والمسلحين بالمهارات التقنية وغير التقنية اللازمة، وبفهم العملية، والمواكبين لآخر المستجدات حسب أدوار واحتياجات مهامهم. واستعداد أعضاء فريق التصدي للحوادث الأمنية الحاسوبية لمواجهة التحديات التشغيلية اليومية، ولدعم الفريق وعملائه على السواء.

3.9 خدمة: التمارين

الغرض: إجراء تمارين لتحسين فعالية وكفاءة خدمات الأمن السيبراني ووظائفه.

الوصف: الخدمات التي تقدمها المنظمة للجهات المخدَّمة والتي تدعم تصميم وتنفيذ وتقييم التمارين السيبرانية الساعية إلى تدريب و/أو تقييم قدرات فرادى الجهات المخدَّمة ومجتمع أصحاب المصلحة ككل، بما في ذلك قدرات الاتصالات. ويمكن استخدام هذه الأنواع من التمارين من أجل:

- **سياسات وإجراءات الاختبار:** تقييم ما إذا كانت هناك سياسات وإجراءات كافية لكشف الحوادث والتصدي لها والتخفيف من آثارها على نحو فعال. وبوجه عام، يتخذ ذلك شكل تمرين نظري أو تمرين محاكاة.

- **اختبار الجاهزية التشغيلية**: تقييم ما إذا كانت لدى المنظمة قدرة على إدارة الحوادث يمكنها كشف الحوادث والتصدي لها والتخفيف من وطأتها في الوقت المناسب وبنجاح، وكذلك اختبار ما إذا كان الأشخاص المناسبون في مكانهم الصحيح، وما إذا كانت الأدلة مواكبة لآخر المستجدات، وما إذا كانت الإجراءات تنفَّذ على الوجه الصحيح.

وتتناول هذه الوظيفة 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 يُتوقع أن يكونوا على دراية بها. ويلزم التمرين للمهارات القابلة للتراجع ويساعد على تحسين الكفاءة والحفاظ عليها.
  - تقييم: تحليل وفهم مستوى فعالية وكفاءة خدمات الأمن السيبراني ووظائفه، وكذلك مستوى جاهزية الموظفين.
  - التحقق: تحديد ما إذا كان مستوى معين من الفعالية و/أو الكفاءة يمكن أن يتحقق لخدمات الأمن السيبراني ووظائفه.

النتيجة: تحسن فعالية وكفاءة الخدمات الأمن السيبراني ووظائفه، وتحديد الفرص السانحة لمزيد من التحسينات.

وحسب الهدف المحدد (الأهداف المحددة) من التمرين، يمكن أيضاً أن يُعرض لأصحاب المصلحة الداخليين أو الخارجيين بيان عملي للأمن السيبراني، ويمكن تدريب الموظفين، ويمكن تقييم كفاءة وفعالية الخدمات والوظائف و/أو التحقق من ذلك. ويمكن كذلك تحديد الدروس المستفادة لتحسين التمارين في المستقبل، وتقديم تقرير عن ذلك إلى الإدارة أو أصحاب المصلحة الرئيسيين الآخرين.

وتُعتبر الوظائف التالية جزءاً من تنفيذ هذه الخدمة:

- تحليل المتطلبات.
- إعداد النسق والبيئة.
- إعداد السيناريو.
- تنفيذ التمارين.
- استعراض نتيجة التمرين.

1.3.9 وظيفة: تحليل المتطلبات

الغرض: ضمان نتيجة فعالة للتمرين بالتركيز على قضايا محددة ضمن نطاق معين ومحور التمرين.

الوصف: تحديد أهداف التعلم ونطاق التمرين. وتعريف الخدمات والقدرات والمواضيع المحددة التي سيغطيها التمرين. والتأكد من أن يتضمن التمرين أنشطة ومواضيع تتعلق بالمهارات المطلوبة أو المرغوبة التي يحتاجها المشاركون، بالإضافة إلى العمليات التي ينبغي اختبارها.

النتيجة: يتحدد وصف الغرض من التمرين، إلى جانب الخطوط العريضة لأهداف التعلم التي يتعين تحقيقها.

2.3.9 وظيفة: إعداد النسق والبيئة

الغرض: توصيف وتحديد الموارد الداخلية والخارجية والبنية التحتية اللازمة لإجراء التمرين.

الوصف: تحديد النسق والمنصة اللازمين لتحقيق الأهداف وتقديم النتائج المتوقعة من التمرين.

النتيجة: يتحدد نوع التمرين (مضاهاة، تمرين عملي، محاكاة، وما إلى ذلك)، بالإضافة إلى الموارد الداخلية والخارجية اللازمة لإجراء التمرين.

3.3.9 وظيفة: إعداد السيناريو

الغرض: إتاحة الفرصة للجمهور المستهدف لتحسين كفاءة وفعالية خدماته ووظائفه، ومهاراته ومعارفه وقدراته، من خلال التعامل مع محاكاة أحداث/حوادث الأمن السيبراني، بما في ذلك جوانب الاتصالات.

الوصف: وضع سيناريوهات التمرين في دعم أهداف صاحب المصلحة. وتشمل النواتج أيضاً تعليمات وإرشادات للمشاركين ومديري التمرين؛ وتتضمن هذه التعليمات الإجراءات الموصى بها للمشاركين وتتناول بالتفصيل بعض/جميع خطوات السيناريو.

النتيجة: إعداد سيناريو رئيسي مشفوعاً بأشكال متنوعة وأنواع مختلفة من وحدات الإدراج الرسمية، إلى جانب توزيع المهام والأدوار على فريق إدارة التمرين.

4.3.9 وظيفة: تنفيذ التمارين

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

الوصف: تتضمن هذه الوظيفة تنفيذ اختبار لجاهزية "طلاب" الجهة المخدَّمة لفحص قدرتهم على تطبيق التدريب وأداء وظائف العمل أو المهمة. ويمكن أن يكون ذلك في شكل بيئات حقيقية أو افتراضية، أو محاكاة، أو اختبارات ميدانية، أو مضاهاة، أو سيناريوهات وهمية، أو توليفة مما سبق، مع تقديم وحدات الإدراج بطريقة مهيكَلة. وسيساعد ذلك في تحديد المستوى الذي يعمل فيه الفريق، وكذلك تحديد ما إذا كانت هناك مجالات يمكن أن يتحسن فيها، وماهيتها.

النتيجة: قيام فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) بتقييم جهوزيته واستعداده، وضمان أن المعارف والمهارات والقدرات، والعمليات الرئيسية، والتنفيذ تعمل جميعها معاً بنجاح، أو يجب تكييفها/تحسينها.

5.3.9 وظيفة: استعراض نتيجة التمرين

الغرض: إجراء تحليل رسمي وموضوعي للتمرين، بناءً على الرصدات الفعلية.

الوصف: وضع تقرير ما بعد العمل يتضمن الدروس المستفادة أو الاكتشافات/أفضل الممارسات المستقاة من التمرين، ويقدم تقييماً إلى أصحاب المصلحة/الإدارة.

النتيجة: تحقيق نواتج تسلط الضوء على نجاح التمرين، ومجالات التحسين، والنتائج العامة، والإجراءات الموصى باتخاذها من أجل التحسين أي: قدرات إدارة حوادث المنظمة، وعمليات فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT)، وقدرات فرادى الجهات المخدَّمة ومجتمع أصحاب المصلحة ككل، بما في ذلك قدرات وإجراءات الاتصالات.

4.9 خدمة: المشورة التقنية والسياساتية

الغرض: التأكد من أن سياسات وإجراءات الجهات المخدَّمة تتضمن اعتبارات مناسبة لإدارة الحوادث، وفي النهاية، تمكين الجهات المخدَّمة من تحسين إدارة المخاطر والتهديدات، بالإضافة إلى تمكين فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) من تعزيز فعاليته.

الوصف: دعم الجهات التي يخدمها فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) وأصحاب المصلحة الرئيسيين، الداخليين أو الخارجيين بالنسبة إلى هذه الجهات، في الأنشطة المتعلقة بإدارة المخاطر واستمرارية الأعمال، وتقديم المشورة التقنية حسب الحاجة والمساهمة في وضع وتنفيذ سياسات الجهات المخدَّمة، وكذلك حثها على تمكين فريق CSIRT من تعزيز فعاليته. وتكتسي السياسات أهمية أيضاً في إضفاء المشروعية على خدمات فريق CSIRT.

النتيجة: تمكين الجهة المخدَّمة من اتخاذ قرارات على مستوى المنظمة تستند إلى أفضل ممارسات الأمن التشغيلي التي تتضمن استمرارية الأعمال وأفضل ممارسات التعافي من الكوارث، مع فهم الحاجة أيضاً إلى إشراك أفرقة إدارة الحوادث، كمستشارين موثوقين، في قرارات الأعمال عند الاقتضاء.

وتُعتبر الوظائف التالية جزءاً من تنفيذ هذه الخدمة:

- دعم إدارة المخاطر.

- دعم استمرارية الأعمال والتخطيط للتعافي من الكوارث.
- دعم السياسات.
- المشورة التقنية.

1.4.9 وظيفة: دعم إدارة المخاطر

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

الوصف: دعم الأنشطة المتعلقة بتقييم المخاطر أو الالتزام. ويمكن أن يشمل ذلك إجراء تقييم فعلي أو تقديم الدعم لتقدير نتائج التقييم.

النتيجة: قدرة الجهات المخدَّمة على تبيُّن المخاطر والتهديدات واختيار خيارات إدارة المخاطر ذات الصلة، بما في ذلك استراتيجيات إدارة الحوادث المناسبة والفعالة، وضوابط الأمن، أو تخفيف التهديدات.

2.4.9 وظيفة: دعم استمرارية الأعمال والتخطيط للتعافي من الكوارث

الغرض: العمل كمستشار موثوق بشأن استمرارية الأعمال وإعادتها إلى نصابها إثر وقوع كوارث من خلال إسداء المشورة المحايدة القائمة على الواقع، مع الأخذ بعين الاعتبار البيئة التي يمكن أن تُستخدم فيها المشورة وأي قيود تسري على الموارد.

الوصف: دعم الجهات المخدَّمة في الأنشطة المتعلقة بتجاوز المنظمة للعثرات، بناءً على المخاطر المحددة.

النتيجة: قدرة الجهات المخدَّمة على التنفيذ المناسب لخطط استمرارية الأعمال وإعادتها إلى نصابها إثر وقوع كوارث وهي خطط تتضمن استراتيجيات لإدارة الحوادث وتتواءم معها.

3.4.9 وظيفة: دعم السياسات

الغرض: العمل كمستشار موثوق بشأن وضع السياسات وتنفيذها من خلال إسداء المشورة المحايدة القائمة على الواقع، مع الأخذ بعين الاعتبار البيئة التي يمكن أن تُستخدم فيها المشورة وأي قيود تسري على الموارد.

الوصف: تدعم هذه الوظيفة الجهات المخدَّمة في وضع السياسات وإدارتها وإضفاء الطابع المؤسسي عليها وإنفاذها، مع ضمان تمكينها ودعمها لأنشطة إدارة الحوادث. وبالنسبة إلى أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) الداخلية، يتضمن ذلك عادةً دعماً لأمن المعلومات وسياسات التشغيل الأخرى. وفيما يخص التنسيق، وأفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) الوطنية، يمكن أن يشمل ذلك دعم السياسات العامة والتشريعات الجديدة.

النتيجة: قدرة الجهات المخدَّمة على وضع سياسات فعالة، وإضفاء الطابع المؤسسي على السياسات، وتمكين استراتيجيات إدارة الحوادث الفعالة.

4.4.9 وظيفة: المشورة التقنية

الغرض: تقديم المشورة التقنية التي يمكن أن تساعد الجهات المخدَّمة على تحسين إدارة المخاطر والتهديدات وتنفيذ أفضل الممارسات التشغيلية والأمنية الحالية، مع تمكين أنشطة معالجة الحوادث الفعالة.

الوصف: تقدم هذه الوظيفة للجهات المخدَّمة الدعم والتوصيات بشأن تحسين البنى التحتية والأدوات والخدمات المتعلقة بالأمن السيبراني، بهدف تحسين الوضع الأمني وإدارة الحوادث إجمالاً.

يمكن أن يشمل ذلك مشورة بشأن:

- اعتبارات أمنية بشأن الحيازة والتحقق من الالتزام والصيانة والترقيات.
- عمليات التدقيق الداخلية والخارجية للبنى التحتية والأدوات المتعلقة بالأمن السيبراني.
- تأمين متطلبات تطوير البرمجيات والتشفير الآمن.

النتيجة: تقديم الدعم لتصميم وحيازة وإدارة وتشغيل وصيانة البنية التحتية والأنظمة والأدوات الخاصة بالجهات المخدَّمة، بالإضافة إلى المساعدة في بناء قدرات أنشطة إدارة الحوادث وفي زيادة سعتها وإنضاجها.

الملحق 1: شكر وتقدير

قدم المتطوعون التالية أسماؤهم من مجتمعات أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) مساهمات ذات شأن في هذا الإصدار من إطار خدمات فريق التصدي للحوادث الأمنية الحاسوبية. وترد أسماؤهم بالترتيب الأبجدي حسب الكنية، دون ذكر الألقاب، ولكن مع الإشارة إلى الانتماء والدور والبلد:

- Vilius Benetis، NRD CIRT (ليتوانيا)
- Olivier Caleff، (منسق مجال الخدمة)، مؤسسة openCSIRT (فرنسا)
- Cristine Hoepers، (منسقة مجال الخدمة)، CERT.br، (بريطانيا)
- Angela Horneman، CERT/CC, SEI, CMU، (الولايات المتحدة)
- Allen Householder، CERT/CC, SEI, CMU، (الولايات المتحدة)
- Klaus-Peter Kossakowski، (محرر)، جامعة هامبورغ للعلوم التطبيقية، (ألمانيا)
- Art Manion، CERT/CC, SEI, CMU، (الولايات المتحدة)
- Amanda Mullens، (منسقة مشاركة لمجال الخدمة)، CISCO، (الولايات المتحدة)
- Samuel Perl، (منسق مجال الخدمة)، CERT/CC, SEI, CMU، (الولايات المتحدة)
- Daniel Roethlisberger، (منسق مجال الخدمة)، Swisscom، (سويسرا)
- Sigitas Rokas، NRD CIRT، (ليتوانيا)
- Mary Rossell، Intel، (الولايات المتحدة)
- Robin M. Ruefle، (منسق مشارك لمجال الخدمة)، CERT/CC, SEI, CMU، (الولايات المتحدة)
- Désirée Sacher، Finanz Informatik، (ألمانيا)
- Krassimir T. Tzvetanov، Fastly، (الولايات المتحدة)
- Mark Zajicek، (منسق مشارك لمجال الخدمة)، CERT/CC, SEI, CMU، (الولايات المتحدة)

الملحق 2: المصطلحات والتعاريف

يعرِّف هذا القسم مصطلحات معينة مستخدمة في إطار خدمات فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT).

الإجراءات – وصف لكيفية القيام بشيء ما على مستويات مختلفة من التفاصيل.

مشورة[9] – إعلان أو منشور يعمل على إعلام وتقديم المشورة والتحذير من ثغرة في منتَج.

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.

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

تعداد الثغرات الشائعة (CVE)[10] – قائمة الإدراجات التي تحتوي على رقم تعريف ووصف ومرجع علني واحد على الأقل للثغرات المعروفة للعموم. وهي تعمل كمعرف معياري للثغرات المرجعية.

نظام تحديد درجات الثغرات الشائعة (CVSS)[11] – درجة رقمية تعكس مدى خطورة الثغرة.

التعداد المشترَك لنقاط الضعف (CWE)[12] – قائمة رسمية بأنواع ضعف البرمجيات أنشئت لتكون لغة مشتركة لوصف ضعف أمن البرمجيات في المعمارية أو التصميم أو الشفرة؛ وهي بمثابة مسطرة قياس معيارية لأدوات أمن البرمجيات تستهدف هذه الثغرات؛ وتقدم خط أساس معياري مشترك لتحديد الضعف والتخفيف والجهود الوقائية.

الجهات المخدَّمة – مجموعة محددة من الأشخاص و/أو المنظمات يمكنها النفاذ إلى مجموعة محددة من الخدمات التي يقدمها فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT).

مصدر البيانات السياقية – مصدر البيانات السياقية الذي يعطي السياق لنقاط البيانات، أي لهوية أو أصل أو حدث أمن معلومات، على سبيل المثال. وتتضمن الأمثلة المحددة قواعد بيانات المستخدم أو قوائم جرد الأصول أو خدمات التنصل من بروتوكول الإنترنت أو بيانات استخبارية عن التهديدات.

الكشف المنسَق عن الثغرات – مصطلح يستخدم للدلالة على عملية الكشف التي تتضمن التنسيق. المصدر: ISO/IEC 29147:2018، المصطلحات والتعاريف.

المنسِق[13] – مشارك اختياري يمكنه مساعدة المورِّدين والمكتشفين في التعامل مع معلومات عن الثغرات والكشف عنها.

حالة استخدام الكشف – ظرف محدد يتعين أن يكتشفه مجال خدمة إدارة أحداث أمن المعلومات. ويعود منشأ هذا المصطلح إلى هندسة البرمجيات، ولكنه يُستخدم الآن على نطاق واسع في هندسة الكشف.

الحظر – تعليق نشر تفاصيل الثغرة إلى أن يتمكن المورِّدون المتأثرون من إصدار التحديثات أو عوامل التخفيف الأمنية والحلول الالتفافية لحماية العملاء.

المكتشِف[14] – فرد أو منظمة يتعرفان على ثغرة محتملة في منتج أو في خدمة عبر الإنترنت. ويرجى أخذ العلم بأن المكتشفين يمكن أن يكونوا باحثين أو جهات مبلِّغة أو شركات أمنية أو قراصنة حوسبة أو مستخدمين أو حكومات أو منسقين.

---

9 ISO/IEC 29147: 2014 تكنولوجيا المعلومات – تقنيات الأمن – الكشف عن الثغرات – المصطلحات/التعاريف 3.1.

10 https://cve.mitre.org/.

11 https://www.first.org/cvss/.

12 https://cwe.mitre.org/about/index.html.

13 ISO/IEC 30111:2013 تكنولوجيا المعلومات – تقنيات الأمن – عمليات التعامل مع الثغرات – المصطلحات/التعاريف 3.1.

14 ISO/IEC 29147: 2014 تكنولوجيا المعلومات – تقنيات الأمن – الكشف عن الثغرات – المصطلحات/التعاريف 3.3.

الوظيفة – نشاط أو مجموعة أنشطة تهدف إلى تحقيق الغرض من خدمة معينة. وتتضمن التعاريف الأخرى: مجموعة من الإجراءات ذات الصلة[15] للقيام بفعل أو نشاط، أو عمل، أو تشغيل محدد.[16]

حدث أمن المعلومات – حدث يمكن رصده في بيئة تكنولوجيا المعلومات ذات الصلة بالأمن؛ من قبيل تسجيل دخول مستخدم أو تنبيه نظام كشف التسلل (IDS). وعادة ما تنتج أحداث أمن المعلومات نوعاً من الأدلة، مثل سجل التدقيق أو إدراج في ملف السجل، ويمكن جمعها وتحليلها كجزء من مجال خدمة إدارة أحداث أمن المعلومات.

حادث أمن المعلومات[17] – أيًّما يضر من حدث أمن معلومات (أو مجموعة من أحداث أمن المعلومات) فينال من بعض جوانب المستخدم و/أو النظام و/أو المنظمة، و/أو أمن معلومات الشبكة. ويمكن أن يختلف تعريف حادث أمن المعلومات بين المنظمات، ولكنه يسري عموماً على الفئات التالية على الأقل:

- ضياع كتمان المعلومات.
- اختلال سلامة المعلومات.
- الحرمان من الخدمة.
- إساءة استخدام الخدمة أو الأنظمة أو المعلومات.
- تضرر الأنظمة.

والهجمات، حتى لو فشلت بفضل الحماية المناسبة، يمكن اعتبارها حوادث أمن معلومات.

مؤشر الأداء الرئيسي (KPI)[18] – قيمة قابلة للقياس توضح مدى فعالية الشركة في تحقيق أهداف الأعمال الرئيسية. وتستخدم المنظمات مؤشرات الأداء الرئيسية على مستويات متعددة لتقييم نجاحها في بلوغ الأهداف.

النضج – مدى فعالية تنفيذ منظمة لقدرة معينة ضمن مهام وسلطات المنظمة. وهو مستوى الكفاءة المتحققة سواء في تنفيذ وظائف محددة أو في مجموع الوظائف أو الخدمات. وستتحدد قدرة المنظمة بمدى وجودة السياسات والوثائق المعمول بها والقدرة على تنفيذ عملية محددة.

مفتوحة المصدر – الأعمال المرخصة بطريقة تمكن إعادة توزيعها وتعديلها بحرية، حيث تتاح شفرة المصدر للعموم، وتوزَّع بحرية ولا تميز ضد أي أشخاص أو مجموعات أو مساع، وهي محايدة تجاه التكنولوجيا. وكثيراً ما يدير مجتمع من الأفراد والكيانات البرمجيات مفتوحة المصدر فيقوم بإنشائها وصيانتها بشكل تعاوني.

المنتج[19] – نظام نُفِّذ أو أُعد للبيع أو ليُعرض مجاناً.

التدارك (أو العلاج)[20] – تغيير يجرى على منتج أو خدمة عبر الإنترنت لإزالة ثغرة أو تخفيفها. عادة ما يتخذ التدارك شكل الاستعاضة عن ملف اثنيني أو تغيير في التشكيلة أو رقعة تصحيحية لشفرة المصدر وإعادة ترجمة برمجية. ومن المصطلحات المختلفة المستخدمة للدلالة على "التدارك"، الرقعة التصحيحية والإصلاح والتحديث والإصلاح العاجل والترقية. وتسمى عمليات التخفيف أيضاً الحلول الالتفافية أو الإجراءات المضادة.

الكشف المسؤول – مصطلح يستخدم للإشارة إلى عملية أو نموذج حيث لا يكُشف عن ثغرة إلا بعد فترة زمنية تسمح بإتاحة تدارك (إصلاح أو رقعة تصحيحية). وهذا المصطلح لا يرادف بالضرورة مصطلح "الكشف المنسق عن الثغرات".

---

15 المصدر: https://www.merriam-webster.com/dictionary/function.

16 المصدر: https://www.dictionary.com/browse/function.

17 استناداً إلى طلب التعليقات رقم RFC2350 بشأن النظر في "أمن المعلومات" بدلاً من "أمن تكنولوجيا المعلومات"، https://tools.ietf.org/html/rfc2350.

18 https://www.klipfolio.com/resources/articles/what-is-a-key-performance-indicator.

19 ISO/IEC 29147: 2014 تكنولوجيا المعلومات – تقنيات الأمن – الكشف عن الثغرات – المصطلحات/التعاريف 3.5.

20 ISO/IEC 29147: 2014 تكنولوجيا المعلومات – تقنيات الأمن – الكشف عن الثغرات – المصطلحات/التعاريف 3.6.

المخاطر[21] – "تأثير عدم اليقين على الأهداف". وفي هذا التعريف، تشمل حالات عدم اليقين الأحداث (التي يمكن أن تحدث أو لا تحدث) والشكوك الناجمة عن الغموض أو نقص المعلومات.

قبول المخاطر[22] – استراتيجية تصدٍ للمخاطر يقرر فيها فريق المشروع الاعتراف بالمخاطر وعدم اتخاذ أي إجراء ما لم تتحقق المخاطر.

سجل المخاطر[23] – وثيقة تسجَّل فيها نتائج تحليل المخاطر وتخطيط التصدي للمخاطر.

الخدمة – مجموعة إجراءات متماسكة يمكن تمييزها تسعى إلى نتيجة محددة. ويمكن أن تكون هذه النتائج متوقعة أو مطلوبة من الجهات المخدَّمة أو نيابة عن أو لأصحاب المصلحة في كيان ما.

اتفاق مستوى الخدمة (SLA) – عقد بين مقدم الخدمة (سواء كان داخلياً أو خارجياً) والمستخدم النهائي يحدد مستوى الخدمة المتوقع من مقدم الخدمة.

أصحاب المصلحة[24] – الأفراد أو المجموعات التي تحدد وتعدل مجالات الخدمة أو الخدمات وتضمن استراتيجية اتصالات مناسبة للخدمة ومجموعات يمكنها الاستفادة من الخدمات المقدمة.

المهام – قائمة الإجراءات التي يجب تنفيذها لإنجاز وظيفة محددة.

المورِّد[25] – شخص أو منظمة طورت المنتجات أو الخدمة أو تتولى مسؤولية صيانتها.

الثغرة[26] – ضعف يمكن استغلاله في البرمجيات أو العتاد أو خدمة عبر الإنترنت.

21 ISO 31000: 2009/ISO Guide 73: 2002 إدارة المخاطر – المبادئ والإرشادات – المصطلحات/التعاريف 2.1.

22 دليل ومعايير معارف إدارة المشاريع (PMBOK).

23 دليل ومعايير معارف إدارة المشاريع (PMBOK).

24 إطار محتوى المعمارية.

25 ISO/IEC 30111: 2013 تكنولوجيا المعلومات – تقنيات الأمن – عمليات التعامل مع الثغرات – المصطلحات/التعاريف 3.7.

26 ISO/IEC 30111: 2013 تكنولوجيا المعلومات – تقنيات الأمن – عمليات التعامل مع الثغرات – المصطلحات/التعاريف 3.8.

الملحق 3: الموارد الداعمة

Alberts, David S., et.al. Understanding information age warfare. In *DOD Command and Control Research Program Publication Series*. ADA395859. Booz Allen & Hamilton, McLean, VA. 2001.
https://apps.dtic.mil/docs/citations/ADA395859

Barford P., et al. (2010) Cyber SA: Situational Awareness for Cyber Defense. In: Jajodia S., Liu P., Swarup V., Wang C. (eds) Cyber Situational Awareness. Advances in Information Security, vol 46. Springer, 2010. Boston, MA. ISBN 978-1-4419-0140-8_1
https://link.springer.com/chapter/10.1007/978-1-4419-0140-8_1

Boyd, John R. Destruction and Creation. Goal Systems International. September 3, 1976.
http://www.goalsys.com/books/documents/DESTRUCTION_AND_CREATION.pdf

Cartwright, James E. Joint Concept of Operations for Global Information Grid NetOps. *United States Strategic Command*. PDF August 10, 2005. Homeland Security Digital Library. August 10, 2005.
https://www.hsdl.org/?view&did=685398

Committee on National Security Systems Instruction CNSSI 4009. *Committee on National Security Systems Website.* June 23, 2019 [accessed].
https://www.cnss.gov/cnss/

Cybersecurity Situation Awareness. *The MITRE Corporation Website.* June 25, 2019 [accessed].
https://www.mitre.org/capabilities/cybersecurity/situation-awareness

Endsley, Mica R. Toward a theory of situation awareness in dynamic systems. *Human factors* Volume 37. Number 1. March 1995 Pages 32-64.
https://journals.sagepub.com/doi/10.1518/001872095779049543

FIRST *Product Security Incident Response Team (PSIRT) Services Framework*, Version 1.0, 2018. North Carolina: First.org, 2018
https://www.first.org/education/FIRST_PSIRT_Service_Framework_v1.0

FIRST Vulnerability Reporting and Data eXchange SIG (VRDX-SIG). 2013-2015. North Carolina: First.org, 2015
https://www.first.org/global/sigs/vrdx/

Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure, Version 1.0, 2017. North Carolina: First.org, 2017
https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.0

Hawk, Robert. Situational Awareness in Cyber Security. [blog post]. *Hawk's Posts: Security Essentials from Robert Hawk.* June 11, 2015.
https://www.alienvault.com/blogs/security-essentials/situational-awareness-in-cyber-security

Householder, Allen D.; Wassermann, Garret; Manion, Art; King, Christopher. *The CERT® Guide to Coordinated Vulnerability Disclosure*. CMU/SEI-2017-SR-022. Software Engineering Institute, Carnegie Mellon University. 2017 https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330

Householder, Alan. Vulnerability Discovery for Emerging Networked Systems [blog post]. *Vulnerability discovery techniques*. November 20, 2014. https://insights.sei.cmu.edu/cert/2014/11/-vulnerability-discovery-for-emerging-networked-systems.html

International Organization for Standardization. *Information technology -- Security techniques -- Vulnerability disclosure.* Second Edition. ISO/IEC 29147:2018. Geneva, Switzerland: ISO: IEC. 2018 https://www.iso.org/standard/72311.html

International Organization for Standardization. *Information technology -- Security techniques -- Vulnerability handling processes*. First Edition. ISO/IEC 30111:2013. Geneva, Switzerland: ISO: IEC. 2013 https://www.iso.org/standard/53231.html

Jajodia, Sushil, et al., (Eds.). *Cyber Situational Awareness: Issues and Research*. Part of the Advances in Information Security book series (ADIS, volume 46). 2010. ISBN 978-1-4419-0140-8 https://link.springer.com/book/10.1007/978-1-4419-0140-8

Kossakowski, Klaus-Peter. *Information Technology Incident Response Capabilities*. Hamburg: Books on Demand, 2001. ISBN: 9783831100590.

Kossakowski; Klaus-Peter & Stikvoort, Don. *A Trusted CSIRT Introducer in Europe*. Amersfoort, Netherlands: M&I/Stelvio, February, 2000. http://www.ti.terena.nl/process/ti-v2.pdf

Manion, Art & Householder, Alan. *Vulnerability Analysis.* CERT Coordination Center (CERT/CC). May 30, 2019. https://vuls.cert.org/

McGuinness, B. &, Foy, L. A subjective measure of SA: The crew awareness rating scale (cars). In Kaber, D.B.; Endsley, M.R.; p. 286-291. *Proceedings of the First Human Performance, situation awareness and automation conference; user-centered design for the new millennium*. Savannah, Georgia, October 2000.

Salerno, John; Hinman, Michael & Boulware, Douglas. Situation awareness model applied to multiple domains. In *Proceedings of the Defense and Security Conference*, Orlando, FL, March 2005. https://www.spiedigitallibrary.org/conference-proceedings-of-spie/5813/0000/A-situation-awareness-model-applied-to-multiple-domains/10.1117/12.603735.full?SSO=1

Stone, Steve. Data to Decisions for Cyberspace Operations. *The MITRE Corporation Website*. January 2016 https://www.mitre.org/publications/technical-papers/data-to-decisions-for-cyberspace-operations

Tadda G.P., Salerno J.S. (2010) Overview of Cyber Situation Awareness. In: Jajodia S., Liu P., Swarup V., Wang C. (eds) Cyber Situational Awareness. Advances in Information Security, vol 46. Springer, Boston, MA. 2010. ISBN 978-1-

4419-0140-8
https://link.springer.com/chapter/10.1007/978-1-4419-0140-8_2

West-Brown, Moira J.; Stikvoort, Don; & Kossakowski, Klaus-Peter. *Handbook for Computer Security Incident Response Teams (CSIRTs)*. CMU/SEI-98-HB-001. Software Engineering Institute, Carnegie Mellon University. 1998.
http://www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html

الملحق 4: نظرة عامة على جميع خدمات فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT) والوظائف ذات الصلة

مجال الخدمة
نقل المعارف

التوعية
- البحوث وتجميع المعلومات
- إعداد التقارير والمواد التوعوية
- نشر المعلومات
- مد الجسور

التدريب والتعليم
- جمع متطلبات المعارف والمهارات والقدرات
- إعداد مواد التعليم والتدريب
- إيصال المحتوى
- الإرشاد
- التطوير المهني لطاقم فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT)

التمارين
- تحليل المتطلبات
- إعداد النسق والبيئة
- إعداد السيناريو
- تنفيذ التمارين
- استعراض نتيجة التمرين

المشورة التقنية والسياساتية
- دعم إدارة المخاطر
- دعم استمرارية الأعمال والتخطيط للتعافي من الكوارث
- دعم السياسات
- المشورة التقنية

مجال الخدمة
الوعي الظرفي

تحصيل البيانات
- تجميع السياسات واستخلاصها والتوجه وفقها
- رسم خارطة ارتباطات الأصول مع الوظائف والأدوار والإجراءات والمخاطر الرئيسية
- جمع المعلومات
- معالجة البيانات وإعدادها

التحليل والتركيب
- التوقع والاستدلال
- كشف الأحداث (من خلال التنبيه و/أو المطاردة)
- التأثير الظرفي

الاتصالات
- الاتصالات الداخلية والخارجية
- إعداد التقارير والتوصيات
- التنفيذ

مجال الخدمة
إدارة الثغرات

البحث الساعي لاكتشاف الثغرات
- اكتشاف ثغرة عند التصدي لحادث
- اكتشاف ثغرة من مصدر عام
- البحث عن الثغرات

التقارير الواردة عن الثغرات
- تلقي تقارير عن ثغرات
- فرز التقارير عن ثغرات ومعالجتها

تحليل الثغرات
- فرز الثغرات (التحقق والفهرسة)
- تحليل السبب الجذري للثغرة
- إعداد تدارك الثغرة

التنسيق بشأن الثغرات
- الإبلاغ/إعداد التقارير عن الثغرات
- التنسيق بشأن الثغرات مع أصحاب المصلحة

الكشف عن الثغرات
- إدارة سياسة الكشف عن الثغرات وبنيته التحتية
- الإعلان/الاتصالات/النشر بشأن الثغرات
- الملاحظات التقييمية بشأن الكشف عن الثغرات بعد تداركها

التصدي للثغرات
- كشف/البحث عن الثغرات
- تدارك الثغرات

مجال الخدمة
إدارة حوادث أمن المعلومات

قبول تقرير حادث أمن المعلومات
- استلام تقرير حادث أمن المعلومات
- فرز حوادث أمن المعلومات ومعالجتها
- التعامل مع تقرير حادث أمن المعلومات

تحليل حوادث أمن المعلومات
- فرز حوادث أمن المعلومات (تحديد الأولويات والفهرسة)
- جمع المعلومات
- تنسيق تحليل مفصل
- تحليل الأسباب الجذرية لحادث أمن المعلومات
- التلازم بين الحوادث

تحليل الصنائع والأدلة الاستقصائية
- تحليل الوسائط أو السطح
- الهندسة العكسية
- تحليل وقت التشغيل أو تحليل دينامي
- التحليل المقارن

التخفيف والاستعادة
- وضع خطة التصدي
- تدابير مخصصة واحتواء مخصص
- استعادة الأنظمة
- دعم كيانات أمن المعلومات الأخرى

التنسيق خلال حادث أمن المعلومات
- الاتصالات
- توزيع التبليغات
- توزيع المعلومات ذات الصلة
- تنسيق الأنشطة
- الإبلاغ
- الاتصالات عبر وسائل الإعلام

دعم إدارة الأزمات
- توزيع المعلومات على الجهات المخدَّمة
- الإبلاغ عن حالة أمن المعلومات
- إبلاغ القرارات الاستراتيجية

مجال الخدمة
إدارة أحداث أمن المعلومات

المراقبة والكشف
- إدارة السجل وأجهزة الاستشعار
- إدارة حالات استخدام الكشف
- إدارة البيانات السياقية

تحليل الأحداث
- التلازم
- التأهيل