إطار خدمات فريق التصدي لحوادث أمن المنتجات (PSIRT)
الإصدار 1.1

إشعار: تصف هذه الوثيقة ما يعتقد منتدى أفرقة الأمن والتصدي للحوادث (FIRST.Org) بأنها ممارسات فضلى. 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

إطار خدمات فريق التصدي لحوادث أمن المنتجات (PSIRT)

الغرض

ترد *أطر الخدمات* في وثائق إجمالية توضح بالتفصيل الخدمات التي يمكن أن تقدمها أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) وأفرقة التصدي لحوادث أمن المنتجات (PSIRT). وقد وضعها خبراء معروفون لدى مجتمع منتدى أفرقة الأمن والتصدي للحوادث (FIRST). ويسعى منتدى FIRST لإيراد ملاحظات تقييمية من جميع القطاعات، بما في ذلك أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) ذات المسؤولية على الصعيد الوطني، وأفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) في القطاع الخاص، وأفرقة التصدي لحوادث أمن المنتجات (PSIRT) بالإضافة إلى أصحاب المصلحة الآخرين. وكان القصد من هذه الوثائق أن تقدم أساساً لإعداد مواد تدريبية جديدة. بيد أنها تُستخدم اليوم على نطاق أوسع بكثير، ومثال ذلك استخدامها عند تحديد فهرس الخدمة الأولي للأفرقة الجديدة.

وعند إنشاء إطار خدمات فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT)، اتضح أن أفرقة التصدي لحوادث أمن المنتجات (PSIRT) تقدم خدمات مختلفة تماماً وتعمل عادةً في بيئات مختلفة تماماً. لذلك تقرر إنشاء وثيقة منفصلة تغطي أفرقة التصدي لحوادث أمن المنتجات (PSIRT). وستواءم الوثيقتان مع تسليط الضوء على العديد من أوجه التشابه المشتركة. ويدفع المجلس الاستشاري للتعليم عجلة تطوير الأطر.

والأطر موجودة لمساعدة المنظمات في بناء وصيانة وتنمية قدرات أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) أو أفرقة التصدي لحوادث أمن المنتجات (PSIRT) لديها. والأطر هي أدلة وتحدد مختلف النماذج والقدرات والخدمات والنتائج. وبهذه الطريقة، تتاح للأفرقة حرية تنفيذ نموذجها الخاص وبناء القدرات الملبية للاحتياجات التي ينفرد بها أصحاب المصلحة. وتسعى هذه الأطر إلى مساعدة أفرقة التصدي للحوادث الأمنية (SIRT) من خلال تحديد المسؤوليات الأساسية، وتقديم التوجيه بشأن كيفية بناء القدرات للإيفاء بهذه المسؤوليات، وتقديم رؤى بشأن كيفية قيام الأفرقة بإضافة القيمة إلى منظماتها الأكبر وإبلاغها عنها.

مقدمة

إن فريق التصدي لحوادث أمن المنتجات (PSIRT) هو كيان داخل منظمة يركز في جوهره على تحديد وتقييم وإزالة المخاطر المرتبطة بالثغرات الأمنية داخل المنتجات، بما فيها العروض و/أو الحلول و/أو المكونات و/أو الخدمات التي تنتجها المنظمة، و/أو تبيعها.

ولا يعد فريق التصدي لحوادث أمن المنتجات (PSIRT) المشغَّل بشكل سليم مجموعة تشغيل مستقلة، منفصلة عن تطوير منتجات المنظمة. بل إنه جزء من مبادرة الهندسة الآمنة الأوسع لدى المنظمة. ويضمن هذا الهيكل دمج أنشطة ضمان الأمن في دورة حياة التطوير الآمن (SDL).

وكثيراً ما يرتبط التصدي لحوادث أمن المنتجات بمرحلة الصيانة في دورة حياة التطوير الآمن (SDL) لأن معظم الثغرات الأمنية في المنتج يبلَّغ عنها كعثرات في الجودة بعد طرح المنتج في السوق. ولكن يمكن أن يكون فريق التصدي لحوادث أمن المنتجات (PSIRT) مؤثراً في المتطلبات السابقة التي تجمع مراحل المعمارية والتصميم والتخطيط ونمذجة المخاطر. ويمكن أن تقدم وظائف PSIRT أيضاً القيمة من خلال تقديم التوجيه والإشراف للتعامل مع المشاكل الأمنية التي تصادَف داخلياً.

هيكل إطار فريق التصدي لحوادث أمن المنتجات (PSIRT)

مجالات الخدمة - الخدمات - الوظائف - الوظائف الفرعية

مجالات الخدمة

خدمات إعادة تجميع مجالات الخدمة ذات صلة بجانب مشترَك. وهي تساعد على تنظيم الخدمات وفق فهرسة إجمالية تسهيلاً للفهم. ويتضمن توصيف كل مجال خدمة حقل "الوصف" الذي يتكون من نص سردي عام إجمالي يصف مجال الخدمة وقائمة الخدمات ضمن مجال الخدمة.

الخدمات

مجموعة إجراءات متماسكة يمكن تمييزها تسعى إلى نتيجة محددة نيابةً عن الجهات التي يخدمها فريق التصدي للحوادث.

وتوصَّف الخدمة بالصيغة النموذجية التالية:

- حقل "الوصف" الذي يصف طبيعة الخدمة.
- حقل "الغرض والنتيجة" الذي يصف المقصد والنتائج القابلة للقياس من الخدمة.

الوظائف

الوظيفة هي نشاط أو مجموعة من الأنشطة التي تهدف إلى تحقيق الغرض من خدمة معينة. ويمكن التشارك في أي وظيفة واستخدامها في سياق عدة خدمات.

وتوصَف الوظيفة بالصيغة النموذجية التالية:

- حقل "الوصف" الذي يصف الوظيفة.
- حقل "الغرض والنتيجة" الذي يصف المقصد والنتائج القابلة للقياس من الخدمة.
- قائمة الوظائف الفرعية التي يمكن إجراؤها كجزء من الوظيفة.

الوظيفة الفرعية

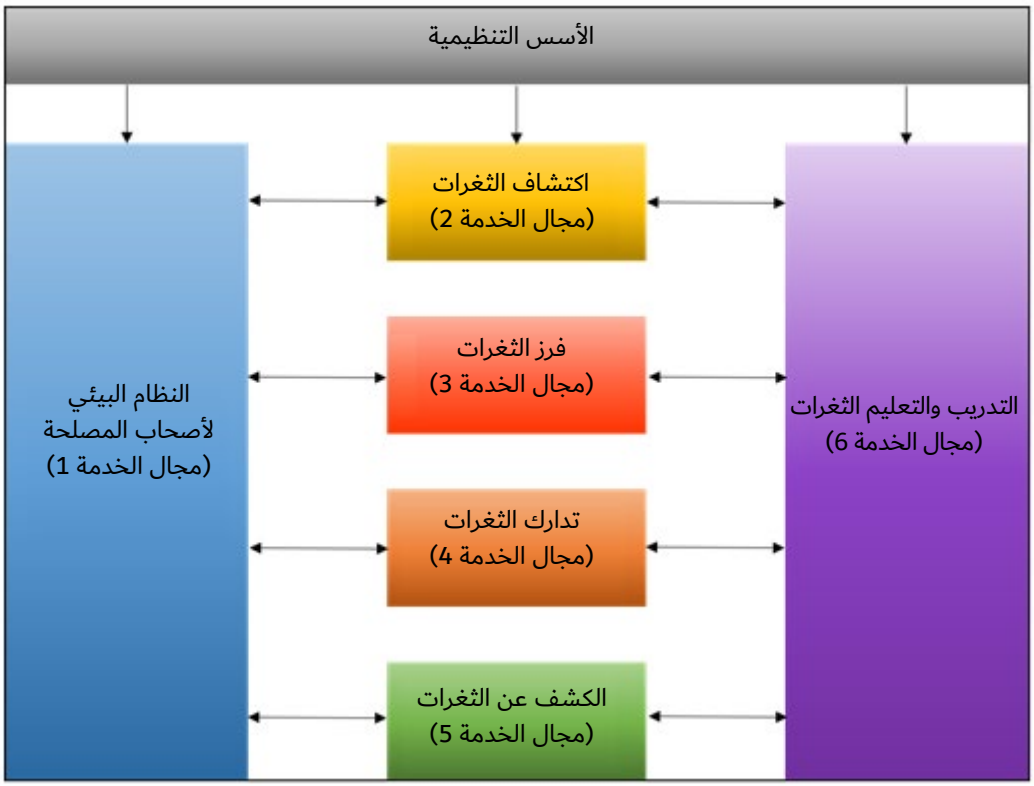
الوظيفة الفرعية هي نشاط أو مجموعة أنشطة تهدف إلى تحقيق الغرض من وظيفة معينة. ويمكن التشارك في أي وظيفة فرعية واستخدامها في سياق عدة وظائف.

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

إن التركيز على المنتجات هو الفرق الرئيسي بين فريق التصدي لحوادث أمن المنتجات (PSIRT) في منظمة وأفرقة التصدي للحوادث الأخرى الممثلة في نفس المنظمة، مثل فريق التصدي للحوادث الأمنية الحاسوبية (CSIRT). وبوجه عام، يركز فريق CSIRT المؤسسي على أمن الأنظمة و/أو الشبكات الحاسوبية التي تشكل البنية التحتية للمنظمة.

وفي حين أن هناك اختلافات مهمة بين فريق تصدي للحوادث الأمنية الحاسوبية (CSIRT) المؤسسي وفريق استجابة لحوادث أمن المنتجات (PSIRT)، فمن المهم إدراك أن هناك تآزراً أيضاً بين المجموعتين. والنقطة المهمة التي تُستنتج هي أن فريق PSIRT لا يعمل بمعزل عن عن الأجزاء الأخرى في المنظمة، وفي كل جوانب هذا الإطار سنسلط الضوء على مجالات التعاون والتآزر التي ينبغي تعزيزها.

الهيكل التنظيمي لفريق التصدي لحوادث أمن المنتجات (PSIRT)

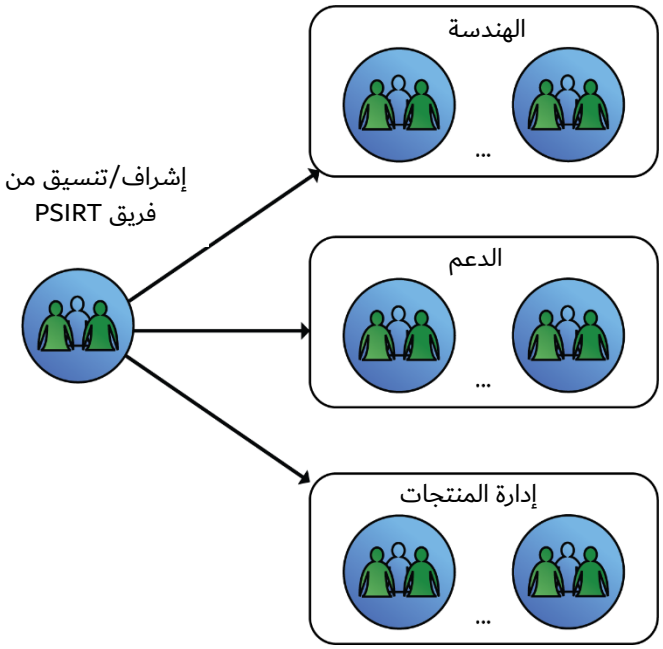


الشكل 1 - الهيكل التنظيمي

ويمكن أن تكون أفرقة التصدي لحوادث أمن المنتجات (PSIRT) فريدة ومتنوعة مثل المنتجات التي تساعد على حمايتها. وبين المنظمات في نفس القطاع أو الصناعة، ستظهر اختلافات في خصائص الأعمال، ونماذج التشغيل، وأضابير المنتجات، والهياكل التنظيمية، واستراتيجيات تطوير المنتجات. ونتيجة لذلك، لا يوجد مقاس واحد يناسب جميع إستراتيجيات التصدي لحوادث أمن المنتجات أو صيغة فريق نموذجية تتبعها جميع المنظمات. غير أن معظم الشركات تستخدم ثلاثة نماذج لفريق PSIRT: الموزَّع والمركزي والهجين.

النموذج الموزَّع

يستخدم النموذج الموزَّع فريق PSIRT أساسي صغير يعمل مع ممثلين من أفرقة المنتجات لمعالجة الثغرات الأمنية في المنتجات. وفي هذا النموذج، تتحمل عمليات فريق PSIRT الأصغر عدة مسؤوليات أساسية:



الشكل 2 - النموذج الموزَّع

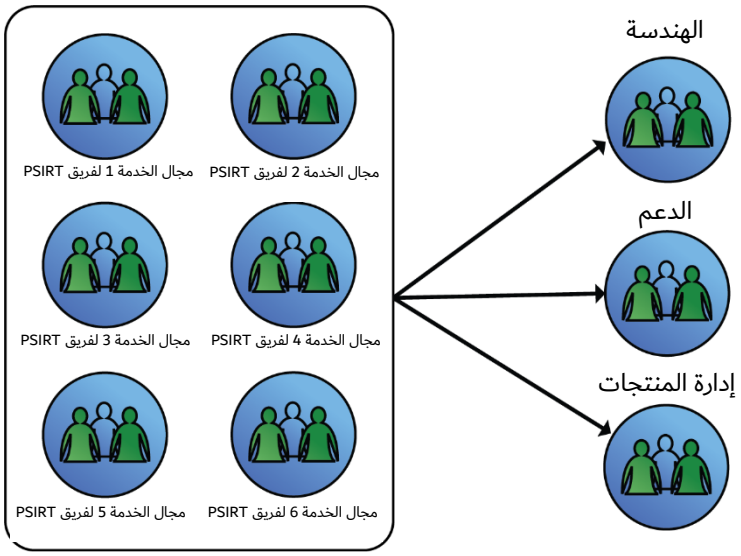
- إنشاء السياسات وإجراءات العمليات والمبادئ التوجيهية للفرز، والتحليل، والتدارك، وإبلاغ الإصلاحات، وتدابير التخفيف أو المعلومات الاستشارية الأخرى لمعالجة الثغرات الأمنية.
- إنشاء مصفوفة من ممثلي هندسة أمن المنتجات (ذوي المستويات المتدرجة) في جميع أقسام المنظمة.
- تقديم القيادة والتوجيه فيما يتعلق بالتصدي لثغرة أمنية في منتج والمخاطر المحتملة للأعمال.
- العمل كنقطة تجميع للثغرات الأمنية الواردة حيث تستفيد وفورات الحجم من نقطة تحكم مركزية.
- تبليغ مالك/مدير المنتج ومهندس الأمن بالثغرات الأمنية الجديدة، والمساعدة في إعداد خطط التدارك، وصياغة/نشر الاتصالات بشأن الإصلاح أو التخفيف، بما في ذلك إدارة الحوادث.

ويمكن لمنظمة لديها مجموعة منتجات كبيرة ومتنوعة الاستفادة من النموذج الموزَّع لأن تكلفة مهمة فريق التصدي لحوادث أمن المنتجات (PSIRT) تُسدَد عبر المنظمة. ويسمح هذا النموذج أيضاً لمهمة PSIRT بالتوسع من خلال الاستفادة من الأشخاص المهرة في أفرقة هندسة المنتجات.

وتكمن صعوبة نموذج PSIRT الموزَّع في عدم التحكم المباشر لعمليات PSIRT في الأشخاص المسؤولين عن إجراء الفرز وإيصال إصلاحات الثغرات الأمنية وعدم تبعيتهم لها.

النموذج المركزي

يحتوي النموذج المركزي على عدد أكبر من موظفي فريق التصدي لحوادث أمن المنتجات (PSIRT) المنتدبين من أقسام متعددة تقدم تقارير إلى واحد أو أكثر من كبار المديرين التنفيذيين المسؤولين عن أمن منتجات المنظمة. ويمكن أن يكون لهذا النموذج هيكل مشابه لما يلي:



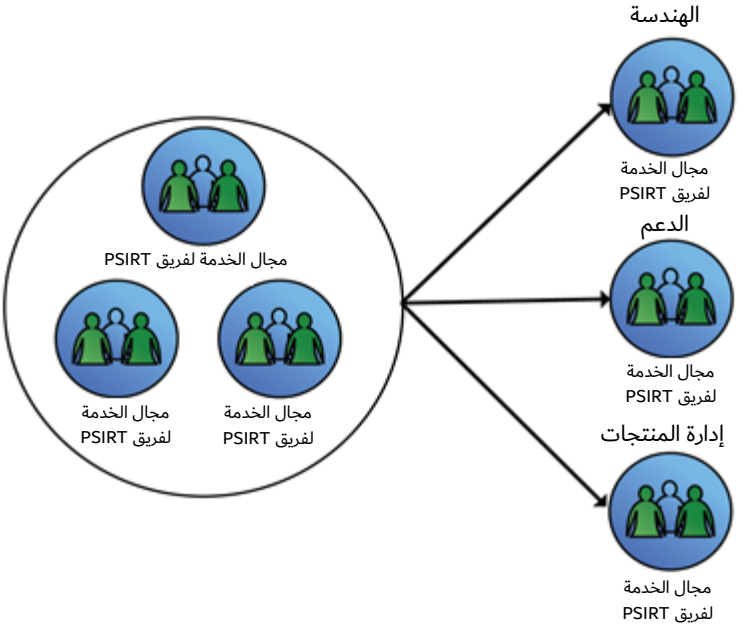
الشكل 3 - النموذج المركزي

- *قسم إدارة برمجيات فريق التصدي لحوادث أمن المنتجات (PSIRT)*: يضع السياسات والعمليات والإجراءات والمبادئ التوجيهية للفرز والتحليل والتدارك والتواصل بشأن إصلاحات الثغرات الأمنية. ويدير عمليات مبادرة فريق PSIRT بمجملها ونظام التذاكر ويمثل قيادة فريق PSIRT لدى المنظمة.
- *الاستخبار والفرز الأمني لدى فريق التصدي لحوادث أمن المنتجات (PSIRT)*: يراقب مختلف المصادر الخارجية لثغرات أمنية. ويقيِّم التأثير الأولي للثغرات الأمنية على مجموعة منتجات المنظمة.
- *التدارك والاتصالات لدى فريق التصدي لحوادث أمن المنتجات (PSIRT)*: يقدم إلى أفرقة هندسة المنتجات بشكل مباشر إصلاحات الشفرة للثغرات الأمنية.

ويُحْسن هذا النموذج العمل مع منظمة أصغر، و/أو منظمة ذات مجموعة منتجات متجانسة. ويكثِّف هذا النموذج وينمي مستوىً رفيعاً من المهارات والخبرات الأمنية في مجال واحد من مجالات المنظمة. وتكمن صعوبة هذا النموذج في تكلفة الحفاظ على فريق مركزي متخصص لا يُحْسن توسعه مواكبة نمو مجموعة المنتجات، و/أو زيادة التنوع.

النموذج الهجين

- النموذج الهجين هو نموذج يتضمن خصائص النموذجين الموزَّع والمركزي معاً. ويمكن أن تختار المنظمة تنفيذ بعض خصائص وميزات كلا النموذجين، وإنشاء نموذج هجين يأخذ في الاعتبار العوامل التالية:
- الهيكل والحجم المؤسسي للمنظمة
- حجم وتنوع مجموعة المنتجات
- استراتيجية تطوير المنتجات



الشكل 4 - النموذج الهجين

اعتبارات أخرى

من المهم أن يتمتع فريق التصدي لحوادث أمن المنتجات (PSIRT) باستقلالية الحفاظ على موقف مستقل وموضوعي من الثغرات الأمنية في المنتجات. وعلى هذا النحو، عند وضع استراتيجية وهيكل فريق PSIRT لدى المنظمة، ينبغي للمنظمة النظر في أفضل طريقة لدمج الفريق في المنظمة وهيكل إعداد التقارير الخاص به. ومن المهم أن يتبع فريق PSIRT لأحد المديرين التنفيذيين في الشركة الذي يؤكد سلطة فريق PSIRT.

ومع استمرار فريق PSIRT في النضج والتوسع، ومع تطور المهمة، يمكن أن يتغير تكوين الفريق أو هيكل تبعيته. وتتمثل القوة الدافعة لتغيير فريق PSIRT ونضجه في أصحاب المصلحة الرئيسيين، وكذلك للأسف، في تأثير ثغرة فاغرة على مجموعة واسعة من قاعدة أصحاب المصلحة في المنظمة. وكثيراً ما يعرَّف أصحاب المصلحة من خلال النموذج الذي تتبناه المنظمة وكذلك حجم المنظمة.

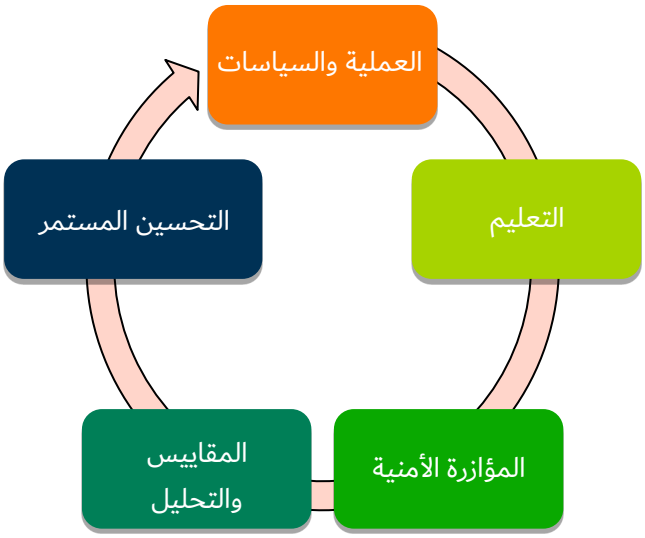
أصحاب المصلحة

تُعتبر مراعاة احتياجات ومتطلبات أصحاب المصلحة جزءاً مهماً من تحديد استراتيجية وهيكل فريق التصدي لحوادث أمن المنتجات (PSIRT). ويمكن للنموذج الذي تتبناه منظمة لتشكيل فريق PSIRT أن يملي هوية أصحاب المصلحة ومقدار تأثيرهم. ومن المهم الاستمرار في الحفاظ على علاقات إيجابية. ويرد في مجال الخدمة 1: إدارة النظام البيئي لأصحاب المصلحة، مزيد من التفاصيل بشأن النظام البيئي لأصحاب المصلحة وكيفية إدارته.

وأحد الاعتبارات النهائية في تشكيل فريق واستراتيجية التصدي لحادث منتجات هو العوامل المؤثرة. وهي عوامل تختلف عن أصحاب المصلحة في أن أصحاب المصلحة هم أشخاص أو مجموعات من الأشخاص تحمل أسماء منفصلة. وعلى النقيض من ذلك، فإن العوامل المؤثرة هي معايير وتشريعات ولوائح واتجاهات دوائر الصناعة والحكومة. ويمكن أن تستلزم هذه العوامل المؤثرة متطلبات أكبر من حيث التشكيل والاستراتيجيات والسياسات والخصائص التشغيلية لفريق PSIRT مما يستلزمه أصحاب المصلحة.

ماذا يفعل فريق التصدي لحوادث أمن المنتجات (PSIRT)؟

سيحدد النموذج المستخدَم النطاق والأنشطة التشغيلية لفريق التصدي لحوادث أمن المنتجات (PSIRT)، ولكنه لن يغير بالضرورة الإجراءات التي تحتاج المنظمة إلى اتخاذها فيما يتعلق بمعالجة الثغرات الأمنية في منتجاتها. وسيحسن النموذج نطاق القدرات والإجراءات والمسؤوليات المنسوبة مباشرة إلى فريق PSIRT بدلاً من تلك الموزَّعة في جميع أقسام المنظمة.



الشكل 5 – أنشطة فريق PSIRT العامة

التطوير الجاري للعملية والسياسات

تضع أفرقة التصدي لحوادث أمن المنتجات (PSIRT) سياسات المنظمة فيما يتعلق بأمن المنتجات. واحتياجات الأعمال هي التي تحرك متطلبات فريق PSIRT وتمليها وليس العكس. وقبل التمكن من تنفيذ سياسات فريق PSIRT، يجب أن تستعرضها قيادة المنظمة وأن تزودها بسلطات. يجب اتباع السياسات المعتمدة بإجراءات واضحة تضمن، عند اتباعها، التزام المنظمة بهذه السياسات.

تثقيف أصحاب المصلحة

إلى جانب سياسات وإجراءات فريق التصدي لحوادث أمن المنتجات (PSIRT)، يحتاج فريق PSIRT إلى بناء أنظمة سير العمل والإدارة التي تبسط تنفيذ وإكمال الإجراءات المطلوبة لمعالجة الثغرات الأمنية في المنتجات. وستسهل هذه التطبيقات على المنظمة تبني أمن المنتجات كجزء من أنشطتها التجارية اليومية.

وأكبر خطأ يمكن ارتكابه عند تنفيذ مهمة وسياسات وإجراءات فريق PSIRT هو اعتبارها مسؤولية أو متطلبات منفصلة. لذلك، تقتضي الضرورة تثقيف جميع أعضاء المنظمة بشأن أساسيات أمن المنتجات والدور الذي تؤديه. ويجب إشراك المنظمة بأكملها وتمكينها وتخويلها لتلبية متطلبات سياسة فريق PSIRT.

أهمية المقاييس

من الأهمية بمكان قياس نجاح مهمة التصدي لحوادث أمن المنتجات. ولا تحدد تقارير المقاييس المتطلبات، ولكنها تدعم البرنامج، وتساعد في تحديد الموارد المطلوبة، ويمكن أن تساعد في تحديد المواضع التي تحتاج إلى تحسينات للعملية/الأداة. ويمكن أن يساعد إنشاء المقاييس وتتبعها أيضاً في نضوج فريق التصدي لحوادث أمن المنتجات (PSIRT) بالكشف عن المشاكل أو الاختناقات فيما يتعلق بنشر فريق PSIRT واعتماده. وتخوض الخدمة 7.1 بشأن مقاييس أصحاب المصلحة والخدمة 3.5 بشأن معايير الثغرات في مزيد من التفاصيل عن أنواع المقاييس التي يعد تتبعها قيّماً.

التعاريف

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

- **مشورة**[1] - إعلان أو منشور يعمل على إعلام وتقديم المشورة والتحذير من ثغرة في منتَج.
- **أشرطة الأخطاء البرمجية** - المعايير التي تحدد أنواع الأخطاء المؤهلة كثغرة أمنية. وستُعالج الأخطاء البرمجية التي تستوفي هذه المعايير كثغرة أمنية من خلال إجراءات التشغيل المعيارية
- **المنسِق**[2] - مشارك اختياري يمكنه مساعدة المورِّدين والمكتشفين في التعامل مع معلومات عن الثغرات والكشف عنها.
- **الحظر** - تعليق نشر تفاصيل الثغرة إلى أن يتمكن المورِّدون المتأثرون من إصدار التحديثات أو عوامل التخفيف الأمنية والحلول الالتفافية لحماية العملاء.
- **المكتشِف**[3] - فرد أو منظمة يتعرفان على ثغرة محتملة في منتج أو في خدمة عبر الإنترنت؛ علماً بأن المكتشفين يمكن أن يكونوا باحثين أو جهات مبلِّغة أو شركات أمنية أو قراصنة حوسبة أو مستخدمين أو حكومات أو منسقين.
- **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 مساعٍ، وهي محايدة تجاه التكنولوجيا. وكثيراً ما يدير مجتمع من الأفراد والكيانات البرمجيات مفتوحة المصدر فيقوم بإنشائها وصيانتها بشكل تعاوني.
- **الشركاء** - مصنعو المعدات الأصليون (OEM) والموردون ومصنعو التصاميم الأصليون (ODM).
- **المنتَج**[4] - نظام نُفِّذ أو أُعد للبيع أو ليُعرض مجاناً.
- **بوابة الجودة** - مجموعة من المعايير التي يجب استيفاؤها قبل انتقال المنتَج إلى المرحلة التالية من التطوير أو الإصدار.
- **التدارك (أو العلاج)**[5] - 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.
- **المخاطر**[6] - "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**[7] - استراتيجية تصدٍ للمخاطر يقرر فيها فريق المشروع الاعتراف بالمخاطر وعدم اتخاذ أي إجراء ما لم تتحقق المخاطر.
- **سجل المخاطر**[8] - وثيقة تسجَّل فيها نتائج تحليل المخاطر وتخطيط التصدي للمخاطر.

---

1 ISO/IEC 29147: 2014 تكنولوجيا المعلومات - تقنيات الأمن - الكشف عن الثغرات - المصطلحات/التعاريف 3.1

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

3 ISO/IEC 29147: 2014 تكنولوجيا المعلومات - تقنيات الأمن - الكشف عن الثغرات - المصطلحات/التعاريف 3.3

4 ISO/IEC 29147: 2014 تكنولوجيا المعلومات - تقنيات الأمن - الكشف عن الثغرات - المصطلحات/التعاريف 3.5

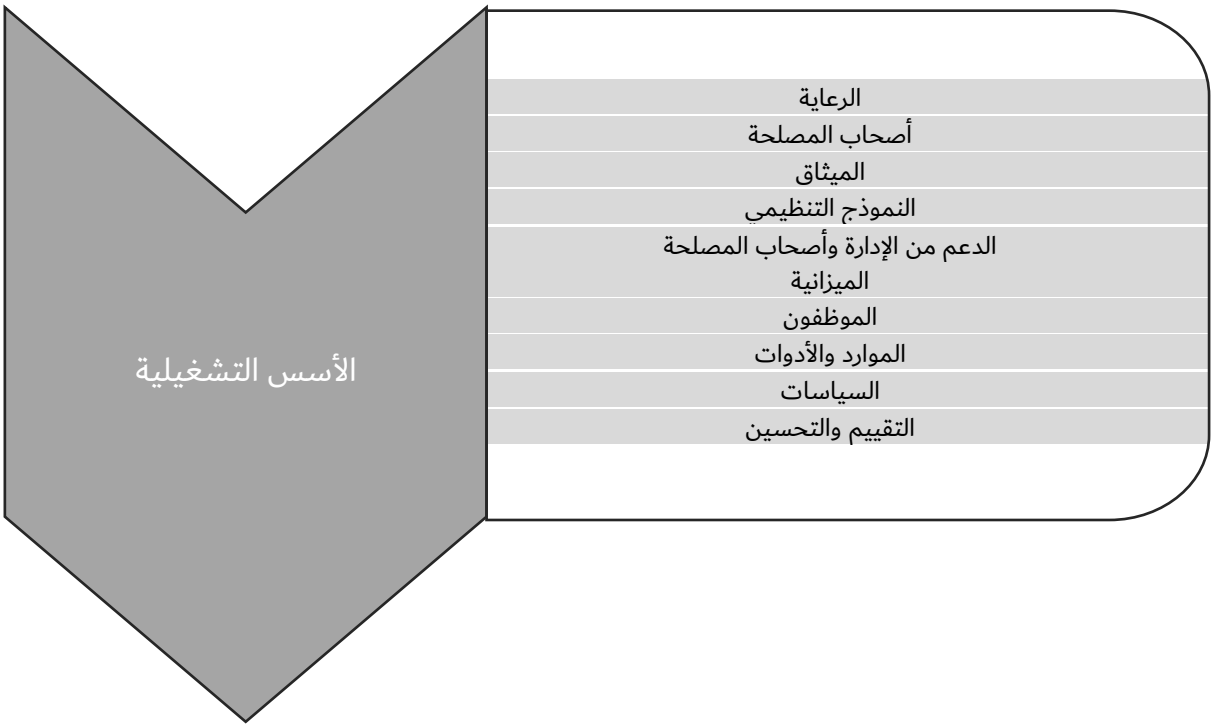
5 ISO/IEC 29147: 2014 تكنولوجيا المعلومات - تقنيات الأمن - الكشف عن الثغرات - المصطلحات/التعاريف 3.6

6 ISO 31000: 2009/ISO Guide 73: 2002 إدارة المخاطر - المبادئ والإرشادات - المصطلحات/التعاريف 2.1

7 دليل ومعايير معارف إدارة المشاريع (PMBOK)

8 دليل ومعايير معارف إدارة المشاريع (PMBOK)

- **دورة حياة التطوير الآمن (SDL)** - هي عملية تطوير تساعد المطورين على إنشاء منتجات أكثر أمناً ومعالجة متطلبات الالتزام بالأمن مع تقليل تكلفة التطوير.
- **اتفاق مستوى الخدمة (SLA)** - عقد بين مقدم الخدمة (سواء كان داخلياً أو خارجياً) والمستخدم النهائي يحدد مستوى الخدمة المتوقع من مقدم الخدمة.
- **أصحاب المصلحة**[9] - الأفراد أو المجموعات التي تحدد وتعدل مجالات الخدمة أو الخدمات وتضمن استراتيجية اتصالات مناسبة للخدمة ومجموعات يمكنها الاستفادة من الخدمات المقدمة. وباختصار، إما يساهم أصحاب المصلحة في فريق التصدي لحوادث أمن المنتجات (PSIRT) أو يستفيدون من أمن المنتجات والتصدي للحوادث.
- **الطرف الثالث** - أي مورد أو منتِج في مصدر المدخلات يقدم مكونات مدمجة في منتَج أو حل/خدمة.
- **المورِّد**[10] - شخص أو منظمة طورت المنتجات أو الخدمة أو تتولى مسؤولية صيانتها.
- **الثغرة**[11] - ضعف يمكن استغلاله في البرمجيات أو العتاد أو خدمة عبر الإنترنت.



يحدد هذا القسم ويصف أساس المكونات المركزية التي تحتاجها المنظمة للتخطيط لفريق التصدي لحوادث أمن المنتجات (PSIRT) وإنشائه وتشغيله بفعالية.

الغرض: *تمكين المنظمة من تخطيط وتنفيذ المكونات الأساسية لإنشاء وتشغيل فريق PSIRT.*

9 إطار محتوى المعمارية

10 ISO/IEC 30111: 2013 تكنولوجيا المعلومات - تقنيات الأمن - عمليات التعامل مع الثغرات - المصطلحات/التعاريف 3.7

11 ISO/IEC 30111: 2013 تكنولوجيا المعلومات - تقنيات الأمن - عمليات التعامل مع الثغرات - المصطلحات/التعاريف 3.8

__النتيجة:__ إن تحديد وتخطيط وتنفيذ المكونات الأساسية التشغيلية لفريق PSIRT يساعد المنظمة على إنشاء فريق PSIRT الخاص بها وهو ما سيحضِّر فريق PSIRT لتنفيذ مهمته وإدامة قدرة الشركة على تقديم منتجاتها وخدماتها إلى أصحاب المصلحة المحددين.

أولاً المكون الاستراتيجي

أ) الرعاية التنفيذية

الحصول على رعاية من المديرين التنفيذيين وصناع القرار الرئيسيين في المنظمة.

__الغرض:__ الإبلاغ والحصول على دعم (المشاركة) من المديرين التنفيذيين في المنظمة (من قبيل مسؤولي الإدارة العليا (المستوى C)، ومجلس الإدارة) أو صناع القرار الآخرين لتمكين فريق التصدي لحوادث أمن المنتجات (PSIRT) من العمل بفعالية.

__النتيجة:__ التمويل والدعم المستمران بناءً على مقاييس الأعمال المرغوبة.

وللحصول على رعاية المديرين التنفيذيين، ينبغي للمنظمة إبلاغ أو تثقيف المديرين التنفيذيين من خلال تزويدهم بخطة ومعلومات داعمة أخرى لمساعدتهم على فهم الغرض والأهمية والمخاطر المحتملة للثغرات الأمنية وفوائد تشغيل فريق التصدي لحوادث أمن المنتجات (PSIRT). (انظر "ميثاق فريق PSIRT"، و"الميزانية" أدناه).

انظر الخدمة 1.1 بشأن إدارة أصحاب المصلحة الداخليين للاطلاع على المعلومات ذات الصلة.

ب) أصحاب المصلحة

تحديد أصحاب المصلحة والعلاقة التي سيقيمها فريق التصدي لحوادث أمن المنتجات (PSIRT) لديكم مع هذه المجموعات.

__الغرض:__ فهم مَن سيخدمه فريقُ PSIRT ومع مَن سيتفاعل فريق PSIRT.

__النتيجة:__ قائمة بالأطراف المهتمة محددة بوضوح.

وينبغي أن يشمل ذلك أصحاب المصلحة الخارجيين، مثل عملاء المنظمة والباحثين الخارجيين في مجال الأمن، وأفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT)، وأفرقة التصدي لحوادث أمن المنتجات (PSIRT) الأخرى، بالإضافة إلى أصحاب المصلحة الداخليين، مثل مطوري البرمجيات والمهندسين والمعنيين بدعم العملاء والشؤون القانونية والعلاقات العامة/الشركات/وسائل الإعلام.

انظر مجال الخدمة 1 بشأن إدارة النظام البيئي لأصحاب المصلحة (الخدمة 1.1 بشأن إدارة أصحاب المصلحة الداخليين، والخدمة 2.1 بشأن مشاركة مجتمع المكتشفين، والخدمة 3.1 بشأن المشاركة المجتمعية والتنظيمية، والخدمة 4.1 بشأن إدارة أصحاب المصلحة في مَنفذ المخرجات) للاطلاع على المعلومات ذات الصلة.

ج) ميثاق فريق التصدي لحوادث أمن المنتجات (PSIRT)

إعداد ميثاق أو وثيقة أخرى (من قبيل الخطة الاستراتيجية أو خطة التنفيذ أو وثيقة مفهوم العمليات).

__الغرض:__ تحديد عناصر البرنامج الأساسية التي سيعمل فريق PSIRT في إطارها، ووصفها وتوثيقها.

__النتيجة:__ وثيقة تصف سبب إنشاء/تمويل فريق PSIRT والنتائج المرجوة منه.

وينبغي أن يحدد ميثاق/خطة فريق PSIRT ما يلي:

- مهمة فريق PSIRT (وينبغي أن تدعم مهمة المنظمة وتقف في صفها)
- لغرض والأدوار والمسؤوليات.

- المنتجات والخدمات (من قبيل تلقي تقارير عن ثغرات، وتطوير إصلاحات أو رُقع تصحيحية، وتوزيع إعلانات عن رُقع تصحيحية).

د) النموذج التنظيمي

تحديد وتوثيق الهيكل التنظيمي والنموذج التنظيمي اللذين سيستخدمهما فريق التصدي لحوادث أمن المنتجات (PSIRT)

الغرض: *تحديد ووصف وتوثيق النموذج التنظيمي الذي سيعمل فريق PSIRT بموجبه.*

النتيجة: *إنشاء هيكل فريق واضح المعالم ذي أدوار ومسؤوليات موثقة.*

وينبغي أن يصف النموذج التنظيمي الموثق هيكل التبعية الداخلي لفريق PSIRT وأن يحدد السلطة التي يعمل بموجبها فريق PSIRT. انظر "الهيكل التنظيمي لفريق PSIRT" للاطلاع على وصف لبعض النماذج التنظيمية الشائعة (من قبيل النموذج الموزَّع، والنموذج المركزي، والنموذج الهجين). انظر الخدمة 5.1 بشأن تنسيق اتصالات الحوادث ضمن المنظمة للاطلاع على مزيد من المعلومات ذات الصلة.

هـ) الدعم من الإدارة وأصحاب المصلحة

الحصول على دعم "المشاركة" من الإدارة التنظيمية وأصحاب المصلحة الداخليين.

الغرض: *الإبلاغ والحصول على دعم "المشاركة" من الإدارة الداخلية الأخرى وأصحاب المصلحة الآخرين لتمكين فريق التصدي لحوادث أمن المنتجات (PSIRT) من العمل بفعالية.*

النتيجة: *إبلاغ أصحاب المصلحة بمقاييس الأعمال الرئيسية لضمان الدعم المستمر.*

انظر الخدمة 1.1 بشأن إدارة أصحاب المصلحة الداخليين للاطلاع على المعلومات ذات الصلة.

ثانياً المكون التكتيكي

أ) الميزانية

تحديد تكاليف الموارد المطلوبة لتشغيل فريق التصدي لحوادث أمن المنتجات (PSIRT) والحصول على الإيرادات المناسبة لتمويل هذه الموارد.

الغرض: *تحديد ووصف وتوثيق النموذج التنظيمي الذي سيعمل ويموَّل فريق PSIRT بموجبه.*

النتيجة: *توثيق تكاليف ونفقات التشغيل ونموذج التمويل.*

وينبغي أن تتضمن الميزانية نفقات التوظيف في فريق PSIRT (الرواتب والفوائد، بالإضافة إلى التكاليف المستحَقة الأخرى)، والمعدات والمصروفات الرأسمالية الأخرى (على أنظمة/أجهزة تكنولوجيا المعلومات، أو تراخيص البرمجيات مثلاً)، وميزانية التدريب (بما في ذلك نفقات السفر).

ب) الموظفون

تحديد موارد التوظيف اللازمة لتقديم خدمات فريقكم المعني بالتصدي لحوادث أمن المنتجات (PSIRT) والحصول على موظفين مهرة.

الغرض: *تحديد ووصف وتوثيق النموذج التنظيمي الذي سيزوَّد بموجبه فريق PSIRT بالموظفين.*

النتيجة: *توثيق احتياجات موارد التوظيف في فريق PSIRT.*

وهذا يشمل تحديد مختلف وظائف الموظفين أو أدوارهم ومسؤولياتهم لفرادى أعضاء فريق PSIRT، بالإضافة إلى الكفاءات (المعارف والمهارات والقدرات [KSA]) وأي من المتطلبات الأخرى (مثل التعليم والخبرة والشهادات) المتوقعة من تلك الأدوار. ويمكن لموظفين بدوام كامل، ومورِّدين، ومقاولين، أو مزيج من هؤلاء أن يشغلوا هذه المناصب أو الأدوار.

وكجزء من خطة التوظيف (أو على النحو المحدد في وثيقة منفصلة)، ينبغي تحديد متطلبات التدريب والتخطيط لها، بما في ذلك التدريب العام لجميع موظفي فريق PSIRT والتدريب القائم على الأدوار للأفراد (من قبيل الدعم/التوجيه الأولي؛ والتدريب المستمر، والتعليم، والتوعية، وتدريب محدد للتطوير المهني).

انظر الخدمة 1.6 بشأن تدريب فريق PSIRT للاطلاع على المعلومات ذات الصلة.

ج) الموارد والأدوات

تحديد وتحصيل الموارد والأدوات الضرورية الأخرى.

الغرض: *تحديد وتحصيل الموارد والمعدات والأدوات اللازمة لتشغيل فريق PSIRT.*

النتيجة: *توثيق وفهم احتياجات فريق PSIRT من الأدوات والموارد.*

وتتضمن هذه الموارد والأدوات ما يلي:

- البنية التحتية، مثل المرافق (المساحات المكتبية)
- الأدوات/التكنولوجيا/المعدات (العتاد والبرمجيات) (انظر، على سبيل المثال، الخدمة 3.3 بشأن استنساخ الثغرات)
- نظام/أساليب الإبلاغ عن الثغرات (عبر موقع إلكتروني، أو البريد الإلكتروني، أو الهاتف، على سبيل المثال) (انظر الخدمة 1.2 بشأن واردات التقارير عن الثغرات)
- الاتصالات الآمنة (مثل PGP/التجفير) (انظر الوظيفة 2.5.1 بشأن إدارة الاتصالات الآمنة)
- قاعدة بيانات الثغرات/نظام التتبع (انظر، على سبيل المثال، الوظيفة 3.5.1 بشأن تحديثات نظام تتبع العيوب الأمنية والوظيفة 1.2.3 بشأن قاعدة بيانات المكتشف)

ثالثاً المكون التشغيلي

أ) السياسات والإجراءات

توثيق السياسات والعمليات والإجراءات ذات الصلة بإجراء عمليات فريق التصدي لحوادث أمن المنتجات (PSIRT).

الغرض: *تحديد ووصف وتوثيق السياسات والإجراءات التي سيعمل فريق PSIRT بموجبها.*

النتيجة: *يعتمد فريق PSIRT سياسات رسمية تصف سلطته والإدارة/العمليات التي سيقوم بها. ويعتمد فريق PSIRT أيضاً إجراءات/مبادئ توجيهية موثقة رسمياً تصف كيفية أداء الواجبات.*

وسيضمن توثيق السياسات والإجراءات الفهم المشترك بين جميع موظفي فريق PSIRT، وسيتيح الاتساق وقابلية التكرار للمنتجات والخدمات التي يقدمها فريق PSIRT، وسيكون بمثابة مصدر تدريب لموظفي فريق PSIRT الجدد.

ب) التقييم والتحسينات

تحديد مقاييس تقييم الأداء، و/أو الفعالية لتحديد التحسينات.

الغرض: *تقدير أو تقييم مدى جودة عمل فريق PSIRT، وتحديد المجالات المحتملة للتحسين.*

النتيجة: *سيتمكن فريق PSIRT من قياس أدائه وفهم المجالات التي يُرغب التحسين فيها.*

وينبغي لفريق PSIRT أن يقدِّر او يقيِّم بشكل مستمر، و/أو دوري كيفية أدائه (تقديم منتجاته وخدماته) وتحديد أي مجالات محتملة للتحسين.

ويمكن أن تكون مقاييس وأساليب التقييم غير رسمية (من قبيل جمع الملاحظات التقييمية من أصحاب المصلحة) أو رسمية، ويمكن أن تحدث حسب الحاجة (مثل توثيق الدروس المستفادة [انظر الوظيفة 3.1.1 بشأن عملية تحليل الحدث بعد وقوعه]) أو وفقاً لجدول زمني محدد.

ويمكن أن تكون المعلومات المقدمة في وثيقة إطار فريق التصدي لحوادث أمن المنتجات (PSIRT) مصدراً واحداً للمعايير أو القدرات المستخدمة لتقييم عمليات فريق PSIRT.

مجال الخدمة 1

يصف مجال الخدمة هذا الخدمات والوظائف التي يمكن أن يقوم بها فريق التصدي لحوادث أمن المنتجات (PSIRT) للتعامل بشكل مناسب مع أصحاب المصلحة الداخليين والخارجيين. ويسري تنفيذ الخدمات تحت هذه المظلة طوال دورة حياة الحادث أو دورة حياة نضج فريق PSIRT. وكُرس مجال الخدمة هذا لضمان إبلاغ جميع أصحاب المصلحة في فريق PSIRT ومشاركتهم في عملية التصدي للحوادث بشكل مناسب.

وقبل تقديم هذه الخدمات رسمياً، يجب على فريق التصدي لحوادث أمن المنتجات (PSIRT) أولاً تحديد أصحاب المصلحة الفريدين ذوي الصلة بأعماله. ومن بين أصحاب المصلحة جهات مثل القيادة التنفيذية أو قيادة الأعمال، أو أفرقة التطوير الداخلية، أو مقدمو المكونات أو المطورون الخارجيون، أو حتى قاعدة عملاء المنظمة. ولعل من المفيد للغاية تجميع مصفوفة لصلات أصحاب المصلحة بالمنتجات/الإصدارات لترشيد عملية الاتصالات. وقبل التواصل مع أصحاب المصلحة هؤلاء، يستفاد من فهم وجهات النظر أو الصنائع أو الأساليب التي يرغبون في المشاركة من خلالها (بوابة إلكترونية، البريد الإلكتروني المخصص، الدردشة عبر الإنترنت، نظام التذاكر، وما إلى ذلك). ولأغراض هذه الوثيقة، يُقسَّم أصحاب المصلحة إلى عدة مجموعات (وقد تحدد خصوصية ظروف أعمالكم مجموعات أخرى): المكتشفون والنظراء/الشركاء والأفرقة الداخلية والمستهلكون لمنتجاتكم.

الغرض: *تسليط الضوء على العمليات والآليات اللازمة لتبادل المعلومات مع أصحاب المصلحة المختلفين الذين يمكن وينبغي لفريق PSIRT أن يتفاعل معهم.*

النتيجة: *سيضمن التعامل الناجح مع النظام البيئي لأصحاب المصلحة في فريق PSIRT ورود التقارير عن الثغرات المكتشفة في الوقت المناسب وكذلك رضا أصحاب المصلحة/الشركاء عندما يجب إبلاغ أصحاب المصلحة في المنظمة بالثغرات الأمنية.*

الخدمة 1.1 إدارة أصحاب المصلحة الداخليين

الشكل 6 - إدارة أصحاب المصلحة الداخليين

تحدَد العمليات المتعلقة بالتعامل مع أصحاب المصلحة الداخليين لضمان الوعي والمساعدة أثناء الحوادث. وسيحسن التعامل الناجح مع أصحاب المصلحة الداخليين جهود التواصل والتصدي من خلال إيضاح دور فريق التصدي لحوادث أمن المنتجات (PSIRT) ضمن المنظمة وإقامة صلات داخلية بين أفرقة المنتجات والمحللين الأمنيين.

الغرض: *تثبيت سلطة وخبرة أفرقة PSIRT مع أصحاب المصلحة الداخليين لتسهيل التنسيق السلس لتدارك الثغرات وأمن المنتجات.*

النتيجة: *بالمشاركة الكثيفة لأصحاب المصلحة الداخليين، ينبغي أن تتدفق جميع عمليات فريق PSIRT ونتائجه بسلاسة أكبر. فعلى سبيل المثال، تخفف العيوب التي يكتشفها الموظفون الضغط الفوري للحظر الخارجي أو التدقيق الإعلامي، مما يسمح بمعالجة المشكلة وفقاً لجدول زمني يفيد المنظمة، وعملاءها، والمجتمع الأكبر ويقلل إلى أدنى حد من مخاطر الكشف العلني عن الثغرات غير المصحَحة.*

الوظيفة 1.1.1 التعامل مع أصحاب المصلحة الداخليين

الحفاظ على حوار نشط مع الأفرقة الداخلية المشاركة في تطوير واختبار وتعبئة وصيانة عروض المنظمة. وأصحاب المصلحة الداخليون ليسوا مجرد موارد هندسية، بل يمكن أن يكونوا أيضاً طواقم الاختبار/ضمان الجودة، أو هندسة الإصدارات، أو أفرقة الدعم والمبيعات والتسويق المواجِهة لأصحاب المصلحة، أو خبراء تقنيين آخرين متخصصين في هذا المجال.

الغرض: *بناء حضور على منصات المراسلة/المعلومات الداخلية لتبليغ المنتسبين الداخليين بوجود أفرقة التصدي لحوادث أمن المنتجات (PSIRT) وعملياتها ووظائفها.*

النتيجة: *سيمتلك فريق PSIRT قائمة موثقة رسمياً بأصحاب المصلحة الداخليين وفهماً لأدوارهم ومسؤولياتهم.*

الوظيفة الفرعية 1.1.1.1 التعامل مع قادة الشركات/الأعمال والمديرين التنفيذيين

لكي يكون فريق التصدي لحوادث أمن المنتجات (PSIRT) فعالاً، يجب أن يكون قادراً على فهم البيئة التنظيمية الحالية وعلى التفاعل معها. والعمل مع قادة الأعمال والمديرين التنفيذيين يساعد فريق PSIRT على عدة مستويات. وهو يساعد على إضفاء الشرعية على عمل أفرقة التصدي لحوادث أمن المنتجات (PSIRT) ضمن المنظمة بفضل الرعاية التنفيذية. وهو يسمح لفريق PSIRT بتناقل المعلومات مع القادة للمساعدة في تزويد متخذي قرارات الأعمال بالمعلومات. وهو يسمح للقيادة بالتعبير عن التغييرات في السياسة المرعية واتجاه المنظمة التي يمكن أن تغير مهمة فريق PSIRT.

الوظيفة الفرعية 2.1.1.1 التعامل مع اتصالات العلاقات العامة والأفرقة القانونية والمؤسسية

سيضمن التعامل مع أفرقة الاتصالات الداخلية والأفرقة القانونية التزام فريق PSIRT بمعايير العلامة التجارية والمراسلات الحالية وكذلك البيئة التنظيمية/القانونية التي يجب أن تلتزم بها المنظمة (بشأن الخصوصيات، أو الأماكن الفيدرالية، على سبيل المثال). ويقدم كل من أصحاب المصلحة هؤلاء مسارات فريدة لأصحاب المصلحة الأساسيين في فريق PSIRT، وينبغي إنشاء خطوط الاتصالات قبل الأحداث أو الحوادث الحرجة لضمان تمكن جميع الأطراف من العمل معاً بشكل فعال.

الوظيفة الفرعية 3.1.1.1 التعامل مع خطوط الأعمال

يضمن التعامل مع أصحاب المصلحة في التطوير توثيق المشاكل وتحديد أولوياتها ومعالجتها على الوجه الصحيح. فعلى سبيل المثال، يحتاج المهندسون من فريق التصدي لحوادث أمن المنتجات (PSIRT) أو المندوبون المعتمدون إلى تنسيق تدارك الثغرات مع مجموعات هندسة البرمجيات المسؤولة عن الشفرة المختلة. وفي أوقات الحوادث، تساعد هذه الشراكات أيضاً في سرعة إرسال المعلومات وسرعة التدارك الفعال للمشكلة. ومن أصحاب المصلحة هنا مديرو البرامج أو المنتجات، ومجموعات الإشراف على دورة حياة التطوير الآمن (SDL)، ومديرو المشاريع، ومالكو المنتجات، وغيرهم ممن يتحملون مسؤوليات مماثلة تتعلق بالأعمال.

الوظيفة الفرعية 4.1.1.1 التعامل مع التطوير/الهندسة

يحتاج المهندسون من فريق PSIRT إلى تنسيق تدارك الثغرات مع مجموعات هندسة البرمجيات المسؤولة عن الشفرة المختلة. ويضمن التعامل مع أصحاب المصلحة في التطوير توثيق المشاكل وتحديد أولوياتها ومعالجتها على الوجه الصحيح. وفي أوقات الحوادث، تساعد هذه الشراكات أيضاً في سرعة إرسال المعلومات وسرعة التدارك الفعال للمشكلة.

الوظيفة الفرعية 5.1.1.1 التعامل مع الأفرقة المواجِهة للعملاء في المبيعات والدعم

يحتاج المهندسون من فريق التصدي لحوادث أمن المنتجات (PSIRT) إلى تقديم التوضيح والصنائع إلى أفرقة دعم أصحاب المصلحة بحيث يمكن لمنظمة الدعم الاستجابة لاستفسارات أصحاب المصلحة وطلبات الدعم عند تطور المشاكل وظهورها إلى العلن. ويمكن أن يشمل "الدعم" موظفي الخط الأمامي (المعروفين أيضاً باسم "مكتب المساعدة"، وموارد الدعم المأجور (من قبيل إدارة الحسابات التقنية، ومديري نجاح أصحاب المصلحة، وما إلى ذلك)، وأفرقة المبيعات الداخلية/الخارجية، أو الموارد الميدانية (الاستشارات، هندسة المبيعات وما إلى ذلك).

الوظيفة الفرعية 6.1.1.1 مشاركة أفرقة العمل الداخلية

في المنظمات الأكثر نضجاً، يمكن للمهندسين من فريق PSIRT بناء وتعزيز العلاقات مع أصحاب المصلحة الداخليين من خلال المشاركة في مختلف المبادرات أو أفرقة العمل الداخلية. وهذا يساعد على إعادة تأكيد/تأسيس الخبرة التقنية لفريق PSIRT وبناء قنوات التواصل/الاتصالات للجهود المستقبلية.

الوظيفة 2.1.1 دورة حياة التطوير الداخلي الآمن

يعد الحفاظ على دورة حياة التطوير الآمن وإنفاذها حجر الزاوية في إرساء ثقة أصحاب المصلحة والثقة في منتجات المنظمة. وبدون القدرة على إظهار قابلية تكرار تطبيق معايير الأمن من خلال دورة حياة المنتج، يمكن أن يفقد أصحاب المصلحة الثقة في منتجات المنظمة، ويمكن أن يتشددوا في فرض المتطلبات على المنظمة (عبء الإثبات، والحق في التدقيق، وما إلى ذلك)، ويمكن أن يؤدي ذلك في النهاية إلى خسارة الإيرادات وثقة أصحاب المصلحة.

__الغرض:__ ستنفق المنظمات التي تتبع ممارسات دورة حياة التطوير الآمن السليمة قدراً أقل على تدارك العيوب الأمنية في مجموعة منتجاتها بفضل اكتشاف هذه العيوب في وقت أبكر خلال تطوير المنتجات. وستتضح، لجميع المشاركين في دورة الحياة هذه، التوقعات بشأن ميزات الأمن وخواصه الوظيفية ومتطلبات العروض، وسيفهمون أدوارهم ومسؤولياتهم في دورة الحياة. النتيجة:

__النتيجة:__ سيحصل فريق PSIRT على معلومات واضحة عن إصدار المنتج وسيتمكن من تقديم المقاييس والبيانات بشأن أداء التسليم. وفي المنظمات الناضجة، يمكن أن يقدم فريق PSIRT بيانات بشأن نقاط الضعف الشائعة في المنتجات القديمة لتجنب ارتكاب أخطاء مماثلة في الجهود المستقبلية.

الوظيفة الفرعية 1.2.1.1 المشاركة في أنشطة دورة حياة التطوير الآمن (SDL)

تشكل دورة حياة التطوير الآمن عملية إدارة حرجة تساعد المنظمة على إنتاج عروض مستقرة وقابلة للتكرار تلتزم بالمعايير الشائعة. وتساعد مشاركة فريق PSIRT في إنشاء وصيانة دورة حياة التطوير الآمن (SDL) ضمن المنظمة على ضمان اتباع الأعراف والضوابط الأمنية المناسبة.

الوظيفة الفرعية 2.2.1.1 المشاركة في إدارة دورة حياة التطوير الآمن (SDL)

تشكل دورة حياة التطوير الآمن عملية إدارة حرجة تساعد المنظمة على إنتاج عروض مستقرة وقابلة للتكرار تلتزم بالمعايير الشائعة. وتساعد مشاركة فريق PSIRT في إدارة وإنفاذ دورة حياة التطوير الآمن (SDL) ضمن المنظمة على ضمان اتباع الأعراف والضوابط الأمنية المناسبة، وتوثيق الاستثناءات واستعراضها بشكل مناسب.

الوظيفة 3.1.1 عملية تحليل الحدث بعد وقوعه

نظراً لاكتشاف الثغرات في عروض المنظمة، يتطلب فريق التصدي لحوادث أمن المنتجات (PSIRT) عملية لاستعراض هذه المشاكل سواء كانت ذات صلة بشفرة أو بعملية أو بالموظفين لتقديم هذه الملاحظات التقييمية إلى أصحاب المصلحة المشاركين والقادة ضمن المنظمة. ويمكن أن تتطلب بعض الثغرات الأمنية الفاغرة أو شديدة الخطورة على عامة الناس تحليلاً أعمق بشأن كيف تفاعلت الشركة مع المشاكل وصححتها. وتحليل الحدث بعد وقوعه هو اجتماع يضم جميع أصحاب المصلحة الداخليين الذين شاركوا في جهود التدارك والتواصل، ويسعى لتوثيق ما سار سيراً حسناً، وما كان يمكن تحسين فعله، وماهية التغييرات التي ستجرى للأحداث المستقبلية.

__الغرض:__ تقديم سرد واضح وواقعي للأحداث التي تحدث أثناء التصدي لثغرة، بما في ذلك الحوادث الأمنية، من منظور جميع الأطراف/الأفرقة المعنية. وفي أوقات وقوع مشكلة حرجة، يمكن لفريق PSIRT أن يساعد أو يقود تصدي المنظمة لتدارك مشكلة معروفة وشديدة الوطأة.

__النتيجة:__ سيقدم فريق PSIRT بيانات بشأن أداء المنظمة في ردها على ثغرات البرمجيات. وستُدرج هذه البيانات في "الدروس المستفادة" توخياً للتحسين المستقبلي خلال الأحداث.

الوظيفة الفرعية 1.3.1.1 إنشاء عملية استعراض عيوب أمن المنتجات

إن إنشاء عملية متسقة لاستعراض مشاكل تحليل الحدث بعد وقوعه يساعد على ضمان تحسين المنتجات باستمرار من خلال الدروس المستفادة.

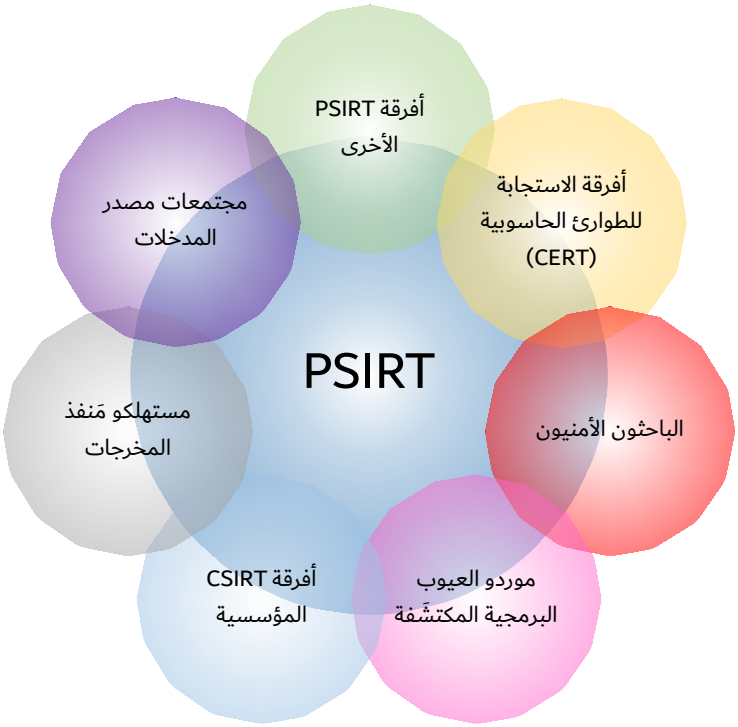
الوظيفة الفرعية 2.3.1.1 استعراض توقيت العمليات وتحديثات الإصدار

تتبع مجالات القوة والضعف.

الوظيفة الفرعية 3.3.1.1 استعراض الحوادث البارزة

تنسيق الدروس المستفادة ضمن المنظمة والتصدي للحوادث البارزة واستعراضها، وتقديم بيانات الإبلاغ إلى مصالح الأعمال وأصحاب المصلحة الآخرين حسب الاقتضاء.

الخدمة 2.1 إشراك مجتمع المكتشفين



الشكل 7 – مثال أصحاب المصلحة الخارجيين في فريق التصدي لحوادث أمن المنتجات (PSIRT)

الخدمات المتعلقة بإشراك مجتمع البحوث كصاحب مصلحة. وللباحثين العديد من الأدوار المتنوعة ووجهات النظر الفريدة - وقد يكونون أكاديميين أو متخصصين في التطوير أو باحثين أمنيين محترفين أو هواة. ويمكن أن يجري المكتشفون أبحاثاً في الهجمات أو العيوب النظرية على أمل النشر والإنجاز الأكاديمي، في حين يمكن أن يكون الآخرون من الباحثين الأمنيين المحترفين بدوافع مالية أو وسائل مؤسسية. ويظل البعض الآخر من الهواة أو المتحمسين الذين يشاركون في أوقات فراغهم، ربما لكسب الاحترام والتقدير من مجتمعاتهم. وتنتهج مشاركة مجتمع المكتشفين نهجاً استباقياً للتصدي لحوادث أمن المنتجات.

الغرض: *إسناد مكانة لفريق التصدي لحوادث أمن المنتجات (PSIRT) في منظمة كمساهم نشط في مجتمع البحوث، وبناء الوعي الظرفي بالتهديدات التي يمكن أن تؤثر على أمن منتجات المنظمة. ويمكن أن تؤدي العلاقات السلبية أو المتعارضة مع المكتشفين إلى ضياع التبليغ المبكر بالأبحاث الذي يمكن أن يضعف من موقف المنظمة في الرد على الثغرات الأمنية، وبالتالي يؤثر على مشاعر أصحاب المصلحة تجاه المنظمة.*

النتيجة: *سيعزز التفاعل المجتمعي الناجح سمعة المنظمة ومكانتها في السوق كنصير لأمن المنتجات. بالإضافة إلى ذلك، ويمكن أن يؤدي التفاعل الإيجابي مع المكتشفين إلى النفاذ المبكر إلى الأبحاث، و/أو عمليات الكشف عن الثغرات الأمنية لمساعدة المنظمة في إعداد ردها ليصار إلى نشره على الملأ في نهاية المطاف.*

الوظيفة 1.2.1 إشراك المكتشفين

تنفَّذ الأنشطة المصممة للحفاظ على حوار نشط مع المكتشفين ذوي الخبرة في أمن منتجات الشركة والنفاذ إلى قنوات مختلفة. ويمكن لأفرقة التصدي لحوادث أمن المنتجات (PSIRT) القيام بالعديد من الأنشطة لمشاركة أعمق في مجتمعات المكتشفين. ويمكن أن تشمل هذه الأشياء دعوة مكتشفين مؤهلين جيداً لإبرام عقود خاصة، والتفاعل معهم في المؤتمرات والمناسبات الأخرى، أو حتى رعاية البحوث الأكاديمية.

الغرض: *بناء حضور على مواقع التواصل الاجتماعي. ومراقبة مواقع التواصل الاجتماعي والمواقع/المنتديات الشائعة الأخرى بحثاً عن مؤشرات على مشكلة ربما وجدها المكتشفون أو أصحاب المصلحة. والنظر في المواظبة على حضور المؤتمرات الأمنية حيث يمكن أن تحدث لقاءات مع المكتشفين وجهاً لوجه.*

النتيجة: *سيتلقى فريق PSIRT تقارير عالية الجودة بتواتر أعلى وبفترة إشعار مسبق أطول من مكتشفين منخرطين بدرجة عالية بفضل توقعات الاتصالات المحددة بوضوح.*

الوظيفة 2.2.1 التعامل مع أفرقة التصدي لحوادث أمن المنتجات (PSIRT) الأخرى

يمكن لتنمية العلاقات بين أفرقة التصدي لحوادث أمن المنتجات (PSIRT) النظراء أن تساعد في تبادل المعلومات وإمكانية العون و/أو التنسيق المتبادل بشأن للحوادث. ويمكن أن يساعد العمل مع هذه المنظمات النظيرة في ملء البيانات الحيوية لتدارك الثغرات وأن يعرِّف المنظمة بخبرة نظيرتها حيث تتشاور المجموعتان بشأن المشاكل. وينبغي أن ينشئ فريق PSIRT قنوات اتصال (عادية ومؤمَّنة على السواء) مع نظرائه الرئيسيين. وتعد إقامة وتعزيز العلاقات مع النظراء في دوائر الصناعة أمراً بالغ الأهمية لتبادل المعلومات والتنسيق بشأن القضايا التي تؤثر على كلتا المنظمتين.

الغرض: *إنشاء قنوات اتصال بين منظمتكم وأفرقة PSIRT الأخرى لتبادل المعلومات عن الثغرات والمعلومات الاستخباراتية عن التهديدات والممارسات الفضلى.*

النتيجة: *يُعتبر مجتمع أفرقة التصدي لحوادث أمن المنتجات (PSIRT) النظيرة قيماً للتصدي للثغرات المتعلقة بسلسلة توريد البرمجيات. ويمكن توقع معدل تصدٍ أسرع.*

الوظيفة الفرعية 1.2.2.1 توثيق وتعريف أفرقة التصدي لحوادث أمن المنتجات (PSIRT) النظيرة

تُجمع معلومات الاتصال وعمليات الانخراط للاستخدام المستقبلي. وينبغي أن يتعامل فريق PSIRT ويتفاعل مع مجتمع PSIRT الأوسع لتبادل أفضل الممارسات والأفكار بشأن الدروس المستفادة. ومع ظهور الثغرات، كثيراً ما يُتوصل إلى حلها بطريقة تعاونية ومتعددة المجموعات تسمح لفريق PSIRT بتوسيع قدراته الداخلية من خلال الاستفادة من هؤلاء النظراء الخارجيين للحصول على المعلومات و/أو المساعدة.

الوظيفة الفرعية 2.2.2.1 تحديد عملية الكشف المنسق

ينبغي أن يوثق فريق PSIRT بعناية معلمات واتفاقات تناقل المعلومات عن الثغرات. وينبغي لفريق PSIRT أن يحترم معايير الحظر التي يحددها مكتشف الثغرات، و/أو المنظمة المبلِّغة (وأن يتوقع احترام معاييره في هذا الصدد).

الوظيفة الفرعية 3.2.2.1 إنشاء عملية تناقل معلومات الأمن

ينبغي لفريق PSIRT وضع أساليب لتناقل المعلومات عن الثغرات والمعلومات المكتومة الأخرى بشكل آمن مع الأطراف المشاركة في ترتيب الكشف المنسق. ويمكن أن يتمثل ذلك في خيارات مثل الاتصالات خارج النطاق، وغير الإلكترونية، والبريد الإلكتروني المجفر/البوابات الإلكترونية أو القوائم البريدية الخاصة.

الوظيفة الفرعية 4.2.2.1 المشاركة في أفرقة الدعم والمعلومات (SIG) وأفرقة العمل لدى دوائر الصناعة

إن العمل مع النظراء على مواضيع تهم دوائر الصناعة يدعم وينمي جهات الاتصال بالإضافة إلى تعزيز الاحتراف في الصناعة من خلال حل المشاكل بشكل تعاوني.

الوظيفة 3.2.1 التعامل مع المنسقين (أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) ومنظمات مركز التنسيق الأخرى)

يساعد العمل مع أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) الحكومية على بناء الثقة لتناقل المعلومات ويساعد فريق التصدي لحوادث أمن المنتجات (PSIRT) على كسب ثقة واحترام النظراء القيِّمين. وتشمل المنظمات الأخرى ذات الاهتمامات أو المجتمعات وثيقة الصلة، منتدى أفرقة الأمن والتصدي للحوادث (FIRST)، وشركة MITRE وجمعية النهوض بالمعايير المفتوحة للمعلومات (OASIS) واتحاد دوائر الصناعة لتعزيز الأمن على الإنترنت (ICASI) والمنظمة الدولية للتوحيد القياسي (ISO) وغيرها. ويمكن النظر إلى المجموعات التي تشارك على أساس القطاعات الوطنية أو التجارية أو الإقليمية أو الصناعية.

__الغرض:__ تعد المنظمات أهدافاً متكررة للجهات الفاعلة في مجال التهديد والتي كثيراً ما تستخدم ثغرات غير معروفة سابقاً لاختراق الشبكات. ويمكّن بناء العلاقات مع أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) اكتساب الثقة وجهات الاتصال اللازمة للحصول على تقارير عن الثغرات المحتملة في مصدر المدخلات.

__النتيجة:__ تعتبر العلاقات الجيدة مع أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) ومنظمات مركز التنسيق الأخرى ذات قيمة للتنبه إلى الثغرات في وقت مبكر. ويمكن توقع معدل تصدٍ أسرع.

الوظيفة الفرعية 1.3.2.1 التعامل مع المجتمعات والشركاء

ينبغي لفريق PSIRT البحث عن المحافل التي يدور فيها الحوار بين المجموعات الخارجية المرغوبة وبذل الجهود للمشاركة في تلك المحافل.

الوظيفة 4.2.1 التعامل مع الباحثين الأمنيين

يرد الباحثون الأمنيون في عديد من الأصناف – فمنهم الأكاديميون والهواة والممارسون الأمنيون المحترفون، على سبيل المثال لا الحصر. وهؤلاء الأشخاص هم المكتشفون الأساسيون للثغرات في أوساط الصناعة. سيحاول الباحثون الاتصال بمالك المنتج، ولكن لأسباب متنوعة لن يصلوا دائماً إلى الطرف المناسب. وستتلقى أفرقة التصدي لحوادث أمن المنتجات (PSIRT) بطريقة غير فاعلة تقارير من هؤلاء الأفراد أو المجموعات وستضطر للعمل وفق أطر زمنية يُتحكم فيها من الخارج. ومن مصلحة فريق PSIRT الفضلى اتخاذ نهج استباقي مع الباحثين الأمنيين المشاركين في دراسة المجالات التي تؤثر على منتجات فريق PSIRT، والتعامل بطريقة فاعلة مع هذه المجموعات لبلورة رؤية أوسع للمشاكل المكتَشفة.

الوظيفة الفرعية 1.4.2.1 التعامل مع موردي الأمن

يعمل كبار موردي الأمن التجاري مع أصحاب المصلحة أثناء الخروقات، وكثيراً ما يملكون بيانات استقصائية قد لا يتمكن فريق PSIRT عادةً من النفاذ إليها. ويساعد تطوير العلاقات مع هؤلاء الموزّدين على بناء الثقة والاحترام المتبادل ويمكن في الحالة المثالية أن يساعد فريق PSIRT على النفاذ إلى بيانات التهديد الحرجة التي يمكن أن لا تتاح له بخلاف ذلك.

الوظيفة الفرعية 2.4.2.1 توثيق موزّدي الأمن ذوي الصلة

يمكن أن تساعد معرفة موزّدي الأمن والتعامل معهم بشكل صحيح على تسريع الاتصالات والجهود المبذولة بشأن الإبلاغ عن الثغرات/تداركها أثناء قيامهم بإبلاغ المشاكل إلى فريق PSIRT. ومن المهم فهم ما يمكن لهؤلاء الموزّدين النفاذ إليه والاحتفاظ به. وينبغي توثيق علاقة المنظمة بموردي العيوب البرمجية المكتشَفة وتفحصها جيداً قبل الدخول في علاقة بحيث تفهم جميع الأطراف المعنية كيفية التصرف، والموارد التي يمكنها النفاذ إليها، وكيفية تناقل البيانات، ومع من تُتناقل.

الوظيفة الفرعية 3.4.2.1 أساليب توثيق التعامل مع موردي الأمن

ينبغي لفريق PSIRT البحث عن المحافل التي يدور فيها الحوار بين المجموعات الخارجية المرغوبة وبذل الجهود للمشاركة في تلك المحافل.

الوظيفة 5.2.1 التعامل مع موردي العيوب البرمجية المكتشَفة

إقامة علاقة مع موردي العيوب البرمجية المكتشَفة لتعزيز جهود الاتصالات وتناقل البيانات بشأن إدارة الثغرات.

__الغرض:__ إذا تلقت منظمتكم تقارير متكررة عن ثغرات من الموزّدين/السماسرة الذين يدفعون للمكتشفين مقابل العيوب البرمجية التي يكتشفونها، انظروا في الحفاظ على علاقة مباشرة مع تلك المنظمات التي كثيراً ما تبرم اتفاقات مستوى الخدمة (SLA) بشأن التصدي للثغرات.

__النتيجة:__ يمكن أن تسمح العلاقة المباشرة مع موردي العيوب البرمجية المكتشَفة بإجراء حوار بناء للتواصل بشأن عملية إصدار الرقعة التصحيحية الأمنية لمنتَج. وبالإضافة إلى إبرام اتفاقات مستوى خدمة مقبولة، ستساعد مثل هذه العلاقات على تقليل مخاطر الثغرات غير المعروفة بعد، بما يعود بالنفع على جميع أصحاب المصلحة.

الوظيفة الفرعية 1.5.2.1 توثيق وتعريف برامج العيوب البرمجية المكتشَفة ذات الصلة

يوثّق ويعرّف موردو العيوب البرمجية المكتشَفة القابلة للتطبيق على العروض التي تقدمها المنظمة.

الوظيفة الفرعية 2.5.2.1 التعامل مع موردي العيوب البرمجية المكتشَفة

تحدَد قنوات للتعامل مع هؤلاء المورِّدين في حوارات نشطة.

الوظيفة 6.2.1 توقُّع احتياجات أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT)

إن أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT) هي فئة خاصة من أصحاب المصلحة "في مَنفذ المخرجات" يقتصر تركيزها على المخاوف الأمنية. وإذ يمكن عادةً التفاعل مع هذه المجموعات من خلال الأعراف العادية للتعامل مع أصحاب المصلحة وإدارة العملاء، ينبغي لفريق التصدي لحوادث أمن المنتجات (PSIRT) فهم ما تفرد به هذه المجموعات التي تركز على الأمن من متطلبات ومنظور والتي ستتصل مع فريق PSIRT وتستهلك معلومات منه. وهذا يشمل أنساق الكشف والجداول الزمنية (انظر الخدمة 3.5 بشأن الكشف)، بالإضافة إلى قنوات الاتصالات بشأن طلبات محددة.

الخدمة 3.1 المشاركة المجتمعية والتنظيمية

تستحق مجموعتان من أصحاب المصلحة الذين تتفاعل معهم أفرقة PSIRT اهتماماً إضافياً. ويشار إليهما أحياناً باسم "مَصدر المدخلات"، و"مَنفذ المخرجات"، والمشاركة المجتمعية ضرورية لرفد جهود التدارك المشتركة أو المساعدة في الإعانة المتبادلة مع الآخرين ضمن مجموعات النظراء في المنظمة. و"مَصدر المدخلات" هو مصطلح يُستخدم للمجموعات أو الأفراد الذين تستصدر منظمتكم منهم المكونات أو المشاريع لمنتجاتهم. ويشير مصطلح "مَنفذ المخرجات" إلى الأفراد أو المجموعات أو المنظمات التي تستصدر مخرجات منظمتكم كأجزاء من عروضها. وترد تغطية التعامل مع مَنفذ المخرجات في الخدمة 4.1 بشأن إدارة أصحاب المصلحة في مَنفذ المخرجات.

ويمكن أن يساعد مجتمع مَصدر المدخلات النابض بالحيوية في ضخ الابتكارات في تدفقات المنتجات بالإضافة إلى المساعدة في تحمل عبء عمليات تدارك الثغرات المعقدة، وكثيراً ما يعوض نقص الخبرة الحاسمة فيها ضمن المنظمة. وبالمثل، يمكن أن تساعد تنمية العلاقات المهنية مع الأفراد والأفرقة من المنظمات الأخرى على توسيع قدرات فريق التصدي لحوادث أمن المنتجات (PSIRT) إذ تتيح له الاطلاع على وجهات النظر والخبرات والمعارف التاريخية الخارجية. ويمكن تحقيق ذلك من خلال إشراك المجتمع الأمني بشكل استباقي كصاحب مصلحة، وإقامة علاقات مع الشركاء، وأفرقة PSIRT النظيرة.

__الغرض:__ يحتاج فريق PSIRT إلى بناء وإدامة نظام بيئي نشط من الشركاء والنظراء. ويمكن أن تساعد الجمعيات المجتمعية هذه في نهج "كثرة العيون" للعثور على العيوب وتداركها، بالإضافة إلى تناقل الممارسات السليمة بين المجموعات المختلفة لتحسين مجمل التجربة في تدارك الثغرات.

__النتيجة:__ ستسهل العلاقات الجيدة والنظام البيئي النشط للشركاء والنظراء تبادل المعلومات بشأن الاستخبارات عن التهديدات والممارسات الفضلى. ويمكن أن يساعد فريق PSIRT حسن السمعة في مجتمع الأمن على جذب الموارد والمتعاونين لمعالجة المواقف الحرجة.

الوظيفة 1.3.1 تحديد المجتمعات والشركاء في مَصدر المدخلات والتعامل معها

كثيراً ما تتضمن المنتجات شفرة أو مكونات لم تنشئها المنظمة. ويطلق على منشئي هذه المواد أحياناً اسم أطراف ثالثة أو مزودين أو مورِّدي مَصدر المدخلات أو مصنعي المعدات الأصلية (OEM) أو مجرد شركاء. ومن المفيد تحديد هوية هؤلاء الشركاء ضمن نظامكم البيئي وتحديد كيف يمكن للمنظمة الاتصال بهم والتعامل معهم عند اكتشاف ثغرات في شفرة طرف ثالث.

__الغرض:__ تأسيس علاقات عمل ودية مع الأفراد أو المجموعات التي تردكم منها مكونات، أو مع المجموعات التي تتلقى مكونات من منظمتكم. وسيبقي فريق PSIRT على علم بالمشاكل التي تلوح في الأفق عند فهم أي من هذه المجموعات يتعين الاتصال بها وكيفية الاتصال بها، بالإضافة إلى فهم من يحتاج فريق PSIRT إلى إبلاغه عند اكتشاف مكونات متأثرة يتلقاها الآخرون منه.

__النتيجة:__ سيحسِّن فريق PSIRT فهمه لمصادر ووجهات المكونات. وينبغي أن يقدم ذلك نفاذاً أسرع إلى المعلومات والإصلاحات عندما يُكتشف أن بهذه المكونات عيوباً.

الوظيفة الفرعية 1.1.3.1 توثيق وتعريف المجتمعات والشركاء في مصدر المدخلات

تقدم المجتمعات والشركاء في مصدر المدخلات شفرة و/أو معارف وخبرات تُدمج في عروض المنظمة. وتقتضي الضرورة معرفة هؤلاء المزودين والانخراط معهم لضمان سرعة وفعالية التفاعلات حيثما يبلَّغ عن الثغرات الأمنية ويُعمل عليها مع فريق PSIRT. ومن الناحية المثالية، يرد توثيق هذه العلاقات في عقود، وتغطيها اتفاقات عدم الكشف وغيرها من أشكال الحماية للمنظمة.

الوظيفة الفرعية 2.1.3.1 التعامل مع المجتمعات والشركاء

يمكن أن يكون لكل مجتمع أو شريك في مَصدر المدخلات أساليب أو أدوات مختلفة يستخدمها لتطوير برمجياته/عروضه والتواصل بشأنها. وينبغي أن يفهم فريق PSIRT كيفية التعامل مع هذه المجموعات الخارجية والتأكد من أن لديها صلات/أساليب مناسبة للتعاون بشأن القضايا الأمنية التي تشمل تلك الأطراف الخارجية.

الوظيفة الفرعية 3.1.3.1 المشاركة في مجتمعات مَصدر المدخلات

تساعد المشاركة مع المجتمعات والشركاء عند مَصدر المدخلات في بناء ثقة قيّمة بين المجموعات، بالإضافة إلى المساعدة في رفد قدرات ذلك الفريق الخارجي بالخبرة التي يمكن أن تتمتع بها المنظمة.

الوظيفة الفرعية 4.1.3.1 المشاركة في الأحداث المجتمعية والصناعية

تعد المؤتمرات والاجتماعات المهنية للمنظمة محافل ممتازة لتفاعل أفرقة PSIRT مع أصحاب المصلحة والشركاء، وتلقي الملاحظات التقييمية المباشرة للمنظمة وكذلك بناء حسن النية والسمعة الطيبة في أوساط المجتمع الخارجي والتي يمكن الاستفادة منها للتنسيق/التعاون في المستقبل.

الوظيفة الفرعية 5.1.3.1 التعامل مع أفرقة الأمن المجتمعية

من الأهمية بمكان أن يفهم فريق PSIRT أياً من أفرقة الأمن لدى مقدمي البرمجيات /العتاد/الخدمات في مصدر المدخلات (PSIRT، CSIRT، مهندسو الأمن) يتعين الاتصال به وكيفية الاتصال به. ويساعد إنشاء خطوط الاتصال والتفاهم بين فريق PSIRT وهذه المجموعات على ضمان التفاعل السلس خلال أوقات الأزمات أو تدارك الثغرات.

الوظيفة 2.3.1 تحديد المجتمعات والشركاء في مَنفذ المخرجات والتعامل معها

"لمَنفذ المخرجات" دلالات عديدة، لكن هذا لا يعني أن فريق التصدي لحوادث أمن المنتجات (PSIRT) ينبغي أن يتجاهل مجموعات أصحاب المصلحة الحيوية هذه. ويشير مصطلح "مَنفذ المخرجات" إلى أي منتج أو منظمة أو فرد يأخذ منتجات وعروض شركة فريق PSIRT ويستخدمها لأغراضه الخاصة. وكثيراً ما يتخذ ذلك شكل عملاء أو مستهلكين للسلع والخدمات المقدمة، ولكن الحال ليس كذلك دائماً. وكثيراً ما يمكن لشركة أخرى استخدام أو ترخيص منتجات شركة فريق PSIRT وإعادة بيعها كعرض من خلال هذا الطرف الثالث، أو في حالة البرمجيات مفتوحة المصدر، حيث يشيع ذلك، ستقدم مجموعة واحدة البرمجيات وتديرها وستستفيد مجموعة كبيرة من الأطراف المساعدة من هذه الموارد، المعروفة أيضاً باسم مَنفذ المخرجات من المصدر.

الوظيفة الفرعية 1.2.3.1 توثيق وتعريف المجتمعات والمستهلكين والشركاء في مَنفذ المخرجات

تستهلك المجتمعات والشركاء في مَنفذ المخرجات شفرة و/أو معارف وخبرات تُدمج في عروض المنظمة. ومن الناحية المثالية، يرد توثيق هذه العلاقات في عقود، وتغطيها اتفاقات عدم الكشف وغيرها من أشكال الحماية للمنظمة.

الوظيفة الفرعية 2.2.3.1 التعامل مع المجتمعات في مَنفذ المخرجات

يمكن أن يكون لكل مجتمع أو شريك في مَنفذ المخرجات أساليب أو أدوات مختلفة يستخدمها لتطوير برمجياته/عروضه والتواصل بشأنها. وينبغي أن يفهم فريق PSIRT كيفية التعامل مع هذه المجموعات الخارجية والتأكد من أن لديها صلات/أساليب مناسبة للتعاون بشأن القضايا الأمنية التي تشمل تلك الأطراف الخارجية.

الخدمة 4.1 إدارة أصحاب المصلحة في مَنفذ المخرجات

للتعامل مع قاعدة أصحاب المصلحة لديكم كصاحب مصلحة، يجب على أفرقة التصدي لحوادث أمن المنتجات (PSIRT) إنشاء عمليات وأساليب للتفاعل مع مجتمع أصحاب المصلحة بشأن الاستجابة لأمن المنتجات. يعد أصحاب المصلحة في منتجات المنظمة من أهم من يتعين كسب رضاهم إذ يمثلون فرص الإيرادات الحالية والمستقبلية للمنظمة.

__الغرض:__ تحتاج أفرقة التصدي لحوادث أمن المنتجات (PSIRT) إلى إنشاء قنوات اتصال مع قاعدة أصحاب المصلحة في المنظمة وصياتها لنقل المعلومات بشأن الثغرات الأمنية في المنتجات أو أثناء أحداث التصدي للحوادث.

__النتيجة:__ العلاقات الجيدة مع أصحاب المصلحة لن تكتفي بتأكيد الإيرادات (أو زيادتها في بعض الحالات)، ولكنها ستقدم أيضاً لأصحاب المصلحة صوتاً بشأن منتجكم، مما يشجع الشعور بالانخراط والمشاركة في الحل.

الوظيفة 1.4.1 التعامل مع أصحاب المصلحة في مَنفذ المخرجات

ينبغي أن تتوفر لأصحاب المصلحة في منتجاتكم وخدماتكم سبل لتناقل المعلومات والآراء والحصول على الدعم بشأن كيفية معالجة المنظمة للثغرات الأمنية. ويساعد العمل الاستباقي مع أصحاب المصلحة لدى المنظمة على تقديم معايشة إيجابية للعلامة التجارية والحفاظ على ولاء أصحاب المصلحة وتحسينه.

__الغرض:__ تقديم أساليب لأصحاب المصلحة في مَنفذ مخرجات المنظمة للتواصل مع فريق PSIRT وتلقي الدعم بشأن إشكالات الأمن. ويمكن لعدم الرد بشكل مناسب على استفسارات أو مطالب أصحاب المصلحة أن يؤثر سلباً على العلامة التجارية من خلال التعليقات العلنية السلبية أو فقدان التجديدات أو فقدان الأعمال الجديدة.

__النتيجة:__ ينبغي أن يتلقى أصحاب المصلحة في مَنفذ المخرجات إرشادات سريعة وواضحة بشأن العيوب الأمنية. وسيؤدي ذلك إلى بناء مستويات من الثقة في المنتَج وسيساعد على زيادة الولاء للعلامة التجارية. ويتعين إنشاء معايشة إيجابية إجمالاً بمساعدة فريق PSIRT وإرساء خبرة فريق PSIRT مع أصحاب المصلحة. وبوجه عام، يتعين تحسين منظور العلامة التجارية بأكملها في أعين أصحاب المصلحة.

الوظيفة الفرعية 1.1.4.1 تقديم سياسات واضحة بشأن دورة الحياة والدعم

ينبغي للمنظمة أن تصف بوضوح وعلناً توقعات أصحاب المصلحة فيما يتعلق بإصلاح الثغرات الأمنية ومدة دعم المنتجات. راجع مجال الخدمة 4 للاطلاع على مزيد من المعلومات.

الوظيفة الفرعية 2.1.4.1 التعامل مع أصحاب المصلحة

سيكون لدى أصحاب المصلحة في منتجات وخدمات المنظمة أسئلة، أو سيتطلبون مساعدة، أو سيحتاجون إلى تدارك العيوب الأمنية المبلغ عنها. وينبغي أن يشارك فريق PSIRT بنشاط في طلبات أصحاب المصلحة، وأن يقدم توجيهاً واضحاً ودقيقاً بشأن الثغرات الأمنية، وأن يقدم تدابير التخفيف من المخاطر حتى يحين الوقت الذي يمكن فيه تقديم العلاج لأصحاب المصلحة.

الخدمة 5.1 تنسيق اتصالات الحوادث ضمن المنظمة

يمس حادث أمني العديد من المجموعات الداخلية، وربما يطال المنتجات ضمن المنظمة. وتُعتبر أفرقة التصدي لحوادث أمن المنتجات (PSIRT) نقطة مركزية لتنسيق جهود تدارك الثغرات بالإضافة إلى كونها مركزاً لنقل المعلومات بشأن الحدث إلى أصحاب المصلحة الداخليين المجازين.

__الغرض:__ ضمان حصول جميع الأطراف ضمن مصلحة أعمال على المعلومات بشأن حالة التصدي لثغرة أمنية كي يتمكنوا من اتخاذ قرارات مدروسة بشأن الخطوات التالية التي يجب اتخاذها. ويمكن أن تتخذ الاتصالات العديد من الأشكال (البريد الإلكتروني، والبريد التقليدي، وتلقيمات RSS، ووسائل التواصل الاجتماعي، وما إلى ذلك)، ولكن في النهاية تقدم جميع المنافذ معلومات واضحة ودقيقة في الوقت المناسب بشأن الثغرات الأمنية والحوادث التي تهم أصحاب المصلحة.

__النتيجة:__ إبلاغ أصحاب المصلحة الداخليين بنطاق وتأثير التهديدات على عروض المنظمة. وينبغي إبلاغ أصحاب المصلحة كي يتمكنوا من اتخاذ الخطوات التالية المناسبة أثناء تدارك الثغرة الأمنية، وإتاحة عمليات التخفيف.

الوظيفة 1.5.1 تقديم قنوات/منافذ الاتصالات

للتعامل بفعالية مع أصحاب المصلحة، يجب على فريق التصدي لحوادث أمن المنتجات (PSIRT) تقديم مجموعة متنوعة من قنوات الاتصالات. ويمكن أن يفضل أصحاب المصلحة المختلفون منافذ معينة على غيرها. وينبغي أن يحسب فريق PSIRT حساب أكبر عدد ممكن من المتابعين عند صياغة الاتصالات وإصدارها. وينبغي أيضاً تجهيز فريق PSIRT لاستيعاب واردات التقارير والتعليقات والأسئلة الأمنية من مجموعة متنوعة من المصادر.

__الغرض:__ تقديم أساليب لأصحاب المصلحة للسماح بالتواصل مع فريق PSIRT.

__النتيجة:__ إن هذه القنوات، سواء كانت بريداً إلكترونياً أو دردشة أو استمارة على شبكة الإنترنت، وما إلى ذلك. تتيح لأصحاب المصلحة الداخليين التواصل وتناقل المعلومات مع فريق PSIRT.

الوظيفة الفرعية 1.1.5.1 تقديم قنوات اتصالات واضحة

ينبغي أن يمتلك أصحاب المصلحة سبلاً لطرح الأسئلة، والتحقق من حالة العيوب، وإبلاغ المشاكل إلى فريق PSIRT. وإذا تأثر أحد أصحاب المصلحة بثغرة أمنية أو اكتشفها، ينبغي أن يتمكن بسهولة من إعداد تقرير وإرساله إلى فريق PSIRT.

الوظيفة الفرعية 2.1.1.5.1 تقديم قنوات اتصالات داخلية

للتعامل بفعالية مع أصحاب المصلحة الداخليين، ينبغي لفريق PSIRT تقديم قنوات اتصالات للإعلان عن حالة تدارك الثغرات. وينبغي أن يتمكن أصحاب المصلحة الداخليين من الاتصال بسهولة مع فريق PSIRT وفهم ما يمكن توقعه من الاستفسارات.

الوظيفة الفرعية 3.1.1.5.1 تقديم قنوات اتصالات خارجية

للتعامل بفعالية مع أصحاب المصلحة الخارجيين، ينبغي لفريق PSIRT تقديم قنوات اتصالات للإعلان عن حالة تدارك الثغرات. وسيشمل ذلك تدقيق/تأهيل الأنشطة بشأن الاتصالات الخارجية لضمان صلاحيتها وتسييرها بشكل مناسب إلى الزملاء الداخليين.

الوظيفة 2.5.1 إدارة الاتصالات الآمنة

في كثير من الأحيان، يجب على فريق PSIRT معالجة معلومات تُعتبر مكتومة (أي قضايا تخضع للحظر). ويحتاج فريق PSIRT القدرة على التواصل بشكل آمن وفي خلوة مع المكتشفين أو المنظمات الأخرى أو مع موارد داخلية متنوعة. والالتزام باتفاقات الكشف والتواصل عبر الأساليب الخاصة حصراً يساعد على بناء الثقة من جانب المكتشفين. وتساعد أيضاً حماية المعلومات المكتومة بشأن الثغرات من الأطراف غير المجاز لهم على ضمان إدارة المشكلة بشكل مناسب وفعال، وفقاً لشروط الحظر. ويمكن أن تساعد القنوات الآمنة أيضاً في حماية هوية المكتشفين الذين لا يرغبون في الكشف عنها. وينبغي وضع سياسة احتفاظ لضمان التخلص من البيانات على الوجه الصحيح بعد انتهاء استخدامها.

__الغرض:__ تقديم مرافق للأطراف لتبادل المعلومات بشأن الثغرات الأمنية في خلوة. وتتيح هذه القنوات حماية بقاء الثغرة الأمنية والمكتشف طي الكتمان إلى أن يتسنى الكشف عنهما علناً.

__النتيجة:__ يمكن للأطراف المشاركة في دعم القضايا الأمنية تناقل المعلومات في خلوة مع الآخرين الذين يحتاجون إلى معرفة أمر ما بشأن مشكلة ما. ويرجح أن يعود المكتشفون إلى المنظمة بتقارير مستقبلية إذا شعروا أن شواغلهم محمية من المنظمة.

الوظيفة الفرعية 1.2.5.1 تقديم قنوات اتصالات آمنة

ينبغي لفريق PSIRT التأكد من أن لدى مكتشفي الثغرات والشركاء الذين يعملون على ثغرات تؤثر على عروض المنظمة أساليب خاصة وآمنة لتبادل المعلومات.

الوظيفة 3.5.1 تحديثات نظام تتبع العيوب الأمنية

ينبغي أن يمتلك فريق PSIRT حق النفاذ إلى نظام (أنظمة) التسجيل لجميع عيوب المنتَج وأن يكون قادراً على إنشاء واستخدام نظام تتبع الثغرات الأمنية وتبادل المعلومات بشأنها.

__الغرض:__ إن تسجيل العيوب الأمنية وتتبعها بشكل صحيح يتيح للمنظمة إمكانية تحديد زمان ومكان معالجة الثغرات. ويسمح نظام العيوب هذا أيضاً بالتواصل بين فريق PSIRT والمكتشفين والمهندسين الذين يعملون بنشاط على حل المشكلة.

__النتيجة:__ عند تتبع الثغرات الأمنية بشكل مناسب باستخدام نظام، يمكن لجميع الأطراف التي تتطلب النفاذ إلى معلومات بشأن خلل ما استعراض تاريخه والتقدم الحاصل والتعليقات بشأنه.

الوظيفة الفرعية 1.3.5.1 تقديم تتبع العيوب الأمنية في المنتجات

ينبغي تتبع العيوب الأمنية، وتنبغي إتاحة النفاذ إلى هذه الأنظمة (ضمن نموذج أقل الامتيازات) لأطراف داخلية وخارجية (حسب الاقتضاء) من أجل تحديث التقدم الحاصل وتتبعه. وينبغي أن يتلقى المكتشفون الخارجيون اتصالات كافية بشأن حالة التقارير التي قدموها إلى فريق PSIRT.

الوظيفة الفرعية 2.3.5.1 إنشاء ونشر عملية تتبع العيوب الأمنية

ينبغي لفريق PSIRT التأكد من أن لدى مكتشفي الثغرات والشركاء الذين يعملون على ثغرات تؤثر على عروض المنظمة أساليب خاصة وآمنة لتبادل المعلومات.

الوظيفة 4.5.1 تبادل المعلومات ونشرها

بعد معالجة مشكلة ما، ينبغي لفريق التصدي لحوادث أمن المنتجات (PSIRT) إتاحة المعلومات بشأن ماهية الثغرة الأمنية، واستخدام نظام تحديد درجات الثغرات الشائعة (CVSS) كعامل، وماهية شدتها وآثارها، وماهية المخاطر المحتملة التي يمكن استغلالها، وكيفية حل المشكلة أو تخفيفها. وتتمثل إحدى الطرق المستخدمة على نطاق واسع لإتاحة معلومات عن الثغرة على نطاق واسع/علني في الحصول على إدراج للثغرة في قائمة تعداد الثغرات الشائعة (CVE). وهذا يضمن الإشارة إلى المشكلة بطريقة فريدة من خلال تقديم رقم تعريف ووصف ومرجع علني واحد على الأقل.

__الغرض:__ تناقل التفاصيل بشأن الثغرات الأمنية التي أُبلغ عنها وجرى تداركها. وينبغي أن يتمكن أصحاب المصلحة من تلقي العلاج أو تدابير التخفيف البديلة لاحتواء المخاطر ريثما يتسنى تقديم الإصلاحات الرسمية.

__النتيجة:__ إبلاغ أصحاب المصلحة عن الإشكالات الأمنية، وكيف يمكن أن يتأثروا بها، وكيف جرى تداركها. ويرجَّح أن ينظر أصحاب المصلحة الذين يتلقون معلومات وتحديثات في الوقت المناسب إلى المنظمة نظرة إيجابية وأن يستمروا فيما لديهم من عروض أو يوسعوا من الاستخدام المستقبلي للمنظمة.

الوظيفة الفرعية 1.4.5.1 تقديم منافذ اتصالات متعددة

سيفضل أصحاب المصلحة المختلفون أساليب مختلفة للتفاعل/الاتصالات عند الكشف عن الثغرات للعموم. وينبغي لفريق PSIRT التأكد من استخدام أساليب أخرى، بالإضافة إلى التحديثات التقليدية ذات طابع المشورة، لضمان أقصى قدر من المشاركة والوعي من أصحاب المصلحة بشأن الثغرات. وبعد تدارك الثغرات الأمنية، ينبغي لفريق PSIRT استخدام أساليب متعددة للإعلان عن الإصلاح.

الوظيفة الفرعية 2.4.5.1 تقديم ملاحظات تقييمية لأصحاب المصلحة

تساعد الملاحظات التقييمية على تحسين العمليات والتصدي في المستقبل. ويمكن أن تسلط الضوء على المجالات التي تُظهر قوة فريق PSIRT وينبغي أن يستمر أداؤه فيها، وعلى المجالات التي يحتاج فريق PSIRT إلى مزيد من التطوير والتحسين فيها.

6.1 الخدمة مكافأة المكتشفين بالشكر والتقدير

يساعد الاعتراف بفضل المكتشفين في إثبات مصداقيتهم ومصداقية منظمتهم (حسب الاقتضاء) ضمن المجتمع بالإضافة إلى الإعراب عن التقدير للشراكة مع فريق التصدي لحوادث أمن المنتجات (PSIRT) بشأن الخلل.

__الغرض:__ الاعتراف بفضل المكتشفين لما بذلوه من جهود لتنسيق الكشف عن الثغرات في المنتَج. ويمكن للمكتشفين بناء سمعتهم من خلال هذه الإقرارات لإنشاء مجموعة خبرات وإظهار القيمة للمنظمة.

__النتيجة:__ سيؤدي التعاون الإيجابي مع المكتشفين إلى تحسين أمن المنتَج. والتنويه بفضل المكتشفين سيعود بالفائدة على الموظفين الداخليين إذ يستنهضهم لبناء سمعتهم وإثبات خبراتهم.

1.6.1 الوظيفة تقديم الشكر والتقدير

يعد الإقرار بفضل الشخص (الأشخاص) المسؤول عن اكتشاف ثغرة أمنية عنصراً حيوياً في سير العمل الساعي لتدارك الثغرة الأمنية. وتعبير وجيز عن الامتنان يبني الثقة والاحترام داخل المجتمع ويُظهر أن المنظمة تتصدى للشواغل الأمنية.

__الغرض:__ يُعترف بفضل المكتشفين لما بذلوه من جهود للكشف عن الثغرات في المنتَج بطريقة مسؤولة. ويمكن للمكتشفين بناء سمعتهم من خلال هذه الإقرارات لإنشاء مجموعة خبرات.

__النتيجة:__ سيؤدي التعاون الإيجابي مع المكتشفين إلى تحسين أمن المنتَج. والتنويه بفضل المكتشفين سيعود بالفائدة على المكتشفين إذ يستنهضهم لبناء سمعتهم ويشجعهم على إرسال تقارير مستقبلية عن الثغرات إلى فريق PSIRT.

1.1.6.1 الوظيفة الفرعية تقديم الشكر والتقدير

إن الاعتراف الكتابي بجهود المكتشف ومشاركته في اكتشاف ثغرة أمنية ينفرد بكونه الأداة الأكثر فعالية والأقل تكلفة التي تجب على فريق PSIRT مكافأة هؤلاء الأفراد بها. وبات تقليدياً إدراج عبارات العرفان للمكتشف (المكتشفين) في الإرشادات الأمنية وملاحظات إصدارات البرمجيات ونصوص CVE. وسيحتاج فريق PSIRT إلى فهم الكيفية التي يعزى بها الفضل في اكتشاف الثغرات على الصعيد الداخلي.

2.6.1 الوظيفة مكافأة المكتشفين

توخياً لتحقيق نتائج إيجابية لأصحاب المصلحة ولتشجيع المزيد من تناقل البحوث، يمكن لفريق PSIRT أن يختار وضع برنامج لمكافأة هذا التعاون أو تحفيزه على أمل أن يستمر ويتوسع في المستقبل.

__الغرض:__ مكافأة الشخص (الأشخاص) الذين يبلغون عن عيوب أمنية في منتجات وخدمات المنظمة. ويمكن أن تتخذ المكافآت أشكالاً عديدة بدءاً مذكرات الشكر الإلكترونية/الورقية، مروراً بالتكريم ضمن المنظمة، ووصولاً إلى الهدايا المالية، أو غيرها من السلع/المشوّقات. ويحتاج فريق PSIRT إلى التصرف بشفافية بشأن المكافآت الممنوحة وقواعد منح هذه الجوائز.

__النتيجة:__ صُمم هذا العرف لإشاعة حسن النية تجاه منظمة فريق PSIRT وتشجيع التعاون المستمر في المستقبل بشأن القضايا الأمنية.

1.2.6.1 الوظيفة الفرعية إنشاء برنامج مكافآت للمكتشفين

يمكن لفريق PSIRT رعاية برنامج مكافآت مصمم لتشجيع السلوك الإيجابي في صفوف المكتشفين الأمنيين. ويمكن أن تكون المكافآت نقدية أو مؤسسية تكريمية أو أي عدد من الأشياء التي يمكن أن يثمّنها المكتشف الأمني بقدر أعلى من تقديره عرفاناً باكتشاف المشكلة.

الوظيفة الفرعية 2.2.6.1 بدء مكافأة نقدية جزاءَ العيوب البرمجية المكتشَفة

يمكن أن يكون التعويض النقدي أحد أشكال المكافآت. وستدفع بعض المنظمات للمكتشفين الذين يكشفون لها عن معلومات عن ثغرات.

الوظيفة الفرعية 3.2.6.1 بدء "لوحة نقاط"

ويتمثل شكل آخر من أشكال التعويض في "لوحة نقاط" تحول العثور على الثغرات الأمنية والإبلاغ عنها إلى مسابقة وتشجع المنافسة الودية من خلال إعلاء شأن "القادة" وتقديم تصنيفات للمكتشفين كي يفاخروا بها.

الخدمة 7.1 مقاييس أصحاب المصلحة

يعد تقديم تفاصيل بشأن حجم فريق التصدي لحوادث أمن المنتجات (PSIRT) أو أدائه أو قياسات أخرى أمراً بالغ الأهمية في إبقاء أصحاب المصلحة على علم بفعالية فريق PSIRT. وسينفرد أصحاب المصلحة المختلفين بوجهات نظر تجب معالجتها بصنائع (أو آراء) ذات أنساق يُحتمل أن تكون مختلفة. ويجب أن يفهم فريق PSIRT كيف ترغب كل مجموعة من أصحاب المصلحة في استهلاك هذه المعلومات. ويمكن أن تكون هذه المقاييس مؤشرات الأداء الرئيسية (KPI) لفريق PSIRT. وتتناول الوظيفة 1.5.2 التقارير التشغيلية وكيف ينبغي أن ينظر فريق PSIRT في تقديم مثل هذه التقارير لضمان سلاسة العمليات. وتستعرض الوظيفة 2.5.2 تقارير الأعمال التي يمكن لفريق PSIRT التفكير في تقديمها إلى أصحاب المصلحة.

الغرض: *تقديم بيانات بشأن قياس وأداء فريق PSIRT. وهذا يساعد أصحاب المصلحة على فهم مدى فعالية فريق PSIRT في تقديم خدمة في مجال معين.*

النتيجة: *من خلال استعراض مقاييس فريق PSIRT، ينبغي أن يعرف أصحاب المصلحة مدى فعالية فريق PSIRT في تقديم الخدمة وأن يكونوا قادرين على تقديم ملاحظات تقييمية لإجراء تعديلات على تقديم تلك الخدمة.*

الوظيفة 1.7.1 فهم متطلبات صنيعة أصحاب المصلحة

تتمثل الخطوة الأولى للتعبير بشكل فعال عن كيفية تقديم فريق PSIRT للخدمات في فهم وجهات النظر التي تنفرد بها كل مجموعة من أصحاب المصلحة. فيمكن أن ينشغل بعض أصحاب المصلحة بشأن تنفيذ الرُقع التصحيحية الأمنية في أوانها، بينما يمكن أن يركز آخرون على الأبعاد المالية لتشغيل فريق PSIRT. وكل وجهة نظر وجيهة وتتطلب صنائع مختلفة لإبلاغ المعلومات المطلوبة بشكل فعال. وينبغي استطلاع كل مجموعة من أصحاب المصلحة لفهم ماهية جوانب فريق PSIRT التي تتطلب بيانات عنها، وأفضل أسلوب لتناقل تلك المعلومات.

الغرض: *فهم ما يسترعي اهتمام صاحب المصلحة فيما يتعلق بتشغيل فريق PSIRT وخدماته. وبمجرد تجميع هذه المتطلبات والاتفاق عليها، تدعو الحاجة لاختيار أسلوب/واسطة التسليم وإيقاع التحديثات.*

النتيجة: *ستُنشأ قائمة موثقة بمتطلبات صنيعة أصحاب المصلحة (تقرير/عرض/لوحة معلومات) للحفظ.*

الوظيفة الفرعية 1.1.7.1 تجميع متطلبات مقاييس أصحاب المصلحة

سيهتم نفر من أصحاب المصلحة بمجموعة معينة من البيانات التي يمكن أن لا تسترعي اهتمام أصحاب المصلحة الآخرين. فعلى سبيل المثال، يمكن أن تكون هذه المقاييس بشأن أداء فريق التدارك الموسع بالرقع التصحيحية، والتكاليف، والجودة.

الوظيفة 2.7.1 جمع مقاييس أصحاب المصلحة

العمليات والإجراءات اللازمة لتوثيق المقاييس المطلوبة لجميع مجموعات أصحاب المصلحة. وكلما أمكن، ينبغي أن تتمكن الأدوات التي يستخدمها فريق PSIRT من جمع وتقديم معلومات بشأن عمليات وأداء فريق PSIRT. ومن الناحية المثالية، ينبغي تخزين المقاييس في موقع مركزي (قاعدة بيانات أو جدول بيانات أو أداة أخرى) بحيث يمكن استعراض السجل الزمني للأداء بشكل دوري، وبحيث تسهل معالجة وجهات نظر أصحاب المصلحة المختلفة بالحد الأدنى من الجهد الإضافي.

__الغرض:__ لملمة نقاط البيانات اللازمة و/أو إنشاؤها و/أو تجميعها، و/أو جمعها لتلبية متطلبات أصحاب المصلحة بشأن أبعاد أداء فريق PSIRT. وينبغي تخزين هذه المعلومات مركزياً بحيث يمكن استعراض سجلها الزمني ومعاودة استخدامها على يد أصحاب المصلحة (أي في حال أن مجموعتين أو أكثر من مجموعات أصحاب المصلحة ترغب في الحصول على نفس المعلومات).

__النتيجة:__ ستُجمع المقاييس المطلوبة لأصحاب المصلحة من أجل إنشاء الصنائع (التقارير، العرض، لوحات المعلومات، وما إلى ذلك).

الوظيفة الفرعية 1.2.7.1 تجميع مقاييس أصحاب المصلحة

ينبغي لفريق PSIRT إنشاء عمليات وأساليب لجمع المقاييس المطلوبة في الفترات الزمنية المحددة (SLA/OLA).

الوظيفة الفرعية 2.2.7.1 تخزين مقاييس أصحاب المصلحة

سيحتاج فريق PSIRT إلى إجراء تحليل تاريخي للأداء والاتجاهات الأخرى، لذلك من المفيد إعداد مستودع لهذه البيانات بحيث يمكن الاستمرار في الاستفادة منه في المستقبل.

الوظيفة 3.7.1 تحليل مقاييس أصحاب المصلحة

البيانات بدون سياق لا معنى لها. ويمكن الاستدلال على الافتراضات غير الصحيحة، وقد لا تعدَّل الخدمات لتلبية متطلبات العمل أو أصحاب المصلحة المتغيرة. وبمجرد أن يقوم فريق PSIRT بجمع البيانات المطلوبة، يجب بذل جهد في استعراض تلك البيانات وتقديم السياق اللازم بشأن ما تعنيه هذه البيانات لأصحاب المصلحة.

__الغرض:__ فهم معنى البيانات التي جُمعت وتقديم سياق لأصحاب المصلحة بشأن ما يجب فعله بالمعلومات. ومن الناحية المثالية، ينبغي أن يكون صاحب المصلحة قادراً على فهم كيفية أداء مؤشر أداء رئيسي معين (KPI)، والعوامل التي أثرت عليه خلال الفترة المشمولة بالتقرير، وأن يتمكن من رؤية الاتجاهات في مؤشر الأداء الرئيسي إياه.

__النتيجة:__ يُحتفظ بالبيانات التاريخية وتقارن بالأداء الحالي لتحديد الاتجاهات.

الوظيفة الفرعية 1.3.7.1 تحليل بيانات القياس واستعراضها

ينبغي أن ينفق فريق PSIRT الوقت والجهد لاستعراض البيانات التي جُمعت وتقديم السياق إلى جانب إعداد تقارير المقاييس.

الوظيفة الفرعية 2.3.7.1 تحليل اتجاهات البيانات والأداء التاريخي

أثناء جمع البيانات التاريخية، يمكن تحديد الاتجاهات الفريدة أو القضايا المزمنة التي يمكن لفريق PSIRT أو شركائها معالجتها.

الوظيفة الفرعية 3.3.7.1 تقديم سياق البيانات

يقدَّم سياق للبيانات كي يتمكن أصحاب المصلحة من فهم ما سيقدَّم لهم بشكل مناسب، وتقدَّم طريقة لمعالجة المسائل أو المخاوف.

الوظيفة 4.7.1 تقديم صنائع المقاييس لأصحاب المصلحة

بعد جمع بيانات المقاييس وتحليلها، يجب تسليمها إلى أصحاب المصلحة في نسق متفق عليه. وتمكن الإشارة إلى هذا النسق على أنه صنيعة أو رأي لمعالجة وجهة نظر صاحب المصلحة. ويمكن أن تتخذ هذه الصنائع شكل صفحة إلكترونية أو بريد إلكتروني أو تقرير ذي صفة رسمية أكبر أو أسلوب آخر.

__الغرض:__ ينبغي إعطاء أصحاب المصلحة بيانات المقاييس بنسق يمكنهم استيعابه لتقديم رؤى وفهم لأداء فريق التصدي لحوادث أمن المنتجات (PSIRT) في تقديم الخدمات. وينبغي أن تكون هذه البيانات مفهومة وذات سياق كافٍ لمساعدة أصحاب المصلحة على اتخاذ القرارات بناءً على هذا الأداء.

__النتيجة__: ستقدَّم المقاييس لأصحاب المصلحة بالنسق المناسب في الأطر الزمنية المتفق عليها.

الوظيفة الفرعية 1.4.7.1 تزويد أصحاب المصلحة بصنائع المقاييس

ينفرد كل صاحب مصلحة بوجهة نظر يمثلها. وتحتاج كل وجهة نظر إلى معالجة من خلال عرض البيانات في شكل صنيعة إبلاغ معينة. وقد يلزم تعديل هذه الصنائع لتطابق وجهات النظر المختلفة. ويمكن أن تشتمل الصنائع على تقارير تُرسَل بالبريد الإلكتروني أو تُنشر في صفحة إلكترونية، أو بوابة إلكترونية دينامية، أو إحاطات تنفيذية، أو مخططات، أو رسوم بيانية، أو أي عدد من آليات تسليم البيانات الأخرى.

الوظيفة الفرعية 2.4.7.1 استعراض المقاييس والدروس المستفادة

ينبغي أن يتمثل أحد أهم أهداف فريق PSIRT في التحسين المستمر لعملية إدارة الثغرات. ويستعين فريق PSIRT باستعراض مقاييس الأداء والملاحظات التقييمية من أصحاب المصلحة لتحديد المجالات التي يجب التركيز عليها أو تحسينها.

مجال الخدمة 2

يصف مجال الخدمة هذا الخدمات والوظائف التي يمكن أن يؤديها فريق التصدي لحوادث أمن المنتجات (PSIRT) لاكتشاف الثغرات المحتملة. وسيؤدي تشغيل مجال الخدمة هذا إلى انطلاق عملية معالجة الثغرات الموضحة في أقسام أخرى من هذه الوثيقة. ويمكن قياس نضج فريق PSIRT من خلال توافر وكفاءة خدمات الاختلاف المنصوص عليها في مجال الخدمة هذا.

الغرض: *وضع عمليات وآليات لجمع المعلومات الاستخبارية المتعلقة بثغرات المنتجات أو مكونات من طرف ثالث معرَّضة للاختراق أو نقاط الضعف المعمارية من مصادر مختلفة.*

النتيجة: *زيادة الوعي الظرفي بالتقارير والثغرات المحتملة التي تتطلب اتخاذ إجراءات من أصحاب المصلحة.*

الخدمة 1.2 واردات التقارير عن الثغرات

السيناريو الرئيسي، بالنسبة إلى فريق PSIRT، هو واردات التقارير التي تؤثر على منتَج صاحب المصلحة. ويتمثل أحد العناصر الأساسية لواردات التقارير عن الثغرات في إنشاء البنية التحتية المطلوبة والمحافظة عليها، وتحديد جهات الاتصال والإعلان عنها، وتحديد الجاهزية والحفاظ عليها.

الغرض: *إنشاء عمليات وآليات تسمح لكيان ما بالإبلاغ بسهولة عن ثغرة في منتَج أحد أصحاب المصلحة والحفاظ على جاهزية فريق PSIRT في حالة الإبلاغ عن ثغرة.*

النتيجة: *جاهزية فريق PSIRT لتقارير الثغرات وتلقيها بشكل احترافي.*

الوظيفة 1.1.2 ضمان سهولة التواصل

يجب على أفرقة التصدي لحوادث أمن المنتجات (PSIRT) أن تجعل وجودها معلوماً على الملأ وأن تكون متاحة للأطراف الخارجية أو لمسارات التصعيد الداخلية. ويمكن أن تساعد قناة اتصالات واضحة ومحددة المكتشفين أو الشركاء أو أصحاب المصلحة في إبلاغ أفرقة التصدي لحوادث أمن المنتجات عن الثغرات.

__الغرض:__ السماح للكيان المهتم بالإبلاغ عن ثغرة بالعثور بسهولة على معلومات الاتصال المطلوبة وطريقة التقديم المفضلة.

__النتيجة:__ الحصول على عدد أكبر من التقارير واستبعاد أي ادعاءات بعدم تيسر فريق PSIRT لتلقي معلومات مقدمة عن ثغرات.

الوظيفة الفرعية 1.1.1.2 تحديد الشكل المفضل لتقديم تقرير

يُتوقع تلقي معلومات عن ثغرات عبر قنوات مختلفة وذات جودة متغيرة. مع ذلك، من المفيد تحديد أفضل طريقة لمعالجة التقرير. ويمكن أن يكون ذلك في شكل استمارة على شبكة الإنترنت أو نظام تذاكر عمومي أو عنوان بريد إلكتروني أو خط ساخن للدعم أو أي وسيلة أخرى لتقديم تقرير.

الوظيفة الفرعية 2.1.1.2 نشر تفاصيل الاتصال

ينبغي أن تظهر معلومات وسيلة الاتصال المفضلة مع فريق PSIRT في وثائق المنتَج، ويُعلن عنها في الصفحة الإلكترونية للشركة، وتفهرَس في محركات البحث، وتسجَّل في قوائم فريق CSIRT/PSIRT الرئيسية، وتبلَّغ إلى الكيانات التي تصدر تعداد الثغرات الشائعة (CVE) مثل هيئات ترقيم CVE (CNA) ويُعلن عنها في المجتمعات الأمنية.

الوظيفة الفرعية 3.1.1.2 تسجيل نقاط الاتصال المشتركة

يستفاد من حجز المصطلحات الشائعة المتعلقة بفريق PSIRT مثل "psirt@" أو "incidents@" أو "security@" ضمن اسم ميدان شركتكم. وسيساعدكم هذا الحجز في توجيه اتصالات فريق PSIRT ذات الصلة إليكم.

الوظيفة الفرعية 4.1.1.2 إقامة صلة الوصل مع فريق PSIRT داخل الشركة

يُتأكد من أن خدمة أصحاب المصلحة (بالنسبة لطلبات أصحاب المصلحة أو التقارير عن الثغرات) وقسم الاتصالات (بالنسبة لطلبات وسائل الإعلام)، بالإضافة إلى أفرقة تطوير المنتجات (بالنسبة لتصعيد المكتشفات الداخلية الحرجة)، على دراية بفريق PSIRT وعلى علم بكيفية الاتصال به.

الوظيفة الفرعية 5.1.1.2 تعريف الجاهزية وإدامتها

حسب الصناعة والمتطلبات التي يحددها أصحاب المصلحة، تؤسَس ورديات عمل حسب الطلب أو على مدار الساعة للحفاظ على الجاهزية اللازمة للاستجابة للتقارير الحرجة.

الوظيفة الفرعية 6.1.1.2 الإعداد للتبليغات المجفَّرة

كثيراً ما تحتوي تقارير الثغرات على معلومات حساسة بشأن البيئة التشغيلية والمنتجات التي رُصدت فيها الثغرة. ولتجنب تسرب المعلومات أو الكشف عنها عن طريق الخطأ، تروَّج وسائل لتقديم التقارير بطريقة مجفرة، مثل رسائل البريد الإلكتروني المحمية بواسطة S/MIME أو PGP، أو استمارات الإنترنت الممكّنة برابط HTTPS.

الوظيفة 2.1.2 معالجة التقارير عن الثغرات

ترد تقارير عن الثغرات من مصادر متنوعة وبأشكال مختلفة. وتعد المراقبة المنتظمة لقنوات الاتصالات الواردة والاستجابة في الوقت المناسب للتقارير الواردة أمراً بالغ الأهمية. وينبغي تحديد أوقات الاستجابة للمكتشفين الخارجيين في اتفاق مستوى خدمة داخلي بالنسبة للشركة.

__الغرض:__ تقديم عمليات وآليات لتلقي تقارير عن الثغرات من أجزاء أخرى من الشركة الموردة، وأصحاب المصلحة، والأطراف الثالثة (من المكتشفين، أفرقة التصدي لحوادث أمن المنتجات (PSIRT)، أفرقة التصدي للحوادث الأمنية الحاسوبية (CSIRT)، وما إلى ذلك).

__النتيجة:__ المعالجة المهنية لتقارير عن الثغرات من أطراف ثالثة.

الوظيفة الفرعية 1.2.1.2 مراقبة قنوات الاتصالات

التحقق بانتظام من الوسائل المُعلن عنها للاتصال بفريق PSIRT، وكذلك من القنوات الأخرى المتاحة مثل البريد الإلكتروني الوارد للأغراض العامة أو حسابات الشركة على وسائل التواصل الاجتماعي.

الوظيفة الفرعية 2.2.1.2 معالجة التقارير بمعزل عن بعضها البعض

سيحقق فريق PSIRT في التقارير عن ثغرات من وبالتالي يسهل استهدافه من خلال تبليغ خبيث. ويستدعي ذلك إعداد السياسات والإجراءات التقنية لحماية بيئة العمل من مثل هذه المحاولات من خلال تقديم وسائل لمعالجة التقارير عن ثغرات بشكل آمن.

الوظيفة الفرعية 3.2.1.2 الإقرار باستلام التقارير في الوقت المناسب

كثيراً ما يكون التحليل التفصيلي للتقرير معقداً ويستغرق وقتاً طويلاً، ولكن يمكن الإشعار باستلام التقرير سريعاً. ويُظهر الرد الفوري أن التقرير يؤخذ على محمل الجد ويساعد كثيراً في إنشاء علاقة ثقة. ويمكن بناء الاتصالات اللاحقة طوال عملية المعالجة على هذا التعامل الأول الذي يظهر التزام فريق PSIRT بحل مفهوم.

الخدمة 2.2 تحديد الثغرات غير المبلَّغ عنها

يسهل استيعاب الثغرات التي يُكشف عنها للمورِّد مباشرة أو من الأطراف المبلغة. ولكن من المهم إدراك وجود ثغرات إضافية يمكن الكشف عنها عبر القنوات غير الرسمية مثل المنافذ الإخبارية أو المدونات التقنية أو قواعد بيانات الخبراء أو وسائل التواصل الاجتماعي أو المنشورات التقنية، والمؤتمرات.

الغرض: *الحفاظ على الوعي الظرفي واختصار الوقت اللازم لكشف التهديدات التي تؤثر على منتَج صاحب المصلحة وكذلك تقليل احتمال عمليات الكشف الكامل.*

النتيجة: *زيادة الوعي الظرفي من حيث التهديدات الأمنية لمجموعة منتجات صاحب المصلحة.*

الوظيفة 1.2.2 مراقبة قواعد بيانات الشفرات الاستغلالية

تنبغي مراقبة قواعد بيانات الشفرات الاستغلالية أو الخلاصات التجارية المتاحة للعموم لاكتشاف ثغرات محتملة غير معروفة بعد تتطلب التحقيق. ويمكن أن تؤدي شفرة استغلالية كاملة الخواص الوظيفية إلى تواصل استباقي بين الشركة وأصحاب المصلحة فيها.

الغرض: *اكتشاف الثغرات التي لم يبلَّغ عنها البتة عبر القنوات المناسبة.*

النتيجة: *تعزيز المعرفة بوجود شفرات استغلالية تفعل أفاعيلها في السوق.*

الوظيفة 2.2.2 مراقبة برامج المؤتمرات

تنبغي مراقبة المؤتمرات الأمنية ذات الصلة للوقوف على الورقات المقدَّمة فيها الجديرة بالاهتمام. وإلى جانب الإشارة مباشرة إلى المنتجات أو العلامات التجارية، يمكن أن تناقش الورقات المقدَّمة مواضيع أوسع مثل عيوب البروتوكول التي يمكن أن تتطلب عمل فريق PSIRT. وإذا أثار الملخص أسئلة، يُستحسن التعامل مع المكتشِف في مرحلة مبكرة لتوضيح ما إذا كانت هناك حاجة لاتخاذ إجراءات. بالإضافة إلى ذلك، يمكن للحضور في المؤتمر والتعامل الاستباقي مع المؤلفين أن يروج للاتصال المباشر بفريق PSIRT بشأن بحوث في المستقبل.

الغرض: *منع المباغتة بأي إفشاء غير منسق أو تحديد لعيوب لم ينظر فيها المؤلفون بعد ويمكن أن تؤثر بشكل مباشر أو غير مباشر على منتجات أصحاب المصلحة.*

النتيجة: *فرصة التقرب بنشاط من المؤلفين قبل نشر أي منشور لتوضيح ما إذا كانت أي منتجات لأصحاب المصلحة ستتأثر أو ما إذا كانت هناك مشكلة في تقديم تقرير.*

الوظيفة 3.2.2 مراقبة منشورات المكتشفين المشهورين

الانتباه إلى ما ينشره المكتشِفون الذين لديهم سجل حافل بالمنشورات ذات الصلة أو خبرة واسعة إما في أوساط الصناعة أو في منتجات وخدمات شركة ما على وجه التحديد. إذ يمكن أن تلمِّح أعمالهم العلمية أو مدوناتهم على الإنترنت أو مشاركاتهم في القوائم البريدية إلى الثغرات أو نقاط الضعف المحتملة التي تتطلب العناية.

الغرض: *مواكبة حالة المعارف العلمية والتقنية في المواضيع الأمنية ذات الصلة بأصحاب المصلحة.*

النتيجة: *خبرة في التهديدات ونقاط الضعف الشائعة والإجراءات المضادة الممكنة لدعم أصحاب المصلحة عند حل مشاكل أمن المنتجات.*

الوظيفة 4.2.2 مراقبة وسائل الإعلام

كثيراً ما تكون وسائل الإعلام سباقة في تلقف حالات الحوادث الكارثية، على وجه الخصوص، التي تضرب المنشآت أو الأفراد لدى أصحاب المصلحة. ويمكن أن تساعد مراقبة وسائل الإعلام على كشف المواقف التي يحتمل أن يكون فيها أصحاب المصلحة لدى فريق PSIRT مورِّداً مهماً أو مهيمناً.

الغرض: *تفنيد الادعاء بأن ثغرة في المنتَج ساهمت في وقوع الحادث.*

النتيجة: *زيادة الجاهزية في حال استفسار أصحاب المصلحة أو وسائل الإعلام عن ثغرات المنتج التي يمكن أن تكون متورطة في التسبب في الحادث.*

الخدمة 3.2 مراقبة الثغرات في مكونات المنتجات

تندرج الثغرات تقريباً في ثلاث فئات: (1) الثغرات في شفرة المصدر الخاصة بالمنتج، و(2) الثغرات في مكونات المنتج التي تحتفظ بها المصادر الداخلية لدى المورِّد، و(3) الثغرات في مكونات التي تقدمها المصادر الخارجية بالنسبة للمورِّد (أطراف ثالثة). ومن منظور المنتَج، (2)، و(3) هما مكونات خارجية، ولكن الثغرات في هذه المكونات يمكن أن تؤثر في النهاية على المنتَج الذي يحل محلها. وعلى الرغم من أن مالك المنتَج ليس لديه سوى سيطرة غير مباشرة على معالجة المشكلة الأساسية، يرى صاحب المصلحة درجة معينة من المسؤولية عبر سلسلة التوريد وتدارك الثغرات فيما يتعلق بالمنتَج المتأثر. وذلك هو الحال بشكل خاص، عندما يتعذر تدارك ثغرة المكون بشكل مستقل عن المنتج الذي يضمه. وتُعتبر مكونات المصدر المفتوح المضمَنة أيضاً مكونات طرف ثالث.

الغرض: *تحديد الثغرات وجمعها ومراقبتها في سلسلة توريد منتجات أصحاب المصلحة، وإبلاغ أفرقة المنتجات بشأن الثغرات التي تؤثر على منتجهم.*

النتيجة: *رؤية أدق في التحديد المبكر للثغرات الموروثة من سلسلة التوريد التي تؤثر على منتجات أصحاب المصلحة.*

الوظيفة 1.3.2 جرد مكونات المنتجات

الاحتفاظ بقائمة بالموردين والمنتجات والإصدارات المقدمة من الجهات الخارجية والداخلية والمضمنة في المنتجات. يعد ذلك ضرورياً للتعرف بسرعة على المنتجات المتأثرة بالثغرات الموروثة.

الغرض: *تحديد المنتجات بما في ذلك المكونات ذات الثغرات يمكن أن تؤدي إلى ثغرة في المنتج نفسه.*

النتيجة: *قائمة مواد مكتملة لجميع المنتجات من أجل البحث عن مكونات المنتَج ذات الثغرات.*

الوظيفة 2.3.2 مراقبة إرشادات الطرف الثالث

الحصول على معلومات في الوقت المناسب بشأن ثغرات في مكونات طرف ثالث من خلال الاشتراك في إرشادات المورِّد أو إنشاء قنوات اتصالات محددة مع الموردين. والاشتراك في القوائم البريدية الأمنية للمشاريع مفتوحة المصدر. ويمكن دعم ذلك باستخدام مقدمي المعلومات عن الثغرات.

الغرض: *تحديد الثغرات في مكونات الطرف الثالث التي ينتج عنها ثغرة في منتج صاحب المصلحة.*

النتيجة: *يمكن أن تبدأ عملية معالجة الثغرات قبل ظهور تقرير خارجي عن المنتجات المتأثرة.*

الوظيفة 3.3.2 مراقبة مصادر الاستخبارات عن الثغرات

يمكن أن لا يتسنى دائماً الاشتراك في إرشادات المورِّد بشان مكونات طرف ثالث. ويحدث ذلك عندما لا ينشر المورِّد المشورة الإرشادية، أو إذا كف المورِّد عن العمل أو لم يكن مجتمع المصادر المفتوحة استباقياً بشأن المكون. ويمكن أن تساعد موارد مثل قاعدة بيانات الثغرات الوطنية (NVD) أو مصادر الاستخبارات التجارية على تحديد الثغرات التي لم ترد مشورة بشأنها.

الغرض: *تحديد الثغرات في مكونات الطرف الثالث التي لم ترد مشورة بشأنها.*

النتيجة: *رؤية أدق للثغرات التي يمكن ان تمر دون أن يلاحظها أحد.*

الوظيفة 4.3.2 إجراءات الإعداد لاستيعاب ثغرات سلسلة التوريد الداخلية بالنسبة للمورد

في معظم الحالات، لن تصدر مكونات المنتج من المصادر الداخلية للمورِّدين إرشادات علنية بشأن المشاكل الأمنية التي سويت. وللحصول على معلومات بشأن الثغرات في سلسلة التوريد الداخلية للمورِّدين، تتعين إقامة قنوات اتصالات محددة مع هؤلاء الموردين.

الغرض: *تحديد الثغرات في سلسلة التوريد الداخلية للمورِّدين والتي تؤدي إلى ثغرة في منتَج صاحب المصلحة.*

النتيجة: *رؤية أدق للثغرات في سلسلة التوريد الداخلية للمورِّدين التي يمكن ان تمر دون أن يلاحظها أحد.*

الوظيفة 5.3.2 تبليغ أفرقة التطوير الداخلية

إنشاء قنوات مؤتمتة لتوزيع إشعارات بشأن الثغرات المحددة من طرف ثالث مباشرةً على أفرقة تطوير المنتجات المتأثرة. وكثيراً ما يكفي اتباع تعليمات مورِّد مَصدر المدخلات لإصلاح مشكلة المنتج في منفذ المخرجات. ووفقاً لسياسة تحديد الأولويات، يحدَد متى ينبغي فرز الثغرات بشكل مختلف وتصعيدها إلى مستوى المعالجة على يد فريق التصدي لحوادث أمن المنتجات (PSIRT). وتكتسي هذه المعالجة أهمية خاصة إذا احتاج صاحب المصلحة إلى اتخاذ إجراء للحصول على نسخة مصححة من المنتج من أجل تأمين التشغيل.

الغرض: *إبلاغ أفرقة التطوير بشكل انتقائي عن التبعيات المعرَّضة للثغرات ومعلومات الرُقع التصحيحية (إذا كانت متوفرة) للسماح بالإصلاح في الإصدار التالي للمنتج.*

النتيجة: *تقليل الجهد المبذول في التعامل اليدوي لفريق PSIRT مع الثغرات حيث يمكن لطرف ثالث معالجة المعلومات الإرشادية مباشرة خلال عمليات التطوير.*

الخدمة 4.2 تحديد الثغرات الجديدة

يمكن أن ينخرط فريق التصدي لحوادث أمن المنتجات (PSIRT) بنشاط في الاكتشاف الداخلي للثغرات الجديدة كفرصة لمعالجة المشاكل الأمنية في المنتجات لتقليل إدارة العلاقات الخارجية وربما تقليل جهد التنسيق بمجمله. وينبغي أن تتمم هذه الأنشطة أنشطة التحقق الأمني التي تشكل جزءاً من دورة حياة التطوير الآمن (SDL). ويمكن أن تتضمن أنشطة فريق PSIRT تقييمات أمن المنتج قبل إصدار المنتج أو في مرحلة الصيانة، بالإضافة إلى تقديم خبرة أداة اختبار الأمن للبحث والتطوير. وينبغي التعامل مع الثغرات التي يُعثر عليها في الداخل والتي تؤثر على المستخدمين النهائيين بنفس الطريقة التي يُتعامل بها مع الثغرات التي يُعثر عليها في الخارج، بما في ذلك تسجيل النقاط وإعداد التقارير، بالتنسيق مع منشور الإصلاح.

الغرض: *كشف الثغرات في المنتج وإصلاحها قبل اكتشافها في الخارج.*

النتيجة: *الخبرة والإجراءات والآليات الكفيلة باكتشاف ثغرات المنتج الداخلي، وإمكانية تخفيف جهود التنسيق.*

الوظيفة 1.4.2 تقييم أمن المنتجات

يتمثل تقييم أمن المنتجات في ممارسة السعي بنشاط لاكتشاف الثغرات غير المعروفة حالياً. ويمكن أن يشمل ذلك مجموعة واسعة من التقنيات والأدوات مثل اختبار الاختراق أو الماسحات الباحثة علن الثغرات. وتحاكي تقنيات التقييم الأمني للصندوق الرمادي/الصندوق الأسود القرصنة الخارجية ضد الشركات لأنها تحتكم إلى منهجية تقل أو تنعدم فيها معارف المهاجم عن النظام الذي يتعرض للهجوم.

الغرض: كشف الثغرات من خلال الآليات الاستباقية.

النتيجة: خطوة لضمان الجودة تكمل أنشطة التحقق من أمن دورة حياة التطوير الآمن (SDL).

الوظيفة الفرعية 1.1.4.2 تقييم أمن منتجاتكم

يمكن لنتائج تحليل تقييم أمني تتحدى ضوابط الأمن الخاصة بمنتجكم أن تكون عوناً كبيراً للمطورين الذين يتطلعون إلى تحسين وضع منتجهم قبل طرحه في السوق أو عند إعداد علاج.

الوظيفة الفرعية 2.1.4.2 تقييم أمن مكونات الطرف الثالث

بالنسبة للمكونات المحصَّلة من أطراف ثالثة، تدعو الحاجة إلى زيادة تقييم الأمن المخصص، بالإضافة إلى الإجراءات العامة لإدارة المشتريات. وهذا ضروري بوجه خاص للمكونات الحرجة لضمان العناية الواجبة عالية الجودة.

الوظيفة 2.4.2 الحفاظ على الخبرة في أدوات اختبار الأمن

تواظب الكيانات التجارية والمجتمعات معاً على تطوير أدوات تحليل أمني وأدوات هجومية جديدة. وينبغي أن تواكب معرفة فريق التصدي لحوادث أمن المنتجات (PSIRT) أحدث الأدوات المتاحة. فهذا مفيد لإجراء تقييمات للمنتجات، أو التحقق من صحة مكتشفات المكتشفين الخارجيين، أو توجيه أفرقة التطوير باختيار الأدوات المناسبة للاختبارات الداخلية.

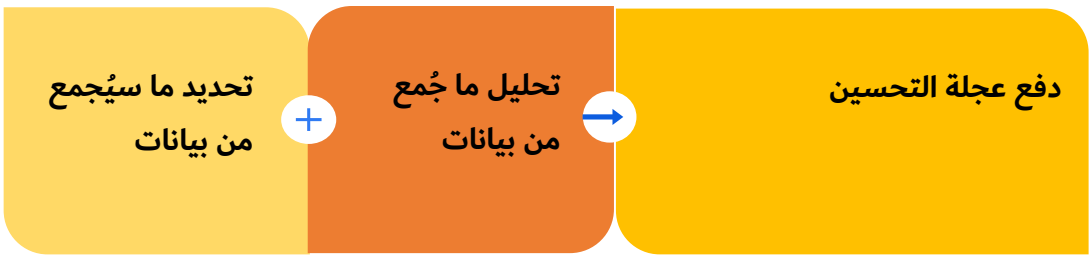
الغرض: تزويد فريق خبراء مُعد جيداً بالمهارات اللازمة للتعامل مع الأدوات المعقدة وتقديم المشورة بشأن الاستخدام.

النتيجة: الاستفادة من أفضل الأدوات المتاحة.

الوظيفة الفرعية 1.2.4.2 تدريب موظفي فريق PSIRT على أدوات اختبار الأمن

يعد تدريب الموظفين عنصراً رئيسياً في مواكبة المعارف لآخر مستجدات أدوات اختبار الأمن المتاحة. وتقدم الخدمة 3.6 بشأن التحقق من الصحة الآمن شرحاً لتدريب موظفي فريق PSIRT بمزيد من التفاصيل.

الخدمة 5.2 مقاييس اكتشاف الثغرات



الشكل 8 - عملية مقاييس اكتشاف الثغرات

يُعد تقديم تفاصيل بشأن حجم فريق PSIRT أو أدائه أو قياسات أخرى أمراً بالغ الأهمية لإبقاء أصحاب المصلحة على علم بفعالية فريق PSIRT (انظر أيضاً الأساس التشغيلي في القسم الثالث: التقييم والتحسينات). وسينفرد أصحاب المصلحة المختلفين بوجهات نظر تجب معالجتها بصنائع (أو آراء) ذات أنساق يُحتمل أن تكون مختلفة. ويجب أن يفهم فريق PSIRT

كيف ترغب كل مجموعة من أصحاب المصلحة في استهلاك هذه المعلومات. ويمكن أن تكون هذه المقاييس مؤشرات الأداء الرئيسية (KPI) لفريق PSIRT.

__الغرض:__ تقديم بيانات بشأن قياس وأداء فريق PSIRT. وهذا يساعد أصحاب المصلحة على فهم مدى فعالية فريق PSIRT في تقديم خدمة في مجال معين.

__النتيجة:__ من خلال استعراض مقاييس فريق PSIRT، ينبغي أن يعرف أصحاب المصلحة مدى فعالية فريق PSIRT في تقديم الخدمة وأن يكونوا قادرين على تقديم ملاحظات تقييمية لإجراء تعديلات على تقديم تلك الخدمة.

الوظيفة 1.5.2 التقارير التشغيلية

تقدم التقارير التشغيلية معلومات بشأن حجم وكذلك أنواع الثغرات التي تُكتشف ويمكن نشر هذه التقارير بانتظام وتداولها داخلياً ضمن فريق التصدي لحوادث أمن المنتجات (PSIRT) وكذلك مع أصحاب المصلحة الداخليين.

__الغرض:__ جمع البيانات بانتظام لإعداد التقارير العامة.

__النتيجة:__ تحديد المجالات التي تتطلب التحليل والموارد والتحسين.

الوظيفة الفرعية 1.1.5.2 إجمالي الثغرات المكتشفة مقابل الثغرات المؤكَدة

تساعد هذه البيانات في التعرف على الحجم الذي يتعامل معه فريق PSIRT من منظور الموارد. ويمكن فرز هذه البيانات وفق مستوى وحدة الأعمال أو نوع المنتجات أو منتجات محددة.

الوظيفة الفرعية 2.1.5.2 فرز إجمالي الثغرات المؤكدة وفق مكونات طرف ثالث

تساعد هذه البيانات في التعرف على المخاطر المرتبطة بمكونات مدمجة محددة وردت من طرف ثالث.

الوظيفة الفرعية 3.1.5.2 فرز إجمالي الثغرات المؤكدة وفق التعداد المشترَك لنقاط الضعف (CWE)

يمكن تغذية هذه البيانات في مصدر مدخلات دورة حياة تطوير الأمن وتأثير التدريب والتعليم. ويمكن فرز هذه البيانات وفق مستوى وحدة الأعمال أو نوع المنتجات أو منتجات محددة.

الوظيفة الفرعية 4.1.5.2 فرز إجمالي الثغرات المكتشفة وفق نهج اكتشاف الثغرات

تساعد هذه البيانات في تحديد الثغرات التي يسهل اكتشافها ويمكن تغذيتها في مصدر مدخلات دورة حياة تطوير الأمن. ويمكن فرز هذه البيانات وفق مستوى وحدة الأعمال أو نوع المنتجات أو منتجات محددة.

الوظيفة الفرعية 5.1.5.2 فرز إجمالي الثغرات المكتشفة وفق المصدر

تساعد هذه البيانات في وصف مدى شهرة فريق PSIRT.

الوظيفة 2.5.2 تقارير الأعمال

تقدم تقارير الأعمال معلومات بشأن صحة التصدي للثغرات في المنظمة من حيث صلتها بمعالجة الثغرات الأمنية والتصدي لها.

__الغرض:__ وضع مقاييس لتحديد تعريف المنظمة للنجاح، وجمع البيانات بانتظام لإعداد تقارير الإدارة من أجل التعرف على المخاطر.

__النتيجة:__ لوحة عرض تسلط الضوء على النجاحات وفرص التحسين.

الوظيفة الفرعية 1.2.5.2 معدل التصدي في أوانه

تعرِّف هذه البيانات بمدى جودة أداء فريق PSIRT زمنياً في الاستجابة الأولية لتقارير عن ثغرات ضمن الأطر الزمنية الخاصة باتفاق مستوى الخدمة.

الوظيفة الفرعية 2.2.5.2 إجمالي وقت تعطل قنوات اتصالات فريق PSIRT

تبين هذه البيانات ما إذا كانت قنوات اتصالات فريق PSIRT متاحة على النحو المحدد في اتفاق مستوى الخدمة.

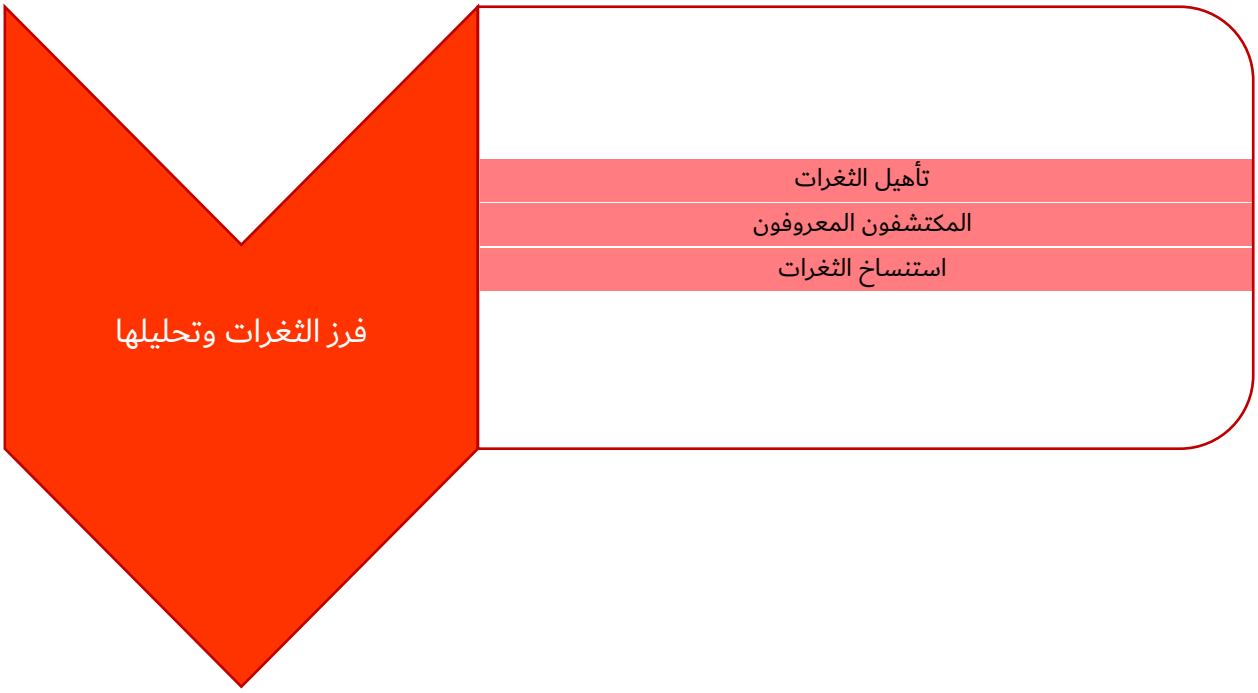
الوظيفة الفرعية 3.2.5.2 معدل الوقت المستغرَق للفرز

هذه وظيفة فرعية تقيس الوقت بدءاً من ورود التقرير الأولي وحتى الانتهاء من أنشطة الفرز. وتبين هذه البيانات أداء و/أو عبء عمل موظفي فريق PSIRT.

الوظيفة الفرعية 4.2.5.2 عدد عمليات الكشف الكامل، والثغرات المستغَلة بلا ضوابط، والثغرات التي عُرفت من خلال وسائل الإعلام

تبين هذه البيانات المخاطر المحيطة بمنتجات أصحاب المصلحة.

مجال الخدمة 3 فرز الثغرات وتحليلها



تتألف وظيفة إدارة الحالة في فريق PSIRT من واردات الثغرات وفرزها. وفي حين أن ترتيب العمليات يتشابه جداً بين أفرقة التصدي لحوادث أمن المنتجات (PSIRT)، إلا أن هناك اختلافات، مثل النقطة الدقيقة التي تُنشأ عندها "حالة" أو الأفراد الذين يؤدون وظائف مختلفة ضمن حالة. وعندما تتلقى المنظمات حجماً كبيراً من التقارير عن ثغرات، يمكن أن تفكر في إجراء فرز أولي للتحقق من صحة التقارير قبل إنشاء الحالات. وفي المقابل، في المنظمات التي ينخفض فيها حجم التقارير عن ثغرات، يمكن إنشاء حالة قبل الفرز. والهدف النهائي في صفوف فريق PSIRT هو إنشاء عملية فعالة ومحددة.

__الغرض:__ تحديد كيفية فرز التقارير عن ثغرات.

__النتيجة:__ إنشاء عملية ينتظم في إطارها فريق PSIRT والأفرقة الهندسية ذات الصلة.

الخدمة 1.3 تأهيل الثغرات

تحدد المنظمات معايير التأهيل المناسبة لنوع ونطاق القضايا التي ترغب في معالجتها. وستساعد معايير التأهيل هذه على تحديد خط الأساس الأمني وستعين في فرز التقارير الواردة عن ثغرات بشكل فعال.

الشكل 9 - عملية تأهيل الثغرات

الوظيفة 1.1.3 بوابة الجودة وأشرطة الأخطاء البرمجية

يقدم نظام تحديد درجات الثغرات الشائعة (CVSS) طريقة لاستخلاص الخصائص الرئيسية لثغرة وإنتاج درجة رقمية تبيّن حدّة هذه الثغرة. ويمكن بعد ذلك ترجمة هذه الدرجة الرقمية إلى تمثيل نوعي (يحدد مثلاً ما إذا كان المستوى منخفضاً أو متوسطاً أو عالياً أو حرجاً) بغية مساعدة المنظمات على إجراء تقييم صائب للعمليات التي تتبعها لإدارة الثغرات وعلى ترتيبها بحسب الأولوية، وهي تُسمى أحياناً بوابة الجودة و/أو أشرطة الأخطاء البرمجية، وتُستخدم لتحديد المستويات الدنيا المقبولة لجودة الأمن، ومعايير تحديد أولويات الثغرات الأمنية. ويقدم تحديد هذه المعايير قبل إصدار المنتجات شفافية لعملية معالجة الثغرات من خلال التحديد المسبق لما سيؤهله فريق التصدي لحوادث أمن المنتجات (PSIRT) كثغرة في المنتَج تنبغي معالجتها. ويتمثل استخدام الثغرات والمخاطر الشائعة (CVE) في قائمة من الإدراجات تحتوي على رقم تعريف ووصف ومرجع علني واحد على الأقل يُستخدم في الغالب لضمان الوضوح بشأن المشكلة التي يجري تناولها.

الغرض: *تحديد معايير دنيا واضحة ومعايير لتحديد الأولويات تقدم الشفافية لأصحاب المصلحة الداخليين والخارجيين.*

النتيجة: *تقديم توقعات واضحة للمهندسين والمكتشفين على حد سواء بشأن ما يشكل ثغرة. وبزيادة معايير تحديد الأولويات سيخف الارتباك والنزاع في إدارة دورة حياة الثغرات - من الفرز الأولي حتى التبليغ بالرُقع التصحيحية.*

الوظيفة الفرعية 1.1.1.3 توثيق تعاريف الثغرات الأمنية في المنتجات

ينبغي توثيق بوابة الجودة أو أشرطة الأخطاء البرمجية، وتخزينها في موقع مركزي، وجعلها جزءاً من التدريب العادي للمطورين/المهندسين.

الوظيفة الفرعية 2.1.1.3 التعامل مع أفرقة تطوير المنتجات

في حال وجود العديد من المنتجات وأفرقة تطوير المنتجات داخل المنظمة، فإن التعامل مع كل منها لتقييس تعريف ثغرة أمنية في المنتجات هو أمر بالغ الأهمية.

الوظيفة 2.1.3 التحسين المستمر

ينبغي أن يتبنى فريق PSIRT الناضج عقلية التحسين المستمر لمراجعة معايير التأهيل الخاصة به حيثما كان ذلك مناسباً كي تبين الخبرة السابقة وأفضل الممارسات الصناعية وتغييرات المنتَج والملاحظات التقييمية من أصحاب المصلحة. ومن المهم إبلاغ التغييرات لأصحاب المصلحة الداخليين والخارجيين لإدارة توقعاتهم في هذا الصدد.

الغرض: *إدراك أن معايير التأهيل تخضع للمراجعة. ويرجح أن تؤدي الديناميات المحيطة بفريق PSIRT مثل توقعات أصحاب المصلحة، واتجاهات الصناعة، أو حجم الثغرات الواردة إلى تعديلات متكررة.*

النتيجة: *ستؤدي سيولة معايير تأهيل الثغرات إلى كفاءة ممارسة تأهيل الثغرات.*

الوظيفة الفرعية 1.2.1.3 جمع البيانات

تُجمع البيانات بشأن عملية الفرز بما في ذلك عدد التقارير الواردة، والعدد المؤهل منها كثغرة، والعدد غير المؤهل منها كثغرة، وأي اختلافات تصادَف.

الغرض: *دفه عجلة التحسينات بناءً على البيانات.*

النتيجة: *البيانات هي قاطرة التغييرات في بوابات الجودة وأشرطة الأخطاء البرمجية,*

الخدمة 2.3 المكتشفون المعروفون

مع نضوج فريق التصدي لحوادث أمن المنتجات (PSIRT) في المنظمة، يمكن أن يرصد الفريق مجموعة من المكتشفين المعهودين المسؤولين عن الإبلاغ عن حجم ثغرات يفوق المعتاد. ويوصى النظر في سمعة المكتشف والجودة العالية لما يقدمه من تبليغات، وتجاوز بعض الوظائف مثل التأهيل والفرز للانتقال مباشرة إلى تحليل الأسباب الجذرية وتطوير التدارك. إذ يمكن أن يساعد ذلك على تحسين كفاءة العملية وتعزيز العلاقات مع المكتشفين.

الغرض: *فهم مجتمع البحوث ومن هم الأكثر إبلاغاً عن الثغرات في منتجاتكم وخدماتكم والنظر في التصعيد الفوري للتقارير الواردة من مكتشفين موثوقين.*

النتيجة: *اختصار وقت التصدي عند التعامل مع مكتشفين ذوي جودة عالية.*

الوظيفة 1.2.3 قاعدة بيانات المكتشفين

إعداد وصيانة قاعدة بيانات للأفراد والمنظمات التي أبلغت عن ثغرات من أجل تتبع السجل الزمني والنتائج وأي اعتبارات أخرى لتعامل ذلك المكتشف مع الحالات.

الغرض: *تحسين كفاءة عملية الفرز وتنمية علاقات أفضل مع المكتشفين ذوي السجل الحافل في تقديم تبليغات عالية الجودة.*

النتيجة: *انتقال أسرع للتقارير الواردة من المكتشفين المؤهلين عبر النظام. وشعور المكتشفين بالرضا عن النتائج وإنتاج التدارك قبل أي جداول زمنية محتملة للكشف العلني عنه.*

الوظيفة 2.2.3 المعالجة المعجَّلة عند التعامل مع مكتشفين معروفين

يمكن أن يكون بعض المكتشفين غزير الإنتاج أو متسقاً (مدقَّقاً/ذا مصداقية) في العثور على أخطاء البرمجيات ضمن منتجاتكم أو خدماتكم وفي الإبلاغ عنها. فعلى سبيل المثال، يمكن أن يستخدموا أدوات فحص عشوائي مخصصة وتقارير أعطال دون بيان أو إثبات جدوى محدد. وعند المعرفة الجيدة بالمكتشف والبت في أن معظم المشاكل التي يبلغ عنها تجد حلاً، يُنظر في تخطي عملية التأهيل/التدقيق تماماً والانتقال مباشرةً إلى التدارك.

الغرض: *تحسين كفاءة عملية الفرز وتنمية علاقات أفضل مع المكتشفين ذوي السجل الحافل في تقديم تبليغات عالية الجودة.*

النتيجة: *انتقال أسرع للتقارير الواردة من المكتشفين المؤهلين عبر النظام. وشعور المكتشفين بالرضا عن النتائج وإنتاج التدارك قبل أي جداول زمنية محتملة للكشف العلني عنه.*

الوظيفة 3.2.3 ملف تعريف بالمكتشف

يُنظر في إنشاء ملفات تعريف بالمكتشفين لإبلاغ المتعاملين معهم بأفضل طريقة للعمل معهم. ويمكن أن تحتوي ملفات التعريف على أشياء مثل الموقع الجغرافي، واللغات التي يتحدثون بها، والمؤتمرات التي قدموا عروضاً فيها، والمنهجيات المستخدمة للعثور على الثغرات، والمنتجات/التقنيات التي يركزون عليها عادةً، وما إذا مارسوا الكشف المنسق عن الثغرات، وما إذا كانوا يرغبون في عرض اكتشافاتهم في المؤتمرات، وما إذا دفعتم لهم المكافآت أو قدمتم حوافز أخرى، وما إلى ذلك. وتستشار الأفرقة القانونية، و/أو أفرقة الالتزام لتحديد المعلومات التي يمكن جمعها ومدة الاحتفاظ بها.

الغرض: *التعرف على الأشخاص الذين يجدون ثغرات في منتجاتكم.*

النتيجة: *يمكن تفصيل التعامل على مقاس مكتشف محدد للحصول على أفضل النتائج.*

الوظيفة 4.2.3 تحديد جودة تقرير المكتشف

لعل المنظمات ترغب في النظر في تحديد ونشر المبادئ التوجيهية لما يشكل تقريراً عن الثغرات بالحد الأدنى من الجودة من أجل تقديم إرشادات للمكتشفين بشأن نوع المعلومات التي يحتاجونها لتقييم تقاريرهم بسرعة. ويمكن أن يتضمن خط الأساس، على سبيل المثال لا الحصر، بياناً، وخطوات الاستنساخ، والمنصة (المنصات) التي جرى الاختبار عليها، وإثبات الجدوى.

الغرض: *تقديم مبادئ توجيهية للمكتشفين بشأن خط الأساس لتقرير عن الثغرات ذي جودة.*

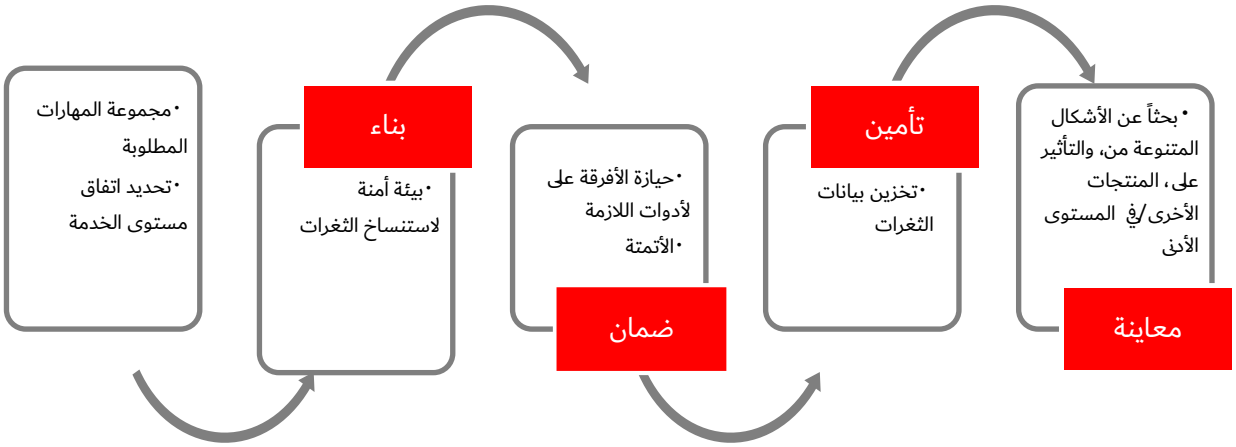
النتيجة: *التقليل إلى أدنى حد من الأخذ والرد بين المورِّد والمكتشِف، بحيث يمكن للمورِّد التركيز بسرعة على خطة الإصلاح.*

الخدمة 3.3 استنساخ الثغرات

إضافة إلى التأهيل، وما لم يُحدد خلاف ذلك، يحتاج فريق التصدي لحوادث أمن المنتجات (PSIRT) إلى ضمان إمكانية استنساخ تقرير المكتشف من أجل التحقق من صحة الظروف التي تؤدي إلى حالة ظهور ثغرات وفهم هذه الظروف.

الغرض: *تقديم الأدوات والبيئة اللازمة لتأهيل تقارير عن ثغرات.*

النتيجة: *التحقق من صحة تقرير عن ثغرة بشكل كفء وآمن.*



الشكل 10 – تأكيد/استنساخ الثغرات

الوظيفة 1.3.3 وضع اتفاق مستوى الخدمة لاستنساخ الثغرات

قد لا يمتلك فريق التصدي لحوادث أمن المنتجات (PSIRT) خبرة تقنية كافية لاستنساخ جميع الثغرات الواردة. ويمكن أن تحتاج أفرقة PSIRT إلى التشاور أو العمل مع، أو الاعتماد على، خبرات في تطوير المنتجات أو الأفرقة الأخرى، لذا من المهم أن يكون هناك اتفاق مواءم ومحدَد بوضوح لضمان سهولة توفر الخبرات المطلوبة. ومن الناحية المثالية يوصى بمورد مخصص بدوام كامل أو جزئي. ولكن إذا تعذر ذلك بسبب قيود الميزانية، ينبغي على الأقل، كجزء من عملية فريق PSIRT، التحديد المسبق لخبراء متخصصين يمكنهم العمل بإشعار قصير الأجل لفترات محدودة في حال وقوع حادث.

الغرض: *إدراك أن فريق PSIRT لا يمتلك خبرات تقنية لاستنساخ الثغرات الواردة كافة.*

النتيجة: *سيضمن التواؤم الداخلي المسبق سهولة توفر الخبرات بإشعار قصير الأجل للمساعدة في استنساخ الثغرات.*

الوظيفة 2.3.3 بيئة اختبار الاستنساخ

ينبغي إعداد بيئة اختبار مخصصة لفريق PSIRT أو فريق مخصص من أجل استنساخ الثغرات. وينبغي عزل بيئة الاختبار لتجنب الأنشطة الضارة والتحقق من صحة تقرير المكتشف. وعند الاقتضاء، يمكن استخدام بيئة شبكة أو محاكاة أو تمثيل افتراضي مخصصة لإنشاء بيئة آمنة.

الغرض: *إنشاء بيئة آمنة للسماح بمعاينة الثغرات واستنساخها.*

النتيجة: *ستساعد بيئة اختبار الاستنساخ المنفَّذة جيداً على معالجة الثغرات وتأهيلها بكفاءة، مع حصر الثغرات في نطاق بيئة الاختبار.*

الوظيفة 3.3.3 أدوات الاستنساخ

تحتاج الأفرقة المشاركة في استنساخ الثغرات التي أُبلغ عنها إلى امتلاك أدوات وتراخيص منتجات محدَّثة تحت تصرفها لإجراء هذه العمليات (من قبيل مصحح أخطاء برمجية).

الغرض: *التأكد من امتلاك أفرقة الاستنساخ للأدوات التي تحتاجها.*

النتيجة: *ضمان استنساخ الثغرات المبلَّغ عنها بأكبر قدر ممكن من الكفاءة.*

الوظيفة 4.3.3 تخزين الثغرات

يوصى بتخزين المعلومات الحساسة، مثل التقارير عن الثغرات، وملفات إثبات الجدوى، وما إلى ذلك، تخزيناً آمناً وبقصر النفاذ إليها على من يحتاجون إلى النفاذ إليها، وضمان أمن المعلومات في حالة السكون والعبور. وعلى سبيل المثال، انظر المرجع ISO 27001.

الغرض: *الحفاظ على أمن المعلومات الحساسة التي يمكن أن تكون ضارة بشأن الثغرات.*

النتيجة: *الحفاظ على أمن المعلومات الحساسة بنفاذ محدود إليها دون أن تكون عرضة للاختراق ضمن الشبكة الأساسية للمنظمة.*

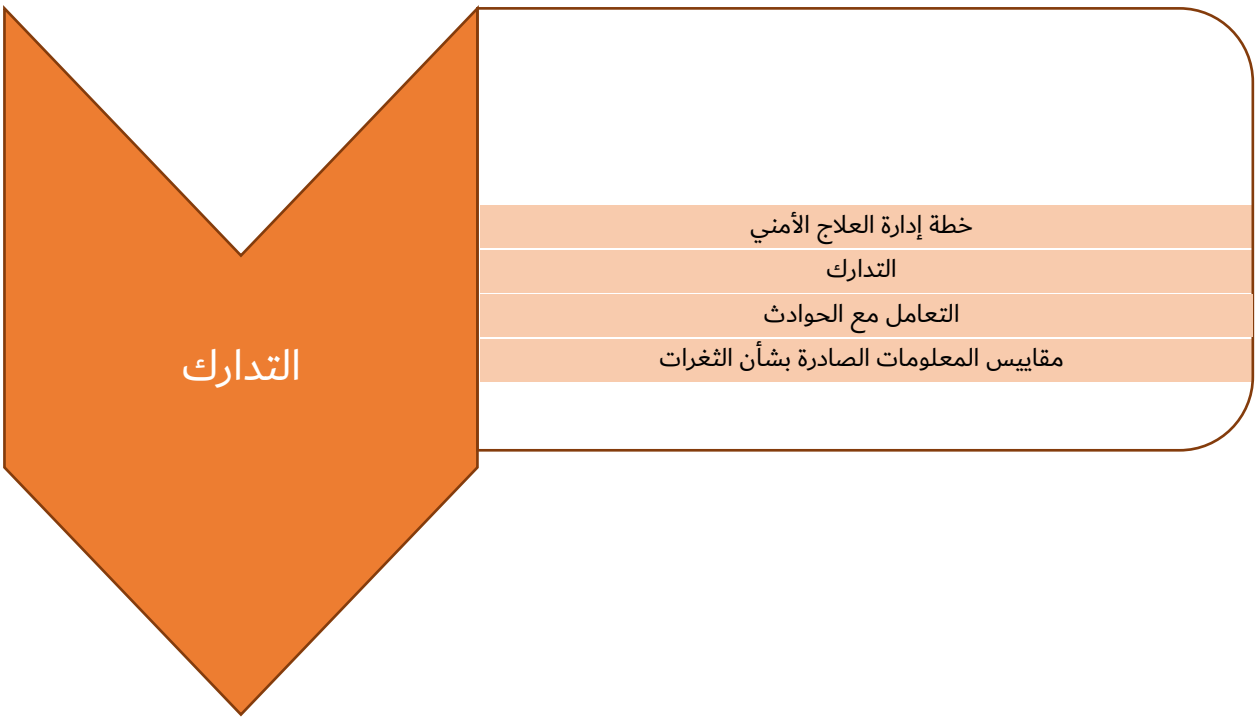
الوظيفة 5.3.3 المنتجات المتأثرة

أثناء الاستنساخ، ينبغي أن يسعى الفريق الذي يقوم بالتحليل لتحديد المنتجات المتأثرة وما إذا كانت هناك أي منوعات من الثغرات. انظر أيضاً الوظيفة 1.1.4 بشأن إدارة دورة حياة المنتجات.

الغرض: *اكتساب فهم ومنظور كاملين للثغرات عبر المنتجات.*

النتيجة: *إصلاحات شاملة للثغرات عبر المنتجات المدعومة.*

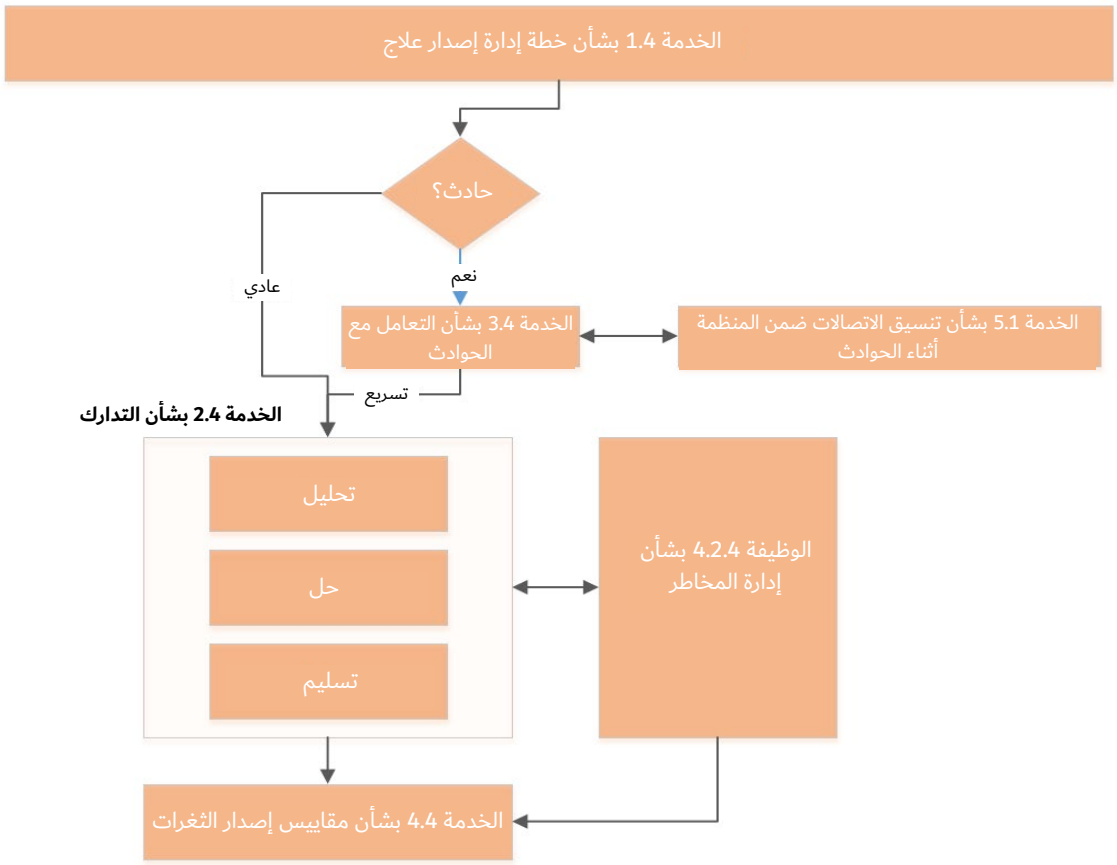
مجال الخدمة 4



يبين مجال الخدمة هذا الخدمات المختلفة المطلوبة لتقديم علاج وإعلانه لأصحاب المصلحة وكذلك للموردين في مَنفذ المخرجات. وينبغي تحديد آلية تقديم التدارك بناءً على تأثير الثغرات على أصحاب المصلحة عند استغلالها. وينبغي إنشاء العمليات لضمان تقديم علاج وفقاً لجدول زمني يمكن التنبؤ به كي يتمكن أصحاب المصلحة وكذلك الموردين في مَنفذ المخرجات من التخطيط وفقاً لذلك لاختبار ونشر هذه العلاجات.

الغرض: *تسليط الضوء على العمليات والآليات المطلوبة لإصدار علاج وإعلانه لأصحاب المصلحة والموردين في مَنفذ المخرجات.*

النتيجة: *تمكين أصحاب المصلحة والموردين في مَنفذ المخرجات من التخطيط وفقاً لذلك العلاج.*



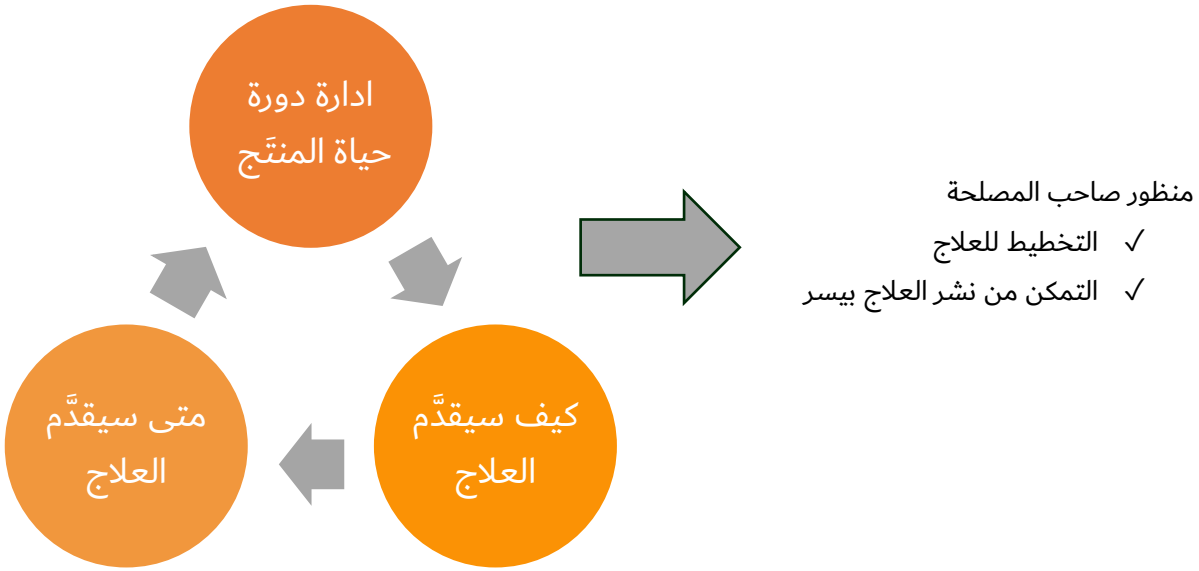
الشكل 11 – مثال عملية أساسية لإصدار علاج

الخدمة 1.4 خطة إدارة إصدار علاج

تركز هذه الخدمة على تقديم إرشادات بشأن كيفية تخطيط المورِّد لإنشاء إيقاع لإصدار علاج لنسخ المنتجات المدعومة في السوق. ويحتاج أصحاب المصلحة، وخاصة في الحيز المؤسسي، إلى التخطيط لنشر علاج. ويمكن أن يكون لبعض عمليات النشر، مثل الحوسبة السحابية، تحديثات تلقائية أو سياسة مختلفة لإدارة الرُقع التصحيحية.

***الغرض**: تثقيف الجهات المخدَّمة بشأن المنتجات التي ستُدعم وآليات تقديم العلاج بالإضافة إلى الإيقاع الذي سيقدَّم فيه.*

***النتيجة**: سيتمكن أصحاب المصلحة من التخطيط مسبقاً لنشر الإصلاحات الأمنية.*



الشكل 12 – إرساء الأساس للجهات المخدَّمة

الوظيفة 1.1.4 ادارة دورة حياة المنتَج

يمكن أن يكون لدى الشركات سياسات واتفاقات دعم مختلفة مع أصحاب المصلحة. واستناداً إلى هذه العوامل، يمكن أن يتشارك فريق التصدي لحوادث أمن المنتجات (PSIRT) مع وحدات الأعمال/خطوط الأعمال ووحدات دعم أصحاب المصلحة لتحديد كيف، وما إذا كانت، ستُدعم المنتجات التي خرجت عن نطاق الدعم أو عن التزامات الدعم. ويمكن أن يعتمد ذلك على شدة الثغرة ويمكن أن يتضمن مدخلات من وحدات الأعمال/خطوط الأعمال ودعم أصحاب المصلحة.

الغرض: *تقديم سياسة واضحة لأفرقة المنتجات بشأن كيفية دعم المنظمة للمنتجات ذات الثغرات الأمنية.*

النتيجة: *سياسة واضحة بشأن ماهية توقعات وحدة الأعمال/خط الأعمال بشأن تقديم علاج لهذه الأنواع من المنتجات.*

الوظيفة الفرعية 1.1.1.4 جرد المنتجات

إنشاء جرد لجميع المنتجات التي طُرحت في السوق لضمان تقييم جميع المنتجات المشمولة بالدعم وتداركها.

الوظيفة الفرعية 2.1.1.4 نماذج الدعم

فهم الأنواع المختلفة لنماذج دعم المنتجات بما في ذلك الخدمات المدفوعة الأجر أو الضمانات الموسعة أو اتفاقات الصيانة أو العقود مع أصحاب المصلحة المحددين.

الوظيفة الفرعية 3.1.1.4 دورة حياة المنتَج

يحدَّد متى يكف دعم المنتَج في دورة حياة المنتَج.

الوظيفة 2.1.4 أسلوب التسليم

يمكن أن تتشارك أفرقة التصدي لحوادث أمن المنتجات (PSIRT) مع أفرقة المنتجات ووحدات دعم أصحاب المصلحة لتحديد الخيارات المختلفة لتسليم علاج لأصحاب المصلحة. وينبغي أيضاً وضع معايير لتحديد موعد نشر العلاج من خلال الوسائل المحددة.

الغرض: *الحفاظ على آلية متسقة لتقديم الثغرات المتدارَكة بناءً على مجموعة من الشروط.*

النتيجة: *يمكن لأصحاب المصلحة تخطيط العلاج ونشره بسهولة.*

الوظيفة الفرعية 1.2.1.4 أنساق تغليف المنتج

فهم أنساق التغليف المختلفة ذات الصلة بتقديم علاج (من قبيل ملف اثنيني قابل للتنفيذ، ومقارنات شفرة المصدر، وما إلى ذلك.).

الوظيفة الفرعية 2.2.1.4 تسليم علاج

فهم الآليات المختلفة لتقديم علاج مثل الإصلاح السريع والرُقع التصحيحية وإصدارات الصيانة وتحديثات البرمجيات الثابتة وكيفية توزيع العلاج.

الوظيفة الفرعية 3.2.1.4 نشر علاج

يحدَد عبر المنتجات المختلفة كيف يمكن نشر العلاج، أي عن بعد، أو بنسق قابل للتثبيت على يد العملاء، أو بتحديثات تلقائية أو أنه يتطلب التنفيذ في الموقع.

الوظيفة 3.1.4 إيقاع التسليم

يحتاج أصحاب المصلحة والمورِّدون المتلقون للمعلومات إلى خطة علاجية كي يتمكنوا من الحفاظ على الوضع الأمني لبيئتهم. وبتحديد إيقاع لموعد تسليم العلاج، سيتمكن أصحاب المصلحة من جدولة وتخطيط الموارد للتحديثات الضرورية لبيئتهم.

الغرض: *الحفاظ على إيقاع ثابت عند إصدار علاج لأصحاب المصلحة.*

النتيجة: *يمكن لأصحاب المصلحة تخطيط العلاج ونشره.*

الوظيفة الفرعية 1.3.1.4 إيقاع تسليم علاج

يُتشارك مع أفرقة إدارة المنتج وإدارة الإصدار لتحديد إيقاع مواعيد تسليم العلاج. وتُدمج بعض العلاجات كجزء من إصدار واحد وتواءم مع هذه الجداول الزمنية للإصدار. وإذ يمكن أن يحتاج الآخرون إلى إصلاح طارئ فإنه يُعتبر إصداراً خارج النطاق الزمني المعتاد.

الوظيفة الفرعية 2.3.1.4 توثيق الاستثناءات

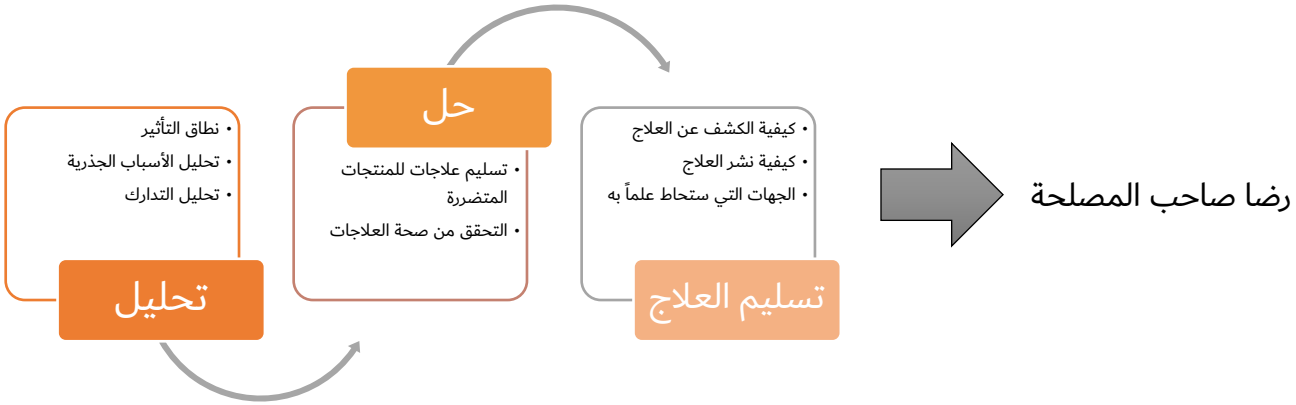
تحديد وتوثيق الاستثناءات عند عدم تسليم العلاج من خلال الإيقاع العادي.

الخدمة 2.4 التدارك

تتعلق هذه الخدمة بإدارة الثغرات التي بلِّغ المكتشفون عنها وتتضمن تحليل التصدي بالإضافة إلى التخفيف، وتحدد الإصدارات التي ستُتدارك ويمكن أن تأخذ في الاعتبار كيفية تسليم العلاج. ويمكن أن تنظر أيضاً في أي حلول التفافية يمكن لأصحاب المصلحة تطبيقها على الفور قبل تسليم العلاج.

الغرض: *تقديم العمليات وأفضل الممارسات في تسليم علاج لأصحاب المصلحة بناءً على ما تأثر بالثغرات من منتَج (منتجات) وإصدار (إصدارات) وأصحاب المصلحة المتضررين.*

النتيجة: *علاج متوافق مع المنتجات المتأثرة واحتياجات أصحاب المصلحة.*



الشكل 13 – عملية تدارك الثغرات المبلَّغ عنها

الوظيفة 1.2.4 التحليل

يمكن أن يتضمن المنتَج المتأثر تطبيق برمجيات واحد أو برمجيات ثابتة أو برامج عتاد متعددة بإصدارات مختلفة من البرمجيات أو البرمجيات الثابتة. وتدعو الحاجة إلى مراعاة عدد من المعلمات عند صياغة خطة التدارك لضمان تلبية احتياجات أصحاب المصلحة لديكم.

الغرض: *تحديد ما تأثر بالثغرات من منتَج (منتجات) وإصدارات وأصحاب مصلحة.*

النتيجة: *علاج متوافق مع المنتجات المتأثرة واحتياجات أصحاب المصلحة*

الوظيفة الفرعية 1.1.2.4 التحقق من صحة وجود ثغرات

يُتحقق من صحة تقرير عن ثغرة أو حادث ضد بوابة الجودة أو شريط الأخطاء البرمجية. انظر الوظيفة 1.1.3 بشأن بوابة الجودة وأشرطة الأخطاء البرمجية.

الوظيفة الفرعية 2.1.2.4 تدارك إصدارات المنتجات

تحدَد المنتجات والإصدارات المتأثرة بالإضافة إلى أي منوعات منبثقة عنها يمكن أن تحتاج إلى تدارك في نفس الوقت.

الوظيفة الفرعية 3.1.2.4 استعراض اتفاقات الدعم

تُستعرض اتفاقات الدعم والنماذج المرتبطة بإصدارات المنتجات المتأثرة. راجع الوظيفة الفرعية 2.1.1.4 بشأن نماذج الدعم.

الوظيفة الفرعية 4.1.2.4 تحليل السبب الجذري

يُفهم عيب التصميم أو التنفيذ الذي تسبب في الثغرة.

الوظيفة الفرعية 5.1.2.4 تحديد آلية رفض الثغرة

على سبيل المثال، يمكن أن تكون الثغرة تأكيداً كاذباً أو عيباً في تصميم أمني.

الوظيفة الفرعية 6.1.2.4 تحليل التدارك

تحدَد وسائل لتخفيف أو تدارك المخاطر الناتجة عن الثغرة.

الوظيفة الفرعية 7.1.2.4 حلول التدارك الالتفافية

يحدَد ما إذا كانت هناك أي حلول التفافية يمكن تنفيذها للتخفيف من الثغرة عندما يكون العلاج قيد التطوير.

الوظيفة الفرعية 8.1.2.4 الاستثناءات

تحدَد أي استثناءات حيثما يتعذر تدارك الثغرة. راجع الوظيفة 4.2.4 بشأن عملية إدارة المخاطر.

الوظيفة 2.2.4 الحل العلاجي

قبل إصدار علاج لثغرة أُبلغ عنها، ينبغي التحقق من صحتها من خلال ضمان الجودة (QA)، والاختبار الأمني، وحسب الاقتضاء، من خلال المكتشف الذي أبلغ عن الثغرة. وتصف هذه الوظيفة عملية وآليات التحقق من صحة العلاج داخلياً وكذلك الشراكة مع المكتشف ليتحقق من صحة العلاج ويذيله بتوقيعه.

__الغرض:__ تقديم عملية وآلية للتحقق الداخلي من صحة العلاج وكذلك الشراكة مع المكتشف كي يقر العلاج، حسب الاقتضاء.

__النتيجة:__ موافقة مكتشف داخلي، و/أو خارجي على العلاج الذي سيصدر.

الوظيفة الفرعية 1.2.2.4 التحقق من تدارك الثغرات المبلَّغ عنها

التحقق لضمان تدارك جميع الثغرات المبلغ عنها عبر جميع إصدارات المنتجات المتأثرة.

الوظيفة الفرعية 3.2.2.4 إقرار العلاج

الحصول على إقرار العلاج من مهندس أو فريق ضمان الجودة المسؤول. وينبغي دمج التحقق من صحة العلاج في الاختبار المعياري/ممارسة ضمان الجودة.

الوظيفة الفرعية 4.2.2.4 التحقق من صحة العلاج مع المكتشفين

إقامة شراكة مع مكتشف أو صاحب مصلحة تابع لطرف ثالث للتحقق من صحة العلاج.

الوظيفة 3.2.4 تسليم العلاج

كجزء من إصدار علاج لثغرة أُبلغ عنها، يمكن أن تختلف الأطر الزمنية للكشف عنها حسب متطلبات العمل في منظمتكم. فعلى سبيل المثال، يمكن أن تتزامن بعض عمليات الكشف عند توفر العلاجات، ويمكن أن يقوم البعض الآخر منها بتوقيت الكشف ليأتي بعد إصدار العلاجات خاصة إذا كانت العلاجات مرحلية؛ أو في بعض الحالات يمكن ترتيب أولويات عمليات الكشف وفق علاقات أصحاب المصلحة (مع الشركاء أو الكيانات الحيوية مثلاً). وأياً يكن الحال، يحتاج أصحاب المصلحة الرئيسيون في دوائر الصناعة، بمن فيهم المكتشِف، لأن يظلوا على علم بالأطر الزمنية.

__الغرض:__ تخطيط عمليات الكشف وفقاً للعلاجات وإبلاغ أصحاب المصلحة بهذه الأطر الزمنية.

__النتيجة:__ تقديم علاج إلى جانب الكشف لأصحاب المصلحة.

الوظيفة الفرعية 1.3.2.4 نوع الكشف

تحدَد الآلية المفضلة للكشف عن الثغرة. ويمكن أن يعتمد ذلك على شدة الثغرة أو نوعها.

الوظيفة الفرعية 2.3.2.4 تنسيق الكشف، حسب الاقتضاء

الوظيفة الفرعية 3.3.2.4 إدراج العلاج في قاعدة البيانات الداخلية

التشارك مع فعاليات دعم أصحاب المصلحة أو أصحاب المصلحة الآخرين لنشر العلاج على بوابة إلكترونية أو موقع دعم أصحاب المصلحة أو الإصدار إلى التصنيع (RTM) كأمثلة.

الوظيفة الفرعية 4.3.2.4 إصدار الكشف عن علاج

التشارك مع فعاليات دعم أصحاب المصلحة أو أصحاب المصلحة الآخرين لنشر الكشف عن الثغرة المُبلغ عنها.

الوظيفة 4.2.4 عملية إدارة المخاطر

تقع على عاتق فريق التصدي لحوادث أمن المنتجات (PSIRT) مسؤولية تزويد أصحاب المصلحة بالمعلومات الكافية كي يتمكنوا من تقييم المخاطر على أنظمتهم جراء ثغرات فيها وفي المنتجات التي تدعمها منظمة فريق PSIRT. وينبغي إجراء تقييمات لإدارة المخاطر في جميع أقسام المنظمة عند عدم تدارك الثغرة في إطار زمني محدد (وفقاً لاتفاقات مستوى الخدمة أو للأهداف). وهذا يشمل وجود آلية شفافة لتحديد كم المخاطر وكذلك التصعيد إلى أصحاب المصلحة المناسبين المدرجين في سجل المخاطر بالمنظمة.

__الغرض:__ تحديد عملية قبول المخاطر الرسمي لأي ثغرات غير متدارَكة ضمن المتطلبات الزمنية لاتفاقات مستوى الخدمة الداخلية.

__النتيجة:__ الشفافية بشأن المخاطر عبر المنظمة والتأكد من أن المخاطر تصعَّد ويُعترف بوجودها بشكل مناسب.

الوظيفة الفرعية 1.4.2.4 الأدوار السلطوية

تحدَد الأدوار صاحبة سلطة قبول المخاطر، من قبيل رئيس مكتب أمن المعلومات (CISO)/مكتب الأمن الرئيسي (CSO) أو مدير المخاطر، وأي الأدوار ينبغي إبلاغها بالمخاطر.

الوظيفة الفرعية 2.4.2.4 تحديد عملية إدارة المخاطر

تحدَد ممارسات إدارة المخاطر للتعامل مع المخاطر والتصدي لها داخل المنظمة بما في ذلك مجموعة الشروط التي يمكن أن تؤدي إلى تشغيل العملية.

الوظيفة الفرعية 3.4.2.4 تقييم المخاطر وتحديد كَمها

تقيَّم المخاطر ويحدَد كَمها من خلال إجراء تقييم للمخاطر لفهم التهديد والآثار على مصالح الأعمال.

الوظيفة الفرعية 4.4.2.4 توثيق المخاطر في سجل المخاطر

لمساعدة مكتب الأمن الرئيسي (CSO) أو مدير المخاطر أو أصحاب المصلحة الآخرين في تتبع حالة تقييم المخاطر وتتبع تنفيذ التوصيات لاحقاً.

الوظيفة الفرعية 5.4.2.4 التوصيات

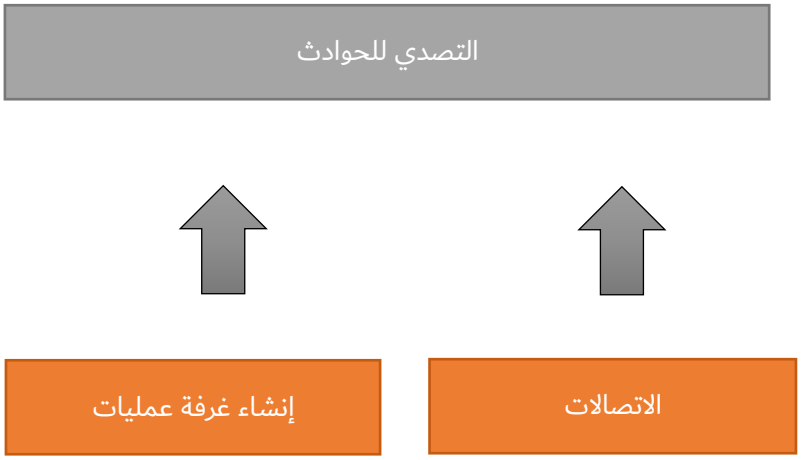
يجري تحديث سجل المخاطر بالاكتشافات والتوصيات.

الخدمة 3.4 التعامل مع الحوادث

يحتاج فريق التصدي لحوادث أمن المنتجات (PSIRT) إلى آلية لتسريع وقت التدارك لمعالجة "الثغرات الحرجة" التي يمكن تعريفها على أنها شفرة استغلالية نشطة في عمليات الكشف العلني غير المنضبطة، وغير المسبوقة، وغير المنسقة. وتقدم هذه الخدمة إرشادات بشأن الحادث بالإضافة إلى تنبيه أصحاب المصلحة وتنسيق الأنشطة المرتبطة بالتصدي والتخفيف من حدة الحادث والتعافي منه لتقليص الوقت الفاصل بين الإبلاغ عنه وتسليم علاجه.

__الغرض:__ وضع خطة لإدارة الثغرات الحرجة وتطوير القدرة على تعبئة جميع الموارد اللازمة لمعالجتها.

__النتيجة:__ تقديم إصلاحات الطوارئ بشأن الكشف المعلق أو العلني عن الثغرات أو في المواقف الأخرى التي يمكن أن يتعرض فيها أصحاب المصلحة للخطر وتتطلب لذلك إجراءً سريعاً.



الشكل 14 - التعامل مع الحوادث

الوظيفة 1.3.4 إنشاء غرفة عمليات

عندما تلزم إدارة الحوادث، يتعين إنشاء غرفة عمليات تضم بين جدرانها فريق PSIRT، والقانون، والاتصالات، والتطوير، ودعم أصحاب المصلحة، والمورِّد والأدوار الأخرى حسب الحاجة. يمكن أن تكون هذه الغرفة موقعاً فعلياً أو افتراضياً طالما أن جميع الأطراف متاحة للرد حسب الحاجة بطريقة آمنة. وعادةً ما تكون الخيارات على أرض الواقع والخيارات عن بعد ضرورية لضمان حضور أصحاب المصلحة. وينبغي تحديد الموارد مسبقاً من أجل تقديم الدعم الكافي لعملية إدارة الحوادث.

__الغرض:__ التأكد من تيسر أصحاب المصلحة للإجابة على الأسئلة وتقديم التوجيه. وضمان تخصيص الموارد المناسبة لإدارة الحوادث.

__النتيجة:__ تنظيم الموارد المدقّقة.

الوظيفة الفرعية 1.1.3.4 خطة إدارة الحوادث

توضع خطة لإدارة الثغرات الحرجة وتطوَّر القدرة على تعبئة جميع الموارد اللازمة لمعالجتها. ومن المهم إجراء تمرين الجاهزية للتصدي للحوادث من أجل التحقق من جاهزية هذه الخطة للتعامل مع الأحداث والطوارئ غير المتوقعة.

الوظيفة الفرعية 2.1.3.4 تحديد الموارد المطلوبة للتعامل مع الحادث وإدارته

يمكن أن تتضمن الموارد قاعات اجتماعات وخطوط خاصة وقوى بشرية إضافية. وللتعامل مع الحوادث على المدى الطويل، ينبغي النظر في الغذاء وأماكن الإيواء.

الوظيفة الفرعية 3.1.3.4 إشراك أصحاب المصلحة في خطة التصدي للحوادث

يحدَد جميع أصحاب المصلحة الرئيسيين المطلوبين للمشاركة في التعامل مع الحادث كجزء من خطة التصدي للحوادث لديكم. ويحدَد جميع أصحاب المصلحة الرئيسيين المطلوبين للمشاركة في التعامل مع الحوادث كجزء من خطة التصدي للحوادث لديكم. انظر الخدمة 1.1 بشأن إدارة أصحاب المصلحة الداخليين والخدمة 5.1 بشأن الاتصالات أثناء الحوادث.

الوظيفة الفرعية 4.1.3.4 إسناد أدوار ومسؤوليات واضحة لإدارة الحادث

يجب على الموظفين معرفة أدوارهم وترتيب العمليات عند الحاجة إلى التصدي. وينبغي إجراء تدريبات وتمارين المحاكاة لإعداد المشاركين الرئيسيين في التصدي.

الوظيفة 2.3.4 إدارة الحوادث

عند الإعلان عن حادث، ينصب التركيز الرئيسي لفريق PSIRT بالشراكة مع أصحاب المصلحة لديه على الحد من تأثير الحادث والعمل على استعادة وظيفة المنتَج في مصلحة الأعمال وكذلك عند أصحاب المصلحة.

__الغرض:__ إنشاء مجموعة سيناريوهات ممكنة وتنفيذ خطة لاحتواء الحادث.

__النتيجة:__ إعادة العمليات إلى أفرقة المنتجات وكذلك أصحاب المصلحة في أقرب وقت ممكن.

الوظيفة الفرعية 1.2.3.4 جمع المعلومات

تلقي المعلومات المتعلقة بالحادث وفهرستها وتخزينها.

الوظيفة الفرعية 2.2.3.4 التحليل

يعتمد التعامل مع الحوادث على تحليل الأنشطة المعرَّفة في فقرة "التحليل".

الوظيفة الفرعية 3.2.3.4 التصدي

الخدمات ذات الصلة بالتخفيف من تأثير حادثة والعمل على استعادة وظائف مصالح الأعمال لدى الجهة المخدَّمة.

الوظيفة الفرعية 4.2.3.4 تتبع الحوادث

توثيق المعلومات بشأن الإجراءات المتخذة لحل حادثة، بما في ذلك المعلومات الهامة التي جمُعت، والتحليل الذي جرى وخطوات التدارك والتخفيف المتخذة، والاختتام والحل.

الوظيفة الفرعية 5.2.3.4 عملية تحليل الحدث بعد وقوعه

إجراء استعراض بعد التنفيذ لتحديد التحسينات على العمليات والسياسات والإجراءات والموارد والأدوات للمساعدة في التخفيف من وطأة أي خرق في المستقبل ومنعه.

الوظيفة 3.3.4 خطة الاتصالات

يجب على جميع أصحاب المصلحة وأصحاب الإجراءات معرفة أحدث الخطط والتقدم الحاصل لمواصلة السير على المسار الصحيح. ويتعين إشراك الإدارة حسب الحاجة لكسر أي حواجز يمكن أن تعرقل الاتصالات التعاونية المفتوحة خلال حادث.

__الغرض:__ وضع خطة اتصالات وتعيين نقطة اتصال مركزية بشأن الحادث لإطلاع الجميع على آخر التطورات.

__النتيجة:__ تنظيم الاتصالات المدقّقة.

الوظيفة الفرعية 1.3.3.4 نشر المعلومات لأصحاب المصلحة الداخليين

إدارة القوائم المستخدمة لتوزيع الإعلانات والتنبيهات والتحذيرات ومصادر التغذية بالبيانات، والمطبوعات الأخرى من أجل الوعي الظرفي.

الوظيفة الفرعية 2.3.3.4 حسن إدارة وتنسيق العلاقات العامة

ضمان توزيع المعلومات على وسائل الإعلام وأصحاب المصلحة، ولكن من خلال القنوات المجازة في المنظمة حصراً. ويشمل ذلك منشورات وسائل التواصل الاجتماعي.

الوظيفة الفرعية 3.3.3.4 الإبلاغ عن أنشطة التعافي

تبلّغ أنشطة التعافي إلى أصحاب المصلحة الداخليين والمديرين التنفيذيين وأفرقة الإدارة.

الوظيفة الفرعية 4.3.3.4 جمع الملاحظات التقييمية عن تحليل الحدث بعد وقوعه

يقدم فريق PSIRT إحاطات عن تحليل الحدث بعد وقوعه وتُجمع الملاحظات التقييمية لتحسين التصدي للحوادث وكذلك أنشطة مكتبة تطوير الأمن (SDL) (على سبيل المثال، ما هو نشاط مكتبة تطوير الأمن (SDL) الذي كان يمكن أو كان ينبغي أن يمنع المشكلة في المقام الأول؟).

الخدمة 4.4 مقاييس إصدار الثغرات

ينبغي أن تشمل البيانات التي تُجمع، على سبيل المثال لا الحصر، حجم المشكلة، أو تصنيفها، أو الوقت المستغرَق لإصلاحها، أو المنتجات أو الخدمات المتأثرة.

الغرض: *جمع البيانات بانتظام لإعداد تقارير الإدارة من أجل التعرف على المخاطر.*

النتيجة: *لوحة عرض تسلط الضوء على النجاحات وفرص التحسين.*

الشكل 15 – المقاييس التشغيلية ومقاييس الأعمال

الوظيفة 1.4.4 التقارير التشغيلية

تقدم التقارير التشغيلية معلومات بشأن حجم وكذلك أنواع الثغرات التي يرد الإبلاغ عنها وتأكيدها عبر المنتجات والإصدارات المختلفة. وينبغي نشر هذه التقارير بانتظام وتداولها داخلياً ضمن فريق التصدي لحوادث أمن المنتجات (PSIRT) وكذلك مع أصحاب المصلحة الداخليين.

الغرض: *جمع البيانات بانتظام لإعداد التقارير العامة.*

النتيجة: *تحديد المجالات التي تتطلب التحليل والموارد والتحسين.*

الوظيفة الفرعية 1.1.4.4 إجمالي عدد الثغرات المبلَّغ عنها مقابل المؤكَد منها (حسب المنتجات/وحدات الأعمال)

تساعد هذه البيانات في التعرف على الحجم الذي يتعامل معه فريق PSIRT من منظور الموارد.

الوظيفة الفرعية 2.1.4.4 فرز إجمالي الثغرات المؤكدة وفق مكونات طرف ثالث

تساعد هذه البيانات في التعرف على المخاطر المرتبطة بمكونات مدمجة محددة وردت من طرف ثالث.

الوظيفة الفرعية 3.1.4.4 فرز إجمالي الثغرات المؤكدة وفق التعداد المشترَك لنقاط الضعف (CWE) (حسب المنتجات/وحدات الأعمال)

يمكن تغذية هذه البيانات في مصدر مدخلات دورة حياة تطوير الأمن وتأثير التدريب والتعليم.

الوظيفة 2.4.4 تقارير الأعمال

تقدم تقارير الأعمال معلومات بشأن صحة قدرات التصدي للثغرات في المنظمة.

__الغرض:__ وضع قياسات لمستوى نجاح المنظمة في الإيفاء بالالتزامات المحددة زمنياً في اتفاقات مستوى الخدمة. وجمع البيانات التي تقيس مستوى تحقيق هذه الأهداف وتحليلها ونشرها بانتظام،

__النتيجة:__ إنشاء لوحة عرض تسلط الضوء على النجاحات وفرص التحسين.

الوظيفة الفرعية 1.2.4.4 تقييم التأثير في أوانه

يوضح هذا المقياس مدى جودة أداء أفرقة المنتجات في إكمال تقييمات التأثير ضمن الأطر الزمنية لاتفاق مستوى الخدمة الخاص بتقييم التأثير.

الوظيفة الفرعية 2.2.4.4 تخطيط الإصلاح في أوانه

يوضح هذا المقياس مدى جودة أداء أفرقة المنتجات في تقديم خطة إصلاح ضمن اتفاق مستوى الخدمة المحدد.

الوظيفة الفرعية 3.2.4.4 تتبع التدارك

يوضح هذا المقياس مدى جودة أداء أفرقة المنتجات في تقديم الإصلاح ضمن الأطر الزمنية لاتفاق مستوى الخدمة المحدد.

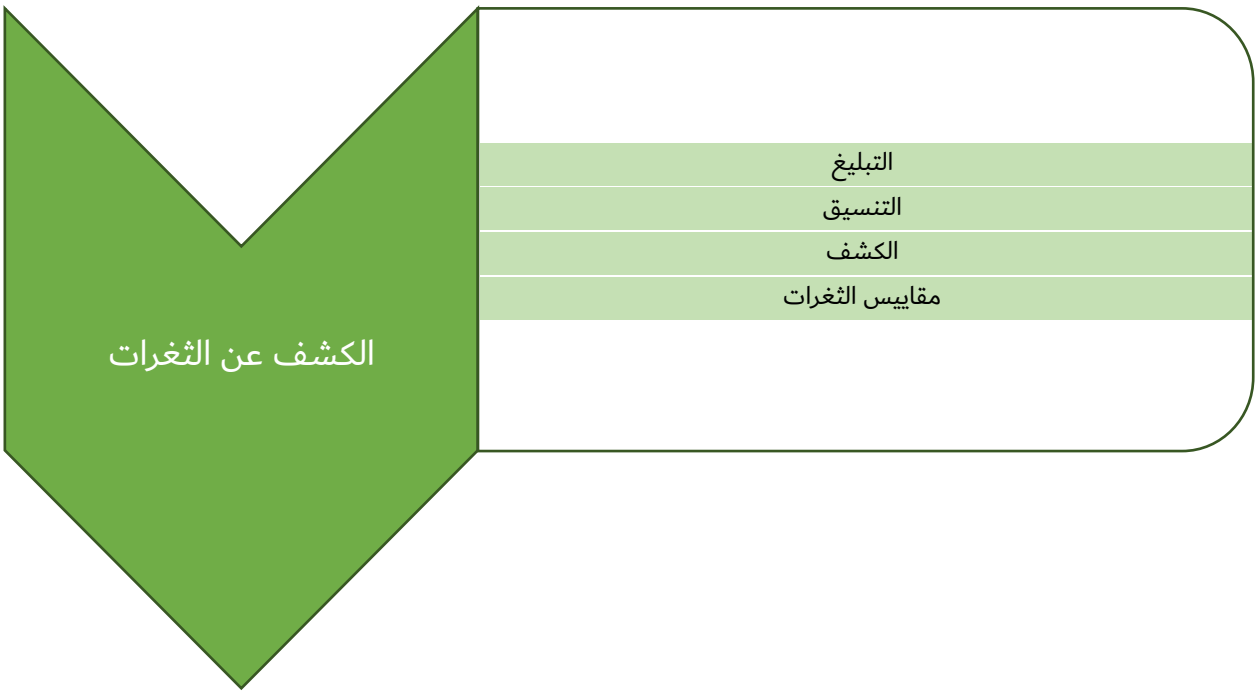
الوظيفة الفرعية 4.2.4.4 معدل التدارك في أوانه

يوضح هذا المقياس مدى جودة أداء أفرقة المنتجات في تحقيق مجمل الأهداف أو الاتفاقات بشأن تسليم إصلاح منذ وقت الإبلاغ إلى حين تسليم الإصلاح. يمكن فرز ذلك حسب الخطورة أو حسب نوع الثغرة (خط المنتَج، نوع الثغرة).

الوظيفة الفرعية 5.2.4.4 عدد الحوادث

توضح هذه البيانات المخاطر على المنظمة.

مجال الخدمة 5

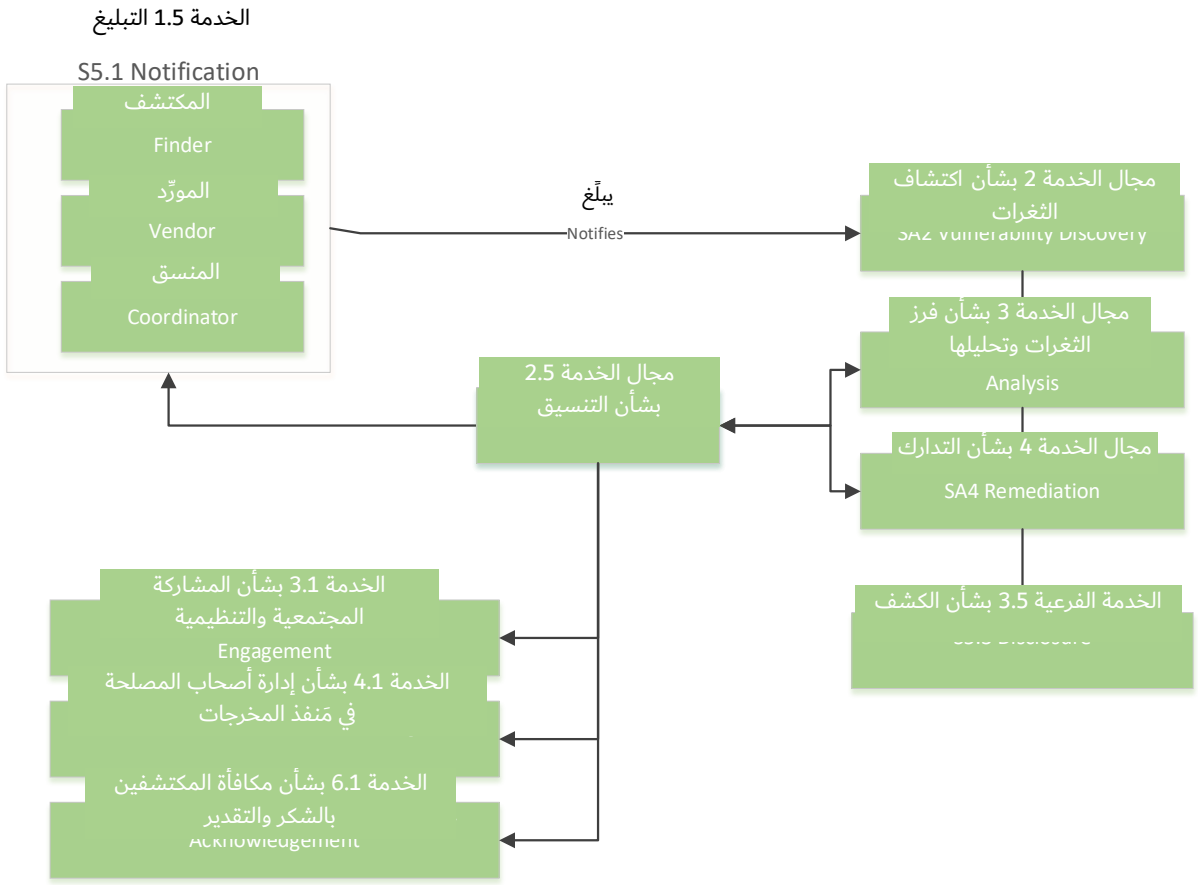


من المهم خلق بيئة شفافة وتعاونية يمكن فيها للمورِّدين والمنسقين والمكتشفين تبادل المعلومات مع أصحاب المصلحة ومع بعضهم البعض والتفاوض على خطط الكشف المتفق عليها بشكل متبادل. ومن خلال الشراكة بهذه الطريقة، يمكن تحقيق الاحتياجات الأساسية لحل الثغرات وحماية أصحاب المصلحة والاعتراف بفضل المكتشفين. وينبغي للمورِّد نشر سياسة الكشف عن الثغرات الخاصة به كي يتسنى للمنسقين والموردين الآخرين وكذلك المكتشفين الرجوع إليها.

الشكل 16 – عملية التبليغ عن الثغرات

الغرض: *تقديم الشفافية لأصحاب المصلحة والشركاء من خلال التعاون مع المكتشفين والمنسقين والموردين في منفَذ المخرجات للكشف بشكل مسؤول عن الثغرات والإصلاحات.*

النتيجة: *زيادة الثقة والتعاون والتحكم في الكشف.*



الشكل 17 – مثال إجمالي للتنسيق بشأن الثغرات

الخدمة 1.5 التبليغ

تتضمن هذه الخدمة تحديد عملية التبليغ المناسبة لتقديم معلومات لأصحاب المصلحة في الوقت المناسب بشأن استراتيجية التخفيف والعلاجات والحلول الالتفافية لإبقائهم على اطلاع عليها وتمكينهم من التخطيط وفقاً لذلك. وفي بعض الحالات، يمكن أن توجد اتفاقات تعاقدية بين المورّدين من قبيل أن يُتطلب من مورّد في مَصدر المدخلات تبليغ مورّد آخر في منفذ المخرجات بالثغرات المكشوفة أو الحوادث المعروفة. والقصد من عملية التبليغ هو التأكد من قدرة جميع أصحاب المصلحة والمورّدين على فهم وإدارة المخاطر التي تفرضها الثغرة.

الغرض: *تقديم الشفافية للمورّدين والمكتشفين من خلال التعاون.*

النتيجة: *زيادة الثقة والتعاون مع المكتشفين.*

الوظيفة 1.1.5 المورّد الوسيط (مورّد في منفذ المخرجات)

يجوز لمورّد وسيط مثل الشركة المصنّعة للمعدات الأصلية أو الشريك تطوير و/أو إنتاج قطعة أو نظام فرعي أو برمجيات تُستخدم في منتج نهائي لمورد آخر. وفي مثل هذه الحالات، ينبغي لفريق التصدي لحوادث أمن المنتجات (PSIRT) إجراء ترتيبات لتناقل معلومات عن الثغرات مع مورديه. وينبغي أن يكون على دراية بسياسة معالجة الثغرات لدى المورّدين المختلفين. وفي بعض الأحيان توضَّح هذه التوقعات في اتفاق تعاقدي. وينبغي التفاوض على الجدول الزمني للتدارك والكشف في أقرب وقت ممكن.

الغرض: *إنشاء بيئة تعاون وتوقعات واضحة بين مصنّعي المعدات الأصلية (OEM) والشركاء والموردين الآخرين.*

__النتيجة:__ زيادة الثقة والتعاون والتحكم في الكشف بين جميع الأطراف المعنية.

الوظيفة الفرعية 1.1.1.5 التقارير المقدمة من فريق PSIRT إلى المورِّدين الوسطاء

يمكن أن تعلم أفرقة PSIRT بالثغرات التي أبلغ عنها أصحاب المصلحة لديها وينبغي أن تبلِّغ فريق PSIRT لدى المورِّد الوسيط بتلك الثغرات.

الوظيفة الفرعية 2.1.1.5 التقارير المقدمة من المورِّد الوسيط

يمكن لمورِّد وسيط يزود مورِّداً آخر بمكونات أو أدوات أن يعلم بالثغرات التي يبلَّغ عنها مباشرةً، وينبغي أن يبلِّغها لأفرقة التصدي لحوادث أمن المنتجات (PSIRT) لدى المورِّدين.

الوظيفة الفرعية 3.1.1.5 الاتفاقات التعاقدية

ينبغي لأفرقة التصدي لحوادث أمن المنتجات (PSIRT) تحديد جميع المورِّدين الوسطاء والنظر في الشراكة مع المورِّدين الحقوقيين لضمان إضافة بنود إلى الاتفاقات التعاقدية تكفل التصدي للثغرات في الوقت المناسب.

الوظيفة الفرعية 4.1.1.5 تبليغ أفرقة PSIRT لأصحاب المصلحة

يمكن أن تقوم أفرقة التصدي لحوادث أمن المنتجات (PSIRT) لدى المورِّدين بإبلاغ أصحاب المصلحة خاصةً إذا عجز المورِّد الوسيط عن تدارك الثغرة أو طال الوقت الذي يستغرقه لتداركها. وفي بعض الحالات، يجوز أن يطبق فريق PSIRT لدى المورِّد عملية تبليغ متدرجة فيبلِّغ أصحاب المصلحة الأكثر تأثراً بالثغرة.

الوظيفة 2.1.5 المنسقون

يمكن أن يطلب فريق PSIRT من منسق المشاركة في تبليغ المورِّدين الآخرين وكذلك تنسيق توقيت العلاج بشأن إرشاداته خاصة إذا كان هناك العديد من المورِّدين. ويقدم المنسقون مثل مركز تنسيق فريق CERT (CERT/CC)[12] أو منسقي طرف ثالث مساهمات قيِّمة باستمالة العديد من المنظمات المختلفة نحو الشراكة والتعاون في معالجة الثغرات.

__الغرض:__ يمكن أن يُطلب من المنسقين التدخل ومساعدة منظمة فريق PSIRT في التبليغ والتعاون بشأن الثغرات مع جميع المورِّدين.

__النتيجة:__ زيادة الثقة والتعاون والتحكم في الكشف بين جميع الأطراف المعنية.

الوظيفة الفرعية 1.2.1.5 التعرف على المنسق

توثيق وفهم مختلف المنسقين على أساس سياسة الكشف عن الثغرات.

الوظيفة الفرعية 2.2.1.5 التعامل مع المنسق

التشارك مع منسق لضمان تبليغ جميع أفرقة PSIRT لدى المورِّدين المتأثرين.

الوظيفة 3.1.5 المكتشف

يمكن أن يقوم مكتشف من قبيل عميل أو باحث لدى طرف ثالث بتبليغ فريق PSIRT بوجود ثغرة من خلال القنوات الموثقة في مجال الخدمة 2 بشأن اكتشاف الثغرات.

__الغرض:__ خلق بيئة تعاون وتوقعات واضحة مع المكتشفين.

__النتيجة:__ زيادة الثقة والتعاون والتحكم في الكشف مع المكتشفين.

12 www.cert.org

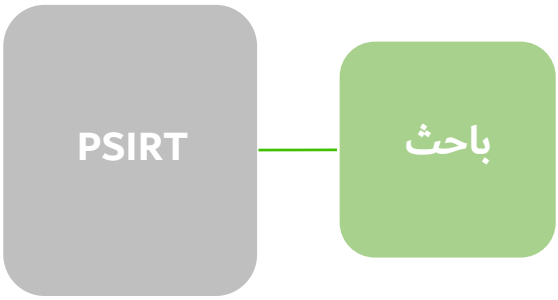
الخدمة 2.5 التنسيق

عند الاقتضاء، ينبغي لفريق PSIRT لدى المورِّد اتخاذ ترتيبات لتناقل معلومات عن الثغرات مع المنسقين أو المورِّدين الآخرين. وينبغي أن يكونوا على دراية بسياسة التعامل مع الثغرات لدى المورِّد. وينبغي التفاوض على الجداول الزمنية للتدارك والكشف في أقرب وقت ممكن.

الغرض: *توثيق الثغرات التي أزيلت من المنتج بواسطة التدارك.*

النتيجة: *الوضوح فيما يتعلق بفائدة تنفيذ العلاج ومكان الحصول عليه.*

الوظيفة 1.2.5 التنسيق الثنائي



الشكل 18 - التنسيق الثنائي

يتولى فريق التصدي لحوادث أمن المنتجات (PSIRT) لدى مورِّد مسؤولية الحفاظ على التواصل مع المكتشفين الذين يبلغون عن الثغرات المحتملة. ومن المهم للمورِّدين أن يفهموا نية المكتشف ومآربه وموقفه من الثغرات بشكل عام، من أجل تعزيز وتسهيل الكشف المنسق وفق جدول زمني متفق عليه. وينبغي أن تنظر أفرقة PSIRT في الاعتراف بفضل المكتشفين الذين يلتزمون بالكشف العلني.

الغرض: *خلق بيئة من التعاون يعرف فيها المكتشفون أنهم سيؤخذون على محمل الجد.*

النتيجة: *خطة كشف متفاوض عليها تكرّم جهود المكتشفين.*

الوظيفة الفرعية 1.1.2.5 استلام التقرير

الإقرار باستلام تقرير عن ثغرات من مكتشف لدى طرف ثالث.

الوظيفة الفرعية 2.1.2.5 تحديثات منتظمة

تزويد المكتشفين بتحديثات منتظمة بشأن حالة الثغرة المبلغ عنها.

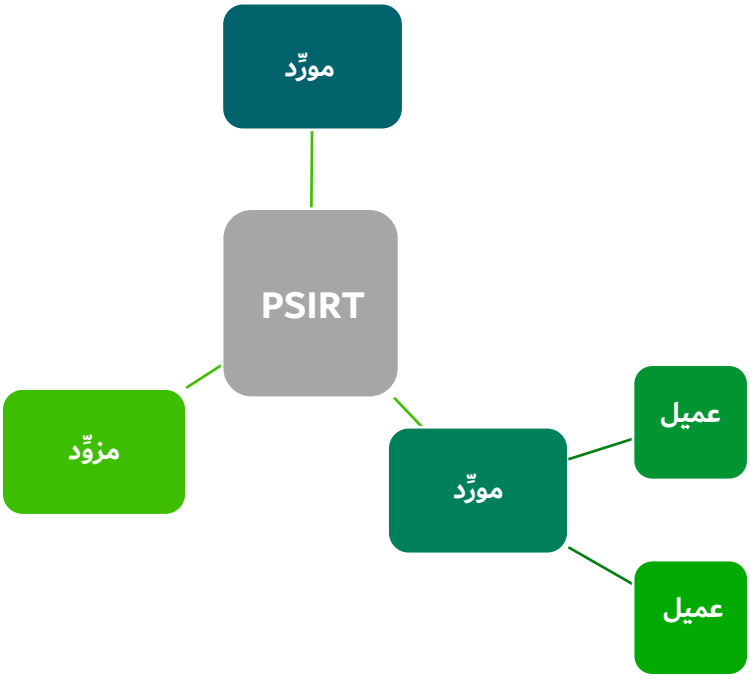
الوظيفة الفرعية 3.1.2.5 التحقق من جانب المكتشف

يقدَّم العلاج إلى المكتشف كي يتمكن من التحقق من صحته أيضاً.

الوظيفة الفرعية 4.1.2.5 الاعتراف بفضل المكتشفين

يبدى التقدير من خلال الاعتراف بمساهمات المكتشف الذي أبلغ عن الثغرة. وينبغي أن يتحقق المورِّد مع المكتشف من أن التقدير مقبول.

الوظيفة 2.2.5 التنسيق مع موزّدين متعددين



الشكل 19 - التنسيق مع موزّدين متعددين

عند الاقتضاء، ينبغي لفريق PSIRT لدى المورِّد اتخاذ ترتيبات لتناقل معلومات عن الثغرات مع المنسقين أو المورِّدين الآخرين. وينبغي أن يكونوا على دراية بسياسة التعامل مع الثغرات لدى المورِّد. وينبغي التفاوض على الجداول الزمنية للتدارك والكشف في أقرب وقت ممكن.

الغرض: *تقديم الشفافية لأصحاب المصلحة والشركاء من خلال التعاون مع جميع الأطراف للكشف بشكل مسؤول عن الثغرات والتدارك.*

النتيجة: *زيادة الثقة والتعاون والتحكم في الكشف.*

صاحب مصلحة متعدد الأطراف	العلاقة معكم	المصلحة في التنسيق
موردون في مصدر المدخلات	مزود OEM يقدم التكنولوجيا.	يوصى الموردون في مصدر المدخلات بإدارة أصحاب المصلحة لديهم في منفذ المخرجات بغية تقديم علاج (انظر الخدمة 4.1).
موردون في منفّذ المخرجات	ترد التكنولوجيا من مورِّد في مصدر المدخلات.	تلقي التبليغ بلزوم تطبيق العلاج الأمني. ويوصى الموردون في منفذ المخرجات بتحديد، والتعامل مع، مجتمعات الموردين والشركاء في مصدر المدخلات (انظر الوظيفة 1.3.1).

الجدول 1: مثال التنسيق مع مورِّدين متعددين

الوظيفة الفرعية 1.2.2.5 استلام التقرير

يقر فريق التصدي لحوادث أمن المنتجات (PSIRT) لدى المورِّد باستلام تقرير عن الثغرات من المورِّد أو المنسق.

الوظيفة الفرعية 2.2.2.5 التعرف على المورِّد المتأثر

يمكن أن يحتاج فريق PSIRT لدى المورِّد أو المنسق إلى تحديد المورِّدين المتأثرين بتقرير عن ثغرات.

الوظيفة الفرعية 3.2.2.5 تناقل المعلومات عن الثغرات

يطلع فريق PSIRT لدى المورِّد أو المنسق مختلف المورِّدين على المعلومات عن الثغرات.

الوظيفة الفرعية 4.2.2.5 تخطيط إصدار العلاج

يتشارك فريق PSIRT لدى المورِّد أو المنسق مع المورِّدين بشأن توقيت وتيسر برمجيات التدارك، وكيف يمكن للمورِّدين في منفذ المخرجات تلقي العلاج.

الوظيفة الفرعية 5.2.2.5 التحقق من صحة العلاج

يتحقق فريق PSIRT لدى المورِّد أو المنسق مع المورِّدين من أن التدارك الأمني يعالج الثغرة.

الوظيفة الفرعية 6.2.2.5 تنسيق الكشف

يتفاوض فريق PSIRT لدى المورِّد أو المنسق مع جميع المورِّدين للاتفاق على كيفية الكشف عن الثغرة وكذلك توقيت إصدار الكشف عنها علناً.

الخدمة 3.5 الكشف

عند إصدار تدارك أمني، ينبغي أن تواكبه عمليات كشف مناسبة لضمان تبليغ أصحاب المصلحة والمورِّدين بالعلاج على الوجه الصحيح. وفي كل منها، تدعو الحاجة إلى حُسن تحديد متابعيها (يمكن أن يختلف المتابعون على اختلاف أنواع التبليغات).

الغرض: *توثيق تغييرات الشفرة وإصدار برمجيات التدارك الأمني.*

النتيجة: *الوضوح فيما يتعلق بالعلاجات التي نُفذت على الشفرة ومكان الحصول عليها.*

الوظيفة 1.3.5 ملاحظات الإصدار

ينبغي أن تتضمن ملاحظات الإصدار، بما فيها الملف التمهيدي (readme) وسجل التغييرات الزمني، مرجع (مراجع) تعداد الثغرات الشائعة (CVE) بشأن العلاج. وينبغي أن توضح ملاحظات الإصدار بوضوح كيف عولجت الثغرة.

الغرض: *تقديم بيان بشأن العلاجات المضمَّنة في الشفرة المحدَّثة.*

النتيجة: *يمكن لأصحاب المصلحة حماية أنفسهم من التعرض المحتمل لأضرار الثغرة.*

الوظيفة الفرعية 1.1.3.5 الكشف ضمن ملاحظات الإصدار

تحدَد الثغرات التي ينبغي الكشف عنها في ملاحظات الإصدار.

الوظيفة الفرعية 1.1.3.5 استعراض ملاحظات الإصدار

تحدَد عملية الاستعراض.

الوظيفة الفرعية 2.1.3.5 الموافقات على ملاحظات الإصدار

إجراء استعراض وموافقة على الكشف.

الوظيفة 2.3.5 الإرشادات الأمنية

ينبغي أن يكون لدى المورِّدين آلية تصدر من خلالها إرشادات أمنية لأصحاب المصلحة على صفحة إلكترونية علنية وتكشف عن الثغرات التي استُدركت.

الغرض: *تقديم مستودع عام للإرشادات الأمنية المنشورة.*

النتيجة: *تيسر إرشادات أمنية كي تستعرضها الجهات المخدَّمة وتتخذ الإجراءات وفقها.*

الوظيفة الفرعية 1.2.3.5 الصيغة النموذجية للإرشادات

تحدَد صيغة نموذجية مقيَّسة للإرشادات الأمنية. ويُدرَج فيها العنوان، والملخص، ومرجع (مراجع) تعداد الثغرات الشائعة (CVE)، وتأثير المنتج المدعوم وحالته، وفقرة الشكر والتقدير، والمراجع وسجل المراجعة الزمني.

الوظيفة الفرعية 2.2.3.5 أسلوب تسليم الإرشادات

تحدَد آلية تقديم الإرشادات الأمنية بما في ذلك، على سبيل المثال لا الحصر، وثيقة إلكترونية على شبكة الإنترنت أو تلقيم RSS أو الاشتراك في منشورات دورية.

الوظيفة الفرعية 3.2.3.5 تحديد نسق الإرشادات

توخياً لأن يستهلك أصحاب المصلحة والجهات المخدَّمة الإرشادات باستخدام أدوات الأتمتة، يُنظر في نشر الإرشادات في نسق تمكن قراءته آلياً مثل إطار الإرشادات الأمنية المشترك (CSAF).[13]

الوظيفة الفرعية 4.2.3.5 الظروف المحركة للإرشادات

تحدَد مجموعة الشروط التي يمكن أن تؤدي إلى إصدار إرشادات أمنية. ومثال ذلك، إذا دعت الحاجة لاتخاذ إجراء لتبليغ أصحاب المصلحة بأن البيئة المستضافة قد أُصلحت (في سيناريو خرق).

الوظيفة الفرعية 5.2.3.5 تخصيص معرف CVE

تحدَد عملية تخصيص ثغرة بمعرّف CVE.

الوظيفة الفرعية 6.2.3.5 الاعتراف بفضل المكتشف

13 https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=csaf

يحدَد ما إذا كان المكتشف يرغب في نيل اعتراف علني بفضله أو شكر وتقدير.

الوظيفة الفرعية 7.2.3.5 التخطيط للكشف

تحدَد عملية الاستعراض لأمور مثل من هم أصحاب المصلحة ومتى تنبغي صياغة الكشف.

الوظيفة الفرعية 8.2.3.5 عملية استعراض الإرشادات

تجرى عملية الاستعراض مع أصحاب المصلحة المحددين.

الوظيفة 3.3.5 المواد القائمة على المعارف

ينبغي أن يكون لدى المورِّد آلية لنشر مواد قائمة على المعارف يمكن أن تصاحب بعض العلاجات الأمنية التي تعتبر أقل شدة أو يمكن استخدامها بدلاً من ذلك كوسيلة للتعبير عن سبب رفض ثغرات محددة أُبلغ عنها على أنها تأكيدات خاطئة.

الغرض: *تقديم مستودع لمواد قاعدة المعارف.*

النتيجة: *: تيسر مواد قاعدة المعارف كي تستعرضها الجهات المخدَّمة وتتخذ الإجراءات وفقها.*

الوظيفة الفرعية 1.3.3.5 الكشف عن مادة تستند إلى المعارف

تحدَد الثغرات التي ينبغي الكشف عنها في مادة قاعدة المعارف.

الوظيفة الفرعية 2.3.3.5 استعراض المادة المستندة إلى المعارف

تحدَد عملية الاستعراض.

الوظيفة الفرعية 3.3.3.5 الموافقات على المادة المستندة إلى المعارف

إجراء استعراض وموافقة على الكشف.

الوظيفة 4.3.5 الاتصالات الداخلية مع أصحاب المصلحة

بالإضافة إلى أرباب الأعمال التنفيذيين الذين ينبغي تبليغهم بخطط اتصالات بشأن الثغرات؛ هناك العديد من الموظفين الذين يعملون في الخطوط الأمامية مع أصحاب المصلحة وجهاً لوجه وعبر الهاتف كل يوم. وتقديم تبليغ مسبق ومكتوم وأسئلة متداولة بشأن الإرشادات القادمة يُعِّد أولئك الذين قد يُسألون عنها عند النشر.

الغرض: *إبلاغ أرباب الأعمال التنفيذيين وهيئات الاتصالات العالمية والموظفين الذين يتعاملون مع أصحاب المصلحة بإرشادات "آتية قريباً" وبالردود المعتمدة.*

النتيجة: *سيتمكن الموظفون من الرد على أسئلة أصحاب المصلحة ووسائل الإعلام يوم نشر الإرشادات، مما يؤدي إلى التحكم في الرسالة الموجَهة.*

الوظيفة الفرعية 1.4.3.5 التعامل مع أصحاب المصلحة الداخليين

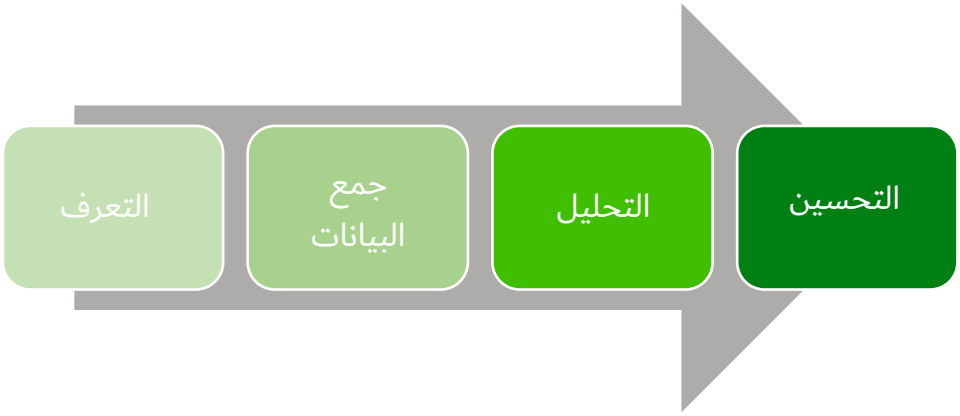
التعاون مع أصحاب المصلحة الداخليين لصياغة، و/أو استعراض التصريحات التي ستدلي بها أفرقتهم عندما يسأل العملاء عن مشكلة الثغرات.

الخدمة 4.5 مقاييس الثغرات

ينبغي أن تشمل البيانات التي ستُجمع، على سبيل المثال لا الحصر، حجم الإصدار، والتصنيف، والجدول الزمني للتدارك، والمنتجات أو الخدمات المتأثرة.

الغرض: *جمع البيانات باتنظام لإعداد تقارير الإدارة.*

النتيجة: *تحديد المجالات التي تتطلب التحليل والموارد والتحسين.*



الشكل 20 - عملية مقاييس الثغرات

الوظيفة 1.4.5 التقارير التشغيلية

يمكن أن تقدم التقارير التشغيلية معلومات إضافية بشأن حجم عمليات الكشف المنشورة بالإضافة إلى عدد مشاهدات الصفحة. وينبغي نشر هذه التقارير بانتظام وتداولها داخلياً ضمن فريق التصدي لحوادث أمن المنتجات (PSIRT) وكذلك مع أصحاب المصلحة الداخليين.

الغرض: *جمع البيانات بانتظام لإعداد التقارير العامة.*

النتيجة: *تحديد المجالات التي تتطلب التحليل والموارد والتحسين.*

الوظيفة الفرعية 1.1.4.5 عدد الإرشادات الأمنية المنشورة

يمكن الإبلاغ عن عدد عمليات الكشف المختلفة وفرزها حسب المنتجات. ويمكن أن يساعد ذلك في دفع الفريق إلى تخصيص مورد تقني.

الوظيفة الفرعية 2.1.4.5 عدد معرفات CVE المرسَلة إلى قاعدة بيانات الثغرات الوطنية (NVD)

يمكن استخدام عدد معرفات CVE المخصَصة للترويج لحالتكم لدى هيئة ترقيم CVE (CNA).

الوظيفة الفرعية 3.1.4.5 مشاهدات صفحة الإرشادات الأمنية

يمكن أن تؤدي إلى توجه استراتيجيتكم نحو إعلام استباقي إذا قلت أعداد أصحاب المصلحة الذين يشاهدون إرشاداتكم.

مجال الخدمة 6

يمر عالم أمن المنتجات في حالة تغير مستمر يجعل فيه جديد التكنولوجيات والخدمات والتكامل من التدريب والتعليم المستمر أولوية عليا لمحترفي الأمن. وإذ تتغلغل البرمجيات في كل جانب من جوانب العالم الذي نعيش فيه من سياراتنا إلى ثلاجاتنا، تزداد أهمية مواكبة احتياجات تأمين المنتجات أكثر من أي وقت مضى. وتؤدي أفرقة التصدي لحوادث أمن المنتجات (PSIRT) دوراً رئيسياً في دعم منهاج قوي لتثقيف جميع أصحاب المصلحة بشأن تعقيدات تطوير واعتماد وشحن المنتجات/الخدمات التي تلبي معايير العالم الموصول اليوم.

ويمكن أن تختلف احتياجات التدريب والتعليم كثيراً عبر شركة ما. فتختلف اهتمامات مطور البرمجيات الثابتة عن اهتمامات مطور خدمات البرمجيات اختلافاً كبيراً وكثيراً ما تتطلب أنواعاً محددة وفريدة للغاية من التدريب. ولأغراض هذه الوثيقة، ستُفرز احتياجات التدريب إلى أربع مجموعات من أصحاب المصلحة هي: مجموعة فريق PSIRT، ومجموعة تطوير المنتجات، ومجموعة التحقق من المنتجات، ومجموعة أصحاب المصلحة الآخرين المشاركين في عملية فريق PSIRT.

1) يعد **تدريب فريق PSIRT** فريداً لأن على أعضاء فريق PSIRT الإلمام بالعديد من الجوانب كالجوانب القانونية وجوانب الاتصالات والتطوير.

2) **تطوير المنتجات** (الهندسة الداخلية والتطوير): يتطلب المطورون التدريب في مجالاتهم المحددة وبالتالي فإنهم يحتاجون إلى تدريب بالقدر نفسه من التركيز. ويتطلب تطوير البرمجيات الثابتة الآمنة التي يصعب تحديثها في الميدان متطلبات مختلفة تماماً عن متطلبات مهندس تطبيقات سطح المكتب.

3) **التحقق من المنتجات** (الهندسة الداخلية والتطوير): تتطلب أدوات التحقق تدريباً مستمراً للتعرف على أحدث الأدوات والتقنيات لأشياء مثل اختبار الاختراق والمسح الباحث عن الثغرات واستعراضات التصميم المبكرة لوضع اليد على المشاكل قبل أن يلزم إصلاحها.

4) **جميع أصحاب المصلحة الآخرين:** تمثل هذه المجموعة جمهوراً أقل انشغالاً بالجوانب التقنية ويتطلب ركيزة صلبة في فهم أساسيات تطوير المنتجات الآمنة والتحقق منها وشحنها وكذلك التفاعل عندما تتخلل المنتَجَ المشحون ثغرة.

ولا يُعتبر التدريب على التطوير الآمن جزءاً من برنامج فريق التصدي لحوادث أمن المنتجات (PSIRT) ويُتعامل معه خارج عملية فريق PSIRT. ولكن من المهم أن تؤازر أفرقة PSIRT جميع الجوانب المتعلقة بطرح منتجات آمنة في السوق، وعلى هذا النحو ينبغي أن تتعاون مع أفرقة التطوير المختلفة للتأكد من تيسر التدريب المناسب. وفي العديد من المنظمات الصغيرة، قد

لا توجد مجموعة منفصلة تتحمل مسؤولية التأكد من تطوير المنتجات مع التركيز على الأمن. وفي هذه الحالات، يمكن أن يشارك فريق PSIRT في سد الفجوة (ويقع ذلك خارج نطاق هذه الوثيقة).

وفي كل قسم، سنحدد مجموعات أصحاب المصلحة المختلفة ونلخص بعض مجالات التركيز التي يمكن أن تساعد فريق PSIRT على المشاركة في مناقشات ذات مغزى بشأن تدريب وتعليم أصحاب المصلحة. يمكن أن تنشئ أفرقة التصدي لحوادث أمن المنتجات (PSIRT) جميع مواد التدريب داخل الشركة، أو أن تستخدم مواد خارجية أو تستخدم موارد تدريب خارجية لتدريب أصحاب المصلحة لديها.

الخدمة 1.6 تدريب فريق التصدي لحوادث أمن المنتجات (PSIRT)

يحتاج موظفو فريق PSIRT لأن يكونوا في طليعة ما يحدث في عالم الأمن بما في ذلك، على سبيل المثال لا الحصر، ماهية الاتجاهات الشائعة، والشفرات الاستغلالية الجديدة، وأنشطة دوائر الصناعة. ويبدأ هذا المستوى الواسع من المعارف بتطلب أساس متين في مواضيع عالم الأمن العامة على النحو الموضح في الشهادات الأمنية الرائدة. ولكن الشهادات لا تقدم إلا قاعدة تحتاج إلى تحديث مستمر من خلال أنشطة مثل مؤتمرات تركز على الأمن، وإشراك اتحاد دوائر الصناعة، والوعي البصير بالصناعة ككل من خلال المطالعة النهم للمدونات، وصحافة أوساط الصناعة، ومنشورات اتحاد دوائر الصناعة، وما إلى ذلك. ويحتاج أعضاء فريق PSIRT أيضاً إلى مواكبة المستجدات المتطورة باستمرار في عالم التشريعات المعنية بالأمن والخصوصيات.

الوظيفة 1.1.6 التدريب التقني

من المهم أن يتكون لدى موظفي فريق PSIRT فهم راسخ للمفاهيم الأمنية الأساسية ومعرفة بالمنتجات الجاري دعمها. ويجب استعراض مواد التدريب بانتظام للتأكد من تضمين تقنيات جديدة بشأن الثغرات في مواد التدريب مع تغير المشهد الأمني.

__الغرض:__ تدريب طاقم فريق PSIRT كي يتمكن من فهم المشكلة التي يبلَّغ عنها ومن أداء الفرز الأولي بالقدر الكافي قبل تسليمها إلى الأفرقة المسؤولة عن تطوير الإصلاحات واختبارها وإصدارها.

__النتيجة:__ يحظى موظفو فريق PSIRT بتدريب تقني كافٍ لأداء واجباتهم.

يمكن أن يختلف التدريب على مفاهيم الأمن حسب نوع المنتجات التي يدعمها المورد (كالعتاد أو البرمجيات الثابتة أو البرمجيات أو التوصيل الشبكي أو المنتجات السحابية أو كل ما سبق). وعلى مستوى عالٍ جداً، يجب أن يغطي التدريب مواضيع الأمن الأساسية مثل الهجمات الشائعة، والتجفير، والكتمان، والسلامة، والتيسر، والاستيقان، والتخويل، ونماذج التحكم في النفاذ، والإيجار المتعدد، والالتزام ذي الصلة، واللوائح، في جملة أمور أخرى. وينبغي أن يتضمن هذا التدريب أيضاً أي لوائح تخص صناعة بعينها يمكن أن تؤثر على أنشطة فريق PSIRT مثل HIPAA لقطاعات الرعاية الصحية، وPCI DSS لمورِّدي بطاقات الدفع والخدمات المصرفية. ويجب أيضاً تغطية مستوى معين من التدريب على المنتجات لموظفي فريق PSIRT كي يتمكن من فهم المشاكل التي يبلَّغ عنها.

الوظيفة 2.1.6 التدريب على التواصل

نظراً لأن المكتشفين الخارجيين يبلغون فريق PSIRT بالمشاكل، من المهم أن يتدرب موظفو فريق PSIRT على سياسات التواصل والمهارات الشخصية التي تغطي كيفية التعامل مع الاتصالات مع المكتشفين الخارجيين وأصحاب المصلحة الداخليين في الوقت المناسب.

__الغرض:__ التأكد من اتباع موظفي فريق PSIRT لسياسات التواصل الخاصة بالمنظمة أثناء التفاعل مع الكيانات الخارجية وبالتالي منع وقوع أي مشاكل تنظيمية/قانونية يمكن أن تنتج عن التواصل غير السليم.

__النتيجة:__ سيحصل موظفو فريق PSIRT على تدريب كاف في مجال التواصل لأداء واجباتهم المحددة بدقة واضحة وبدون غموض في الاتصالات.

الوظيفة 3.1.6 التدريب على إجراءات العملية

ينبغي أن تكون هناك مبادئ توجيهية للعملية تحدد كيفية تتبع القضايا المُبلغ عنها وإدارتها وقياسها. وينبغي تحديد أدوار مختلف أصحاب المصلحة المشاركين في عملية حل القضايا المبلغ عنها. وينبغي أن تغطي العملية الرد على المكتشفين في الوقت المناسب وموافاتهم بتحديثات دورية لجميع المشاكل المفتوحة. وينبغي أن تكون هناك أيضاً وسيلة محددة وآمنة لإبلاغ المعلومات بين المكتشف الخارجي والمورِّد.

الغرض: *التأكد من وجود تدفق سلس للمعلومات في إدارة حوادث أمن المنتجات يؤدي إلى حل المشاكل في الوقت المناسب.*

النتيجة: *تدريب موظفي PSIRT بشكل كافٍ على العمليات الداخلية كي يتمكنوا من أداء واجباتهم.*

الوظيفة 4.1.6 التدريب على الأدوات

الوظيفة الفرعية 1.4.1.6 تتبع الأخطاء البرمجية وأدوات الإدارة الأخرى لفريق PSIRT وملاك المهندسين

ينبغي تحديد أداة تتبع الأخطاء البرمجية المعترف بها رسمياً لكل منتَج (ويفضل أن تكون هي نفسها لجميع المنتجات) في منظمة معينة. وينبغي تعريف جميع الأخطاء البرمجية في هذه الأداة وينبغي تعريف الأخطاء البرمجية الأمنية بشكل موحد على هذا النحو. وينبغي قصر إمكانية مشاهدة المعلومات المتعلقة بالثغرات الأمنية في المنتَج وإمكانية النفاذ إليها على مَن يحتاجون للمعرفة بها. بالإضافة إلى ذلك، ينبغي أن تتضمن الأداة القدرة على دعم متطلبات مقاييس البرنامج مع إمكانات إعداد التقارير اليدوية والمؤتمتة.

الغرض: *التأكد من تتبع المشاكل بشكل فعال وحماية معلومات الثغرات في أدوات التتبع المعتمدة بحيث لا يستطيع النفاذ إلى هذه المشاكل وتتبعها وإدارتها إلا من لديهم حاجة مُثبتة للمعرفة بها.*

النتيجة: *تزويد موظفي PSIRT بالقدر الكافي من التدريب والمعرفة بالأدوات كي يتمكنوا من أداء واجباتهم.*

الوظيفة الفرعية 2.4.1.6 أدوات تتبع الطرف الثالث

تتضمن معظم المنتجات العديد من مكونات من أطراف ثالثة (بما فيها المكونات ذات المصدر المفتوح) تُشحن معها. وكثيراً ما يجهل العملاء مضمون برمجيات الأطراف الثالثة المشحونة داخل المنتج، وبالتالي فإنهم يعتمدون على المورِّد لتقديم إصلاحات أو معلومات بشأن العلاج. ومن المهم تحديد أدوات تتبع الطرف الثالث لتغطية تبعيات منتجات المورِّد على مختلف مكونات الطرف الثالث. وتجب مراقبة قاعدة بيانات الثغرات الوطنية (NVD)، والإرشادات الأمنية لمورِّدي الطرف الثالث والمواقع الخارجية الأخرى لتتبع الثغرات والإصلاحات لمكونات الطرف الثالث كي يتسنى تقديم هذه الإصلاحات للعميل.

الغرض: *تحديد أدوات لتتبع مكونات الأطراف الثالثة المضمنة في المنتجات بحيث يمكن تتبع الثغرات وإصدارها في هذه المكونات.*

النتيجة: *سيفهم موظفو فريق PSIRT مكونات المنتجات وسيتمكنون من تتبع مكونات الأطراف الثالثة داخل المنتجات المشحونة.*

الوظيفة 5.1.6 تتبع جميع مبادرات التدريب

ستحتاج أفرقة التصدي لحوادث أمن المنتجات (PSIRT) إلى تتبع جميع الدورات التدريبية المتاحة لمختلف أصحاب المصلحة. وسيحتاج الفريق إلى التأكد من أن جميع هذه الدورات التدريبية تقدَّم بتواتر معين حين يتغير المشهد الأمني بسرعة كبيرة، وبالتالي تلزم إعادة تعريف الدورات التدريبية والعمليات باستمرار.

الغرض: *التأكد من تتبع جميع الدورات التدريبية لمختلف أصحاب المصلحة.*

النتيجة: *سيعرف موظفو فريق PSIRT أن العديد من أصحاب المصلحة تدربوا على أدوارهم في عملية فريق PSIRT.*

الخدمة 2.6 تدريب فريق التطوير

يشير التطوير الآمن إلى المنهجيات والخطوات التي اتُخذت طوال عملية التطوير والتي صُممت خصيصاً لتقليل عدد وشدة الثغرات في المنتجات والخدمات المتعلقة بالبرمجيات. وبوجود منهاج قوي والتركيز على منهجيات التطوير الآمن، يمكن تقليل الثغرات كثيراً قبل إصدار المنتج وهو أقل تكلفة بكثير من التعامل معها بعد طرح المنتجات بالفعل في السوق.

ويبدأ التطوير الآمن بمتطلبات المنتج ومعماريته. بالإضافة إلى ذلك، تعد استعراضات التصميم الآمنة مفتاحاً لاكتشاف الثغرات المحتملة قبل أن يدخل المنتَج في طور التطوير.

وهناك العديد من الأنشطة التي تشارك في برنامج تطوير آمن، وتقع تفاصيلها خارج نطاق هذه الوثيقة. ويوصى بشدة بوجود برنامج منفصل لإدارة الجهد المناسب بدورة حياة التطوير الآمن. وينبغي أن يتبع هذا البرنامج نموذج برنامج معيار الصناعة المقبول. ويرد مثال على دورة حياة التطوير الآمن في نموذج دورة حياة التطوير الآمن لشركة Microsoft.[14]

الغرض: *تشجيع المنظمة على الحصول على برنامج مناسب لدورة حياة التطوير الآمن (SDL) حيث يدرَّب التطوير على كتابة الشفرة الآمنة واستخدام المبادئ التوجيهية الأمنية الموثقة أثناء إنشاء معمارية المنتَج وتصميمه.*

النتيجة: *ستتمكن أفرقة التطوير من كتابة شفرة آمنة وإصدار منتجات أكثر أمناً.*

ولا يُعتبر التدريب على التطوير الآمن دائماً جزءاً من الجهات التي يخدمها فريق PSIRT ويمكن التعامل معه خارج عملية فريق PSIRT. وعلى أي حال، إنه خطوة مهمة يجب أن ينظر فيها أي مورِّد يهتم بالوضع الآمن لمنتجاته.

الوظيفة 1.2.6 التدريب على عملية فريق PSIRT

يحتاج كل عضو في عملية التطوير إلى فهم سبب وجود عملية فريق التصدي لحوادث أمن المنتجات (PSIRT)، وكيف تعمل، وما الذي يحتاجون لفعله لتطوير المنتجات لدعمها. ففي كثير من الأحيان بعد إصدار المنتَج، تنتقل أفرقة التطوير إلى مشاريع مختلفة وتتضاءل جهود الاستدامة. ويعد تدريب الأفرقة وتزويدها بالأساليب المناسبة لتخزين المعلومات الرئيسية بشأن المنتَج أمراً بالغ الأهمية كي يتصدى فريق PSIRT لمشكلة ثغرات المنتَج تماماً. ويتعين توثيق معلومات مثل من كان مهندس الأمن ومن تولى التطوير ومن تولى الاختبارات كي يتمكن فريق PSIRT من العودة إلى الذين يعرفون أكثر لتقييم المخاطر وإعداد عوامل التخفيف. وينبغي أن يتضمن هذا التوثيق أيضاً أشياء مثل: ما هي مكونات الطرف الثالث الجاري استخدامها، وما هي عملية تحديث المنتج، وما هي السجلات القائمة، وما هي الاستثناءات الأمنية التي سُمح بها وكيف يبلَّغ أصحاب المصلحة. فهذه المعلومات حرجة أيضاً كي يسد فريق PSIRT ثغرة أمنية. وبمجيء ورحيل أعضاء فريق التطوير الجدد يرتدي التدريب التجديدي أهمية بالغة أيضاً.

الغرض: *التأكد من فهم جميع أصحاب المصلحة لعملية فريق PSIRT وكيفية ارتباطها بدورهم في تطوير المنتجات.*

النتيجة: *انتشار ثقافة الأمن بين المطورين وتحسين التعاون في التعامل مع الثغرات.*

الخدمة 3.6 تدريب فريق التحقق

يحتاج المتحققون إلى الاستمرار في مواكبة أحدث أدوات وتقنيات أشياء مثل اختبار الاختراق والمسح الباحث عن ثغرات والفحص العشوائي والاختراق الأخلاقي وغيرها. ويقع تدريب المتحققين على ذلك ضمن دورة حياة التطوير الآمن (SDL) وهو خارج نطاق هذا الوثيقة. ولكن ينبغي لفريق PSIRT تشجيع المنظمة على تشكيل مجموعة تركز على هذا الأمر.

الغرض: *تشجيع المنظمة على اعتماد برنامج مناسب لدورة حياة التطوير الآمن (SDL) تتحدد فيه أدوات اختبار الأمن المناسبة.*

النتيجة: *منتجات عالية الجودة وعلى درجة أعلى من الأمن.*

[14] https://www.microsoft.com/en-us/sdl/

وتماماً مثل التطوير الآمن، لا يُعتبر التدريب على التحقق جزءاً من الجهات التي يخدمها فريق PSIRT ويُتعامل معه خارج عملية PSIRT. بيد أن هذا التدريب يخطو خطوة على نفس القدر من الأهمية وعلى المورِّد تغطيته كجزء من دورة حياة التطوير الآمن (SDL) للمنتجات.

الوظيفة 1.3.6 التدريب على عملية فريق PSIRT

يمكن أن يشارك بعض أعضاء فريق التحقق في اختبار الإصلاحات المطلوبة لسد ثغرات المنتجات. ويحتاج أعضاء الفريق هؤلاء إلى فهم عملية فريق PSIRT، وكيف تعمل، وما هي الأطر الزمنية المتوقعة وما هو دورهم في العملية. ويحتاجون إلى فهم جيد لدورة حياة المنتَج كي يعرفوا الإصدارات المدعومة التي يتعين اختبارها لإصلاح الثغرات. وسيحتاجون أيضاً إلى اختبار الحلول الالتفافية، إن وجدت. وسيكون مهماً لهم أيضاً اختبار إمكانية وقوع انتكاسات.

الغرض: *التأكد من فهم جميع أصحاب المصلحة لعملية فريق PSIRT ومدى ارتباطها بدورهم في التحقق من صحة المنتجات.*

النتيجة: *انتشار ثقافة الأمن بين المتحققين وتحسين التعاون في التعامل مع الثغرات.*

خدمة 4.6 التعليم المستمر لجميع أصحاب المصلحة

سيحتاج جميع أصحاب المصلحة إلى مستوى ما من التدريب والتوعية ببرنامج فريق PSIRT. هناك العديد من أصحاب المصلحة الذين يشاركون في عملية فريق PSIRT من البداية إلى النهاية. لذلك، من المهم تحديد مختلف مجموعات أصحاب المصلحة وتطوير التدريب الخاص باحتياجاتهم.

الغرض: *التأكد من حصول جميع مجموعات أصحاب المصلحة على التدريب أو الوعي الأساسي الذي يحتاجونه لأداء دورهم في برنامج PSIRT.*

النتيجة: *حُسن اطلاع الجهات الداخلية المخدَّمة بحيث تعرف كيف ستعمل مع فريق PSIRT في إدارة قضايا الثغرات الطارئة والخدمات التي سيقدمها فريق PSIRT في مثل هذه المواقف.*

الوظيفة 1.4.6 تدريب الإدارة التنفيذية

عادة ما تشارك هذه المجموعة في إقرار اتصالات الشركة، وفي الوقاية من الثغرات والسياسات الأخرى. وقد تكون موافقة الإدارة مطلوبة أيضاً لإنشاء إرشادات أمنية. وكثيراً أيضاً ما تكون موافقة الإدارة التنفيذية مطلوبة في مواقف حرجة تنطوي على مخاطر عالية أو حضور مرئي كبير أو تبعات جسيمة. ويمكن أن ترغب الإدارة أيضاً في إجراء فحوصات دورية لحالة الوضع الأمني لجميع المنتجات. وبالتالي، من المهم إبلاغ إدارة بعمليات فريق PSIRT.

الغرض: *توعية أفرقة الإدارة بدورها في برنامج فريق PSIRT.*

النتيجة: *إعداد الموافقات التي تتطلب توقيع الإدارة في الوقت المناسب.*

الوظيفة 2.4.6 تدريب الفريق القانوني

يشارك الفريق القانوني في وضع سياسات الشركة الأولية. ويمكن أن تحتوي بعض المشاكل التي يبلغ عنها المكتشفون على مشاكل تتعلق بالتبعات ويمكن أن تتطلب المساعدة من المجموعات القانونية لذلك من المهم تحديد نقاط الاتصال مسبقاً.

الغرض: *توعية الفريق القانوني بدوره في برنامج PSIRT والجداول الزمنية المعنية.*

النتيجة: *إغلاق ملفات المشاكل الأمنية التي تتطلب موافقة قانونية في الوقت المناسب.*

الوظيفة 3.4.6 تدريب فريق الشؤون الحكومية والالتزام

يعنى موظفو الشؤون الحكومية بقضايا الالتزام التنظيمي. لذلك، من المهم تحديد نقاط الاتصال مسبقاً.

الغرض: *توعية فريق الشؤون الحكومية بدوره في برنامج فريق PSIRT.*

__النتيجة:__ تسوية الثغرات الأمنية التي تتطلب الالتزام بمعايير تنظيمية معينة في الوقت المناسب.

الوظيفة 4.4.6 تدريب فريق التسويق

كثيراً ما يكون التسويق معنياً عندما يتعرض اسم العلامة التجارية للخطر. ويمكن لأفرقة التسويق أيضاً أن تستعرض الإرشادات الأمنية كي تُنشر إلى جانبها معلومات التسويق المرتبطة بها. وتشارك هذه الأفرقة كذلك في تسويق الجانب الأمني للمنتجات.

__الغرض:__ توعية أفرقة التسويق بدورها في برنامج فريق PSIRT وتثقيفها بشأن ما يمكن وما لا يمكن ادعاؤه فيما يتعلق بأمن المنتجات.

__النتيجة:__ سيؤدي التنسيق المناسب بين فريق PSIRT وأفرقة التسويق إلى حُسن مواءمة الوضع الأمني الخارجي بين المواد التسويقية والإرشادات الأمنية.

الوظيفة 5.4.6 تدريب فريق العلاقات العامة

يمكن أن تتولى أفرقة العلاقات العامة (PR) مسؤولية عن الرد على منشورات أو مدونات الأمن الخارجية، أو الاستفسارات الصحفية المتعلقة بالثغرات الحرجة في المنتجات. وينبغي تحديد نقاط الاتصال بحيث يمكن إشراك فريق العلاقات العامة إذا دعت الحاجة إلى أي نشر خارجي.

__الغرض:__ توعية أفرقة العلاقات العامة بدورها في برنامج فريق PSIRT.

__النتيجة:__ سيؤدي التنسيق المناسب بين فريق PSIRT وأفرقة العلاقات العامة إلى سلامة الوضع الأمني الخارجي للموِّرد.

الوظيفة 6.4.6 تدريب فريق المبيعات

يمكن أن تدرَّب أفرقة المبيعات على مفاهيم الأمن الأساسية وعلى الاتصالات فيما يتعلق بالأعراف الأمنية. ومن المهم جداً أيضاً أن يعرف مندوبو المبيعات ما يمكن وما لا يمكن البوح به خارجياً. ويوصى بأن يحيل موظفو المبيعات أي مخاوف بشأن الأمن من أصحاب المصلحة/العملاء المحتملين إلى موظفي فريق PSIRT أو موظفي الدعم بدلاً من تناولها مباشرة.

__الغرض:__ توعية أفرقة المبيعات بشأن ما يمكن وما لا يمكن ادعاؤه فيما يتعلق بأمن المنتجات، وأين يذهبون بالأسئلة التي لا يملكون الإجابة عليها.

__النتيجة:__ سيؤدي التنسيق المناسب بين فريق PSIRT وأفرقة المبيعات إلى تلبية توقعات العملاء.

الوظيفة 7.4.6 تدريب فريق الدعم

يجب تدريب أفرقة الدعم على التعامل مع تقارير عن ثغرات أمنية من العميل. ويمكن أن يتدخل فريق PSIRT في بعض الحالات للتعامل مع هذه المشاكل. وينبغي أن ينشر فريق الدعم سياسات تحدد عمر كل منتج والإصدارات المدعومة وما إذا كانت ستصدر إرشادات أمنية أم لا. ويكتفي معظم الموزِّدين بتقديم إرشادات أمنية للإصدارات التي يدعمونها. لذا، تعد هذه السياسات شديدة الأهمية ويجب نشرها على الموقع الإلكتروني للموزِّد كي تكون على مرأى سهل من أصحاب المصلحة. وتقيم أفرقة التصدي لحوادث أمن المنتجات (PSIRT) عادةً علاقة وثيقة مع فريق الدعم كي يفهم نوع المشاكل التي يبلّغ العملاء عنها. وفي بعض الأحيان، يمكن أن يكون المكتشف عميلاً أيضاً لذا يمكن أن تتأرجح معالجة المشكلة بين فريق الدعم وفريق PSIRT.

__الغرض:__ توعية أفرقة الدعم بدورها في عملية PSIRT.

__النتيجة:__ سيؤدي التنسيق المناسب بين فريق PSIRT وأفرقة الدعم إلى تلبية توقعات العملاء والجهة المبلِّغة.

الخدمة 5.6 تقديم آليات الملاحظات التقييمية

تُستخدم المعلومات المكتسبة أثناء تحليل السبب الجذري للحادث لتثقيف الأشخاص المعنيين ومنع ظهور ثغرات مماثلة في المستقبل

الغرض: *تحسين التدريب باستمرار لمواكبة المشهد المتغير بسرعة في صناعة الأمن.*

النتيجة: *سيؤدي الارتقاء بجودة التدريب إلى تحسين التجربة لجميع أصحاب المصلحة.*

الملحق 1: الموارد الداعمة

15 إطار محتوى المعمارية.

16 ISO 31000:2009 إدارة المخاطر - المبادئ والإرشادات

ISO/IEC 27000/2018 تكنولوجيا المعلومات - تقنيات الأمن – أنظمة إدارة أمن المعلومات

17 ISO/IEC 30111:2013 تكنولوجيا المعلومات - تقنيات الأمن - الكشف عن الثغرات

18 ISO/IEC 29147:2014 تكنولوجيا المعلومات - تقنيات الأمن - الكشف عن الثغرات

19 المبادئ التوجيهية والأعراف في التنسيق بشأن الثغرات والكشف عنها بين أطراف متعددة

دليل ومعايير معارف إدارة المشاريع (PMBOK)

15 http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap35.html

16 https://www.iso.org/iso-31000-risk-management.html

17 https://www.iso.org/obp/ui/#iso:std:53231:en

18 https://www.iso.org/obp/ui/#iso:std:iso-iec:29147:ed-1:v1:en

19 https://www.first.org/global/sigs/vulnerability-coordination/multiparty/FIRSTMultiparty-Vulnerability-Coordination-v1.0.pdf

الملحق 2: شكر وتقدير

- MetLife ،Barbara Cosgriff
- Lenovo ،Beverly Finch
- Siemens ،Carl Denis
- Red Hat ،Chris Robinson
- Honeywell ،Jeff Hahn
- Intel ،Jerry Bryant
- Intel ،Josh Dembling
- Broadcom ،Jean-Robert Hountomey
- NetApp ،Kevin Ryan
- Red Hat ،Langley Rock
- Dell Technologies ،Lisa Bradley
- Red Hat ،Peter Allor
- Oracle ،Reshma Banerjee
- Siemens ،Rupert Wimmer
- NVIDIA ،Shawn Richardson
- Johnson Controls ،Steve Brukbacher
- Dell Technologies ،Tania Ward
- SAP ،Vic Chung

الملحق 3: الجداول والرسوم التوضيحية

الملحق 4: محاسن ومساوئ النماذج التنظيمية لفريق التصدي لحوادث أمن المنتجات (PSIRT)

النموذج	الوصف	المحاسن	المساوئ
الموزع	فريق عمليات PSIRT أساسي مصغر يوزع العمل على ممثلين لمختلف المجالات الوظيفية، (من قبيل الدعم والهندسة وإدارة المنتجات)	• مثالي لشركات كبيرة لديها مجموعة منتجات كبيرة ومتنوعة. • تُسدَد تكلفة مهمة فريق PSIRT. • توزيع أعباء العمل على وظائف مختلفة. • قابل للتوسعة لينمو مع نمو مجموعة المنتجات.	• تملك منظمة PSIRT بعض الصلاحيات لتحديد السياسة والاتجاهات العامة. • في كثير من الأحيان لا يتحكم فريق PSIRT مباشرة بالموارد التي تعالج الثغرات وبالتالي فإن سيطرته أقل. • يمكن أن تتقدم المصلحة الفضلى لمجالات المنتجات المختلفة على أنشطة PSIRT.
المركزي	منظمة PSIRT أكبر تضطلع مباشرةفي أنشطة فريق PSIRT (من قبيل إدارة البرنامج والفرز والتعرف والتدارك والاتصالات) بشأن جميع مجالات المنتجات المختلفة.	• مثالي لشركات صغيرة لديها مجموعة منتجات أصغر. • فريق مركزي من خبراء المنتجات ذوي المهارات العالية. • تتخذ منظمة PSIRT كل القرارات بشأن ميزانيات PSIRT وسياساته وموارده. • سيطرة ومساءلة أفضل بشأن الأنشطة التشغيلية لفريق PSIRT.	• لا يُحْسن توسعه مواكبة نمو مجموعة المنتجات. • يحتاج اتخاذ القرارات الكبرى فيه إلى تعاون أو موافقة مدير وظيفي مختلف. • التكلفة العالية للحفاظ على فريق مركزي ذي مهارات متخصصة.
الهجين	هذا لفيف يتضمن خصائص النموذجين الموزَّع والمركزي معاً		

الملحق 5: أنواع أفرقة التصدي للحوادث

- **الفريق الوطني للتصدي للحوادث الأمنية الحاسوبية (CSIRT)** - يشير الفريق الوطني للتصدي للحوادث الأمنية الحاسوبية إلى كيان تشكله هيئة وطنية ليقوم بالتنسيق على المستوى الوطني للتصدي لحوادث الأمن السيبراني. وتشمل الجهات التي يخدمها الفريق عموماً جميع الإدارات والوكالات الحكومية، وهيئات إنفاذ القانون والمجتمع المدني. وهو أيضاً، بشكل عام، السلطة التي تتفاعل مع أفرقة التصدي للحوادث الأمنية الحاسوبية الوطنية في البلدان الأخرى، وكذلك مع الجهات الفاعلة الإقليمية والدولية.
- **فريق التصدي للحوادث الأمنية الحاسوبية القطاعي/المعني بالبنية التحتية الحرجة** - هو الفريق المسؤول عن مراقبة حوادث الأمن السيبراني المتعلقة بقطاع معين (مثل الطاقة والاتصالات والتمويل)، وعن إدارتها والتصدي لها.
- **الفريق المؤسسي (التنظيمي) للتصدي للحوادث الأمنية الحاسوبية** - يشير الفريق المؤسسي للتصدي للحوادث الأمنية الحاسوبية إلى الفريق المسؤول عن مراقبة حوادث الأمن السيبراني التي تؤثر على البنى التحتية والخدمات الداخلية لتكنولوجيا المعلومات والاتصالات في منظمة محددة، وعن إدارتها والتعامل معها.
- **فريق التصدي الإقليمي/متعدد الأطراف** للحوادث الأمنية الحاسوبية - يشير فريق التصدي **الإقليمي/متعدد الأطراف** للحوادث الأمنية الحاسوبية إلى فريق أو نفر تضم عضويته ممثلين عن دوائر مختلفة ويتولى المسؤولية عن مراقبة حوادث الأمن السيبراني المتصلة بمنطقة معينة أو عدد من المنظمات، وعن إدارة هذه الحوادث والتصدي لها.
- **فريق التصدي لحوادث أمن المنتجات (PSIRT)** - فريق التصدي لحوادث أمن المنتجات هو فريق داخل كيان تجاري (مَنفذ بيع عادة) يدير تلقي المعلومات بشأن الثغرات الأمنية المتعلقة بمنتجات أو خدمات تتعاطى بها المنظمة تجارياً، ويدير التحقيق فيها والإبلاغ عنها داخلياً وللعموم.

مسرد مصطلحات

- **الإجراءات** - قائمة بكيفية القيام بشيء ما على مستويات مختلفة من التفاصيل/النضج
- **القدرة** – نشاط قابل للقياس يمكن القيام به كجزء من أدوار منظمة ومسؤولياتها. ولأغراض إطار خدمات أفرقة التصدي للحوادث الأمنية، يمكن أن تعرَّف القدرات كالخدمات الأوسع، أو كالوظائف المطلوبة أو المهام أو الإجراءات.
- **السعة** - عدد العمليات أو الوقائع المتزامنة لقدرة خاصة يمكن أن تنفذها المنظمة قبل أن تتعرض لنوع ما من استنفاد الموارد.
- **تعداد الثغرات الشائعة (CVE)** - 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)**[20] - درجة رقمية تعكس مدى خطورة الثغرة.
- **التعداد المشترَك لنقاط الضعف (CWE)**[21] - قائمة رسمية بأنواع ضعف البرمجيات أنشئت:
  - لتكون لغة مشتركة لوصف ضعف أمن البرمجيات في المعمارية أو التصميم أو الشفرة؛
  - لتكون بمثابة مسطرة قياس معيارية لأدوات أمن البرمجيات تستهدف هذه الثغرات؛
  - لتقدم خط أساس معياري مشترك لتحديد الضعف والتخفيف والجهود الوقائية.
- قانون نقل التأمين الصحي والمساءلة (HIPPA)[22] - قانون أمريكي وُضع لتقديم معايير الخصوصيات من أجل حماية السجلات الطبية للمرضى والمعلومات الصحية الأخرى المقدمة للخطط الصحية والأطباء والمستشفيات ومقدمي الرعاية الصحية الآخرين.
- **مؤشر الأداء الرئيسي (KPI)**[23] - 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 الإجراءات أو المهام أو في مجموع الوظائف أو الخدمات.
- **معيار أمن بيانات صناعة بطاقات الدفع (PCI DSS)**[24] - هو معيار أمن المعلومات يعزز سلامة بيانات حامل البطاقة في جميع أنحاء العالم..
- **المهام** - قائمة الإجراءات التي يجب تنفيذها لإنجاز المهمة

---

20 https://www.first.org/cvss/
21 https://cwe.mitre.org/about/index.html
22 https://www.medicinenet.com/script/main/art.asp?articlekey=31785
23 https://www.klipfolio.com/resources/articles/what-is-a-key-performance-indicator
24 https://www.pcisecuritystandards.org/pci_security/