الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

X.1500

(2011/04)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

تبادل معلومات الأمن السيبراني – تبادل معلومات مواطن الضعف/الحالة

نظرة عامة على تبادل معلومات الأمن السيبراني

التوصيـــة ITU-T X.1500

ITU-T

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليـــل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	X.1229–X.1200
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة	
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1339–X.1310
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	**X.1539–X.1520**
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580

لمزيد من التفاصيل، يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصيـــة ITU-T X.1500

نظرة عامة على تبادل معلومات الأمن السيبراني

ملخص

تشرح التوصية ITU-T X.1500 تقنيات تبادل معلومات الأمن السيبراني. ويمكن استعمال هذه التقنيات فرادى أو جماعات حسب المطلوب أو المناسب، لتعزيز الأمن السيبراني من خلال عملية لتبادل المعلومات تتسم بالتماسك والشمول والعالمية والضمان والتوقيت المناسب. ولا يوجد أي التزام بتبادل المعلومات المتداولة ولا بوسائل الحصول عليها أو استعمالها النهائي. وتبادل معلومات الأمن السيبراني (CYBEX) هو أحد عناصر توفير الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات.

التسلسل التاريخي

الصيغة	التوصية	تاريخ الموافقة	لجنة الدراسات
1.0	ITU-T X.1500	2011/04/20	17

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA)، التي تجتمع مرة كل أربع سنوات، المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

مقـــدمة

هذه التوصية مصممة بحيث يمكن مواءمتها وتوسيع نطاقها بحيث تكون غير نهائية بما يسمح بتطبيق عدد كبير من التقنيات – التي لا يزال بعضها يشهد تطوراً مستمراً وفي مراحل مختلفة من الاكتمال – على حالات مختلفة لتعزيز عملية تبادل معلومات الأمن السيبراني المتعلقة بالبنية التحتية للاتصالات/تكنولوجيا المعلومات والاتصالات وأجهزتها وخدماتها. وستخضع هذه التوصية للمراجعة الدورية مع تطور هذه التقنيات – فيما ستنشر التوصيات التي يُرى أنها ملائمة ضمن سلسلة التوصيات ITU-T X.1500 لقطاع تقييس الاتصالات.

والتقنيات المشمولة بهذه التوصية يتوقع أن توفر لمنظمات الاتصالات/تكنولوجيا المعلومات والاتصالات بما فيها أفرقة الاستجابة للحوادث الحاسوبية (CIRT)، سواء داخل سلطاتها القضائية أو بين هذه السلطات:

أ) معلومات تمكن من صنع القرارات وتحديد الأعمال التي من شأنها التعزيز الكبير لسرية مرافق وخدمات الاتصالات/تكنولوجيا المعلومات والاتصالات العالمية وسلامتها وتيسرها؛

ب) المعلومات التي تسهل عمليات وضوابط التعاون الآمن التي تحسن من مستوى الضمان في عملية تبادل المعلومات بين المنظمات؛

ج) نهج متماسك لإدارة معلومات الأمن السيبراني وتبادلها على الصعيد العالمي؛

د) تحسين الوعي والتعاون الأمنيين للحد من التهديدات والهجمات والبرمجيات الضارة السيبرانية.

وتشمل هذه التقنيات:

- إعداد معلومات الأمن السيبراني لأغراض التبادل؛
- تحديد واكتشاف معلومات وكيانات الأمن السيبراني؛
- إبرام اتفاق ثقة وسياسات بين الكيانات القائمة بعملية التبادل؛
- عمليات الطلب والاستجابة المتعلقة بمعلومات الأمن السيبراني؛
- ضمان سلامة عملية تبادل معلومات الأمن السيبراني؛

وتصنف هذه التقنيات إلى "مجموعات":

- مواطن الضعف والتعرض والحالة.
- الحدث والحدث العرضي ووسائل الكشف.
- سياسة تبادل المعلومات.
- التحديد والاكتشاف ومظاهر الشك.
- ضمان الهوية.
- بروتوكولات التبادل.

التوصيـــة ITU-T X.1500

نظرة عامة على تبادل معلومات الأمن السيبراني

1 مجال التطبيق

تقدم هذه التوصية نموذجاً لتبادل معلومات الأمن السيبراني (CYBEX) وتناقش التقنيات التي يمكن استعمالها لتسهيل عملية التبادل تلك. ويمكن استعمال هذه التقنيات فرادى أو مجموعات حسب المطلوب والملائم لتعزيز الأمن السيبراني من خلال عملية لتبادل المعلومات تتسم بالتماسك والشمول والعالمية والضمان والتوقيت المناسب. ولا يوجد أي التزام بتبادل المعلومات أو بشأن وسائل الحصول عليها أو استعمالها النهائي. وتتضمن التقنيات عملية منظمة لاكتشاف معلومات الأمن السيبراني مع إمكانية تداولها بينياً على الصعيد العالمي بصورة تسمح بالتطور المستمر لتأمين التطور الكبير للأنشطة والمواصفات الذي تشهده منتديات عديدة للأمن السيبراني. وتبادل معلومات الأمن السيبراني (CYBEX) هو أحد عناصر توفير الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات.

وتتضمن هذه التوصية الوظائف الأساسية التالية التي يمكن استعمالها كل على حدة أو مجتمعة حسب الحالة وتوسيع نطاقها بما يزيد من إمكانية تبادل معلومات الأمن السيبراني:

- إعداد معلومات الأمن السيبراني لأغراض التبادل؛
- تحديد واكتشاف معلومات وكيانات الأمن السيبراني؛
- إبرام اتفاق ثقة وسياسات بين الكيانات القائمة بعملية التبادل؛
- عمليات الطلب والاستجابة المتعلقة بمعلومات الأمن السيبراني؛
- ضمان سلامة عملية تبادل معلومات الأمن السيبراني.

وحسب السياسات المتفق عليها والقوانين واللوائح المطبقة، فإن وسائل حيازة المعلومات واستعمالاتها تقع تحديداً خارج نطاق هذه التوصية ولا تتم مناقشتها فيها. وقد تفرض بعض اللوائح والتشريعات الوطنية والإقليمية المحددة تنفيذ آليات لحماية المعلومات التي تؤدي إلى تعرف هوية أصحابها. والتقنيات الخاصة بحماية هذه المعلومات الموصوفة في هذه التوصية أو عملية تبادلها لا تخولها هذه التوصية.

2 المراجع

لا توجد.

3 التعاريف

1.3 مصطلحات معرَّفة في وثائق أخرى

تستعمل هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 الأمن السيبراني [التوصية b-ITU-T X.1205]: مجموع الأدوات والسياسات ومفاهيم الأمن وتحفظات الأمن والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وآليات الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية وأصول المؤسسات والمستعملين. وتشمل أصول المؤسسات والمستعملين أجهزة الحوسبة الموصولة بالشبكة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات ومجموع المعلومات المنقولة و/أو المحفوظة في البيئة السيبرانية.

ويسعى الأمن السيبراني إلى تحقيق خصائص أمن أصول المؤسسة والمستعملين والحفاظ عليها وحمايتها من المخاطر الأمنية ذات الصلة في البيئة السيبرانية. وتضم الأهداف العامة للأمن التيسر والسلامة (التي قد تضم الاستيقان وعدم الرفض والسرية).

ملاحظة – قد تفرض بعض اللوائح والتشريعات الوطنية المحددة استعمال آليات لحماية المعلومات التي تؤدي إلى تعرف هوية أصحابها.

2.1.3 الحادث الأمني [ITU-T E.409]: أي حدث سلبي يمكن أن يهدد بعض الجوانب الأمنية.

2.3 مصطلحات معرفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالي:

1.2.3 الضمان: درجة الثقة في أن عملية أو معلومة ما تفي بخصائصها أو أهدافها المعرَّفة.

2.2.3 بروتوكول التبادل: مجموعة من القواعد والأنساق التقنية تعمل على تنظيم تبادل المعلومات بين كيانين.

3.2.3 سياسة تبادل المعلومات: الشروط والمقتضيات المرتبطة باستعمال معلومات الأمن السيبراني وتبادلها.

4.2.3 حالة النظام: الوضع الراهن لأي كيان أو نظام، بما في ذلك المعلومات التي على غرار تشكيلته أو استعمال ذاكرته أو أي بيانات أخرى ذات صلة بالأمن السيبراني.

5.2.3 تعرّض: (مصطلح مواءم مع التوصية [b-ITU-T X.800]) أي نقطة يمكن استغلالها لانتهاك نظام ما أو المعلومات التي يحتوي عليها.

6.2.3 نقطة ضعف: قصور أو نقص لا يُعتبر تعرضاً بحد ذاته، ويمكن، في مرحلة ما أن يصبح تعرضاً، أو يمكن أن يساهم في إدخال ثغرات أمنية أخرى.

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

ARF نسق نتائج التقييم أو نسق الإبلاغ عن الموجودات (حسب السياق) *(Assessment Results Format)*

BEEP بروتوكول تبادل موسع الفدرات *(Blocks Extensible Exchange Protocol)*

CA سلطة منح التراخيص *(Certification Authority)*

CAPEC تعداد نماذج الاعتداءات الشائعة وتصنيفها *(Common Attack Pattern Enumeration and Classification)*

CCE تعداد التشكيلات الشائعة *(Common Configuration Enumeration)*

CEE التعبير عن الحدث الشائع *(Common Event Expression)*

CEEE تبادل التعبير عن الحدث الشائع *(Common Event Expression Exchange)*

CIRT فريق الاستجابة للحوادث الحاسوبية *(Computer Incident Response Team)*

CPE تعداد المنصات الشائعة *(Common Platform Enumeration)*

CVE مواطن الضعف والتعرض الشائعة *(Common Vulnerabilities and Exposures)*

CVSS نظام تقييم مواطن التعرض الشائعة *(Common Vulnerability Scoring System)*

CWE تعداد مواطن الضعف الشائعة *(Common Weakness Enumeration)*

CWSS نظام تقييم مواطن الضعف الشائعة *(Common Weakness Scoring System)*

CYBEX تبادل معلومات الأمن السيبراني *(Cybersecurity Information Exchange)*

CYIQL لغة الاستفهام عن معلومات الأمن السيبراني *(Cybersecurity Information Query Language)*

DDoS الرفض الموزع للخدمة *(Distributed Denial of Service)*

EVC شهادات ممتدة الصلاحية *(Extended Validation Certificates)*

EVCERT شهادة ممتدة الصلاحية *(Extended Validation Certificate)*

HTTP بروتوكول نقل النص الموسوعي *(Hypertext Transfer Protocol)*

IC دارة متكاملة *(Integrated Circuit)*

ICT تكنولوجيا المعلومات والاتصالات *(Information and Communications Technology)*

IDS نظام كشف الدخلاء

IODEF نسق تبادل وصف الشيء العرضي *(Incident Object Description Exchange Format)*

IPS نظام منع دخول الدخلاء

IT تكنولوجيا المعلومات *(Information Technology)*

MAEC تعداد نعوت البرمجيات الخبيثة وتحديد خصائصها *(Malware Attribute Enumeration and Characterization)*

OID معرف هوية الشيء *(Object Identifier)*

OS نظام التشغيل *(Operating System)*

OVAL لغة التعرض والتقييم المفتوحة *(Open Vulnerability and Assessment Language)*

RID دفاع بين الشبكات في الوقت الفعلي *(Real-time Inter-network Defense)*

SCAP بروتوكول أتمتة المحتوى الأمني *(Security Content Automation Protocol)*

SOAP بروتوكول النفاذ البسيط إلى الأشياء *(Simple Object Access Protocol)*

TLP بروتوكول الإشارات الضوئية للحركة *(Traffic Light Protocol)*

TLS أمن طبقة النقل *(Transport Layer Security)*

TNC توصيل شبكي موثوق *(Trusted Network Connect)*

TPM وحدة نمطية موثوقة من المنصة *(Trusted Platform Module)*

XCCDF نسق وصف القائمة المرجعية القابل للتوسع في التشكيلة *(eXensible Configuration Checklist Description Format)*

5 الاصطلاحات

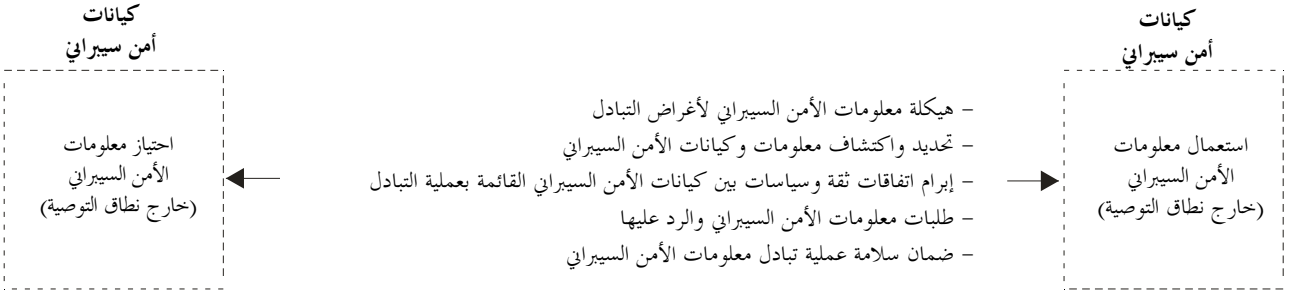
عند استخدام مصطلح "معيار" أو "معايير" في هذه التوصية بالمعنى العام، ينبغي تفسير ذلك على أنه يشمل: المعايير والمواصفات والتوصيات.

6 المفهوم الأساسي – تقنيات تبادل معلومات الأمن السيبراني (CYBEX)

هذه التوصية الخاصة بتبادل معلومات الأمن السيبراني وضعت لكي تقدم وصفاً بسيطاً محدد الأهداف للتقنيات التي يمكن أن تستعملها كيانات الأمن السيبراني في تبادل معلومات الأمن السيبراني باستخدام الأساليب التي توفر مستوى مناسباً من الضمان. وتتألف هذه الكيانات عادة من منظمات أو أشخاص أو أجهزة أو عمليات لديها أو تبحث عن معلومات بشأن الأمن السيبراني. وتكون هذه الكيانات في أغلب الأحوال أفرقة الاستجابة للحوادث الحاسوبية وشركات تشغيل أو شركات بيع المعدات أو البرمجيات أو الأنظمة القائمة على الشبكات.

وتبادل معلومات الأمن السيبراني ذو قيمة كبيرة بالنسبة لتحقيق أمن سيبراني معزز وبالنسبة لتحقيق حماية البنى التحتية فضلاً عن المساهمة في الوظائف الأساسية التي تقوم بها أفرقة الاستجابة للحوادث الحاسوبية.

ويمكن لتبادل معلومات الأمن السيبراني أن يجرى داخل مجتمعات ثقة مقسمة إلى حد كبير إلى جهات مستقلة تعتنق مبادئ الحاجة إلى المعرفة القائمة على سياسات متفق عليها سلفاً، وكذلك داخل الميدان العمومي. ومن الأمثلة النمطية لأنواع معلومات الأمن السيبراني التي يتم تبادلها بين الكيانات، المعرفة بالتهديدات ومواطن الضعف والحوادث والمخاطر وإجراءات التخفيف ووسائل العلاج المرتبطة بها. والتقنيات ذات الصلة الواردة في هذه التوصية مقصود بها تسهيل عملية تبادل هذه المعلومات وبالتالي تعزيز الأمن السيبراني.



الشكل 1 – نموذج لعملية تبادل معلومات الأمن السيبراني

النموذج العام لتبادل معلومات الأمن السيبراني المستعمل في هذه التوصية والمبين في الشكل 1 يتكون من الوظائف الأساسية التي يمكن استعمالها منفصلة أو مجمعة حسب الحالة، ويمكن توسيعها حسب الحاجة لتسهيل عمليات التبادل المضمونة لمعلومات الأمن السيبراني. وهذه الوظائف هي:

- هيكلة معلومات الأمن السيبراني لأغراض التبادل؛
- تحديد واكتشاف معلومات وكيانات الأمن السيبراني؛
- إبرام اتفاقات ثقة وسياسات بين كيانات الأمن السيبراني القائمة بعملية التبادل؛
- طلبات معلومات الأمن السيبراني والرد عليها؛
- ضمان سلامة عملية تبادل معلومات الأمن السيبراني.

ويشرح القسم 7 تقنيات إنجاز هذه الوظائف.

وقد يكون تبادل معلومات الأمن السيبراني ثنائي الاتجاه. وثنائية الاتجاه هذه تسمح لطلبات وردود بشأن معلومات محققة بما يسهل الحصول على مستويات الضمان المطلوبة بين الأطراف أو بتقديم ترخيص بالتزويد.

وطبقاً لسياسات متفق عليها وحسب القوانين واللوائح السارية، فإن وسائل احتياز المعلومات فضلاً عن استعمالها تقع تحديداً خارج نطاق هذه التوصية ولا يجري تناولها فيها. فمثلاً، بعض التطبيقات المتخصصة لتبادل معلومات الأمن السيبراني مثل تتبع أصل مصادر الهجمات قد تحتاج إلى تطبيق آليات محددة بالتطبيق تسمح لسلسلة متكررة من الطلبات والردود بالحصول على المعلومات المطلوبة. بيد أن هناك تطبيقات أخرى مثل جعل الأمن السيبراني موضوع يمكن قياسه وإدارته عن طريق استعمال قدرات الأتمتة الأمنية، تقع ضمن نطاق هذه التوصية. وهذه الأنماط وغيرها من حالات الاستعمال يمكن تسهيلها عن طريق التقنيات المدرجة في هذه التوصية. ولا تزكي هذه التوصية لا التقنيات المدرجة فيها ولا تبادل معلومات الأمن السيبراني المتصلة بها؛ حيث إن هناك تقنيات أخرى قد تكون مناسبة.

7 تقنيات تبادل معلومات الأمن السيبراني المهيكلة

لتبادل معلومات الأمن السيبراني بين أي كيانين، يجب هيكلة التبادل ووصفه بشكل متسق يمكن لهذين الكيانين فهمه. والهدف من CYBEX هو تسهيل تبادل معلومات الأمن السيبراني التي تتضمن "قوائم تعداد مشتركة" أي قوائم مرتبة لقيم موضوعة بشكل جيد لمعلومات من نفس النمط من البيانات. وتسمح قوائم التعداد المشتركة هذه بربط قواعد البيانات وغيرها من القدرات الموزعة ببعضها وتسهيل المقارنات المتعلقة بالأمن السيبراني.

ولأغراض إنجاز هذه التبادلات، تتضمن معلومات الأمن السيبراني معلومات أو معارف مهيكلة تتعلق بما يلي:

- "حالة" المعدات أو البرمجيات أو الأنظمة القائمة على الشبكة فيما يتعلق منها بالأمن السيبراني، والثغرات الأمنية خاصة؛
- الأدلة القضائية المتعلقة بالوقائع أو الأحداث؛
- الوسائل الحدسية المُساعِدة والتواقيع المستقاة من التجربة؛
- الكيانات المشاركة في الأمن السيبراني؛
- مواصفات تبادل المعلومات المتعلقة بالأمن السيبراني بما في ذلك الوحدات، والمخططات، والشروط والأحكام، والأرقام المخصصة؛
- الهويات ونعوت الضمان لكل المعلومات المتعلقة بالأمن السيبراني؛
- متطلبات التنفيذ ومبادئه التوجيهية وممارساته.

وباعتبارها وسيلة لوصف النعوت المطلوبة لعملية تبادل معلومات الأمن السيبراني بوجه عام، رُتبت قدرات المعلومات المهيكلة في ست "مجموعات" من التقنيات لمجموعات تبادل معلومات الأمن السيبراني المختلفة. وهي كالتالي:

- مواطن الضعف والثغرات الأمنية والحالة؛
- الحدث والحادث العرضي والوسائل الحدسية المُساعِدة؛
- سياسات تبادل المعلومات؛
- التحديد والاكتشاف والاستجواب؛
- ضمان الهوية؛
- بروتوكول التبادل.

وهذه المجموعات ما هي إلا تصنيفات واسعة ويمكن لقدرات إحدى المجموعات أن تستعمل فعلياً في واحدة أو أكثر من المجموعات الأخرى، وذلك حسب التطبيق.

ويرد وصف كل مجموعة من المجموعات المدرجة أعلاه بالتفصيل في الفقرات الفرعية أدناه. ويقدم كل وصف لهذه المجموعات نظرة عامة عن دورها في CYBEX مع ذكر التقنيات الخاصة بإنجاز هذا الدور. ومن غير المزمع أن تكون أي من التقنيات المحددة ملزمة؛ بل هي خلافاً لذلك توضح ببساطة التقنيات التي يُرى أنها تتسق مع أغراض المجموعة المعنية. ويتعين أن يتم اختيار المعالجة بدرجة من التخصص لمجتمع المستعمل "المالك" والفوائد العالمية التي تعود من عملية الاستيراد.

وتحدد تقنيات CYBEX الواردة في هذه التوصية صفيفاً من التقنيات التكميلية التي تمكن من تفعيل هذه الحالات وتسهيلها.

وتشرح البقية الباقية من هذه الفقرة والتذييل I المرتبط بها كل مجموعة مع نظرة عامة بشأن دور كل منها ضمن CYBEX وتدرج تقنيات تنفيذ كل مجموعة. والمراجع غير معيارية وترد بتفصيل أكبر في البيبليوغرافيا الواردة في نهاية هذه التوصية.

يجب على منفذي تقنيات المجموعات ومستعمليها الالتزام بكافة القوانين واللوائح والسياسات الوطنية والإقليمية المطبقة.

1.7 مجموعة التبادل الخاصة – بمواطن الضعف ومواطن التعرض والحالة

تدعم القدرات التمكينية المرتبطة بمجموعة تبادل معلومات مواطن الضعف والتعرض و/أو إجراء تقييم لحالة الأنظمة والتطبيقات.

ويقدم الجدول 1.I قائمة بالقدرات التمكينية التي تمثل الأنواع التي بإمكانها أن تسهل دعم تبادل معلومات مواطن الضعف والتعرض والحالة.

2.7 مجموعة تبادل معلومات – الحدث والحادث العرضي والوسائل الحدسية المساعدة

تدعم القدرات التمكينية المرتبطة بمجموعة تبادل معلومات الحدث والحادث العرضي والوسائل الحدسية المساعدة تبادل المعلومات المتعلقة بالأحداث أو الحوادث العرضية أو الوسائل الحدسية المساعدة التي يتم رصدها.

ويقدم الجدول 2.I قائمة بالقدرات التمكينية التي يمكنها أن تسهل دعم تبادل معلومات الأحداث أو الحوادث العرضية أو الوسائل الحدسية المساعدة التي يتم رصدها بشكل منظم بين أفرقة الاستجابة للحوادث الحاسوبية والهيئات الأخرى. ويمكن الاستفادة من تبادل المعلومات هذا لاستنباط ردود شاملة على الهجمات وتقلل من مواطن الضعف والتعرض القائمة.

3.7 مجموعة تبادل – سياسات تبادل المعلومات

تدعم القدرات التمكينية المرتبطة بمجموعة تبادل سياسات تبادل المعلومات تبادل معلومات الأمن السيبراني واستعمالها بين الكيانات والمتعلقة بالشروط والمقتضيات المرتبطة بالمعلومات الجاري تبادلها. وقد يرتبط هذا المفهوم بالمعلومات المحددة الجاري تبادلها أو بصنف أوسع من المعلومات التي تتعلق أو ترتبط بالكيانات المشاركة. وحسب ما تمليه الظروف، يفضل تقديم مذكرة بهذه السياسات إلى الكيانات المشاركة. ويجوز أن تأخذ هذه المذكرة عدة أشكال وترسل مشفوعة بالمعلومات أو تقدم منفصلة من خلال آلية للرد على الاستجواب.

ويقدم الجدول 3.I قائمة بالقدرات التمكينية التي تمثل الأنواع التي يمكنها تسهيل تبادل معلومات السياسات بين كيانات الأمن السيبراني. ويلاحظ أن المتطلبات والبروتوكولات الخاصة بتبادل السياسات مستمرة في الظهور في منتديات تبادل أمن المعلومات وينبغي توخي الحذر من أجل ضمان تنفيذها على الوجه الأمثل.

4.7 مجموعة تعرف الهوية والكشف والاستجواب

إن مجموعة القدرات التمكينية المرتبطة بتحديد الهوية والاكتشاف والاستفسار تدعم عمليات تحديد الهوية والاكتشاف والاستفسار.

توجد مصالح مشتركة بين مجتمعات الأمن السيبراني فيما يتعلق بمعرفات هوية الأمن السيبراني وتكوينها وإدارتها والكشف عنها والتحقق منها واستعمالها. ومن بين هذه المصالح:

- تعزيز قيمة معلومات الأمن السيبراني بتمكين التبادل على نطاق واسع لمعلومات الأحداث ذات الصلة وتحليل الأحداث عبر فترات زمنية طويلة.
- تعزيز أمن عمليات تبادل معلومات الأمن السيبراني بإتاحة الحصول على معلومات معرفات الهوية لأغراض التحقق مع معرفة السياسات ذات الصلة.
- تعزيز مرونة عمليات تبادل معلومات الأمن السيبراني بإتاحته للحصول على معلومات جديدة أو إضافية ترتبط بالرسالة، كحالة المعلومات مثلاً.

وقد ترغب منظمات الأمن السيبراني المختلفة في تطبيق بروتوكولات مشتركة للأمن السيبراني لالتقاط المعلومات المتعلقة بحالة النظام ومواطن الضعف والأدلة القانونية للحوادث والحلول الحدسية لها في التطبيقات التشغيلية وتبادل هذه المعلومات. وحيث

إن هذه المعلومات تتاح من الكثير من المصادر المختلفة، ينبغي للمنفذين تنسيق الكيفية التي يقومون من خلالها بتحديد منظمات الأمن السيبراني والثقة وسياسات تبادل المعلومات والمعلومات نفسها التي يتم تبادلها أو نشرها.

وربما يجعل وجود معرف هوية متفرد عالمياً يُستعمل في عمليات تبادل معلومات الأمن السيبراني على الصعيد العالمي، من الضروري أن يتسم بالخصائص التالية:

- البساطة وسهولة الاستعمال والمرونة وقابلية التوسع والقدرة على الترقي والنشر؛
- إدارة موزعة لمخططات معرفات الهوية المتنوعة؛
- اعتمادية طويلة الأجل لسجلات معرفات الهوية وتوفر أدوات عالية الأداء لاكتشاف المعلومات المرتبطة بأي معرف هوية معين.

ويقدم الجدول 4.I قائمة بالقدرات التمكينية التي تمثل أنواع يمكن أن تسهل عمليات تحديد منظمات الأمن السيبراني واكتشاف معلومات الأمن السيبراني والاستجواب بشأنها.

5.7 مجموعة ضمان الهوية

إن مجموعة القدرات التمكينية المرتبطة بمجموعة ضمان الهوية تدعم ضمان الهوية.

يمكن للتبادل الفعلي للمعلومات المهيكلة في إطار CYBEX أن يتم بالكثير من الأساليب المختلفة – سواء عبر شبكة أو من خلال النقل المادي. ومن العناصر الرئيسية في هذا التبادل الثقة – الثقة في هوية الأطراف فضلاً عن المعلومات الجاري نقلها.

ويقدم الجدول 5.I قائمة بالقدرات التمكينية التي تمثل الأنواع التي يمكنها دعم ضمان الهوية.

6.7 مجموعة بروتوكول التبادل

تشمل القدرات التمكينية داخل مجموعة بروتوكول التبادل بروتوكولات التبادل التي يمكن استخدامها في مختلف سياقات تبادل المعلومات المتعلقة بالأمن السيبراني. ويتطلب التبادل الآمن للمعلومات توليفة من البروتوكولات المذكورة أدناه. ويوفر الدفاع بين الشبكات في الوقت الفعلي (RID) إطار مراسلات لتبليغ معلومات الحوادث والسياسات المرتبطة بتلك المعلومات. ورسائل RID المغلِّفة لوثائق أحداث نسق تبادل وصف الشيء العرضي، IODEF، (وكذلك أي توسعات لنسق IODEF) تتضمن خيارات النقل المدرجة لبروتوكولات BEEP وSOAP وHTTPS. ويمكن الاستعاضة عن نقل رسائل RID (البروتوكول الأولي الذي وُضع لنقل RID) ببروتوكول SOAP أو BEEP أو بروتوكولات مستقبلية حال إعدادها. وترد الاعتبارات الأمنية والخصوصية في RID لتمكين فصل المراسلات عن النقل.

ويقدم الجدول 6.I قائمة بالقدرات التمكينية التي تمثل أنواع بروتوكولات التبادل التي يمكن أن تستخدم لتبادل المعلومات.

التذييل I

التقنيات المهيكلة لتبادل معلومات الأمن السيبراني

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

الجدول 1.I – تقنيات مجموعة تبادل معلومات مواطن الضعف ومواطن التعرض والحالة

التقنيـــة	الوصـــف	المراجـــع
مواطن الضعف والتعرض الشائعة (CVE)	مواطن الضعف والتعرض الشائعة عبارة عن طريقة لتحديد وتبادل معلومات مواطن الضعف والتعرض الأمنية وهي تهدف إلى توفير معرفات مشتركة للمشكلات المعروفة للجمهور. ويتمثل الهدف من تقنية CVE في تسهيل تبادل البيانات عبر قدرات معرضة منفصلة (أدوات ووسائل تخزين وخدمات) باستخدام "قوائم التعداد المشتركة هذه. وهذه التقنية مصممة بحيث تسمح بربط قواعد بيانات مواطن التعرض وغيرها من الموارد ببعضها وتسهيل مقارنة الأدوات والخدمات الأمنية. ولذلك، لا تتضمن تقنية CVE معلومات لكل المخاطر أو الآثار أو معلومات بشأن تداركها أو معلومات تقنية مفصلة. حيث لا تشمل هذه التقنية إلا رقم معرف هوية قياسي مع مؤشر للحالة ووصف مختصر وإحالات إلى تقارير التعرض والجهات الاستشارية ذات الصلة. والغرض من تقنية CVE أن تكون شاملة فيما يخص جميع مواطن الضعف والتعرض المعروفة لدى العموم. ففي حين أن هذه التقنية مصممة بحيث تحتوي على معلومات مكتملة، فإن التركيز الأساسي لها ينصب على تحديد مواطن الضعف والتعرض المكتشفة بالأدوات الأمنية إضافة إلى تحديد أي مشكلات جديدة تصبح شائعة للجمهور وفي النهاية التصدي لأي مشكلات أمنية أقدم في حاجة إلى التصديق عليها.	التوصية [b-ITU-T X.1520]
نظام تقييم مواطن التعرض الشائعة (CVSS)	توفر عملية النظام CVSS إطاراً مفتوحاً لتوصيل خصائص وآثار مواطن التعرض الخاصة بتكنولوجيا المعلومات والاتصالات. ويتألف النظام CVSS من ثلاث مجموعات: مجموعة أساس ومجموعة زمنية ومجموعة بيئية. وتنتج كل مجموعة علامة تقييم تتراوح من صفر إلى 10 ومتجهاً وتمثيل نصي مضغوط يعكس القيم المستعملة لاشتقاق العلامة. وتمثل المجموعة أساس السمات المتأصلة لموطن التعرض. وتعكس المجموعة الزمانية خصائص موطن التعرض المتغيرة مع الزمن. فيما تمثل المجموعة البيئية خصائص موطن التعرض التي تنفرد بها بيئة المستعمل. ويمكن النظام CVSS مديري تكنولوجيا المعلومات والاتصالات وموردي نشرات مواطن التعرض وبائعي الخدمات الأمنية وبائعي التطبيقات والباحثين من الاستفادة جميعاً من خلال اعتماد لغة مشتركة لتقييم مواطن تعرض تكنولوجيا المعلومات والاتصالات.	التوصية [b-ITU-T X.1521]
تعداد مواطن الضعف الشائعة (CWE)	تعداد مواطن الضعف الشائعة عبارة عن عملية لتحديد وتبادل مجموعة موحدة وقابلة للقياس من مواطن الضعف الخاصة بالبرمجيات. وتتيح عملية CWE المجال أمام مناقشة الأدوات والخدمات الأمنية الخاصة بالبرمجيات ووصفها والاختيار فيما بينها واستعمالها بصورة أكثر فعالية، تمكن من التوصل إلى مواطن الضعف هذه في شفرة المصدر وأنظمة التشغيل. وتسمح العملية كذلك بزيادة فهم مواطن الضعف المتعلقة بالمعمارية والتصميم الخاصة بالبرمجيات وإدارتها. ويجري تجميع تطبيقات العملية CWE وتحديثها بواسطة فريق دولي متنوع من الخبراء من قطاع الأعمال والمؤسسات الأكاديمية والهيئات الحكومية بما يضمن اتساع وعمق المحتوى. وتوفر عملية CWE مصطلحات قياسية وتمكن موردي الخدمات من إحاطة المستعملين علماً بمواطن الضعف المحتملة المحددة مع اقتراح الحلول، كما تتيح لمشتري البرمجيات المقارنة بين المنتجات المتشابهة المقدمة من بائعين متعددين.	[b-CWE]

الجدول 1.I – تقنيات مجموعة تبادل معلومات مواطن الضعف ومواطن التعرض والحالة

التقنيـــة	الوصـــف	المراجـــع
نظام تقييم مواطن الضعف الشائعة (CWSS)	يوفر نظام تقييم مواطن الضعف الشائعة إطاراً مفتوحاً للإبلاغ عن خصائص وآثار مواطن ضعف البرمجيات.	[b-CWSS]
لغة التعرض والتقييم المفتوحة (OVAL)	لغة التعرض والتقييم المفتوحة عبارة عن جهد من أجل وضع مواصفة دولية للنهوض بمحتوى أمني مفتوح ومتاح للجمهور ولتقييس نقل هذه المعلومات عبر كامل طيف الأدوات والخدمات الأمنية. وتتضمن OVAL لغة تستخدم لتشفير تفاصيل النظام وتشكيلة متنوعة لوسائل تخزين المحتوى الموجودة عبر المجتمع بأكمله. وتعمل اللغة على تقييس الخطوات الرئيسية الثلاث لعملية التقييم: تمثيل معلومات تشكيلة الأنظمة لأغراض الاختبار؛ وتحليل النظام من حيث وجود حالة محددة للآلة (مواطن التعرض والتشكيلة وحالة الآلة وما إلى ذلك)؛ والإبلاغ عن نتائج هذا التقييم. ووسائل التخزين ما هي إلا تجميعات للمحتوى المتاح للجمهور والمفتوح الذي يستخدم اللغة. وقد وُضعت مخططات OVAL المكتوبة باللغة XML لكي تعمل كإطار ومفردات للغة OVAL. وتقابل هذه المخططات خطوات عملية التقييم الثلاث: مخططات خصائص النظام OVAL لتمثيل معلومات النظام ومخططات تعريف OVAL للتعبير عن حالة محددة للآلة ومخططات نتائج OVAL للإبلاغ عن نتائج التقييم.	[b-OVAL]
نسق وصف القائمة المرجعية القابل للتوسع في التشكيلة (XCCDF)	النسق XCCDF عبارة عن مواصفة للغة من أجل كتابة قوائم الأمن المرجعية ومؤشرات التقييم والأنواع ذات الصلة من الوثائق. وأي وثيقة XCCDF تمثل تجميع مهيكل لقواعد التشكيلة الأمنية لبعض مجموعات الأنظمة المستهدفة. والمواصفة مصممة بحيث تدعم تبادل المعلومات ووضع الوثائق والمواءمة المنظماتية والوضعية والاختبار المؤتمت للامتثال وتقييم الامتثال. كما تحدد المواصفة نموذج ونسق البيانات الخاص بتخزين نتائج اختبار الامتثال لمؤشرات التقييم. والغرض من النسق XCCDF توفير أساس منتظم للتعبير عن قوائم الأمن المرجعية ومؤشرات التقييم وغيرها من توجيهات التشكيل وبالتالي زيادة تعزيز التطبيق الواسع الانتشار للممارسات الأمنية الجيدة. ويعبر عن الوثائق XCCDF باللغة XML.	[b-XCCDF]
تعداد المنصات (CPE)	تعداد المنصات الشائعة عبارة عن طريقة قياسية لتحديد ووصف أنظمة البرمجيات وأجهزة العتاد الموجودة في قائمة الموجودات من المعدات الحاسوبية لأي شركة. وتوفر طريقة CPE: مواصفة تسمية، بما في ذلك البنية المنطقية لأسماء CPE مصاغة بشكل جيد وإجراءات ربط وتفكيك هذه الأسماء بشفرات يمكن للآلة قراءتها؛ ومواصفة مواءمة تحديد إجراءات مقارنة أسماء CPE لتحديد ما إذا كانت تعود لبعض أو لكافة المنتجات أو المنصات ذاتها؛ ومواصفة معجم تحدد المفهوم الخاص بمعجم لمعرفات الهوية وتحدد قواعد رفيعة المستوى للقائمين على شؤون هذا المعجم.	[b-CPE]
تعداد التشكيلات الشائعة (CCE)	توفر عملية تعداد التشكيلات الشائعة معرفات هوية متفردة لقضايا التشكيلات لتسهيل الترابط السريع والدقيق لبيانات التشكيل عبر مصادر وأدوات المعلومات المتعددة. فمثلاً، يمكن استعمال معرفات CCE لربط عمليات الفحص في أدوات تقييم التشكيل بالبيانات الواردة في وثائق أفضل الممارسات المتعلقة بالتشكيل.	[b-CCE]
نسق نتائج التقييم (ARF)	النسق ARF عبارة عن مواصفة مفتوحة توفر لغة مهيكلة لتبادل بيانات نتائج التقييم لكل جهاز بين أدوات التقييم وقواعد بيانات الموجودات والمنتجات الأخرى التي تقوم بإدارة معلومات الأصول. وهذا النسق مصمم من أجل استعماله في الأدوات التي تقوم بتجميع بيانات التشكيل المفصلة عن أصول تكنولوجيا المعلومات. كما يتضمن النسق ARF مواصفة إبلاغ إجمالية لإتاحة الإبلاغ عن المعلومات عبر أصول وموجودات متعددة ولغة تحديد مهام واستجواب للسماح بطلب نتائج التقييم. وتشرح مواصفات أتمتة الأمن عملية من طرف إلى طرف لتوصيل محتويات التقييم إلى مخازن البيانات ولطلب تقييمات بخصوص هذه المحتويات وللإبلاغ عن نتائج هذه التقييمات وتجميع نتائج التقييمات على مستوى المؤسسة.	[b-ARF]

الجدول 2.I – التقنيات ذات الصلة بمجموعات تبادل معلومات الحدث والحادث العرضي والوسائل الحدسية المساعدة

التقنيـــة	الوصـــف	المراجـــع
التعبير عن الحدث الشائع (CEE)	تعمل التقنية CEE على تقييس أسلوب وصف الأحداث الحاسوبية وتسجيلها وتبادلها. وباستعمال اللغة المشتركة وقواعد تركيب التقنية CEE، يمكن وبصورة أكثر فعالية إجراء وظائف إدارة سجل المؤسسة بالكامل والربط والتجميع والمراجعة والمعالجة المتعلقة بالحوادث مع الخروج بنتائج أفضل. والهدف الأساسي للتقنية هو تقييس تمثيل وتبادل السجلات الصادرة عن الأنظمة الإلكترونية. وتقسم التقنية CEE عملية تسجيل السجلات وتبادلها إلى أربعة مكونات: تصنيف للأحداث؛ وقواعد التركيب الخاصة بالسجل ونقل السجل وتوصيات إعداد السجلات.	[b-CEE]
نسق تبادل وصف الشيء العرضي (IODEF)	يحدد النسق IODEF تمثيلاً للبيانات يوفر إطاراً لتبادل المعلومات التي يكثر تبادلها بين أفرقة الاستجابة للحوادث الحاسوبية بخصوص الحوادث العرضية الأمنية الحاسوبية. ويصف النسق IODEF نموذجاً للمعلومات ويوفر نموذجاً للبيانات المصاحبة الموصفة بمخططات بلغة XML.	[b-IETF RFC 5070]
النسق الخاص بالانتحال والاحتيال وإساءة الاستعمال	يعمل النسق الخاص بالانتحال والاحتيال وإساءة الاستعمال على تمديد نسق IODEF بحيث يدعم الإبلاغ عن الانتحال والاحتيال والأنماط الأخرى من إساءة الاستعمال. وتدعم هذه التمديدات كذلك تبادل المعلومات المتعلقة بحوادث الرسائل الاقتحامية واسعة الانتشار. وهذه التمديدات مرنة بما يكفي بحيث تدعم المعلومات التي يجري تجميعها شيئاً فشيئاً من الأنشطة عبر الدورة الإلكترونية الكاملة لعملية الاحتيال أو الرسالة الاقتحامية. وكل من الإبلاغ البسيط والإبلاغ القانوني الكامل يمكن تحقيقهما، كما هو الحال في تجميع حوادث متعددة. ملاحظة: تصف هذه التوصية فقط التقنيات التي يتسنى للجميع فهمها والوسائل المضمونة التي تتيح لكيانات الأمن السيبراني تبادل معلومات الأمن السيبراني ولا تتضمن استعمالات هذه المعلومات.	[b-IETF RFC 5901]
تعداد نماذج الاعتداءات الشائعة وتصنيفها (CAPEC)	التقنية CAPEC عبارة عن مواصفة لطريقة من أجل تحديد ووصف وتعداد نماذج الاعتداءات. ونماذج الاعتداءات عبارة عن آلية قوية لالتقاط المنظور الخاص بالقائم بالاعتداء وتوصيله. وهذه النماذج عبارة عن أوصاف للطرق الشائعة لاستغلال البرمجيات. وهي تشتق من مفهوم نماذج التصميم التي تُطبق في سياق هدام وليس في سياق بناء وتتولد من تحليل متعمق لأمثلة محددة للاستغلال من الواقع. والهدف من التقنية CAPEC هو توفير بيان بنماذج الاعتداءات للجمهور إلى جانب مخطط XML شامل وتصنيف علمي لها.	[b-CAPEC]
نسق تعداد وتحديد خصائص نعوت البرمجيات الخبيثة	نسق تعداد نعوت البرمجيات الخبيثة وتحديد خصائصها (MAEC) عبارة عن لغة رسمية تتضمن مخططاً لتوفير كل من قاعدة لتركيب المصطلحات المشتركة للنعوت ومظاهر السلوك المعددة ونسق لتبادل المعلومات المهيكلة عن عناصر البيانات تلك. وتكون التعدادات على مستويات متفاوتة من التجريد: أعمال المستوى الأدنى ومظاهر السلوك الخاصة بالمستوى المتوسط والآليات رفيعة المستوى. وفي المستوى الأدنى، تصف التقنية MAEC النعوت المرتبطة بالوظيفة الأساسية والتشغيل على المستوى الأدنى للبرمجية الضارة. وفي المتوسط، تنظم لغة MAEC أعمال المستوى الأدنى المذكورة آنفاً في مجموعات بغرض تحديد مظاهر سلوك المستوى المتوسط. وعلى المستوى المفاهيمي الأكبر وعلى المستوى الرفيع، تسمح مصطلحات التقنية MAEC بناء آليات تقوم بتجريد مجموعات من مظاهر سلوك البرمجيات الضارة في المستوى المتوسط استناداً إلى تحقيق درجة أعلى من التصنيف.	[b-MAEC]

الجدول 3.I – التقنيات ذات الصلة بمجموعة تبادل السياسات

التقنيـــة	الوصـــف	المراجـــع
بروتوكول الإشارات الضوئية للحركة (TLP)	استحدث البروتوكول TLP لتشجيع زيادة تبادل المعلومات الحساسة. وتقوم جهة المنشأ ببيان إلى أي مدى ترغب في تعميم معلوماتها لأبعد من المستقبل الأول. ويوفر البروتوكول TLP طريقة بسيطة لتحقيق ذلك. هذا البروتوكول مصمم بحيث يحسن من تدفق المعلومات بين الأفراد أو المنظمات أو المجتمعات بأسلوب موثوق ومتحكم به. ويقوم البروتوكول TLP على مفهوم قيام جهة المنشأ برسم المعلومات بلون من أربعة ألوان لبيان النشر التالي، إن وجد، الذي يمكن للمستقبل القيام به. ويجب على المستقبل الاستفسار من جهة المنشأ بشأن ما إذا كان يتعين النشر على مستوى أوسع. ويُقبل البروتوكول TLPعلى أنه نموذج للتبادل المضمون للمعلومات بين المجموعات الأمنية في أكثر من 30 بلداً. و"مستويات تبادل المعلومات" الأربعة المتعلقة بتداول المعلومات الحساسة هي: الأحمر (RED) – شخصية. هذه المعلومات لا تخص إلا المستقبلين المحددة أسماؤهم فقط. وفي سياق اجتماع، على سبيل المثال، تقتصر معلومات اللون الأحمر على الحاضرين فقط. وفي معظم الظروف تسلم معلومات اللون الأحمر شفهياً أو شخصياً. أصفر (AMBER) – توزيع محدود. يجوز للمستقبل تبادل هذه المعلومات مع آخرين داخل منظماتهم ولكن على أساس "الحاجة إلى العلم". أخضر (GREEN) – على مستوى المجتمع. يمكن تعميم معلومات هذه الفئة على نطاق واسع داخل مجتمع معين. بيد أنه يمكن عدم نشر المعلومات أو وضعها على الإنترنت وكذلك عدم نشرها خارج المجتمع. أبيض (WHITE) – غير مقيدة. تخضع للقواعد العادية لحقوق المؤلف، ويمكن توزيع هذه المعلومات بحرية دون أي قيود.	[b-TLP]

الجدول 4.I – التقنيات ذات الصلة بمجموعة تعرف الهوية والكشف والاستجواب

التقنيـــة	الوصـــف	المراجـــع
آليات الكشف في تبادل معلومات الأمن السيبراني	تشمل هذه التقنيات الأساليب التي يمكن استعمالها لتعرف هوية وتحديد مكان مصادر معلومات الأمن السيبراني وأنواعها وحالات محددة لهذه المعلومات والأساليب المتاحة للنفاذ إلى معلومات الأمن السيبراني فضلاً عن السياسات التي يمكن تطبيقها للنفاذ إلى هذه المعلومات.	
مبادئ توجيهية لإدارة التمديدات OID arc الخاصة بتبادل معلومات الأمن السيبراني	يتم وصف مسافة اسم معروفة عالمياً لمعرف هوية الأمن السيبراني إلى جانب المتطلبات الإدارية كجزء من OID arc ويشمل معرفات هوية لكل من: • معلومات الأمن السيبراني؛ • منظمة الأمن السيبراني؛ • سياسات الأمن السيبراني.	
لغة الاستجواب بشأن معلومات الأمن السيبراني	تحدد لغة الاستجواب بشأن معلومات الأمن السيبراني تمثيل مرن للبيانات يوفر إطاراً لطلب المعلومات الشائع تبادلها بين أفرقة الاستجابة للحوادث الحاسوبية عن حوادث الأمن الحاسوبية. وتصف هذه المواصفة نموذج المعلومات الخاصة باللغة CYIQL وتوفر نموذجاً للبيانات المصاحبة يحدد بمخطط بلغة XML.	

الجدول I.5 – التقنيات المتعلقة بمجموعة ضمان الهوية

التقنيـــة	الوصـــف	المراجـــع
منصات موثوقة	تزيد منتجات الحاسوب والاتصالات المدمج بها وحدات منصات موثوقة (TPM) من قدرة الأعمال التجارية والمؤسسات والهيئات الحكومية والمستهلكين على إجراء تبادل موثوق للمعلومات؛ وبالتالي، تتصل الوحدات TPM بمعظم تطبيقات تبادل معلومات الأمن السيبراني CYBEX. والوحدات TPM عبارة عن دارات متكاملة (IC) ذات وظائف خاصة تدمج في منصات مختلفة للتمكين من الاستيقان القوي من المستعمل والتحقق من الآلة – وهو أمر ضروري لمنع النفاذ غير المناسب إلى المعلومات السرية والحساسة والوقاية من الشبكات الملوثة. وتقوم تكنولوجيا وحدات المنصات الموثوقة على معايير مفتوحة لضمان قابلية التشغيل البيني للمنتجات المتنوعة في بيئات يختلط فيها البائعون. ويتألف المعيار السائد للوحدات TPM من مجموعة من المواصفات قام على وضعها ورعايتها فريق الحوسبة الموثوقة (TCG) إلى جانب مظهر جانبي للحماية من أجل التقييم الأمني إزاء معايير مشتركة. وتعطي مبادئ التصميم المفاهيم الأساسية للوحدات TPM والمعلومات العامة المتعلقة بوظائف هذه الوحدات. ويجب على مصمم الوحدات TPM مراجعة وتنفيذ المعلومات الواردة في المواصفة الرئيسية للوحدات TPM (الأجزاء 1-3) ومراجعة الوثيقة الخاصة بالمنصة بالنسبة للمنصة المقصودة. وتشمل الوثيقة الخاصة بالمنصة بيانات معيارية تؤثر على تصميم وتنفيذ الوحدة TPM. ويجب على مصمم الوحدات TPM مراجعة وتنفيذ المتطلبات، بما في ذلك الاختبار والتقييم على النحو الذي حدده فريق عمل المطابقة التابع للفريق TCG. ويجب أن تلتزم الوحدة TPM بالمتطلبات وأن تجتاز أي تقييمات حددها فريق عمل المطابقة. وقد تخضع الوحدة TPM للمزيد من الاختبارات والتقييمات الأكثر صرامة.	[b-TPM]
توصيل شبكي موثوق	ترغب العمليات الأمنية لتكنولوجيا المعلومات والاتصالات عادة في اكتشاف حالة مستوى نظام التشغيل (OS) وبرمجية التطبيق التي تستعملها الشبكة الداعمة. فمثلاً، عندما تفتقر الأنظمة إلى وسائل الإصلاح الأمنية لنظام التشغيل أو إلى توقيعات ضد الفيروسات، من المحتم احتواء التبليغ الموثوق على الضرر المرتبط بالهجمات القائمة على الشبكة. ولإجراء هذا التقييم يتعين وجود معلومات موثوقة بأن النظام الموصول بحالة معينة. ولمنع الأنظمة (المقرصنة مثلاً) من تزييف المعلومات، فإن التقييم الناجح يحتاج إلى أساس من العتاد على النظام الخاضع للتقييم. وتدمج بالعتاد منصات موثوقة لتسجيل حقائق معينة عن عملية التحميل وتقدمها في صورة موقعة رقمياً. كما أن المصنعين الرئيسيين للرقائق يستكملون حالياً المنصات الموثوقة بقدرة "إطلاق متأخر" تسمح بتنفيذ الشفرة الموثوقة في وقت تال خلال تسلسل عملية التحميل الذاتي. ويسمح هذا بدوره بتسجيل الأحداث بشكل موثّوق بعد عملية التحميل الخاصة بالعتاد. وإدارة تشكيلة الشبكة ما هي إلا عملية نشر فعلية لشهادة النظام: وكلاء برمجيات على آلات المؤسسة ترسل دورياً تقارير التشكيلة إلى المستودع المركزي الذي يقوم بتقييم ووسم الأنظمة غير المطابقة. وفي حين تعتبر المعلومات الصادرة عن وكلاء البرمجيات قيمة، فإنه يسهل تغييرها بواسطة أي مهاجم. وباستعمال النشر على نطاق واسع للمنصات الموثوقة للتمكين من تقييم حالة النظام بشكل أكثر موثوقية، يمكن زيادة ثقة المؤسسة في بيانات إدارة تشكيلتها إلى حد كبير. والتوصيل TNC عبارة عن معمارية مفتوحة للتحكم في النفاذ إلى الشبكة. والهدف من التوصيل TNC هو تمكين مشغلي الشبكات من توفير سلامة طرفية عند كل توصيل شبكي بما يسمح بالشغيل البيني بين النقاط الطرفية الشبكية لبائعين متعددين.	[b-TNC]
ضمان استيقان الكيان	يوفر هذا المعيار إطاراً لدورة حياة الاستيقان لإدارة ضمان هوية الكيان ومعلومات الهوية المرتبطة بها في سياق معين. والمعيار يوفر تحديداً طرق من أجل 1) قياس وتخصيص مستويات الضمان ذات الصلة بشكل جيد لاستيقان هويات أي كيان ومعلومات الهوية المرتبطة بها و2) توصيل مستويات ضمان الاستيقان ذات الصلة.	[b-NIST EAA]

الجدول I.5 – التقنيات المتعلقة بمجموعة ضمان الهوية

التقنيـــة	الوصـــف	المراجـــع
إطار الشهادة الممتدة الصلاحية	يتألف إطار الشهادة الممتدة الصلاحية (EVCERT) من توليفة متكاملة من التكنولوجيات والبروتوكولات وممارسات إثبات الهوية وإدارة دورة الحياة والتدقيق بحيث تصف الحد الأدنى من المتطلبات التي يتعين استيفائها من أجل إصدار ورعاية الشهادات ممتدة الصلاحية ("EV Certificates") المتعلقة بمنظمة معينة. ويؤمن هذا الإطار مجموعة واسعة من متطلبات الأمن والمركزية والتبليغ.	[b-EVCERT]
المتطلبات الخاصة بالسياسات لهيئات إصدار الشهادات التي تقوم بإصدار شهادات المفاتيح العمومية	تحدد الوثيقة المعنية المتطلبات الخاصة بالسياسات لهيئات إصدار الشهادات (CA) التي تقوم بإصدار شهادات المفاتيح العمومية، بما في ذلك الشهادات الممتدة الصلاحية (EVC). وتحدد الوثيقة المتطلبات الخاصة بالسياسات المتعلقة بالتشغيل وممارسات الإدارة لهيئات إصدار الشهادات التي تقوم بإصدار وإدارة الشهادات مثل المشتركين والموضوعات التي تحصل على شهادات من هيئة إصدار الشهادات ويمكن للأطراف المعولة الثقة في تطبيق الشهادة دعماً لآليات التحفير.	[b-ETSI TS102 042]

الجدول I.6 – التقنيات المتعلقة بمجموعة بروتوكولات التبادل

التقنيـــة	الوصـــف	المراجـــع
الدفاع بين الشبكات في الوقت الفعلي (RID)	يوفر الدفاع بين الشبكات في الوقت الفعلي (RID) إطاراً لتبادل معلومات الحوادث. ويوفر معيار RID مجموعة من رسائل تنسيق الحادث اللازمة لتداول وثائق نسق تبادل وصف الشيء العرضي (IODEF) على نحو آمن بين الكيانات. ويغلف الدفاع بين الشبكات في الوقت الفعلي وثائق نسق تبادل وصف الشيء العرضي، بما في ذلك أي توسعات لهذا النسق. وتشمل الرسائل المعيارية وأنساق التبادل خيارات/اعتبارات الأمن والخصوصية والسياسة المتبعة اللازمة في الخطة العالمية للتنسيق بشأن الحوادث. ويشكل الدفاع بين الشبكات في الوقت الفعلي طبقة الأمن بين وثائق IODEF وبروتوكول النقل. وتقرر الكيانات التي تتداول المعلومات المتعلقة بالحوادث ماهية النقل المختار. فيمكن أن يكون النقل نقل RID الموصَّف (HTTP/TLS) أو بروتوكول BEEP أو SOAP أو بروتوكول يوصَّف مستقبلاً.	[b-IETF RFC 6045]
نقل رسائل الدفاع بين الشبكات في الوقت الفعلي	توصف هذه الآلية نقل رسائل الدفاع بين الشبكات في الوقت الفعلي (RID) في إطار رسائل الطلبات والردود للبروتوكول HTTP الجاري نقلها عبر أمن طبقة النقل.	[b IETF RFC 6046]
مظهر جانبي لبروتوكول تبادل موسع القدرات (BEEP) لأغراض تبادل معلومات الأمن السيبراني (CYBEX)	يحدد المظهر الجانبي للبروتوكول BEEP لأغراض تقنيات تبادل معلومات الأمن السيبراني المظهر الجانبي للبروتوكول BEEP للاستعمال في إطار CYBEX. والبروتوكول BEEP عبارة عن نواة لبروتوكول تطبيق تنوعي من أجل المعاملات البينية المحددة بالتطبيق غير المتزامنة الموصوفة في المعيار RFC3080. ويوجد في قلب البروتوكول BEEP آلية نشر تسمح بعمليات تبادل متآونة ومستقلة في سياق قناة -- رابطة بجانب محدد جيداً في التطبيق، مثل أمن النقل أو استيقان المستعمل أو تبادل البيانات. ولكل قناة "مظهر جانبي" مرتبط بها يحدد قواعد التركيب والدلالات اللفظية للرسائل المتبادلة.	[b-IETF RFC3080]
بروتوكول النفاذ البسيط إلى الأشياء (SOAP) لأغراض تقنيات تبادل معلومات الأمن السيبراني (CYBEX)	البروتوكول SOAP عبارة عن بروتوكول بسيط لتبادل المعلومات في بيئة غير مركزية موزعة. وهذا البروتوكول قائم على اللغة XML ويتألف من ثلاثة أجزاء: غلاف يحدد إطاراً لشرح مضمون الرسالة وكيفية معالجته؛ ومجموعة من قواعد التشفير للتعبير عن حالات أنماط البيانات المحددة التطبيق؛ واتفاقية لتمثيل نداءات وردود الإجراءات عن بعد. ويمكن استعمال البروتوكول SOAP بالاشتراك مع مجموعة متنوعة من البروتوكولات؛ بيد أن الروابط المحددة في هذه الوثيقة لا تصف إلا كيفية استعمال البروتوكول SOAP. بالاشتراك مع البروتوكول HTTP وإطاره الموسع.	[b-W3C SOAP]

التذييل II

أنطولوجيا لتبادل معلومات الأمن السيبراني

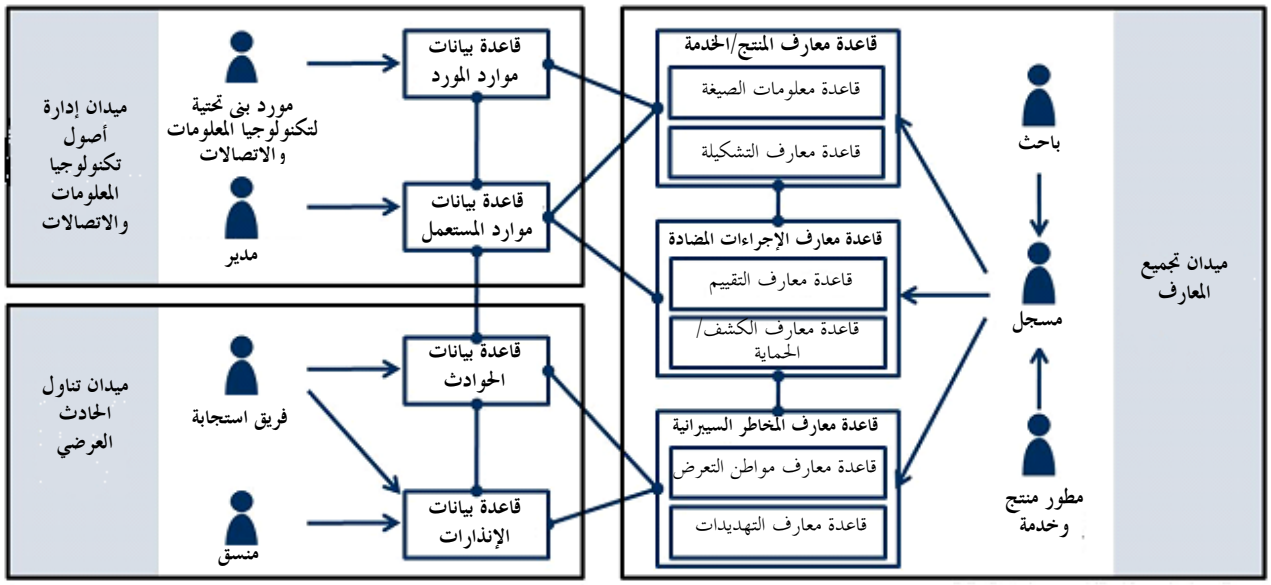
(لا يمثل هذا التذييل جزءاً أساسياً من هذه التوصية)

يقدم التذييل II تقنية لتبادل معلومات الأمن السيبراني. ويوضح هذا التذييل السياق التشغيلي لتقنيات CYBEX وينتهي بنظام إيكولوجي فعال للأمن السيبراني تستعمل فيه المعارف المستقاة من التقارير والاختبارات والتجارب في وضع وتطوير معلومات عن مواطن الضعف والتعرض والتي يمكن بالتالي استعمالها هي ومعلومات حالة النظام في قياس الأمن وتعزيزه.

وتعرِّف أنطولوجيا تبادل معلومات الأمن السيبراني المصطلحات التالية:

1) **عمليات الأمن السيبراني**: الطرق والعمليات المستعملة في مراقبة الأمن وإدارته في إطار حدود تشغيلية محددة من بينها:
   - تجميع وتحليل المعلومات التي قد تؤثر على الأمن؛
   - اكتشاف السلوك أو الأحداث التي تؤثر بالسلب على الأمن أو التي يمكن من خلالها تحديد أرجحية حدوث تأثير سلبي في المستقبل؛
   - الإجراء المتخذ في حالة وقوع سلوك أو حدث ذي تأثير سلبي للحد من أو تخفيف آثار و/أو منع الحوادث في المستقبل؛
   - الاتصالات المتعلقة بالأمن والخاصة بحالة النظام وظروفه.
2) **كيان الأمن السيبراني**: أي كيان يشكل جزءاً من عملية تبادل لمعلومات الأمن السيبراني بما في ذلك عنصر المعلومة نفسه.
3) **المعلومات التشغيلية للأمن السيبراني**: أي معلومات تحتاج إليها كيانات الأمن السيبراني لتشغيل عمليات الأمن السيبراني.

من المفيد وصف تقنيات الأمن السيبراني الموصوفة في CYBEX ثانية في إطار أنطولوجيا CYBEX هذه؛ بمعنى، نموذج لوصف العالم المجرد لعمليات الأمن السيبراني وتتكون هذه الأنطولوجيا من مجموعة من الأنماط والخواص والعلاقات. انظر الشكل II.1، حيث تشير الخطوط المستمرة إلى العلاقة بين أنماط المعلومات في حين يشير الاسم إلى دخل المعلومات من كيان وظيفي إلى قاعدة معارف/بيانات. والكيانات الوظيفية المبينة في الجانب الأيمن عبارة عن كيانات عامة في حين يجوز لكيانات مثل أفرقة الاستجابة للحوادث الحاسوبية أن تضم واحدة أو أكثر من هذه الوظائف.



الشكل 1.II – نموذج أنطولوجيا CYBEX

وفي هذه الأنطولوجيا، يستعمل نموذج لتعريف ميادين عمليات الأمن السيبراني، حيث يستعمل فيما بعد لتحديد كيانات الأمن السيبراني اللازمة لدعم العمليات التي تجرى في كل ميدان. وتشتق في الفقرات التالية أنطولوجيا مفصلة. حيث يوضح ذلك كيف يمكن استعمال تقنيات CYBEX في دعم هذه الأنطولوجيا.

1.II ميادين العمليات

تتكون عمليات الأمن السيبراني في الأساس من ثلاثة ميادين: تناول الحادث وإدارة أصول تكنولوجيا المعلومات والاتصالات وتجميع المعارف.

ويشمل ميدان تناول الحادث كشف الحوادث الخاصة بالأمن السيبراني والاستجابة لها من خلال مراقبة الحوادث والأحداث الحاسوبية التي تشكل هذه الحوادث وسلوك الهجمات المحدد في الحوادث. فمثلاً، يقوم ميدان تناول الحادث باكتشاف الأمور الشاذة من خلال إنذارات تصدر عن الكاشفات ثم يقوم بتجميع التفاصيل بجميع السجلات المختلفة. ويصدر عن هذا الميدان في بعض الأوقات إنذارات وتقارير، مثل الإنذارات المبكرة من التهديدات المرشحة لمنظمات المستعملين.

ويشمل ميدان إدارة أصول تكنولوجيا المعلومات والاتصالات عمليات الأمن السيبراني داخل كل منظمة من منظمات المستعملين مثل تركيب أصول تكنولوجيا المعلومات والاتصالات في المنظمة وتشكيلها وإدارتها. ويتضمن هذا الميدان العمليات الوقائية من الحوادث وعمليات التحكم في الأضرار داخل كل منظمة.

ويشمل ميدان تجميع المعارف المعلومات المتصلة بالأمن السيبراني. ويتم توليد وتجميع المعارف التي يمكن استعمالها ثانية بواسطة منظمات أخرى.

2.II كيانات الأمن السيبراني

طبقاً لميادين العمليات الموضحة أعلاه، يمكن تحديد الكيانات الوظيفية للأمن السيبراني اللازمة لتشغيل عمليات الأمن السيبراني في كل ميدان من هذه الميادين.

وضمن ميدان تناول الحادث، يوجد كيانان من أجل عملياته: فريق الاستجابة والمنسق وفريق الاستجابة عبارة عن كيان يقوم بمراقبة وتحليل الأنواع المختلفة من الحوادث، مثل النفاذ غير المرخص وهجمات الرفض الموزع للخدمة والاحتيال، وتجميع

معلومات الحوادث. واستناداً إلى هذه المعلومات، قد يقوم فريق الاستجابة بتنفيذ إجراءات مضادة، مثل تسجيل عناوين مواقع الاحتيال في القوائم السود. والمنسق عبارة عن الكيان الذي يقوم بالتنسيق مع الكيانات الأخرى والتصدي للتهديدات المحتملة استناداً إلى معلومات معروفة عن الحادث.

وفي ميدان إدارة أصول تكنولوجيا المعلومات والاتصالات، يوجد كيانان للعمليات: المدير ومورد البنى التحتية لتكنولوجيا المعلومات والاتصالات. ويقوم المدير بإدارة نظام منظمته ويستحوذ على المعلومات لديه في أصوله الخاصة بتكنولوجيا المعلومات والاتصالات. والمثال النمطي على ذلك مدير تكنولوجيا المعلومات والاتصالات الموجود داخل كل منظمة. ويقوم مورد البنى التحتية لتكنولوجيا المعلومات والاتصالات بتزويد كل منظمة بالبنى التحتية لتكنولوجيا المعلومات والاتصالات، والتي تشمل توصيلة الشبكة وخدمات الحوسبة السحابية مثل البرمجيات في صورة خدمة (SaaS) ومنصة في صورة خدمة (PaaS) وبنية تحتية في صورة خدمة (IaaS) وخدمات الهوية. ومن الأمثلة على ذلك مورد خدمة الإنترنت (ISP) ومورد خدمة التطبيق (ASP).

وفي ميدان تجميع المعارف، توجد ثلاثة كيانات للعمليات: الباحث ومطور المنتج/الخدمة والمسجل. ويقوم الباحث بالبحث عن معلومات الأمن السيبراني واستخلاص المعارف وتجميعها. ويمتلك مطور المنتج/الخدمة المعلومات الخاصة بالمنتجات والخدمات، مثل التسمية والصيغ ومواطن التعرض الخاصة بها والمعلومات الخاصة بإصلاحها وتشكيلها. ومن الأمثلة النمطية على ذلك جهات بيع البرمجيات وموردو خدمات التطبيق والأفراد من واضعي البرمجيات. والمسجل عبارة عن كيان يقوم بتصنيف وتنظيم معارف الأمن السيبراني المقدمة من الباحثين والمطورين والبائعين بحيث يتسنى لمنظمات أخرى استعمالها.

3.II المعلومات التشغيلية للأمن السيبراني

طبقاً لميادين العمليات والكيانات، تقوم الفقرات الفرعية التالية بتفصيل المعلومات التشغيلية للأمن السيبراني التي تقدمها الكيانات الوظيفية بالنسبة لكل ميدان من ميادين العمليات.

1.3.II ميدان تناول الحادث

في ميدان تناول الحادث، هناك قاعدة بيانات للحادث وقاعدة بيانات للإنذار. وتتضمن قاعدة بيانات الحادث معلومات عن الحوادث مقدمة من فريق الاستجابة. وهي تشمل ثلاثة أنواع من السجلات: الحدث والحادث العرضي والهجمة. ويتضمن سجل الأحداث، الأحداث الحاسوبية مثل المستعملين ذوي الامتيازات بالدخول على نظام. كما يتضمن معلومات عن الرزم والملفات والمعاملات المتعلقة بالحادث. وتقدم معظم السجلات عادة من أجهزة الحاسوب آلياً. ويتضمن سجل الحوادث الأحداث المرشحة لأن تكون حوادث. ويشتق هذا السجل عادة من سجلات عديدة للأحداث وحلولها الحدسية وهي تتولد آليا و/أو يدوياً. ويستند سجل الهجمات إلى تحليل الحوادث ويتضمن التاريخ والتوقيت الدقيق للهجمات فضلاً عن تسلسلها.

وتتضمن قاعدة بيانات الإنذارات معلومات عن إنذارات الأمن السيبراني الصادرة عن فريق الاستجابة والمنسق. وتستند الإنذارات إلى قاعدة بيانات الحوادث إضافة إلى قاعدة معارف المخاطر السيبرانية.

2.3.II ميدان إدارة أصول تكنولوجيا المعلومات والاتصالات

يوجد في ميدان إدارة أصول تكنولوجيا المعلومات والاتصالات قاعدتا بيانات: قاعدة بيانات موارد المستعمل وقاعدة بيانات موارد المورد.

وتقوم قاعدة بيانات موارد المستعمل بتجميع معلومات عن الأصول الموجودة داخل كل منظمة وتتضمن معلومات على غرار قائمة البرمجيات والعتاد وتشكيلاتها وحالة استعمال الموارد والسياسات الأمنية بما فيها سياسات التحكم في النفاذ ونتائج تقييم مستوى الأمن وطوبولوجيا الشبكة الداخلية. ويقدم المدير هذه المعلومات.

وتقوم قاعدة بيانات موارد المورد بتجميع بيانات عن الأصول خارج المنظمة. وهي تشمل في الأساس معلومات عن الموارد الخارجية ومعلومات عن الشبكة الخارجية. وتتألف معلومات الموارد الخارجية من معلومات عن الموارد التي تستخدمها كل

منظمة خارج نطاقها مثل قائمة بالخدمات السحابية الخارجية وحالتها (مثل مركز البيانات والخدمة في صورة خدمة (SaaS). وتتألف معلومات الشبكة الخارجية من معلومات عن الشبكات التي توصل كل منظمة بالمنظمات الأخرى مثل طوبولوجيا هذه الشبكات ومعلومات تسييرها وسياسات التحكم في النفاذ إليها وحالة الحركة ومستوى الأمن. ويقدم مورد البنى التحتية لتكنولوجيا المعلومات والاتصالات هذه المعلومات.

3.3.II ميدان تجميع المعارف

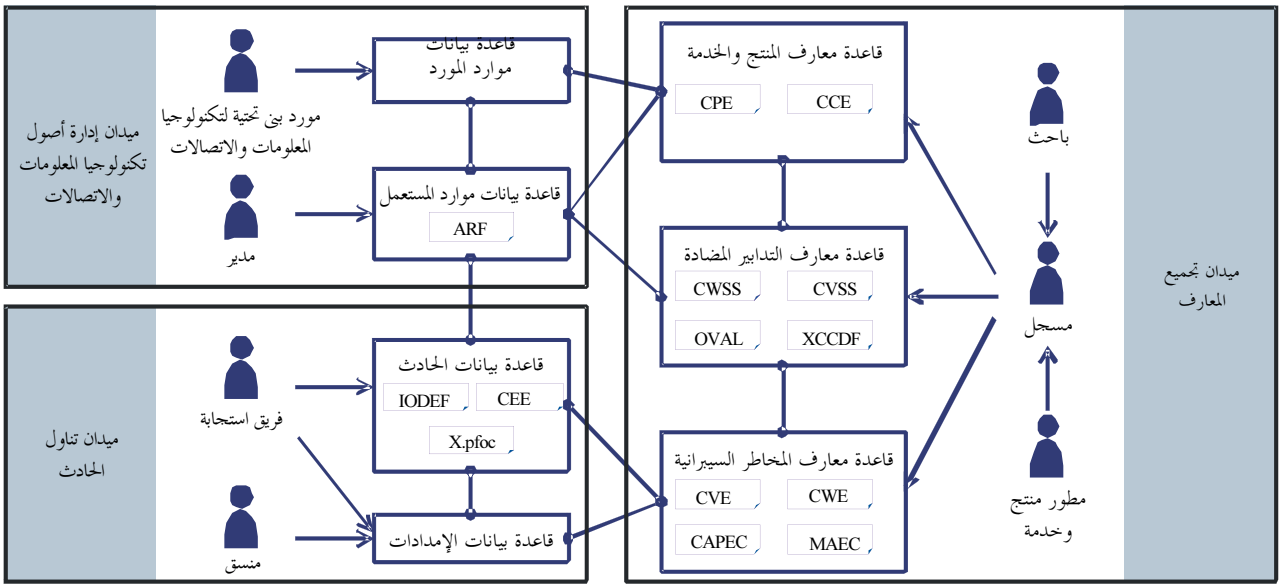
يوجد في هذا الميدان ثلاث قواعد للمعارف: المخاطر السيبرانية والتدابير المضادة والمنتج/الخدمة. وتقوم هذه القواعد بتجميع المعارف عن الأمن السيبراني والتي تقدم من الباحث ومطور المنتج/الخدمة، ثم تُنظم بعد ذلك وتصنف بواسطة المسجل.

وتقوم قاعدة معارف المخاطر السيبرانية بتجميع معلومات عن مخاطر الأمن السيبراني وتتضمن معارف عن مواطن التعرض والتهديدات. وتقوم قاعدة معارف مواطن التعرض بتجميع معلومات عن مواطن التعرض المعروفة بما في ذلك عمليات التسمية والتصنيف والتعداد لمواطن التعرض المعروفة. كما يتضمن مواطن التعرض البشرية التي يتعرض لها مستعملو تكنولوجيا المعلومات والاتصالات من البشر. وتقوم قاعدة معارف التهديدات بتجميع معلومات عن التهديدات المعروفة والتي تشمل معارف عن الهجمات ومعارف عن سوء الاستعمال. وتتضمن معارف الهجمات معلومات عن أنماط الهجمات وأدواتها (مثل البرمجيات الضارة) واتجاهاتها مثل معلومات عن اتجاهات الهجمات السابقة من منظور مصدرها الجغرافي وأهدافها. كما تتضمن معلومات إحصائية عن الهجمات السابقة. وتتضمن معارف سوء الاستعمال معلومات عن حالات سوء الاستعمال الخاصة بتكنولوجيا المعلومات والاتصالات المتسبب فيها مستعملين من البشر دون أي نوايا خبيثة. ومن المعلومات المشمولة كذلك معلومات عن الأخطاء المطبعية والوقوع في فخاخ الاحتيال وحالات عدم الامتثال.

وتقوم قاعدة معارف التدابير المضادة بتجميع معلومات عن التدابير المضادة إزاء مخاطر الأمن السيبراني وتتضمن قاعدتي معارف: التقييم والكشف/الحماية. وتعمل قاعدة معارف التقييم على تجميع القواعد والمعايير المعروفة لتقييم مستوى الأمن لأصول تكنولوجيا المعلومات والاتصالات إضافة إلى قائمة مرجعية بالتشكيلات. وتقوم قاعدة معارف الكشف/الحماية بتجميع القواعد والمعايير المعروفة للكشف عن/الحماية من التهديدات الأمنية، مثل توقيعات IDS/IPS والقواعد ذات الصلة الخاصة بالكشف/الحماية.

وتقوم قاعدة معارف المنتج/الخدمة بتجميع معلومات عن المنتجات والخدمات. وهي تتضمن قاعدتي معارف: معارف بشأن الصيغة ومعارف بشأن التشكيلة. وتقوم قاعدة معارف الصيغة بتجميع معلومات عن صيغ المنتجات والخدمات بما في ذلك أسماء وتعداد هذه الصيغ. وفيما يتعلق بصيغة المنتج، تدرج ضمن قاعدة المعارف تلك أيضاً الحلول الأمنية. وتعمل قاعدة معارف التشكيلة على تجميع معلومات التشكيلة الخاصة بالمنتجات والخدمات. وفيما يتعلق بتشكيلة المنتج، فإن قاعدة البيانات تتضمن أيضاً تسمية وتصنيف وتعداد التشكيلات المعروفة.

ويمكن لأي من قواعد البيانات والمعارف المذكورة آنفاً أن تستخدم تقنيات مختلفة لوصف المعلومات على النحو المبين في الشكل 2.II.



DB = قاعدة بيانات KB = قاعدة معارف

X.1500(11)_FII-02

الشكل 2.II – شكل تفصيلي لنموذج لأنطولوجيا CYBEX مع عرض التقنيات

ولمزيد من المعلومات بشأن أنطولوجيا CYBEX، راجع المرجع [b-Takahashi].

التذييل III

أمثلة CYBEX على مخططات أتمتة الأمن

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

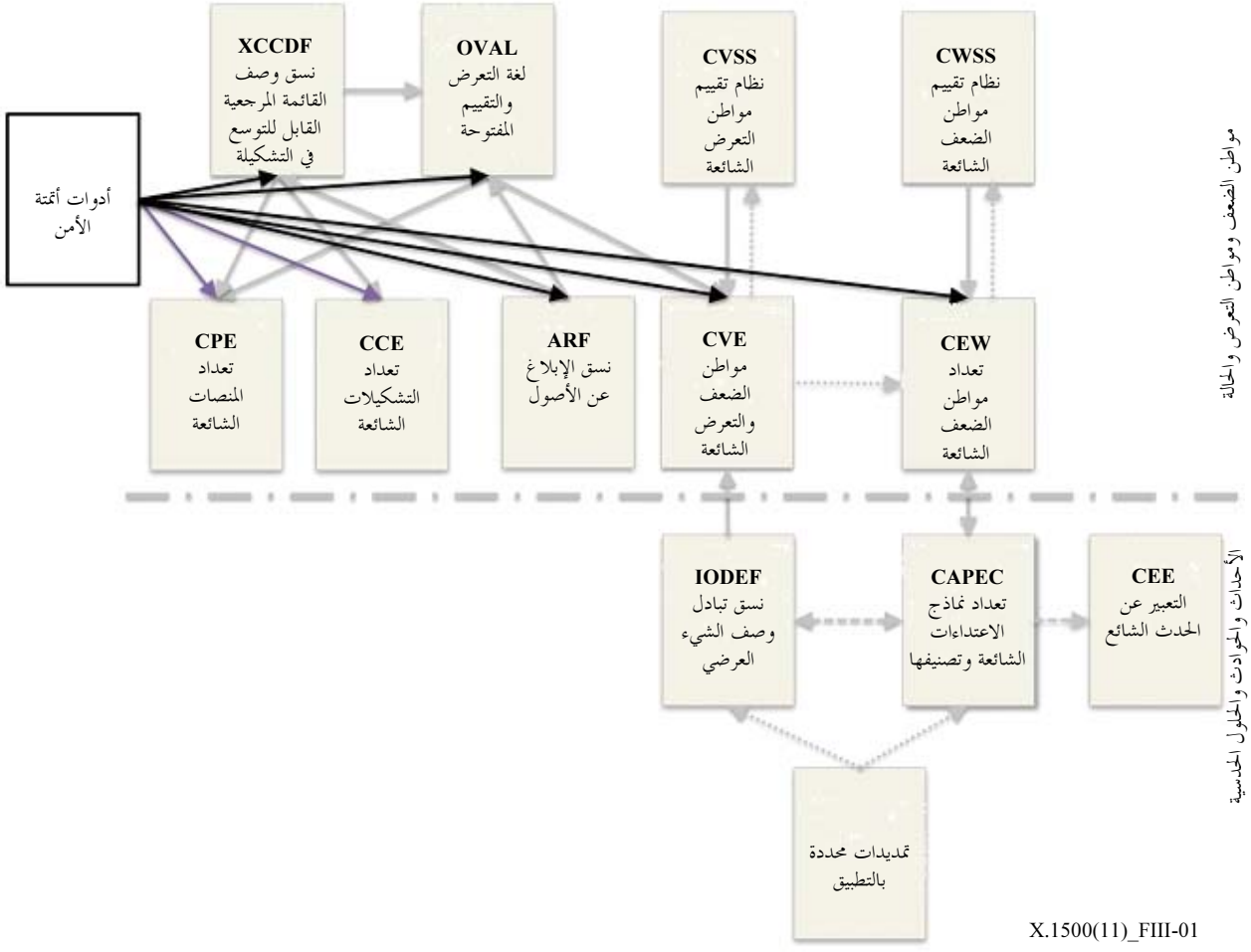
يقدم التذييل الثاني، مثالين لمخططين لأتمتة الأمن. ويمكن استعمال هذه القدرات لاستحداث حالات محددة بخصوص CYBEX تتضمن أتمتة "حالات" مؤمنة ومعروفة أو موثوقة من البرمجيات والخدمات والأنظمة واكتشاف البرمجيات الضارة والحصول على المعلومات المتعلقة بالحوادث وحلولها الحدسية.

ويتوقع ظهور عدد كبير من طرق التنفيذ – خاصة مخطط لأتمتة الأمن للتأكد من تشكيل وإصلاح أنظمة تكنولوجيا المعلومات والاتصالات بالشكل الأمثل. ويشمل المثالان السائدان الأوليان:

1) بروتوكول أتمتة المحتوى الأمني (SCAP) للمعهد الوطني الأمريكي للمعايير والتكنولوجيا (NIST) من أجل تطبيق تشكيلة أساسية لأجهزة الحاسوب المكتبية (FDCC) وبديلتها، التشكيلة الأساسية لحكومة الولايات المتحدة (USGCB)،

2) الإطار الياباني لأتمتة المحتوى الأمني JVN.

ويرد شرح مفصل لكل مثال في هذا التذييل. وطرق تنفيذ أدوات أتمتة الأمن تلك تأخذ بشكل عام النموذج المبين في الشكل 1.III أدناه وتتضمن عدداً متنوعاً من منصات تبادل معلومات CYBEX والممثلة بأسهم غير بارزة في الشكل.



الشكل 1.III – أتمتة ضمان وسلامة الأمن السيبراني

1.III مثال: التشكيلة الأساسية الفيدرالية لأجهزة الحاسوب المكتبية (FDCC) للولايات المتحدة الأمريكية/التشكيلة الأساسية لحكومة الولايات المتحدة (USGCB)

التشكيلة FDCC وبديلتها USGCB واللتان تستعملان البروتوكول SCAP للمعهد الوطني للمعايير والتكنولوجيا (NIST) تتألف من مواصفات لتنظيم المعلومات المتعلقة بالأمن والتعبير عنها بأساليب قياسية فضلاً عن البيانات المرجعية ذات الصلة مثل معرفات الهوية الفريدة لمواطن التعرض. والغرض من هاتين المبادرتين هو استحداث تشكيلتين أساسيتين للأمن من أجل منتجات تكنولوجيا المعلومات والاتصالات يتم نشرهما على نطاق واسع عبر الوكالات الفيدرالية. والتشكيلة USGCB ظهرت من خلال التشكيلة FDCC. والتشكيلة USGCB عبارة عن مبادرة فيدرالية للحكومة ككل توفر توجيهات للوكالات بشأن ما ينبغي عمله لتحسين وصيانة عناصر فعالة للتشكيلة تركز في الأساس على الأمن.

والمواصفة التقنية للتشكيلة USGCB توضح المتطلبات والإصلاحات التي يجب استخدامها لضمان تبادل متسق ودقيق لمحتوى البروتوكول SCAP وقدرة المحتوى على العمل باعتمادية بأدوات SCAP مناسبة. وتتألف الصيغة الأولية من هذه التشكيلة من ست مواصفات: XCCDF وOVAL وCPE وCCE وCVE وCVSS. وتُصنف هذه المواصفات في ثلاث فئات: لغات وأنظمة تعداد وأنظمة قياس تقييم مواطن التعرض.

ويقوم البروتوكول SCAP بتنفيذ 1) نسق وتسمية محددان تقوم منتجات برمجيات الأمن بواسطتهما بتوصيل معلومات تدفق البرمجيات والتشكيلة الأمنية و2) تدفق محدد للبرمجيات وبيانات مرجعية قياسية بخصوص التشكيلة الأمنية تعرف بمحتوى البروتوكول SCAP. ومن بين أهداف البروتوكول SCAP تقييس إدارة أمن النظام وتحسين قابلية التشغيل البيني للمنتجات الأمنية وتعزيز استعمال الصيغ القياسية للمحتوى الأمني. وحيث إن من المرجح ظهور الكثير من محتويات SCAP المختلفة لأنظمة متنوعة ومستويات مختلفة للأمن، فإن اكتشاف التسمية المهيكلة وضمان التحقق بالنسبة للمخطط الحالي يمثلان شرطين هامين. وتولد مبادرة التشكيلة USGSB محتوى وتوجيهات تستند إلى مواصفات البروتوكول SCAP.

2.III مثال: الموقع الشبكي الياباني لمعلومات التعرض، JVN

JVN هي اختصار للكلمات "Japan Vulnerability Notes"، "مذكرات لمواطن التعرض في اليابان" وهي تقدم معلومات عن مواطن التعرض وما يتصل بها بشأن البرمجيات المستعملة في اليابان، وترمي إلى المساهمة في مكافحة التهديدات السيبرانية. ولتمكين مطوري التطبيقات من استعمال البيانات عبر سطح بيني مفتوح، اعتمدت البروتوكول SCAP وتضم معلومات محلية ودولية خلصت إلى إطار أتمتة المحتوى الأمني JVN. وعلى غرار قاعدة بيانات مواطن التعرض الوطنية (NVD)، تشتمل كل مجموعة من معلومات التعرض على رقم CVE وتقدم درجة تقييم للنظام CVSS بالإضافة إلى رقم للتعداد CWE. وعلاوة على ذلك، يُقدم اسم للتعداد CPE للمنتجات المتأثرة أيضاً.

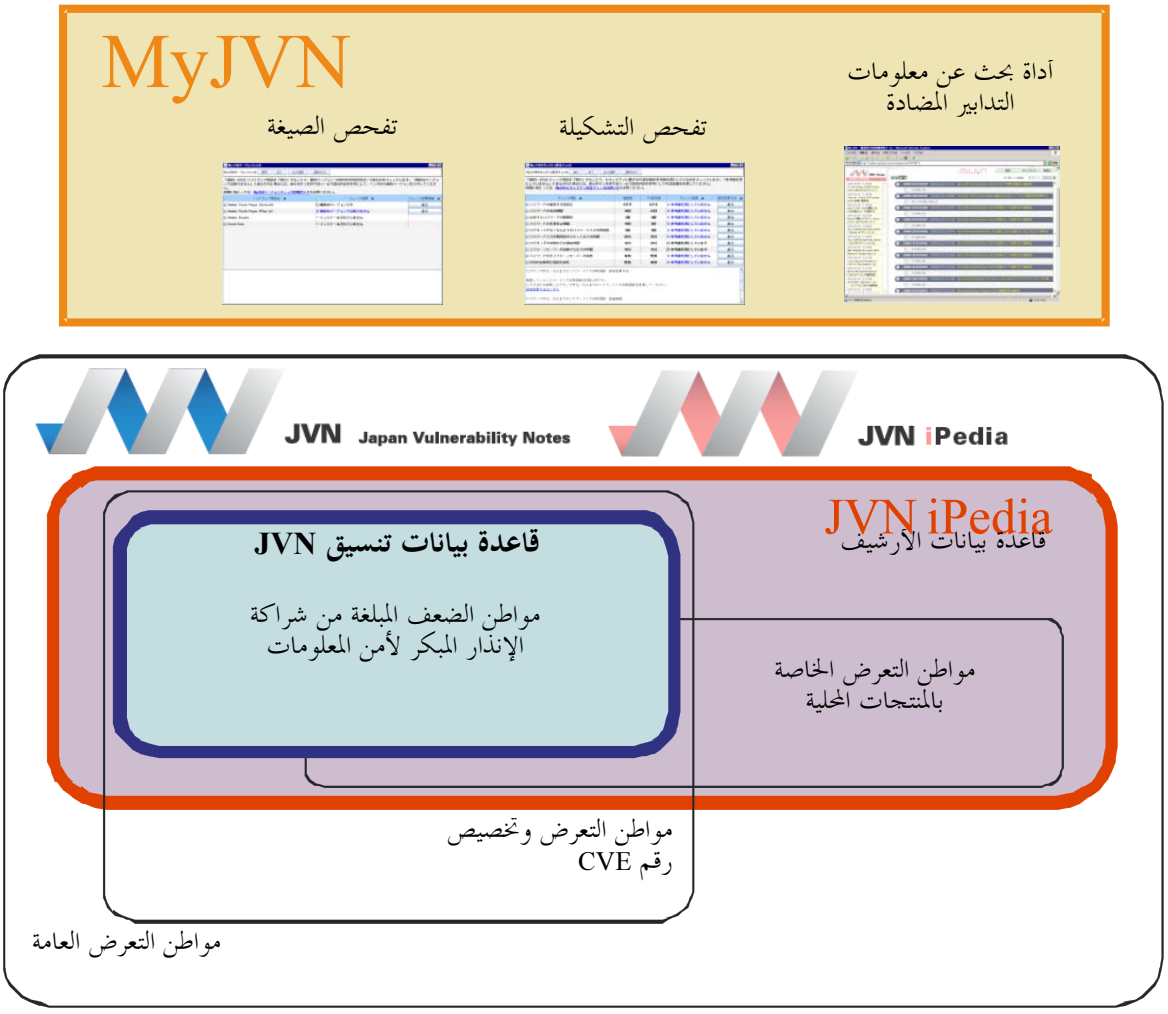
ويتألف الإطار من ثلاثة مكونات: MyJVN وJVN وJVN iPedia (انظر شكل 2.III)، حيث يرد أدناه فكرة مختصرة عن كل منها.

يوفر المكون MyJVN معلومات عن الإجراءات المضادة لمواطن التعرض عبر MyJVN API، وهي عبارة عن سطح بيني تقرأه الآلة يتضمن السطوح البينية لبرمجة التطبيق (API) للويب وأدوات MyJVN مثل أداة تفحص الصيغة. ويحسن هذا المكون من استعمال معلومات الإجراءات المضادة لمواطن التعرض المخزنة في JVN وJVN iPedia بتسهيل وزيادة كفاءة تجميع المعلومات التي يرغب منها المستعملون عن طريق خدمات مثل الترشيح المعدل حسب الحالة والبحث الأوتوماتي ووضع قائمة مرجعية. كما أن "أداة تفحص الصيغة الخاصة بالمكون MyJVN" عبارة عن أداة قائمة على البروتوكول SCAP تسمح للأفراد أن يتفحصوا بسهولة ما إذا كانت البرمجيات المحملة على أجهزة الحاسوب الشخصية الخاصة بهم هي أحدث صيغة.

ويوفر المكون JVN معلومات عن التدابير المضادة للتعرض وحالة البائعين اليابانيين بالنسبة لمواطن التعرض المبلغة من "شراكة الإنذار المبكر لأمن المعلومات"، وهي إطار شراكة بين القطاعين العام والخاص أُنشئت لتعزيز أمن منتجات البرمجيات ومواقع الويب ومنع انتشار الضرر إلى قطاع عريض من أجهزة الحاسوب من جراء الفيروسات الحاسوبية أو النفاذ غير المرخص.

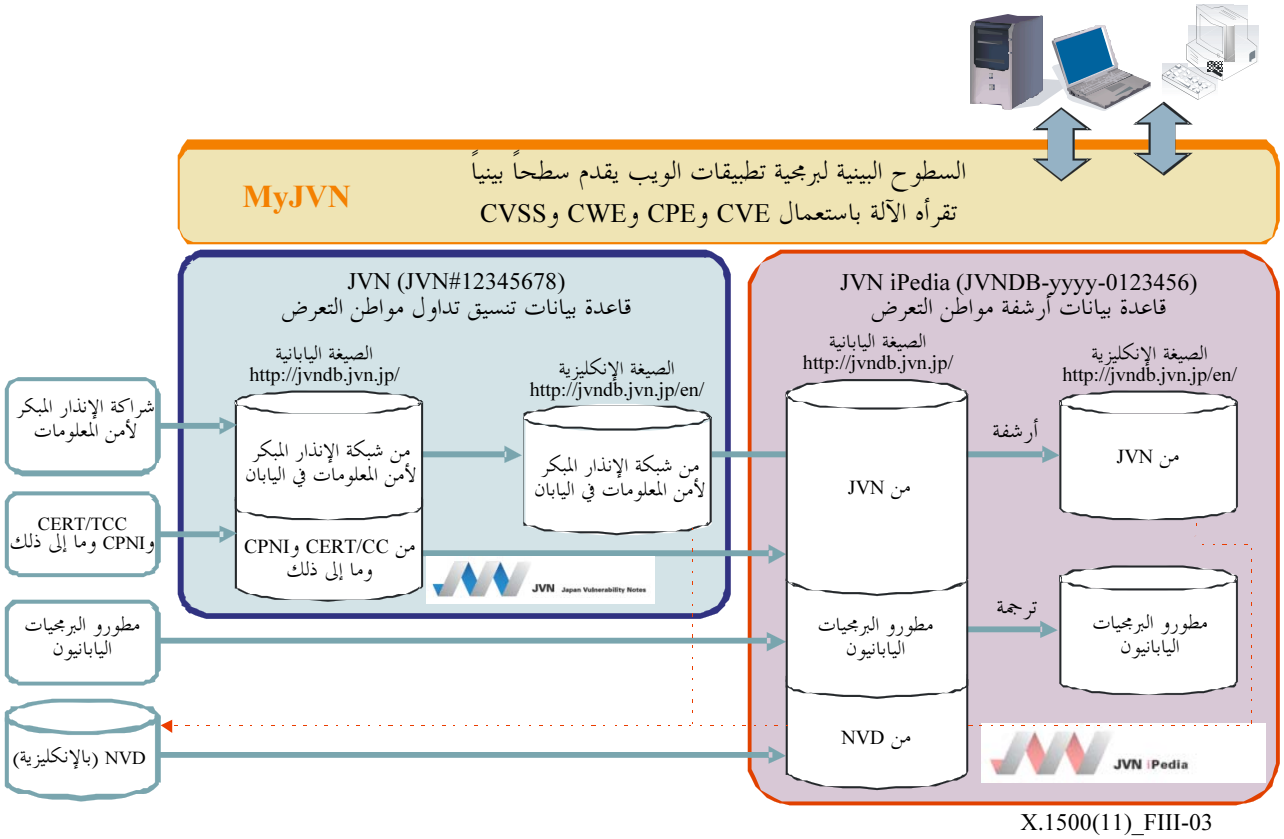
وعند الإبلاغ عن معلومات التعرض إلى وكالة النهوض بتكنولوجيا المعلومات (IPA) في اليابان باعتبارها الهيئة المتلقية لهذه الشراكة، تمرر إلى مركز التنسيق التابع للفريق الياباني للاستجابة للطوارئ الحاسوبية (JPCERT/CC) باعتباره الهيئة المسؤولة عن التنسيق. ويحدد المركز JPCERT/CC منتجات البرمجيات المتأثرة وينسق مع المطورين. وعندما تتوفر للمستعملين حلول بخصوص مواطن التعرض مثل الإصلاحات أو التحديثات الخاصة بالبرمجيات، يُنشر على الموقع JVN تفاصيل مواطن التعرض مع بيانات للمطورين.

ويوفر المكون JVN iPedia معلومات عن الوسائل المضادة للتعرض التي يتم جمعها بخصوص منتجات البرمجيات كل أنظمة التشغيل والتطبيقات والمكتبات والأنظمة المدمجة المستعملة في اليابان. ويهدف الموقع JVN إلى تقديم معلومات التعرض والتدابير المضادة للجمهور بأسرع وقت ممكن. وتقوم جهة تنسيق بالتعامل مع البائعين فيما يتعلق بتوقيت الإفصاح عن مواطن التعرض المبلغة حديثاً. وتتمثل مهمة المكون JVN iPedia من ناحية أخرى في تجميع معلومات إضافية عن مواطن التعرض والتدابير المضادة التي تظهر يومياً على منتجات البرمجيات اليابانية والتي لا تُنشر على الموقع JVN.



X.1500(11)_FIII-02

الشكل III.2 – مفهوم إطار أتمتة المحتوى الأمني JVN



X.1500(11)_FIII-03

الشكل 3.III – قاعدة بيانات مع معلومات دولية ومحلية

ويجوز للمستعملين الذين يتبنون أنساقاً قياسية مثل RSS التمتع بقاعدة بيانات تشمل معلومات دولية ومحلية (انظر الشكل 3.II). ومن بين المكونات الثلاث، تعمل MyJVN تسطح بيني للمستعمل يسهل استعماله مع ما يلي من الأدوات والسطوح البينية لبرمجة التطبيقات (API):

أدوات MyJVN والسطوح البينية لبرمجة التطبيقات

أدوات MyJVN عبارة عن أدوات أمنية تقوم على البروتوكول SCAP وتحسن من استعمال التدابير المضادة للتعرض ومن بيئة تبادل المعلومات بالنسبة للمستعملين والأدوات الرئيسية المتاحة حالياً هي كما يلي:

- **أداة ترشيح معلومات التدابير المضادة للتعرض** – تحسن هذه الأداة استعمال معلومات التدابير المضادة للتعرض المخزنة في JVN وفي JVNiPedia. حيث تسهل وتزيد من كفاءة المستعملين في تجميع المعلومات التي يؤدونها عن طريق خدمات مثل الترشيح المتوائم حسب الحاجة بواسطة التعداد CPE.
- **أداة تفحص الصيغة** – أداة تفحص الصيغة هي عبارة عن لغة OVAL تقوم على ماسح خطي يتيح للأفراد بسهولة تفحص ما إذا كانت البرمجيات المحملة على حواسيبهم الشخصية بالصيغة الأحدث. فبنقرة واحدة على الفأرة، يمكن للفرد تفحص العديد من البرمجيات. ويسهل فهم النتائج: حيث تميز علامة الصيغة الأحدث فيما تميز علامة الصيغة المتقادمة. فإذا لم تكن صيغة البرمجية هي الأحدث، يمكن للمستعملين النفاذ بسهولة إلى موقع الويب الخاص بالتحميل للبائع من خلال عدد قليل من النقرات. وتدعم أداة تفحص الصيغة الصادرة عن MyJVN منتجات البرمجيات الخاصة بالإنترنت والتي يتم اختيارها سعياً للتعاون من جانب بائعي البرمجيات.

- **أداة MyJVN لتفحص التشكيلة الأمنية** – هذه الأداة هي عبارة عن نسق XCCDF ولغة OVAL تقومان على ماسح خطي. وهي أداة مفتوحة سهلة الاستعمال لتقييم تشكيلة أمن نظام التشغيل ويندوز، بما في ذلك سياسات إنشاء الحساب مثل الحد الأدنى لطول كلمة السر وفترة انتهاء صلاحية كلمة السر والتشغيل الأوتوماتي لواقي الشاشة وخاصية التشغيل الأوتوماتي لمدخل التوصيل USB وما إلى ذلك.
- **السطح البيني MyJVN لبرمجة التطبيق** – هو عبارة عن سطح بيني برمجي للنفاذ إلى معلومات التدابير المضادة للتعرض المخزنة في JVN وJVNiPedia واستعمالها. ولتمكين مطوري التطبيقات من استعمال البيانات من خلال سطح بيني مفتوح، اعتمدت JVNipedia البروتوكول SCAP، وهو مجموعة من المعايير لوصف معلومات التدابير المضادة للتعرض. وباستعمال السطح البيني MyJVN API يمكن لأي تطبيقات متوائمة النفاذ إلى البيانات المخزنة في JVN iPedia ويمكن لمختلف خدمات إدارة مواطن التعرض أن تستعمل حالياً بكفاءة معلومات التدابير المضادة للتعرض.

والوظيفتان **الأساسيتان** للسطح البيني MyJVN API هما توفير سطح بيني API لخدمة معلومات مرشحة وسطح بيني API لخدمة تعاون SCAP. ويدعم السطح البيني الأول خدمات "احصل على قائمة بالمنتجات" و"احصل على قائمة بعرض مجمل لمواطن التعرض" وغيرها من التي تستعملها أداة ترشيح معلومات التدابير المضادة للتعرض. فيما يدعم السطح البيني الثاني خدمات "احصل على قائمة بتعاريف OVAL" و"احصل على بيانات تعاريف OVAL" وغيرها من التي تستعملها أداة تفحص الصيغة خاصة MyJVN وأداة تفحص تشكيلة الأمن خاصة MyJVN.

ولمزيد من المعلومات بشأن JVN، يرجى الرجوع إلى المرجع [b- Terada].

بيبليوغرافيـــا

[b-ITU-T E.409] Recommendation ITU-T E.409 (2004), *Incident organization and security incident handling: Guidelines for telecommunication organizations*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.1205] Recommendation ITU-T X.1205 (2008), *Overview of cybersecurity*.

[b-ITU-T X.1520] Recommendation ITU-T X.1520 (2011), *Common vulnerabilities and exposures (CVE).*

[b-ITU-T X.1521] Recommendation ITU-T X.1521 (2011), *Common vulnerability scoring system*.

[b-ETSI TS 102 042] ETSI TS 102 042 (2011), *Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates*.

[b-IETF RFC 3080] IETF RFC 3080 (2001), *The Blocks Extensible Exchange Protocol Core*. http://datatracker.ietf.org/doc/rfc3080/

[b-IETF RFC 5070] IETF RFC 5070 (2007), *The Incident Object Description Exchange Format*. http://datatracker.ietf.org/doc/rfc5070/

[b-IETF RFC 5901] IETF RFC 5901 (2010), *Extensions to the IODEF-Document Class for Reporting Phishing*. http://datatracker.ietf.org/doc/rfc5901/

[b-IETF RFC 6045] IETF RFC 6045 (2010), *Real-time Inter-network Defense (RID)*. http://datatracker.ietf.org/doc/rfc6045/

[b-IETF RFC 6046] IETF RFC 6046 (2010), *Transport of Real-time Inter-network Defense (RID) Messages*. http://datatracker.ietf.org/doc/rfc6046/

[b-ARF] Assessment Results Format. https://measurablesecurity.mitre.org/incubator/arf/

[b-CAPEC] Common Attack Pattern Enumeration and Classification. https://capec.mitre.org/

[b-CCE] Common Configuration Enumeration. https://cce.mitre.org/

[b-CEE] Common Event Expression. https://cee.mitre.org/

[b-CPE] Common Platform Enumeration. https://cpe.mitre.org/

[b-CWE] Common Weakness Enumeration. https://cwe.mitre.org/

[b-CWSS] Common Weakness Scoring System. https://cwe.mitre.org/cwss/

[b-EVCERT] CA/Browser Forum, *Guidelines for the Issuance and Management of Extended Validation Certificates*, Ver. 1.3

[b-MAEC] Malware Attribute Enumeration and Characterization. https://maec.mitre.org/

[b-NIST EAA] *Electronic Authentication Guideline*, NIST Special Publication 800-63 Version 1.0.2, April 2006

[b-OVAL] Open Vulnerability and Assessment Language. https://oval.mitre.org/

[b-Takahashi] Takahashi, T., Kadobayashi, Y., and Fujiwara, H. (2010), *Ontological Approach toward Cybersecurity in Cloud Computing*, International Conference on Security of Information and Networks, September.

[b-Terada] Terada, Masato, et al. (2009), *Proposal of MyJVN (Web Service APIs) for Security Information Exchange infrastructure*, 21st Annual FIRST Conference on Computer Security Incident Handling, June.
http://jvnrss.ise.chuo-u.ac.jp/jtg/doc/21thFirstConference_paper.pdf

[b-TLP] *CPNI Traffic Light Protocol* (2010), Information Sharing Levels, CPNI Information Exchange, UK, April.

[b-TNC] Trusted Computing Group, *Trusted Network Connect*.

Integrity Measurement Collectors – TCG Version (IF-IMC, Specification Ver. 1.2 Rev. 8, 5 Feb. 2007)

Integrity Measurement Verifiers – TCG Version (IF-IMV Specification Ver. 1.2 Rev. 8, 5 Feb. 2007)

Trusted Network Connect Client-Server – TCG Version (IF-TNCCS TLV Binding Specification Ver. 2.0 Rev. 16, 22 Jan. 2010)

Trusted Network Connect Client-Server Statement of Health – TCG Version (IF-TNCCS-SOH TLV Binding Specification Ver. 2.0 Rev. 10, 23 Jan. 2008)

Policy Enforcement Point – TCG Version (IF-PEP Protocol Bindings for RADIUS Specification Ver. 1.1 Rev. 0.7, 5 Feb. 2007)

Binding for SOAP – TCG Version (IF-MAP Specification Ver. 2.0 Rev. 36, 30 July 2010)

Platform Trust Services Interface – TCG Version (IF-PTS Specification Ver. 1.0 Rev. 1.0, 17 Nov. 2006)

Clientless Endpoint Support Profile – TCG Version (CESP Specification Ver. 1.0 Rev. 13, 18 May 2009)

[b-TPM] Trusted Computing Group, *Trusted Platform Modules*.

Design Principles – TCG Version (TPM Main, Part 1, Specification Ver. 1.2, Level 2 Rev. 103, 9 July 2007), ISO/IEC Version (11889-2, 2009-05-15, Information technology – TPM – Part 2)

TPM Structures – TCG Version (TPM Main, Part 2. Specification Ver. 1.2, Level 2 Rev. 103, 9 July 2007), ISO/IEC Version (11889-3, 2009-05-15, Information technology – TPM – Part 3)

Commands – TCG Version (TPM Main, Part 3, Specification Ver. 1.2, Level 2 Rev. 103, 9 July 2007), ISO/IEC Version (11889-4, 2009-05-15, Information technology – TPM – Part 4)

The TPM 1.2 specifications have also been adopted as ISO/IEC 11889. Overview – TCG Version (N/A), ISO/IEC Version (11889-1, 2009-05-15, Information technology – TPM – Part 1)

[b-W3C SOAP] W3C Recommendation Simple Object Access Protocol (SOAP), 2007.

SOAP Version 1.2 Part 1: Messaging Framework.

SOAP Version 1.2 Part 2: Adjuncts.

[b-XCCDF] The eXtensible Configuration Checklist Description Format.
http://scap.nist.gov/specifications/xccdf/

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات (ISDN)
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	بناء الكبلات وغيرها من عناصر المنشآت الخارجية وإنشاؤها وحمايتها
السلسلة M	إدارة الاتصالات، بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	صيانة الدارات الإذاعية الدولية لإرسال البرامج الصوتية والتلفزيونية
السلسلة O	مواصفات أجهزة القياس
السلسلة P	جودة الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير
السلسلة R	التراسل الإبراقي
السلسلة S	التجهيزات الانتهائية لخدمات الإبراق
السلسلة T	تجهيزات مطرافية للخدمات التلماتية
السلسلة U	التبديل الإبراقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2012