الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1216
(2020/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – الأمن السيبراني

متطلبات جمع أدلة حوادث الأمن السيبراني وحفظها

التوصية ITU-T X.1216

الاتحاد الدولي للاتصالات

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
الدليل	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 (1)	
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 (1)	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	
الامن السيبراني	**X.1229–X.1200**
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1309–X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1319–X.1310
أمن شبكة الكهرباء الذكية	X.1339–X.1330
البريد المعتمد	X.1349–X.1340
أمن إنترنت الأشياء (IoT)	X.1369–X.1360
أمن أنظمة النقل الذكية (ITS)	X.1389–X.1370
أمن سجل الحسابات الموزع	X.1429–X.1400
أمن سجل الحسابات الموزع	X.1449–X.1430
البروتوكول الأمني (2)	X.1459–X.1450
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
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1659–X.1640
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أمن أشكال أخرى للحوسبة السحابية	X.1699–X.1680
الاتصالات الكمومية	
المصطلحات	X.1701–X.1700
مولد الأعداد العشوائية الكمومية	X.1709–X.1702
إطار أمن شبكات توزيع المفاتيح الكمومية	X.1711–X.1710
تصميم أمن شبكات توزيع المفاتيح الكمومية	X.1719–X.1712
تقنيات أمن شبكات توزيع المفاتيح الكمومية	X.1729–X.1720
أمن البيانات	
أمن البيانات الضخمة	X.1759–X.1750
أمن شبكات الجيل الخامس	X.1819–X.1800

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

التوصية ITU-T X.1216

متطلبات جمع أدلة حوادث الأمن السيبراني وحفظها

ملخص

توضح التوصية ITU-T X.1216 إجراءً عاماً للتصدي لحوادث الأمن السيبراني والتحقيق فيها، وتحلل مصادر أدلة حوادث الأمن السيبراني، وتحدد المتطلبات المتعلقة بقدرات الأدوات المستخدمة لجمع هذه الأدلة وحفظها في أي عملية تحقيق. كما توصف هذه التوصية متطلبات ضمان موثوقية هذه الأدوات كمبادئ توجيهية للمطوِّرين المعنيين بتصميم الأدوات المستخدمة لهذا الغرض.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1216	2020-09-03	17	11.1002/1000/14259

مصطلحات أساسية

الأمن السيبراني، أدلة حوادث الأمن السيبراني، التصدي للحوادث والتحقيق فيها.

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

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 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد 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 "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" 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

التوصية ITU-T X.1216

متطلبات جمع أدلة حوادث الأمن السيبراني وحفظها

1 مجال التطبيق

تبين هذه التوصية إجراءً عاماً للتصدي لحوادث الأمن السيبراني والتحقيق فيها. كما أنها تحلل مصادر أدلة حوادث الأمن السيبراني، وتحدد المتطلبات المتعلقة بقدرة الأدوات المستخدمة لجمع هذه الأدلة وحفظها في أي عملية تحقيق. كما تحدد هذه التوصية متطلبات ضمان موثوقية هذه الأدوات كمبادئ توجيهية للمطوِّرين المعنيين بتصميم الأدوات المستخدمة لهذا الغرض.

ولا تشمل هذه التوصية مسائل ولوائح الخصوصية المتصلة بجمع بيانات حوادث الأمن السيبراني ولا الإجراءات القانونية والتأديبية وغيرها من الإجراءات المتصلة بالتعامل مع الأدلة المحتملة لحوادث الأمن السيبراني، إذ تُعد هذه العناصر خارجة عن نطاق عمليتي 'الجمع والحفظ'.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

لا يوجد.

3 التعاريف

1.3 مصطلحات معرَّفة في وثائق أخرى

تُستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 الجمع [b-ISO/IEC 27037]: يُقصد به عملية جمع العناصر المادية التي تحوي أدلة رقمية محتملة.

2.1.3 الأدلة [b-ITU-T X.813]: هي معلومات يمكن أن تستخدم، إما في حد ذاتها أو بالاقتران بمعلومات أخرى، لتسوية نزاع.

3.1.3 التحقيق [b-ISO/IEC 27042]: يُقصد به إجراء الفحوصات والتحليلات وأعمال التفسير اللازمة للمساعدة في فهم الحادث.

4.1.3 الحفظ [b-ITU-R BR.1351]: يشير إلى عمليات الرعاية الواجب إجراؤها لضمان الحفظ السليم للمواد المحفوظة، كالتحقق الدوري من حالة تدهور الوسائط وإعادة إنتاج المحتوى في وسائط جديدة عند اللزوم.

5.1.3 حادث أمني [b-ITU-T E.409]، [b-IETF RFC 2828]: يُقصد به أي حدث ضار يمكن أن يهدد بعض الجوانب الأمنية.

6.1.3 خاتم التوقيت [b-ISO/IEC 27037]: هو مَعلمة متغيرة زمنياً تُشير إلى نقطة زمنية بالنسبة إلى مرجع زمني مشترك.

2.3 المصطلحات المعرَّفة في هذه التوصية

يُعرَّف في هذه التوصية المصطلحان التاليان:

1.2.3 أدلة حوادث الأمن السيبراني: هي المعلومات أو البيانات، المخزَّنة أو المنقولة في نسق إثنيني، والتي ثبتت أهميتها للتحقيق في حادث الأمن السيبراني من خلال عملية تحليل.

ملاحظة – يستند هذا التعريف إلى تعريف 'الأدلة الرقمية' الوارد في المعيار [b-ISO/IEC 27037].

2.2.3 الدفاع بتحريك الهدف: يُقصد به آليات تقوم بالتغيير التلقائي لنعتٍ أو أكثر من نعوت النظام بهدف عدم تمكين الخصوم من التنبؤ بسطح النظام المعرَّض للهجوم.

ملاحظة – يستند هذا التعريف إلى المعيار [b-Jajodia14].

4 الاختصارات والأسماء المختصرة

تُستخدم في هذه التوصية الاختصارات والأسماء المختصرة التالية:

ARP بروتوكول استبانة العنوان *(Address Resolution Protocol)*

BYOD أحضر جهازك الشخصي *(Bring Your Own Device)*

DLL مكتبة موصولة دينامياً *(Dynamic Linked Library)*

IP بروتوكول الإنترنت *(Internet Protocol)*

MAC التحكم في النفاذ إلى الوسائط *(Media Access Control)*

MTD الدفاع بتحريك الهدف *(Moving Target Defence)*

PE File ملف محمول قابل للتنفيذ *(Portable Executable File)*

PII المعلومات المحددة لهوية الأشخاص *(Personally Identifiable Information)*

WORM أسلوب الكتابة مرة والقراءة عدة مرات *(Write Once Read Many)*

5 الاصطلاحات

في هذه التوصية:

تشير كلمة "يُتطلب/يتعيَّن/يلزم/يجب" إلى متطلَّب يجب التقيد به على نحو صارم ولا يجوز أي انحراف عنه إذا أريد إعلان المطابقة مع هذه الوثيقة.

وتشير كلمة "يُوصَى" إلى متطلَّب يُوصى به لكنه ليس ملزِماً إلزاماً مطلَقاً. وبالتالي لا يستلزم إعلانُ المطابقة تحقُّقَ هذا المتطلَّب.

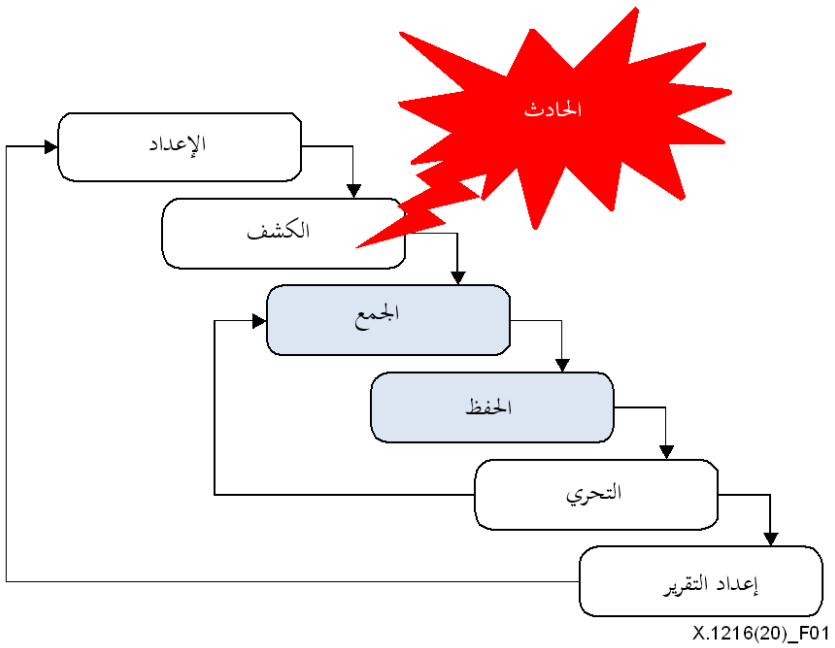
6 نظرة عامة على أدلة حوادث الأمن السيبراني

1.6 الإجراء العام للتصدي للحوادث والتحقيق فيها

عند تحليل سبب وقوع حادث من حوادث الأمن السيبراني، تُشكل عمليتا جمع الأدلة المتصلة بالحادث وحفظها مكوناً حاسماً في التصدي له والتحقيق فيه، إذ قد تصبح بيانات حادث الأمن السيبراني التي جرى تحليلها أدلةً محتملة في القضايا المرفوعة أمام المحاكم. علاوةً على ذلك، يمكن استخدام أدلة حوادث الأمن السيبراني لفحص مواطن الضعف ذات الصلة في المنظمة المعنية بهدف تعزيز الأمن السيبراني للمنظمة.

ويشمل إجراء التحقيق في الحادث، المبين في الشكل 1، المراحل التسلسلية التالية:

- الإعداد: ينبغي في هذه المرحلة إنجاز الأعمال التحضيرية الأولية اللازمة للتحقيق في الحادث.
- الكشف: في هذه المرحلة، يُرصد وقوع حدث غير مصرح به، أي حادث. وينبغي عندئذ اتخاذ قرار، وفقاً لجسامة الحادث، بشأن كيفية التصدي له وجمع بيانات عنه.
- الجمع: ينبغي الحصول على البيانات من الأدوات المستخدمة لجمع بيانات حركة الشبكة. وهذه المرحلة شديدة الأهمية. ونظراً إلى ارتفاع سرعة تبادل بيانات حركة الشبكة، لا يمكن توليد نفس بيانات الحركة في وقت لاحق.
- الحفظ: ينبغي تخزين البيانات الأصلية لحركة الشبكة على جهاز تخزين احتياطي، كما ينبغي تخزين صِيَغ مختزلة لجميع البيانات.
- التحقيق: في هذه المرحلة، ينبغي الدمج بين جميع الخيوط التي تم جمعها ويُبحث عن الأدلة اللازمة لتحديد الآثار الرقمية التي يُخلّفها مرتكب الهجمة وراءه. كما تُصنَّف المؤشرات ويُربط بينها بغرض استنتاج ملاحظات مهمة من الأنساق القائمة للهجمة. ويمكن في هذه المرحلة تحديد مسار الهجمة، ونسبة الهجمة إلى مرتكبها، وبالتالي تحديد هويته، بإجراء تحليلات مراراً وتكراراً في هذه المرحلة للتوصل إلى استنتاج بشأنه.
- إعداد التقرير: تُعرض الملاحظات والتوضيحات المتعلقة بالتحقيق في تقرير يُعد بلغة مفهومة لتقديمه إلى موظفي الشؤون القانونية.

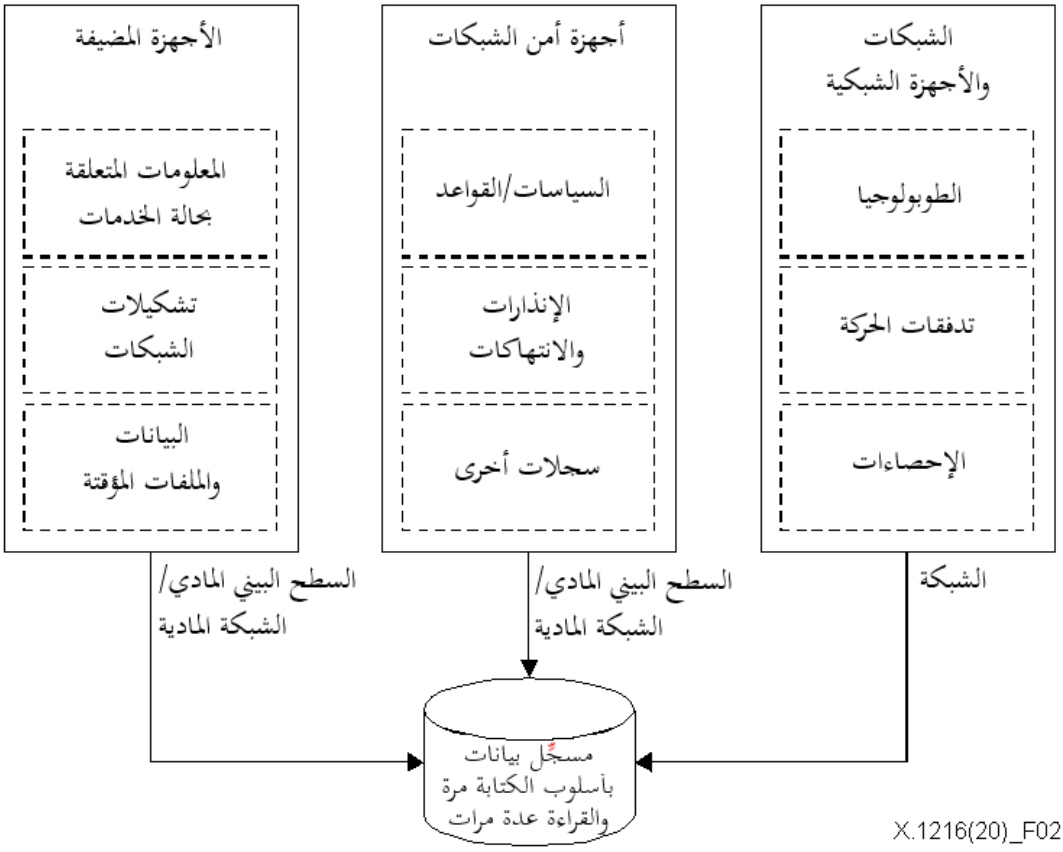


الشكل 1 – الإجراء العام للتحقيق في الحوادث

وقد تم تقييس العديد من المبادئ التوجيهية للمنظمة الدولية للتوحيد القياسي (ISO)/المنظمة الكهرتقنية الدولية (IEC) المتعلقة بالتحقيقات الرقمية والتصدي للحوادث الرقمية، في المعايير [b-ISO/IEC 27035-3] و[b-ISO/IEC 27037] و[b-ISO/IEC 27041] و[b-ISO/IEC 27042] و[b-ISO/IEC 27043]. وتركز هذه المبادئ التوجيهية بشكل أساسي على توفير أفضل الممارسات وكيفية التعامل مع الأدلة الرقمية في جميع مراحل التحقيق في الحادث. ويقدم المعيار [b-IETF RFC 3227] أيضاً المبادئ التوجيهية المتعلقة بجمع الأدلة وحفظها، كالأعمال التحضيرية والاعتبارات المتعلقة بخطوات الجمع؛ واختيار وسائط الحفظ ووثائق سلسلة العهدة؛ ومجموعة الأدوات اللازمة لجمع الأدلة وحفظها. غير أن المبادئ التوجيهية المتعلقة باختيار أدوات التحقيق أو استحداثها غير مبيّنة بوضوح.

2.6 مصادر بيانات حوادث الأمن السيبراني

من المصادر النمطية للبيانات المتعلقة بحوادث الأمن السيبراني الأجهزة المضيفة وأجهزة أمن الشبكات والأجهزة الشبكية والشبكات. ويصور الشكل 2 تصنيفَ المعلومات التي تُتيحها مصادر البيانات.



الشكل 2 – مختلف مصادر الحصول على البيانات المتصلة بحوادث الأمن السيبراني

1.2.6 الأجهزة المضيفة

يُتيح الجهاز المضيف، بوجه عام، أنواعاً مختلفة من البيانات المتصلة بحوادث الأمن السيبراني. وينبغي أن تقوم أدوات جمع هذه البيانات بجمعها بعناية، إذ إن بعضها مؤقت ويمكن إتلافه بسهولة. وفيما يلي أنماط البيانات التي يمكن جمعها من الجهاز المضيف:

(1) بيانات متعلقة بالنظام:

- معلومات عامة (اسم الجهاز المضيف، المعلومات المتعلقة بحساب المستخدِم، التاريخ والوقت في النظام، توقيت آخر تشغيل للجهاز، النطاق الزمني الحالي، جهاز التشغيل)؛
- المعلومات المتعلقة بنظام التشغيل (الجهة المصنِّعة، الاسم، المعمارية، الإصدار، الرقم التسلسلي، تاريخ التثبيت)؛

- برامج التطبيقات (البرامج المثبتة، حالة التصحيح والإصلاح، المتغيرات البيئية)؛
- العمليات: (جدول العمليات، العمليات التي تعمل تلقائياً، الخدمات المجدولة)؛
- جلسة تسجيل الدخول؛
- سائر بيانات سجل النظام.

(2) المعلومات المتعلقة بالبيانات والتخزين:

- بيانات الذاكرة؛
- أنظمة الملفات المؤقتة (الملفات المستخدمة أو المنفَّذة مؤخراً، بما فيها المكتبة الموصولة دينامياً (DLL) ورموز الملفات (handles))؛
- الملفات المخفيّة، الملفات القابلة للتنفيذ، الملفات التي تم فتحها، الملفات المحذوفة، المساحة غير الموزَّعة؛
- وسائط الحفظ؛
- البيانات المشتركة (المجلدات المشتركة، الأجهزة الشبكية)؛

(3) البيانات المتعلقة بالتوصيل الشبكي:

- جدول التسيير، الذاكرة المخفية لبروتوكول استبانة العنوان (ARP)، الإحصاءات المتعلقة بالنواة؛
- تشكيلات الشبكات: (عناوين بروتوكول الإنترنت (IP)، عناوين طبقة التحكم في النفاذ إلى الوسائط (MAC)، المنافذ المفتوحة، السطوح البينية للشبكات)؛
- المعلومات المتعلقة بمتصفِّح الإنترنت (الاستخدامات السابقة لمتصفِّح الإنترنت، أغراض الإنترنت التي تم النفاذ إليها مؤخراً، ملفات البيانات المختصرة لمواقع الويب (Cookies)).

2.2.6 أجهزة أمن الشبكات

ينبغي أن تُجمع البيانات المتصلة بأنشطة الهجمات من أجهزة أمن الشبكات، كأنظمة الكشف عن الاقتحام وجدران الحماية.

- السياسات الأمنية (التحكم في النفاذ، قواعد الكشف)؛
- الأحداث والسجلات الأمنية (التنبيهات، الإنذارات، التحذيرات، الأخطاء)؛
- المعلومات الإحصائية.

3.2.6 الشبكات والأجهزة الشبكية

من المهم جمع البيانات من الشبكات عند التحقيق في الهجمات السيبرانية. وعلى وجه الخصوص، يمكن للمعلومات المتعلقة بطوبولوجيا الشبكة أن تساعد المحققين في الحوادث السيبرانية على فهم مكوّنات شبكة المؤسسة المعنية وتشكيلات الشبكة واكتشاف مسارات الهجمات وتقدير حجم الضرر الذي لحق بالشبكة، وخاصةً في ظل التغير الدينامي في تشكيلات الشبكات المصاحب لنشر التكنولوجيات الأمنية القائمة على الحوسبة السحابية والآلات الافتراضية وسياسة 'أحضر حاسوبك الشخصي' (BYOD) وآلية الدفاع بتحريك الهدف (MTD) في الوقت الحاضر. ومن الأمثلة النمطية لبيانات الشبكات والأجهزة الشبكية ما يلي:

- تشكيلة طوبولوجيا الشبكة؛
- سجلات وقائع المُسيِّر؛
- الخدمات الموصولة شبكياً؛
- المعلومات المتعلقة بالأجهزة المضيفة الموصولة شبكياً (المنافذ المفتوحة، الخدمات العاملة داخلياً، الحالة)؛
- الآثار الدالة على الحركة، بما في ذلك الرأسية والبيانات؛

- بيانات تدفق الدورة (عنوان بروتوكول الإنترنت للمَصدر/رقم مَنفذ المصدر، عنوان بروتوكول الإنترنت للمقصد/رقم مَنفذ المقصد، البروتوكول، المعلومات الأخرى المتعلقة برأسية بروتوكول التحكم في الإرسال (TCP))؛
- الملفات المنقولة عبر الشبكة؛
- الإحصاءات المتعلقة بحركة الشبكة.

7 متطلبات جمع بيانات حوادث الأمن السيبراني

إن تحديد كيفية جمع البيانات وحفظها وتحليلها عند وقوع حادث أمني سيبراني لا يقل أهميةً عن تحديد ماهية البيانات اللازم جمعها. ويبين هذا القسم قدرات جمع بيانات حوادث الأمن السيبراني من الأنماط الثلاثة لمصادر البيانات، المعروضة في القسم 6.

ونظراً إلى أن بيانات تسجيل الوقائع وغيرها من البيانات المتصلة بالحوادث التي يتم جمعها من مصادر البيانات سالفة الذكر قد تشتمل على معلومات محددة لهوية الأشخاص (PII). ينبغي للجهة المنفِّذة أن تُقصِر جمع أي من المعلومات PII على ما تقتضيه الضرورة القصوى حصرياً للإبلاغ عن الحادث والتصدي له، وأن تحمي هذه المعلومات وفقاً للقوانين واللوائح السارية ذات الصلة.

1.7 جمع البيانات المتصلة بحوادث الأمن السيبراني من الأجهزة المضيفة

تشكل الأجهزة المضيفة المصدر الأساسي نمطياً للبيانات اللازمة لتحليل حوادث الأمن السيبراني. إذ تُتيح هذه الأجهزة بيانات السجلات وسجلات الوقائع والملفات التي يُحمِّلها النظام. وإذا استدعى الأمر إجراء تحليل أدق، ينبغي إفراغ محتويات الذاكرة من الجهاز المضيف.

ولدعم إنجاز مهمة الجمع هذه، ينبغي أن تتوفر في أدوات جمع البيانات قدرات من قبيل تلك المسرودة أدناه:

- فحص العمليات وجمع المعلومات المتعلقة بها؛
- جمع معلومات عن حالة النظام؛
- إجراء نُسَخ شاملة لجميع البتّات؛
- إنتاج صور أساسية؛
- أَتمتة عملية الجمع؛
- توريد البيانات التي يتم جمعها وتصديرها؛
- دعم نظم تشغيل مختلفة للأجهزة المضيفة؛
- توفير المكتبات اللازمة لجمع البيانات وعدم استخدام أي من المكتبات القائمة في الأجهزة المضيفة؛
- جمع البيانات المؤقتة أثناء تشغيل النظام؛
- جمع بيانات عن حالة الشبكية للتوصيل الراهن والمقبس المفتوح.

2.7 جمع بيانات حوادث الأمن السيبراني من أجهزة أمن الشبكات

ينبغي الحصول على كم كبير من البيانات المفيدة من أجل تحليل حوادث الأمن السيبراني، من أجهزة أمن الشبكات، كأنظمة الحماية من الاقتحام وأنظمة الكشف عنه وأنظمة منعه وأنظمة جدران الحماية وأنظمة إدارة المعلومات والوقائع الأمنية.

ولدعم إنجاز مهمة الجمع هذه، ينبغي أن تتوفر في أدوات جمع البيانات قدرات من قبيل القدرات التالية:

- جمع سجلات الوقائع من أجهزة أمن الشبكات؛
- جمع سجلات وقائع الإنذارات والانتهاكات من أجهزة أمن الشبكات؛
- جمع سجلات وقائع الاستيقان من المستخدِم من أجهزة أمن الشبكات؛
- جمع البيانات المتعلقة بالسياسات والقواعد الأمنية لأجهزة أمن الشبكات.

3.7 جمع بيانات حوادث الأمن السيبراني من الشبكات والأجهزة الشبكية

تعمد المنظمة إلى جمع الأدلة وإجراء رصد للشبكة لتحديد أي نقاط قد تشير إلى الاشتباه في تورّط متآمرين من داخلها. ففي حال عدم فعالية عملية الرصد القائمة على الأجهزة المضيفة، يمكن لرصد الشبكة أن يزيد من فعالية الأدلة. ولا يستهدف رصد الشبكة منع وقوع هجمات وإنما يرمي، بالأحرى، إلى جمع معلومات مهمة في حال وقوع حادث، كما أنه يوفر عدداً أكبر بكثير من الأدلة اللازمة لتحليل الحادث. ولجمع البيانات المتصلة بالحادث الأمني من الشبكات والأجهزة الشبكية، ينبغي أن تتوفر في أدوات جمع البيانات القدرات التالية:

- جمع البيانات المتعلقة بحركة الشبكة دون فاقد؛
- استخراج تدفقات الدورة من حركة الشبكة المتتبَّعة وجمع المعلومات المتعلقة بهذه التدفقات مثل عنوان بروتوكول الإنترنت للمصدر ورقم مَنفذ المصدر، وعنوان بروتوكول الإنترنت للمقصد ورقم مَنفذ المقصد، والمعلومات المتعلقة ببروتوكول الإنترنت والخدمات، وتوقيتيْ بدء الدورة وانتهائها، وعدد الحِزم الواردة وحجمها، وعدد الحزم الصادرة وحجمها؛
- جمع الملفات المحمولة القابلة للتنفيذ (PE) المنقولة عبر الشبكة واستخراج المعلومات المتعلقة بالملفات كاسم الملف، وحجمه، وتوقيت جمعه، وعنوان بروتوكول الإنترنت للمصدر ورقم منفذ المصدر فيما يتعلق بالدورة التي تحوي ملفات محمولة قابلة للتنفيذ (PE File)، وعنوان بروتوكول الإنترنت للمقصد ورقم منفذ المقصد فيما يتعلق بالدورة التي تحوي ملفات PE، والبروتوكول الخاص باستخدام برتوكول الإنترنت؛
- جمع سجلات الوقائع الخاصة بالأجهزة الشبكية، كالسجلات المتعلقة بالمسيّرات والبدّالات وأنظمة رصد الشبكة.

8 متطلبات حفظ بيانات حوادث الأمن السيبراني

لتحليل أسباب حوادث الأمن السيبراني، يتعين حفظ البيانات الأصلية التي يتم جمعها وتجنب احتمال تلفها. وعلى وجه الخصوص، في حال النظر في قضايا مرفوعة أمام المحاكم، يلزم حفظ البيانات التي يتم جمعها حفاظاً على سلامة الأدلة ومشروعيتها. ودعماً لإنجاز هذه المهمة، ينبغي أن تكون أدوات حفظ البيانات مدعومةً بالقدرات التالية:

- إنتاج المجاميع التدقيقية والتوقيعات الرقمية؛
- التحقق من حفظ البيانات التي يتم جمعها دون فاقد؛
- إنتاج خاتم توقيت (بالوحدات ms) لتوقيتي جمع البيانات وحفظها؛
- تسجيل البيانات التي يتم جمعها على مسجّل للبيانات بأسلوب الكتابة مرة والقراءة عدة مرات (WORM)؛
- تقديم بيان وصفي لسياسات الاحتفاظ بالبيانات، التي ينبغي اعتمادها بناءً على ذلك؛
- ضمان حفظ البيانات التي يتم جمعها طوال مدة تنفيذ السياسة ذات الصلة؛
- حفظ البيانات والبيانات الشرحية التي يتم جمعها في شكل رسمي الطابع (يرد توصيف الاعتبارات المختلفة المتعلقة بهذه المسألة في [b-ITU-T X.1215] و[b-ITU-T X.1541]).

9 متطلبات أدوات جمع البيانات وحفظها لضمان الموثوقية

يمكن أن تُستخدم البيانات التي يتم جمعها وحفظها بأدوات جمع البيانات وحفظها للتحقيق في وقوع حوادث الأمن السيبراني، وكأدلة لتحديد هوية المسؤولين عن الحوادث.

لذا، ينبغي أن تتوفر في أدوات جمع البيانات وحفظها المستخدمة لتحليل حوادث الأمن السيبراني القدرات التالية ضماناً للموثوقية من حيث إدارة المستخدمين وإدارة البيانات:

- ينبغي أن توفر الأداة المستخدمة وسيلةً لتقييد نفاذ المستخدِم إليها وإلى البيانات المخزنة والتحكم في هذا النفاذ؛

- ينبغي ألا تسمح الأداة المستخدمة بمحاولة الكتابة على البيانات المحتفَظ بها أو تغييرها أو حذفها دون الحصول على الإذن المناسب؛
- ينبغي أن توفر الأداة المستخدمة وظائف تتعلق بإدارة الأمن يستطيع المديرون المخول لهم من خلالها تشكيل وإدارة الوظائف والسياسات الأمنية والبيانات المهمة؛
- عند نقل البيانات التي يتم جمعها بين جهازين منفصلين مادياً، يجب تجفير البيانات لضمان سريتها وسلامتها؛
- ينبغي أن تَستعمل جميع وسائل الاتصالات المقترنة بالأداة المستخدمة بروتوكولاً مجفراً مأموناً للاتصالات؛
- ينبغي أن توفر الأداة المستخدمة وظيفة التخزين الاحتياطي للبيانات التي يتم حفظها؛
- ينبغي أن توفر الأداة المستخدمة قدرات تسجيل الوقائع والإبلاغ عن الأخطاء وتدقيقها؛
- ينبغي أن توفر الأداة قدرات لمعالجة البيانات الشرحية والمحتوى الرسمي وتقاسمه وفقاً للسياسات القائمة (كما هو موصف في [b-ITU-T X.1550] و[b-ITU-T X.1582]).

بيبليوغرافيا

[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.813] Recommendation ITU-T X.813 (1996), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework.*

[b-ITU-T X.1215] Recommendation ITU-T X.1215 (2019), *Use cases for structured threat information exchange*.

[b-ITU-T X.1541] Recommendation ITU-T X.1541 (2017), *Incident object description exchange format 2*.

[b-ITU-T X.1550] Recommendation ITU-T X.1550 (2017), *Access control models for incident exchange networks*.

[b-ITU-T X.1582] Recommendation ITU-T X.1582 (2014), *Transport protocols supporting cybersecurity information exchange*.

[b-ITU-R BR.1351] Recommendation ITU-R BR.1351 (1998) *Requirements for the application of digital technology to audio archiving systems for radio broadcasting*.

[b-IETF RFC 2828] IETF RFC 2828 (2000), *Internet Security Glossary*.

[b-IETF RFC 3227] IETF RFC 3227 (2002), *Guidelines for Evidence Collection and Archiving.*

[b-ISO/IEC 27035-3] ISO/IEC 27035-3, *Information technology – Security techniques – Information security incident management – Part 3: Guidelines for incident response operations.*

[b-ISO/IEC 27037] ISO/IEC 27037:2012, *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence.*

[b-ISO/IEC 27041] ISO/IEC 27041:2015, *Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method.*

[b-ISO/IEC 27042] ISO/IEC 27042:2015 *Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence.*

[b-ISO/IEC 27043] ISO/IEC 27043: 2015, *Information technology – Security techniques – Incident investigation principles and processes.*

[b-Jajodia14] Jajodia, Sushil, and Kun Sun. "MTD 2014: First ACM workshop on moving target defense." Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. 2014.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
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
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2020