هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة. ويجب إزالة التظليل الملون بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

.



نموذج معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني

استبدل <اسم الجهة> باسم الجهة في مجمل صفحات الوثيقة. وللقيام بذلك، اتبع الخطوات التالية:

* اضغط على مفتاحي "Ctrl" و"H" في الوقت نفسه.
* أضف "<اسم الجهة>" في مربع البحث عن النص.
* أدخل الاسم الكامل لجهتك في مربع "استبدال" النص.
* اضغط على "المزيد" وتأكّد من اختيار "Match case".
* اضغط على "استبدل الكل".
* أغلق مربع الحوار.

|  |
| --- |
| اختر التصنيف |
| التاريخ: | اضغط هنا لإضافة تاريخ |
| الإصدار: | اضغط هنا لإضافة نص |
| المرجع: | اضغط هنا لإضافة نص |
|  |  |
|  |  |

إخلاء المسؤولية

طُور هذا النموذج عن طريق الهيئة الوطنية للأمن السيبراني كمثال توضيحي يمكن استخدامه كدليل ومرجع للجهات. يجب أن يتم تعديل هذا النموذج ومواءمته مع أعمال <اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة. كما يجب أن يُعتمد هذا النموذج من قبل رئيس الجهة أو من يقوم/تقوم بتفويضه. وتخلي الهيئة مسؤوليتها من استخدام هذا النموذج كما هو، وتؤكد على أن هذا النموذج ما هو إلا مثال توضيحي.

اعتماد الوثيقة

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| التوقيع | التاريخ | الاسم | المسمى الوظيفي | الدور |
| <أدخل التوقيع> | اضغط هنا لإضافة تاريخ | <أدخل الاسم الكامل للموظف> | <أدخل المسمى الوظيفي> | اختر الدور |
|  |  |  |  |  |

نسخ الوثيقة

|  |  |  |  |
| --- | --- | --- | --- |
| النسخة | التاريخ | عُدلَ بواسطة | أسباب التعديل |
| <أدخل رقم النسخة> | اضغط هنا لإضافة تاريخ | <أدخل الاسم الكامل للموظف> | <أدخل وصف التعديل> |
|  |  |  |  |

جدول المراجعة

|  |  |  |
| --- | --- | --- |
| معدل المراجعة | التاريخ لأخر مراجعة | تاريخ المراجعة القادمة |
| مره واحدة كل سنة | اضغط هنا لإضافة تاريخ | اضغط هنا لإضافة تاريخ |
|  |  |  |

قائمة المحتويات

[الغرض 4](#_Toc129614767)

[نطاق المعيار 4](#_Toc129614768)

[المعايير 4](#_Toc129614769)

[الأدوار والمسؤوليات 17](#_Toc129614770)

[التحديث والمراجعة 17](#_Toc129614771)

[الالتزام بالمعيار 17](#_Toc129614772)

# [الغرض](#_الأهداف" \o "يهدف هذا القسم إلى توضيح أسباب تطوير واعتماد المعيار وأهمية الالتزام بالمتطلبات المذكورة. كما يوضح هذا القسم علاقة المعيار بمتطلبات الضوابط الأساسية الصادرة من الهيئة الوطنية للأمن السيبراني ومتطلبات الأعمال والمتطلبات التنظيمية والتشريعية)

*يهدف هذا المعيار إلى تحديد متطلبات الأمن السيبراني التفصيلية لإدارة سجلات الأحداث ومراقبة الأمن السيبراني الخاصة ب<اسم الجهة> وذلك لتحقيق الغرض الأساسي وهو تقليل المخاطر السيبرانية الناتجة عن التهديدات* *الداخلية والخارجية في <اسم الجهة>.* هذه المتطلبات تمت موائمتها مع سياسة إدارة سجلات الأحداث ومراقبة الأمن السيبراني ومتطلبات الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني ويشمل ذلك على سبيل المثال لا الحصر: الضوابط الأساسية للأمن السيبراني (ECC – 1: 2018)، ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC – 1: 2019) وغيرها من المتطلبات التشريعية والتنظيمية ذات العلاقة.

# [نطاق المعيار](#_نطاق_العمل" \o "يهدف هذا القسم في نموذج المعيار إلى تحديد الأصول والأطراف والأشخاص الذين ينطبق عليهم المعيار.)

يطبق هذا المعيار على جميع تقنيات إدارة سجلات الأحداث ومراقبة الأمن السيبراني في <اسم الجهة>، وعلى جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>. كما يجب أن يتوافق هذا المعيار مع النموذج التشغيلي لمراكز عمليات الأمن السيبراني المدارة والمتطلبات التشريعية للهيئة الوطنية للأمن السيبراني.

# [المعايير](#_الضوابط" \o "يهدف هذا القسم إلى تحديد كافة المتطلبات والضوابط الأساسية للمعيار بناء على متطلبات السياسة ومتطلبات الأعمال والمتطلبات التنظيمية والتشريعية الخاصة بها.)

|  |  |
| --- | --- |
| 1 | صيغة السجل  |
| الهدف | استخدام صيغة قياسية ومتسقة للسجل تشتمل على جميع المعلومات المطلوبة. |
| المخاطر المحتملة | قد يصعب الربط بين عدة سجلات مختلفة إذا تم حفظها بصورة غير متسقة، وهذا يؤدي إلى زيادة المخاطر الناتجة عن المعلومات الخاطئة، وبالتالي يُعقِّد التعامل مع الأحداث الأمنية وحلها. |
| الإجراءات المطلوبة |
|  | يجب أن تشتمل صيغة سجل الأحداث على المعلومات التالية:* + 1. **نوع سجل الأحداث:** مثل النظام، والأمن، والتدقيق، (Kernel)، والتصريح، والبريد، وغيرها.
		2. **موقع** الحدث أو مصدر السجل ونظامه.
		3. **تاريخ** سجل الحدث **وختمه الزمني.**
		4. **حالة الحدث:** مثلناجح، أو فاشل، أو نشط، أو غير نشط، أو مسموح، أو مرفوض، أو غيره.
		5. **مستوى خطورة الحدث:** مثلطارئ، أو تنبيه، أو حرج، أو خطأ، أو تحذير، أو إشعار معلوماتي، أو إشعار تصحيحي.
		6. **رسالة الحدث:** رسالة فعلية من الحدث.
 |
|  | يجب تضمين تفاصيل إضافية في السجلات حيثما ينطبق ذلك، مثل المستخدم وعنوان المصدر / المنفذ وعنوان / منفذ الوجهة والعناصر المفيدة الأخرى. |
| 2 | الأختام الزمنية - الخوادم الزمنية المتزامنة الإضافية  |
| الهدف | استخدام نظام موثوق للأصول المعلوماتية والتقنية الداخلية. |
| المخاطر المحتملة | قد يصعب المقارنة بين مجموعتين مختلفتين من السجلات إذا تم حفظها بصورة غير متسقة بسبب اختلاف وقت التسجيل بين مجموعة السجلات حدثت في نفس الوقت، ويؤدي ذلك إلى زيادة المخاطر الناتجة عن المعلومات الخاطئة وبالتالي يُعقِّد التعامل مع الأحداث الأمنية وحلها.  |
| المعايير المطلوبة |
|  | يجب أن تتم مزامنة أصول المعلومات والتكنولوجيا مع ثلاثة خوادم زمنية مركزية متوافرة في غضون مللي ثانية من مصدر موثوق للمزامنة.. |
| 3 | تسجيل الأحداث |
| الهدف | التأكّد من توثيق وتسجيل الأحداث السيبرانية والأنشطة غير المصرّح بها التي تشهدها البيئة.  |
| المخاطر المحتملة | من الضروري تسجيل بعض الأحداث الأساسية التي تُنفذ في البيئة، وإذا تعذّر على <اسم الجهة> تسجيل الأحداث التي حدّدتها متطلّبات الضابط، فسيؤدي ذلك إلى زيادة المخاطر الناتجة عن الأحداث غير المُحدّدة وغير المصرّح بها المحتمل حدوثها في البيئة، والتي قد تؤثّر على أعمال الجهة بناءً على مستوى خطورة الحدث. |
| المعايير المطلوبة |
| 3-1 | تسجيل جميع الأحداث المُحدّدة في متطلّبات هذا الضابط والتي تشمل:* + 1. محاولات الدخول الناجحة.
		2. محاولات الدخول غير الناجحة، بالإضافة إلى تحديد ما إذا كانت محاولة الدخول قد تضمّنت إدخال كلمة مرور خاطئة.
		3. جميع عمليات تسجيل الخروج.
		4. عمليات الإضافة والحذف والتعديل على حسابات / تصريح المستخدمين.
		5. تغيير المستخدم لهويته خلال فترة زمنية معيّنة على الإنترنت.
		6. محاولات لتنفيذ مهام غير مصرّح بها.
		7. أنشطة الحسابات التي تملك صلاحيات هامة وحسّاسة.
		8. إجراء تعديلات على إعدادات النظام (محدّدات النظام).
		9. حق الوصول لقراءة أو تعديل معلومات حساسة التي يُحتمل تعرّضها للسرقة.
		10. تسريب مواد متعلّقة بمعلومات المصنفة خارج <اسم الجهة>.
		11. الأحداث المتعلقة بالاتصالات الواردة والصادرة والتي تتضمّن أنشطة غير عادية أو غير مصرّح بها بما في ذلك وجود برامج ضارة (رموز البرامج الخبيثة "Malicious Code" وبرامج التجسّس "Spyware" والبرامج الدعائية "Adware").
		12. الإضافة والحذف والتعديلات على معايير سجل الأمن والتدقيق.
		13. الأخطاء (أي المشاكل التقنية في الأصول المعلوماتية والتقنية) التي قد تحدث نتيجة حادث أمني.
		14. تشغيل الأنشطة أو إيقافها عن طريق خدمة معيّنة.
		15. تعطّل النظام أو إعادة تشغيله.
		16. تغيير كلمة المرور.
		17. تفعيل جميع السجلات للأنظمة الحسّاسة.
 |
| 4 | مصادر الأحداث  |
| الهدف | التأكّد من مراقبة جميع سجلات الأحداث المتعلّقة بالأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة> لكشف أي نشاط غير مصرّح به في الشبكة والذي قد يتسبب بحدث أمني. |
| المخاطر المحتملة | إن عدم التمكّن من كشف أي نشاط غير مصرّح به سيمنع <اسم الجهة> من التعامل بطريقة مناسبة مع الأحداث المشبوهة قبل أن تتفاقم وتصبح أكثر خطورة. |
| المعايير المطلوبة  |
|  | يجب تكوين مصادر سجل الأحداث وأنظمة التسجيل لنقل السجلات عبر بروتوكولات نقل سجل الأحداث الموثوقة والشائعة الاستخدام، مثل: (Syslog)، و(Windows Instrumentation Interface)، و(SNMP Traps)، وغيرها. |
|  | جمع كافة سجلات الأحداث من المصادر المُحدّدة ضمن هذا المطلب: * + 1. الأنظمة بما فيها أنظمة التشغيل وقواعد البيانات ووسائط التخزين والشبكات والتطبيقات، التي تغطي أحداث النظام وسجلات الأمن والتدقيق.
		2. الأنظمة الحسّاسة بما فيها أنظمة التشغيل وقواعد البيانات ووسائط التخزين والشبكات والتطبيقات، التي تغطي أحداث النظام وسجلات الأمن والتدقيق.
		3. أحداث الحسابات ذات الصلاحيات الهامة والحسّاسة.
		4. أحداث أنظمة التشغيل على سبيل المثال لا الحصر نظام (Linux).
		5. أحداث قواعد البيانات.
		6. أحداث الأنظمة الأمنية على سبيل المثال لا الحصر أنظمة جدار الحماية الخاص بتطبيقات الويب (WAF)، تقنية منع تسرب البيانات (DLP)، تقنية التحقق متعدد العناصر (MFA).
		7. الأحداث الخاصة بالتصفّح والاتصال بالإنترنت والشبكة اللاسلكية.
		8. الأحداث الناتجة عن نقل البيانات إلى وسائط تخزين خارجية.
		9. سجلات الأحداث الصادرة من تقنيات إدارة تغييرات الملفات (File Integrity Monitoring).
		10. سجلات الأحداث التي تم إنشاؤها من تغييرات تكوين النظام وتحديثات النظام والتصحيحات وتغييرات التطبيق.
		11. أنشطة مشبوهة مثل الأنشطة التي يتم الكشف عنها عن طريق نظام منع الاختراقات (Intrusion Prevention System).
		12. الأحداث التي تم إنشاؤها بواسطة الحلول الأمنية بما فيها البرامج المضادة للبرمجيات الخبيثة (Antivirus, Antimalware, Advanced Persistent Threat “APT") وتقنيات الوصول عن بُعد (Remote-Access Technologies) (مثل: الشبكة الافتراضية الخاصة "Virtual Private Network")، ووسطاء الويب (Web Proxies)، وبرنامج إدارة الثغرات، ونظام منع الاختراقات في المستضيف (Host Intrusion Prevention System)، وخوادم التحقّق من الهوية (Authentication Servers)، وغيرها.
		13. الأحداث التي تم إنشاؤها بواسطة أجهزة حماية الشبكة بما في ذلك جدران الحماية والموُجّهات (Routers) وإدارة حركة الشبكة (Traffic Managers)، وغيرها.
		14. سجلات الاحداث الصادرة من Sysmon)) وهي أداة تابعة لشركة ميكروسوفت وتقوم بتسجيل احداث لا يقوم نظام التشغيل بتسجيلها وهي مهمة جدا ومفيدة في المراقبة الأمنية والاستجابة للحوادث.
		15. الأحداث التي تم إنشاؤها بواسطة البيئة الافتراضية وأدواتها وبنيتها التحتية الأساسية.
		16. تفعيل تسجيل (Query Logging) في نظام أسماء النطاقات (Domain Name System) حيثما أمكن ذلك من الناحية التقنية.
		17. سجلات الأحداث التي تم إنشاؤها بواسطة أنظمة التحكّم الصناعي (Industrial Control Systems).
 |
|  | يجب تمكين جميع مستويات التسجيل بالإضافة إلى مسار التدقيق وسجلات الأمان في جميع تطبيقات الويب والمكونات الفنية. |
|  | يجب تخصيص واعداد تسجيل الخادم ومسار التدقيق لإعادة توجيهه إلى نظام تسجيل مركزي وفقًا للمتطلبات التنظيمية للهيئة الوطنية للأمن السيبراني وسياسة ومعيار سجلات أحداث الأمن السيبراني وإدارة المراقبة الخاصات بـ <اسم الجهة>. |

|  |  |
| --- | --- |
| 5 | مراقبة الأحداث  |
| الهدف | كشف أي نشاط غير مصرّح به في الشبكة والذي قد يسبب حدث أمني. |
| المخاطر المحتملة | إن عدم التمكّن من كشف أي نشاط غير مصرّح به في الشبكة يمنع الجهة من التعامل بالطريقة المناسبة مع الأحداث المشبوهة قبل أن تتفاقم وتصبح أكثر خطورة. |
| المعايير المطلوبة |
|  | يجب مراجعة تنبيهات الأحداث الأمنية الناتجة عن جدران الحماية على مدار الساعة للكشف عن أي محاولات وصول غير مصرح بها أو سلوك غير عادي. وتستطيع <اسم الجهة> مراقبة التنبيهات الصادرة عن جدران الحماية على سبيل المثال لا الحصر من خلال مراقبة السجلات يومياً أو من خلال مراقبة جوانب النظام الأخرى مثل أنماط محاولة الوصول، وخصائص الوصول، وغيرها من الإجراءات.  |
|  | تفعيل مراقبة الشبكة اللاسلكية وذلك لكشف نقاط الوصول اللاسلكية غير المصرّح بها. وقد تتجاوز الإشارات اللاسلكية حدود النطاق الخاضع للمراقبة، وعلى ذلك تتخذ الجهات خطوة استباقية للبحث عن الاتصالات اللاسلكية غير المصرّح بها، بما في ذلك إجراء عمليات مسح مكثّفة عن نقاط الوصول اللاسلكية غير المصرّح بها، وهذه العمليات المسحية لا تقتصر فقط على الأصول التي تحتوي على أصول معلوماتية وتقنية، بل تشمل كذلك المناطق الواقعة خارج مبانيها عند الضرورة، وذلك للتحقّق من عدم اتصال نقاط الوصول اللاسلكية غير المصرّح بها بالأنظمة. |
|  | تطبيق آليات مراقبة المستضيف (Host-Based Monitoring Mechanisms) على النهايات الطرفية للأصول المعلوماتية والتقنية ذات الخطورة العالية. وتشمل مكوّنات الأصول المعلوماتية والتقنية التي يُمكن تطبيق آليات مراقبة المستضيف عليها الخوادم وأجهزة المستخدمين والأجهزة المحمولة. |
|  | يجب تنفيذ آليات مراقبة التعليمات البرمجية القائمة على التوقيع والقائمة على السلوك (Signature-based and Behavior-based Code)، (مثل أدوات مكافحة الفيروسات ، و EDR ، و APT) على أصول المعلومات والتكنولوجيا لاكتشاف التعليمات البرمجية الضارة. |
|  | يجب أن تظل آليات مراقبة الكود القائمة على التوقيع والقائمة على السلوك محدثة بجميع التوقيعات أو المؤشرات المتاحة. |
|  | تُنشَر أجهزة المراقبة لمتابعة الاتصالات على المكوّنات الخارجية للنظام (مثل: محيط النظام) وعلى المكوّنات الداخلية الرئيسية (مثل: الواجهات المنطقية والمادية داخل الأصول المعلوماتية والتقنية) لاكتشاف العيوب واكتشاف التسريب المخفي للمعلومات وتتبع أنواع محدّدة من الأنشطة التي تهم <اسم الجهة>. على سبيل المثال لا الحصر: الأجزاء الشبكية حيث تقع الأنظمة التي يُمكن الوصول إليها من الإنترنت. |
|  | يجب استخدام أدوات المراقبة لاكتشاف مؤشرات هجمات حجب الخدمة ضد أصول المعلومات والتكنولوجيا والبنية التحتية الخاصة بـ <اسم الجهة>. |
| 6 | التنبيه بالأحداث  |
| الهدف | التأكّد من تفعيل وضبط خاصية التنبيه بالأحداث وإبلاغ العاملين المعنيين في <اسم الجهة> بشأنها ليتمكّنوا من التعامل مع أي حادث أمني بأكبر قدر من الفاعلية. |
| المخاطر المحتملة | قد يؤدي عدم ضبط خاصية التنبيه بالأحداث في أنظمة التسجيل إلى التعامل مع الأحداث الأمنية بطريقة خاطئة أو حتّى عدم التعامل معها كلياً. |
| المعايير المطلوبة |
| 6-1 | يجب إنشاء تنبيهات لأصول المعلومات والتقنية عند حدوث أحداث مراقبة أمنية محددة مسبقًا و / أو استيفاء مستويات المؤشرات المتعلقة بأي نشاط ضار محتمل. |
| 6-2 | ضبط وسائل التنبيه لإبلاغ العاملين المعنيين، بما في ذلك البريد الإلكتروني والرسائل النصية القصيرة وأنظمة شاشات المراقبة، وغيرها.  |
| 7 | مستويات التنبيه  |
| الهدف | اتباع نهج مُوثّق بشأن الحالات التي ينبغي تشغيل التنبيهات فيها. |
| المخاطر المحتملة | قد يؤدي عدم توثيق نطاق التنبيهات والغرض منها إلى عدم تهيئتها بالشكل المناسب، وقد تمر الأحداث الضارة المحتملة دون أن يلاحظها أحد. |
| المعايير المطلوبة |
| 7-1 | حصر المستويات المحدّدة للتنبيه عن أحداث مراقبة الأمن، ومراجعة مستوى التنبيه وتحديثه دورياً لمواكبة الهجمات الأمنية المستجدة. |
| 8 | التنبيه بالأحداث الناتجة عن جدار الحماية  |
| الهدف | إبلاغ العاملين المعنيين المؤهلين للتعامل مع الأحداث الأمنية المحتملة والناتجة عن الحادث الأمني. |
| المخاطر المحتملة | إن لم يتم إبلاغ العاملين المعنيين بالأحداث الناتجة، فإن <اسم الجهة> لن تكون على دراية بالمحاولات الخبيثة المحتملة غير المصرّح بها للاتصال بالشبكة، وبالتالي إذا تمكّن هذا النشاط من الاختراق، ستتعرّض أعمال <اسم الجهة> لمخاطر ضارة ناتجة عن الحادث الأمني. |
| المعايير المطلوبة |
| 8-1 | يجب ضبط اعدادات الإنذار أو المراقبة لتنبيه الموظفين المناسبين بالأحداث المتعلقة بالأمن الناشئة من جدار الحماية. |
| 9 | التنبيه بالأحداث الناتجة عن التطبيقات  |
| الهدف | التأكّد من توثيق وتسجيل الأحداث الأمنية والأنشطة غير المصرّح بها التي تشهدها البيئة.  |
| المخاطر المحتملة | من الضروري تسجيل بعض الأحداث المحورية المتعلّقة بالتطبيقات الخاصة بـ<اسم الجهة>، فإذا تعذّر على <اسم الجهة> تسجيل الحوادث المتعلّقة بالتطبيق والتي حدّدتها متطلّبات الضابط، سيؤدي ذلك إلى زيادة المخاطر الناتجة عن الحوادث الأمنية غير المُحدّدة وغير المصرّح بها المحتمل حدوثها في التطبيق، والتي قد تؤثّر على أعمال الجهة بناءً على مستوى خطورة الحادث. |
| المعايير المطلوبة |
|  | يجب تسجيل جميع طلبات النهاية الطرفية واستجابات الخادم. |
|  | تسجيل جميع معلومات الحساب (مثل: محاولات التحقّق الناجحة وغير الناجحة والتغييرات على الحساب). |
|  | تسجيل جميع المعلومات المتعلّقة بالاستخدام (مثل: عدد الأنشطة التي تحدث في فترة معيّنة). |
|  | تسجيل جميع الإجراءات التشغيلية المهمّة (مثل: تشغيل وإغلاق التطبيقات وأعطال التطبيقات والتغييرات على إعدادات التطبيقات). |
| 10 | مراقبة البرمجيات الضارة في الاتصالات  |
| الهدف | تحديد وجود البرمجيات الضارة (مثل: رمز البرامج الخبيثة وبرامج التجسّس والإعلانات المتسلّلة) في اتصالات <اسم الجهة> قبل أن تتسبّب بأي ضرر. |
| المخاطر المحتملة | إذا لم يتم كشف أي استخدام غير مصرّح به للأنشطة بما في ذلك وجود البرمجيات الضارة، لن تكون <اسم الجهة> على دراية بوجود البرمجيات الضارة قبل أن تنتشر، مما يعرّض عملها لخطر هجوم أمني واسع النطاق. |
| المعايير المطلوبة |
| 10-1 | مراقبة الاتصالات الواردة والصادرة الخاصة بـ<اسم الجهة> (مثل: رسائل البريد الإلكتروني والملفات المرفقة وعمليات التحميل) لضمان خلوها من البرمجيات الضارة (مثل: الفيروسات وبرامج التجسّس والبرامج الدعائية). |
| 11 | تحليلات مراجعة سجل الأحداث  |
| الهدف | يُمكن أن يسهم تحليل السجل ونظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني (SIEM) في اكتشاف الأنشطة المشبوهة وتعزيز قدرات الاستجابة لحوادث الأمن السيبراني وكشف الهجمات التي تجاوزت الأنظمة الأمنية الأخرى، وذلك من خلال التوافق مع النموذج التشغيلي لمراكز عمليات الأمن السيبراني المدارة والمتطلبات التشريعية للهيئة الوطنية للأمن السيبراني.  |
| المخاطر المحتملة | إن عدم التمكّن من كشف أحداث وحوادث الأمن السيبراني سيزيد من المخاطر الناتجة عن عدم ملاحظة الهجمات السيبرانية مما يؤدي إلى انتهاك الأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة>. |
| المعايير المطلوبة |
|  | يجب إعادة توجيه جميع سجلات الأحداث إلى نظام تحليلات السجل المركزي أو نظام إدارة الأحداث والمعلومات الأمنية (SIEM) لربط السجلات والتحليل والتنبيه. |
|  | إجراء مراجعة دورية لسجلات الأحداث لمراقبة السلوكيات والأحداث المشبوهة واكتشافها. |
|  | يجب ضبط نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني دورياً لتحديد الاحداث المهمة وتقليل تسجيل الاحداث الغير مهمة. |
|  | يجب مراجعة سجلات الأحداث والتنبيهات دورياً باستخدام أساليب يدوية وتقنيات آلية. |
|  | الكشف عن الأحداث غير المصرّح بها والمتعلّقة بالأصول المعلوماتية والتقنية. |
|  | كشف سوء استخدام حسابات المستخدم ذات الصلاحيات الهامة والحسّاسة. |
| 12 | تحويل السجل وتحليله  |
| الهدف | التأكّد من مراقبة جميع سجلات الأحداث المتعلّقة بالأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة> لكشف أي نشاط غير مصرّح به في الشبكة والذي قد يسبب حدثاً أمنياً. |
| المخاطر المحتملة | من الضروري تسجيل بعض الأحداث المحورية التي تُنفذ في البيئة، فإذا تعذّر على <اسم الجهة> تسجيل الأحداث التي حدّدتها متطلّبات الضابط، سيؤدي ذلك إلى زيادة المخاطر الناتجة عن الأحداث غير المُحدّدة وغير المصرّح بها المحتمل حدوثها في البيئة، والتي قد تؤثّر على أعمال الجهة بناءً على مستوى خطورة الحادث. |
| المعايير المطلوبة |
|  | استخدام أدوات لتحويل السجلات غير المدعومة من نظام التسجيل الخاص بـ<اسم الجهة> إلى صيغة قياسية أو مدعومة للسجل. |
|  | تطبيق برنامج تسجيل مزوّد بآليات التحليل لاسترجاع السجلات من الأنظمة غير المدعومة بطريقة مناسبة. |
| 13 | المراقبة المستمرة  |
| الهدف | تفعيل المراقبة المستمرة لجميع سجلات الأصول المعلوماتية والتقنية للكشف عن الأنشطة الخبيثة والحفاظ على فاعلية المراقبة مع الوقت، وذلك من خلال التوافق مع النموذج التشغيلي لمراكز عمليات الأمن السيبراني المدارة والمتطلبات التشريعية للهيئة الوطنية للأمن السيبراني. |
| المخاطر المحتملة | إذا لم تضع الجهة خطّة مراقبة لهذه الأنشطة وتوثّقها، فقد يرتفع خطر عدم وجود مراقبة مخصصة أو كافية لهذا الغرض، مما يزيد من مخاطر عدم الكشف عن الأنشطة الخبيثة. |
| المعايير المطلوبة |
| 13-1 | تطوير وإعداد خطّة للمراقبة المستمرة (والتي تشمل على سبيل المثال لا الحصر: الجوانب التي يجب مراقبتها في نطاق العمل، وآلية المراقبة، واختبار فاعلية المراقبة) للأصول المعلوماتية والتقنية وتحديثها عند الحاجة. |
| 14 | أمن نظام التسجيل  |
| الهدف | ضمان حماية وأمن البنية التحتية الأساسية لنظام التسجيل بما في ذلك جمع سجلات الأحداث وتجميعها وربطها. |
| المخاطر المحتملة | من الممكن أن يؤدي عدم اتخاذ أي إجراء لحماية البنية التحتية لنظام التسجيل في <اسم الجهة> إلى استفادة المهاجمين من نقاط الضعف الكامنة في أنظمة التسجيل واستغلال ثغراتها للوصول غير مصرّح به إلى شبكة <اسم الجهة> وبياناتها. |
| الإجراءات المطلوبة |
|  | تثبيت برامج أنظمة تسجيل الأحداث على خوادم مخصصة لها. |
|  | استخدام جامع الأحداث في كل منطقة من مناطق بنية الشبكة، والسماح فقط لهذه المحرّكات بالتواصل مع نظام التسجيل المركزي أو أنظمة تجميع السجلات، على أن تتوفر في المناطق التالية على الأقل:* + 1. وضع جامع الأحداث في المنطقة المحايدة (DMZ).
		2. وضع جامع الأحداث في منطقة قاعدة البيانات.
		3. وضع جامع الأحداث في منطقة التطبيقات.
		4. وضع جامع الأحداث في منطقة خدمات المؤسسة.
		5. وضع جامع الأحداث في منطقة المستخدم.
		6. وضع جامع الأحداث في منطقة الإدارة.
 |
| 15 | الاحتفاظ بسجلات الأحداث  |
| الهدف | تجنّب حذف سجلات الأحداث الأمنية خلال الفترة التي يُمكن أن تُستخدَم خلالها. |
| المخاطر المحتملة | إذا حُذِفَت سجلات الأحداث الأمنية قبل تدقيقها أو التحقيق فيها، لن تتمكّن <اسم الجهة> من حماية أو فحص الأنشطة التي حدثت في الأصول المعلوماتية والتقنية الخاصة بها. |
| المعايير المطلوبة |
| 15-1 | الاحتفاظ بسجلات الأحداث لمدة 12 شهراً على الأقل، ولمدة 18 شهراً بالنسبة للأصول الحسّاسة كحد أدنى أو لفترة أطول، وفقاً لسياسة الأمن السيبراني المعتمدة في <اسم الجهة>. |
| 15-2 | تقييد أرشفة وحذف سجلات الأحداث وحصره على المستخدمين المصرّح لهم وذلك فقط بعد انتهاء المدّة الزمنية المحدّدة للاحتفاظ بالسجلات، والسماح للمديرين المعنيين بالأصول المعلوماتية والتقنية بإجراء عملية أرشفة سجلات الأحداث وحذفها. |
| 16 | توفير عملية بديلة لتسجيل الأحداث  |
| الهدف | تمكين <اسم الجهة> من مواصلة تسجيل الأنشطة المتعلّقة بالأحداث الأمنية الحسّاسة حتّى في حال تعطّل الوسيلة الأساسية لتسجيل الأحداث (مثل: التسجيل المركزي)، وذلك من خلال التوافق مع النموذج التشغيلي لمراكز عمليات الأمن السيبراني المدارة والمتطلبات التشريعية للهيئة الوطنية للأمن السيبراني. |
| المخاطر المحتملة | إذا تعطّلت وسيلة تسجيل الأحداث الأساسية المتعلّقة بأحد الأصول التقنية الحساسة ولم تتوفّر عملية تسجيل بديلة، فإنه قد يتعذّر إنشاء سجل تدقيق أو تحديد النشاط الخبيث وذلك لعدم وجود سجلات يُمكن أن تستخدمها <اسم الجهة> للقيام بإجراءات المراقبة والتحقيق، علماً بأن الأصول الأعلى خطورة تؤثّر بشكل أكبر على أعمال الجهة في حال وقوع حادث أمني معيّن. |
| المعايير المطلوبة |
| 16-1 | يجب ضبط اعدادات أصول المعلومات والتقنية عالية الخطورة للحفاظ على السجلات المحلية في حالة فشل الاتصال بالشبكة. |
| 17 | توافر سجل الأحداث  |
| الهدف | ضمان استمرارية تشغيل وسيلة تسجيل الأحداث وقابلية استخدامها للأصول المعلوماتية والتقنية الحسّاسة. |
| المخاطر المحتملة | إذا لم تتوفّر وسيلة تسجيل الأحداث، فإن ذلك سيزيد من احتمالية عدم ملاحظة النشاط الخبيث وعدم القدرة على إجراء تحقيق بشأن الحادث والذي قد يؤدي إلى وقوع حادث أمني خطير. |
| المعايير المطلوبة |
| 17-1 | ضبط الأصول المعلوماتية والتقنية الخاصة بـ<اسم الجهة> والتي تحتوي على معلومات **محمية**، أو معلومات مصنفة من خلال تقييم إدارة المخاطر على أنها تتطلب تسجيل أحداثها، لإرسال الأحداث الخاصة بها بشكلٍ دائم. |
| 17-2 | يجب إعداد أنظمة تسجيل إضافية متعدّدة مزوّدة بقدرات توفير الخدمة على مدار الساعة ودون انقطاع. |
| 18 | تصنيف السجلات  |
| الهدف | يجب حماية جميع سجلات أحداث الأمن السيبراني بطريقة آمنة. |
| المخاطر المحتملة | إذا طبّقت السجلات ضوابط مُخصّصة لبيانات ذات تصنيف أدنى على الرغم من احتواء هذه السجلات على بيانات مُصنّفة بأنها **سريّة للغاية**، فستكون هذه البيانات أكثر عرضة لخطر انتهاكها لأن الضوابط المحدّدة لحمايتها تعتبر أقل صرامة. |
| المعايير المطلوبة |
| 18-1 | التعامل مع أنظمة التسجيل المركزي باعتبار أنها تحتوي بحدٍّ أدنى على بيانات **سرية** و**مقيدة** خاصة بـ<اسم الجهة> وأنها ملتزمة بجميع الضوابط ذات العلاقة بسريّة المعلومات. |
| 18-2 | بالنسبة إلى أي سجل للتطبيقات أو للأنشطة يحتوي على بيانات مُصنّفة على أنها **سرية للغاية**، يجب فرض الضوابط المطلوبة لهذا النوع من البيانات. |
| 19 | أمن السجلات وسلامتها  |
| الهدف | اعتماد آلية قادرة على كشف التعديلات على سجلات الأحداث الأمنية للتأكد من الاحتفاظ بها في حالتها الأصلية. |
| المخاطر المحتملة | إذا كان من الممكن تعديل سجلات الأحداث الأمنية دون وجود أي وسيلة لكشف هذا التعديل، فيمكن للمستخدم أن يُخفي نشاطه الخبيث داخل الأصل المعلوماتي والتقني. وفي هذه الحالة، إذا أُجري تحقيق بناءً على الأنشطة الضارة التي قام بها المستخدم، فلن يكون هناك دليل لمحاكمة المستخدم، ولن تُوجّه <اسم الجهة> ادعاءات مبرّرة بحق المستخدم ذي النوايا الضارة أو الخبيثة. كما أنه في حال انتهاك سلامة السجلات، فإنها قد تعتبر غير مقبولة في إجراءات المحكمة. |
| المعايير المطلوبة |
| 19-1 | ضبط إعدادات التحكّم بمعدل إرسال السجلات (Log Rate Limiting) لمنع تعرّض نظام التسجيل إلى هجمات حجب الخدمة، وضبط مستواه عند حد معقول. |
| 20 | موارد تسجيل الأحداث  |
| الهدف | تجنّب فقدان السجلات جرّاء استبدال البيانات المُخزّنة على وسائط التخزين. |
| المخاطر المحتملة | إن عدم التمكّن من توفير مساحة كافية لتخزين أقصى حدّ ممكن من السجلات قد يؤدي إلى استبدال المعلومات المُخزّنة في السجل وفقدان بيانات قيّمة ومهمّة خاصة بـ<اسم الجهة>. وفي هذه الحالة، من الممكن أن تُحذَف السجلات الحسّاسة بالكامل ولن تتمكّن <اسم الجهة> من الاعتماد على هذه السجلات في حال توجيه دعوى قضائية أو إجراء تحقيق معيّن، وهذا الأمر قد يؤثّر على أعمالها. |
| المعايير المطلوبة |
| 20-1 | توفير موارد كافية (مثل: موارد النظام ووسائط تخزين البيانات ونطاق الشبكة) لاستيعاب أنشطة التسجيل المحدّدة. ويجب أن تحتوي أجهزة تخزين السجلات على سعة تخزين كافية لجمع السجلات. |
| 21 | التغييرات على إعدادات تسجيل الأحداث  |
| الهدف | الحد من إمكانية إجراء أي تغييرات غير مصرّح بها أو ضارة على عملية تسجيل الأحداث الجاري تنفيذها في مكوّنات النظام. |
| المخاطر المحتملة | إذا لم تُفرَض أي قيود على المسؤول عن إدخال التغييرات على إعدادات السجل ومكان وموعد إجرائها، فإنه يُمكن أن يقوم مُستخدم خبيث بإيقاف التسجيل على الأجهزة الحسّاسة لتنفيذ هجوم غير ملحوظ.  |
| المعايير المطلوبة |
| 21-1 | تقييد إمكانية تغيير إعدادات سجل الأحداث الأمنية، بما فيها النطاق وآلية المراقبة، وحصرها على المستخدمين المصرّح لهم فقط. |
| 22 | استخدام أجهزة المراقبة  |
| الهدف | منع الكشف عن البيانات الحسّاسة والتأثير على شبكة <اسم الجهة> (مثل: استنزاف موارد الشبكة أو استخدام أدوات ضارة/خبيثة في البيئة). |
| المخاطر المحتملة | إذا لم تصرّح الإدارة المعنية بالأمن السيبراني في <اسم الجهة> ولم تسمح لموظفين معيّنين باستخدام أدوات أو أجهزة المراقبة والفحص، من الممكن أن تُستخدَم إحدى الأدوات بطريقة تضر البيئة وتزيد خطر انتهاك البيانات أو وقوع حادث أمني. |
| المعايير المطلوبة |
| 22-1 | تقييد استخدام أجهزة أو أدوات المراقبة والفحص على المستخدمين المصرّح لهم. |
| 22-2 | يجب تصنيف نتائج جميع أنشطة المراقبة والفحص ضمن المعلومات السريّة بحدٍّ أدنى. |

# [الأدوار والمسؤوليات](#_الأدوار_والمسؤوليات)

1. **مالك المعيار:** <رئيس الإدارة المعنية بالأمن السيبراني>.
2. **مراجعة المعيار وتحديثه:** <الإدارة المعنية بالأمن السيبراني>.
3. **تنفيذ المعيار وتطبيقه:** <الإدارة المعنية بتقنية المعلومات> .
4. **قياس الالتزام بالمعيار:** <الإدارة المعنية بالأمن السيبراني>.

# التحديث والمراجعة

 يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة المعيار سنويًا على الأقل أو في حال حدوث تغييرات تقنية جوهرية في البنية التحتية أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

# [الالتزام بالمعيار](#_الالتزام_بالسياسة" \o "يهدف هذا القسم إلى تحديد متطلبات الالتزام بالمعيار والنتائج المترتبة على مخالفتها أو انتهاكها)

1. يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذا المعيار دورياً.
2. يجب على جميع العاملين في <اسم الجهة> الالتزام بهذا المعيار.
3. قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في <اسم الجهة>.