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 الكشف عن تهديدات النقاط النهائية والاستجابة لها (EDR)

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

طُوّر هذا النموذج عن طريق الهيئة الوطنية للأمن السيبراني كمثال توضيحي يمكن استخدامه كدليل ومرجع للجهات. ويجب 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 بتفويضه. وتخلي الهيئة مسؤوليتها من استخدام هذا النموذج كما هو، وتؤكد على أن هذا النموذج ما هو إلا مثال توضيحي.

اختر التصنيف

الإصدار <1.0>

اعتماد الوثيقة

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

نسخ الوثيقة

النسخة	التاريخ	عُدِّلَ 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

اختر التصنيف

الإصدار <1.0>

قائمة المحتويات

الغرض

الغرض من هذا المعيار هو تحديد متطلبات الأمن السيبراني التفصيلية المتعلقة بحلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" (EDR) في <اسم الجهة>. وستساعد قدرة <اسم الجهة> على استخدام حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" (EDR) وفقًا لهذا المعيار في رصد الأنشطة الضارة والمشبوهة وكشف كل الأحداث غير الطبيعية على نحو ملائم، وكذلك في الحفاظ على سرية وسلامة وتوافر أصول <اسم الجهة> ومعلوماتها.

تمت مواءمة متطلبات هذا المعيار مع متطلبات الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني، وتشمل على سبيل المثال لا الحصر: الضوابط الأساسية للأمن السيبراني (ECC – 1: 2018) وضوابط الأمن السيبراني للأنظمة الحساسة (CSCC – 1: 2019) وغيرها من المتطلبات التشريعية والتنظيمية ذات العلاقة.

نطاق العمل

ينطبق هذا المعيار على جميع الأصول التقنية والمعلوماتية الخاصة ب<اسم الجهة>، وينطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة> والأطراف الخارجية ذات العلاقة.

المعايير

1	المتطلبات العامة (General Requirements)
الهدف	إدارة حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" بشكل آمن واستخدامها بشكل مناسب عند الحاجة.
المخاطر المحتملة	قد يؤدي الخطأ في ضبط إعدادات حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" إلى إهدار فرصة تحديد التهديدات، ويؤدي إلى تسرب المعلومات والإفصاح عنها والوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-1	أن تعمل حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" على توفير مراقبة أمنية لحظية ومستمرة وجمع بيانات النقطة النهائية مع قدرات تحليل واستجابة تلقائية مستندة إلى القواعد.
2-1	استخدام حل "الكشف عن تهديدات النقاط النهائية والاستجابة لها" في البيئة التقنية عن طريق تثبيته كوكيل (agent solution) على مستوى الأجهزة.

3-1	أن توفر حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" الحماية والمراقبة لكل النقاط النهائية في <اسم الجهة>. وأن يكون الحل مستقلًا عن نظام تشغيل النقطة النهائية. وإذا لم تدعم أنظمة تشغيل معينة استخدام حل "الكشف عن تهديدات النقاط النهائية والاستجابة لها"، يجب فصل تلك الأنظمة في مجموعة خاصة ومراقبتها بأسلوب مخصص ومحدد.
4-1	يجب ألا تقتصر حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" على توفير معلومات عن الأساليب والأنماط والعمليات التي يستعملها المهاجم، بل ويجب أن توفر أيضًا معلومات عن كيفية دخول المهاجمين إلى الشبكة الداخلية للجهة، وكيفية انتقالهم إلى الأجهزة الاخرى، وكيفية تصعيد الصلاحيات الممنوحة على النظام لتحقيق أهدافهم في الهجوم.
5-1	تثبيت كل التحديثات الأمنية الخاصة ببرمجيات "الكشف عن تهديدات النقاط النهائية والاستجابة لها" حال إصدار تلك التحديثات من المورد.
6-1	أن تتبع كل التحديثات الأمنية متطلبات سياسة إدارة التحديثات والإصلاحات والتحصين.
7-1	أن تتم تحديثات برمجيات "الكشف عن تهديدات النقاط النهائية والاستجابة لها" وفقًا للدليل الإجرائي لإدارة التغييرات.
8-1	أن توفر حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" قدرات للتحليل العميق والفحوص الجنائية الرقمية عند الحاجة إلى إجراء تحقيقات.
9-1	أن تكون حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" قابلة للتوسع والتطوير للتصدي للمخاوف المرتبطة بالجيل التالي من تهديدات الأمن السيبراني.
10-1	إجراء النسخ الاحتياطي الدوري للبيانات والتحذيرات ذات الصلة، وملفات الإعدادات الخاصة بحلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" (القواعد والتقارير وأدوات المتابعة والمجموعات والإجراءات المقررة)، وإدارة ملفات التخزين وفقًا لسياسة والدليل الإجرائي للنسخ الاحتياطي في <اسم الجهة>.
11-1	تحديد اتفاقية مستوى خدمة (SLA) لإيضاح المسؤوليات المحددة لمزود حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" وتلبية توقعات <اسم الجهة>.
12-1	أن تتحقق <اسم الجهة> من قائمة التصريحات التي يتعين إسنادها لضمان عمل وكيل "الكشف عن تهديدات النقاط النهائية والاستجابة لها" بالشكل السليم. وقد تختلف قائمة التصريحات استنادًا إلى وضع عمل "الكشف عن تهديدات النقاط النهائية والاستجابة لها" (الحجب أو المراقبة) ويجب تعديلها وفقًا لقاعدة الحد الأدنى من الصلاحيات والامتيازات.

اختر التصنيف

الإصدار <1.0>

2	جمع البيانات ومراقبتها (Data Collection and Monitoring)
الهدف	أن يعمل وكلاء (agents) برمجيات "الكشف عن تهديدات النقاط النهائية والاستجابة لها" على مراقبة وجمع بيانات النقاط النهائية بشكل ملائم، مثل: العمليات والاتصالات وحجم النشاط وعمليات نقل البيانات، في قاعدة بيانات مركزية.
المخاطر المحتملة	قد تؤدي المراقبة وجمع البيانات بشكل غير سليم من جانب وكلاء البرمجيات إلى تداعيات خطيرة تسفر عن عدم كشف حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" عن التهديدات والاستجابة لها بشكل سليم.
الإجراءات المطلوبة	
1-2	أن تستعمل حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" وحدة تحكم إدارية مركزية تتمتع بالمزايا التالية: • الوصول المتزامن • مراقبة الأحداث الجارية • تمثيل المعلومات المهمة مرئيًا • عرض تفاصيل حدث معين • وضع العمل متعدد النوافذ • قدرات تصفية متقدمة • تحديث تلقائي • الوصول دون الحاجة إلى تبديل الواجهات • الإبلاغ التلقائي.
2-2	أن تعمل حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" على مراقبة وجمع بيانات النشاط التي قد تشير إلى وجود تهديدات على النقاط النهائية.
3-2	أن تعمل حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" على الربط التبادلي للبيانات عبر كامل البيئة ضمن نطاق مراقبتها.
4-2	أن تعمل حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" على جمع ومراقبة البيانات من دون التأثير على أنشطة النقطة النهائية.
5-2	أن تعمل حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" بغض النظر عن وجود برمجيات مكافحة الفيروسات على النقطة النهائية من عدمها.
6-2	أن تعمل حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" على جمع ومراقبة البيانات ذات الصلة لرسم صورة كاملة عن أنشطة النقطة النهائية.

7-2	أن تشتمل البيانات ذات الصلة بحلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" على معلومات تغطي المجالات التالية: العمليات والاتصالات والملفات ومحركات الأقراص والتشغيل التلقائي والأنظمة والآلات والمستخدمين. ويجوز استخدام مصادر بيانات أخرى، منها على سبيل المثال لا الحصر: • السجلات • مراقبة الأداء • تفاصيل الملف • العمليات الجارية • بيانات الإعدادات
8-2	أن تعمل حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" بشكل صحيح على جمع ومراقبة نشاط نقطة النهاية بغض النظر عن مكان وجودها.
3	تحليل البيانات وتحديد أنماط التهديدات (Data Analysis and Threat Pattern Identification)
الهدف	تحليل لحظي بغرض التشخيص السريع للتهديدات التي لم تكن متوقعة في جداول الاستجابة التلقائية.
المخاطر المحتملة	قد يؤدي تحليل البيانات وتحديد أنماط التهديدات بشكل غير سليم إلى تداعيات خطيرة تفضي إلى عدم عمل ميزة الإشعارات والاستجابة التلقائية بشكل صحيح.
الإجراءات المطلوبة	
1-3	أن تراقب حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" كل نقطة نهائية لدى الجهة بغرض جمع وتحليل البيانات المجمَّعة التي يمكن أن تعطي مؤشرًا على الأنشطة المشبوهة أو التهديدات المحتملة.
2-3	أن ترسل حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" إشارة بالهجمات إلى أعضاء فريق تقنية المعلومات في <اسم الجهة>. يجب أن توفر حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" تفاصيل بشأن مصدر الهجوم والضرر التي تمكن المهاجم من تحقيقه.
3-3	يجب أن تحدد حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" أنماط التهديدات استنادًا إلى البيانات المجمَّعة من كل نقطة من النقاط النهائية، بدلًا من الاكتفاء بنقطة واحدة.

4-3	يجب أن تقارن حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" أنماط مجموعات البيانات الجديدة بالأنماط السابقة وذلك بغرض تحديد الأنشطة الضارة والمشبوهة سواء كانت معروفة مسبقًا أم لا.
5-3	يجب أن توفر حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" قدرات الكشف السلوكي عن التهديدات.
6-3	يجب أن تستخدم حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" قاعدة بيانات معرفية يمكن الوصول إليها عالميًا عن تصنيف تهديدات الأمن السيبراني (مثل القاعدة المعرفية لأساليب وأنماط الخصوم بالاستناد إلى مشاهدات حقيقية MITRE ATT&CK)، والتي يمكن الوصول إليها عالميًا).
7-3	يجب أن تحدد حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" درجات المخاطر وأن تصنف تهديدات الأمن السيبراني استنادًا إلى مستوى الحساسية ومستوى الثقة. مستوى الحساسية يشير إلى تقدير تأثير الكشف غير الفعال على البيئة السيبرانية. ومستوى الثقة يشير إلى احتمالية أن يكون الكشف صالحًا، وليس تنبيه إيجابي خاطيء.
4	**الإشعارات والاستجابة التلقائية Automatic Response and Notification**
الهدف	إنشاء قواعد مسبقة الإعداد للاستجابات السريعة في حالة الانتهاك المحتمل للقاعدة، مقترنًا بتنبيه ملائم.
المخاطر المحتملة	قد يؤدي الخطأ في إعدادات ميزة الإشعارات والاستجابة التلقائية إلى تداعيات خطيرة تؤثر على اتخاذ التدابير الملائمة لمنع أو إيقاف الاختراقات المحتملة.
الإجراءات المطلوبة	
1-4	يجب أن توفر حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" نظامًا للتنبيهات والاستجابة التلقائية يغطي أحدث سيناريوهات الهجمات السيبرانية.
2-4	يجب أن تسرّع حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" أوقات الاستجابة عبر تكامل مرئيات الأمن السيبراني ومشاركتها مع حلول الكشف عن تهديدات الشبكات والاستجابة لها (Network Detection and Response (NDR)) ونظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني (SIEM) وأدوات التنسيق الأمني والأتمتة والاستجابة (SOAR).
3-4	يجب أن تطلق حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" استجابة تلقائية استنادًا إلى التهديدات المحددة مسبقًا (الجدول "أ").
4-4	يجب أن تمنع حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" تشغيل الملفات الضارة والمشبوهة ونشرها عبر الشبكة أثناء أو بعد إجراء التحقيق.
5-4	يجب أن تعزل حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" المضيف المصاب بمجرد أن تجد مؤشرًا على وقوع انتهاك أمني مقترن بتهديد سريع الانتشار.

اختر التصنيف

الإصدار <1.0>

6-4	يجب أن تعزل حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" الملفات المرتبطة بالتهديدات المراوغة على جميع النقاط النهائية.
7-4	يجب أن تعمل حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" تلقائيًا على تسجيل وإشعار <اسم الجهة> عندما تحدد تهديدًا محتملًا سواء أطلق استجابة تلقائية أم لم توجد استجابة تلقائية محددة للتهديد المكتشف.
8-4	يجب أن تجمع حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" في ملف السجلات أي أحداث قد يشملها نطاق تفتيش التدقيق (مثل الأنشطة المشبوهة، تحديد التهديدات، الإجراءات التلقائية، إخطار فريق تقنية المعلومات)
5	معايير أخرى (Other Standards)
الهدف	ضبط إعدادات حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" بشكل آمن، واستخدامها بشكل مناسب عند الحاجة.
المخاطر المحتملة	قد يؤدي عدم التزام <اسم الجهة> بجميع المعايير والمتطلبات المقررة إلى تعريض الجهة لتهديدات خطيرة.
الإجراءات المطلوبة	
1-5	يجب تطبيق المعايير التالية فيما يتعلق بحلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها": 1. إدارة الهويات وحقوق الوصول 2. النسخ الاحتياطي والتعافي من الكوارث 3. التشفير 4. تسجيل الأحداث وسجلات التدقيق 5. الأمن المادي 6. الإعدادات والتحصين الآمن 7. إدارة ومراقبة سجل الأحداث 8. الحماية من البرمجيات الضارة 9. إدارة النسخ الاحتياطي والاستعادة 10. الكشف عن تهديدات الشبكات والاستجابة لها

الجدول "أ" – الاستجابة للتهديدات المكتشفة

يمكن أن تأخذ الاستجابة للتهديدات المكتشفة أحد المسارات التالية:

استرداد الملف	عملية استرداد الملفات.
إنهاء العملية	إنهاء العمليات المشبوهة.
إنهاء التشعب	إنهاء التشعبات المشبوهة.
إغلاق الاتصال	إغلاق الاتصالات المشبوهة.
حذف الملف	حذف الملفات المشبوهة.
حذف السجل	حذف السجلات المشبوهة.
حذف المهمة المجدولة	حذف المهام المجدولة.
حذف الخدمة	حذف الخدمات التي تنطبق عليها معايير معينة.

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 عند 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

1- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذا المعيار دوريًا.

2- يجب على كافة 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>.