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 الشبكات والاستجابة لها (NDR)

اختر التصنيف

التاريخ: اضغط هنا لإضافة تاريخ

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

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.

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.

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	تفاصيل الإصدار
<أدخل رقم النسخة>	اضغط هنا لإضافة تاريخ	<أدخل الاسم الكامل للموظف>	<أدخل وصف الإصدار>

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 بـ"الكشف عن تهديدات الشبكات والاستجابة لها" (NDR) في <اسم الجهة>.

تمت مواءمة 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 المعلوماتية والتقنية الخاصة بـ <اسم الجهة>، وينطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة> والأطراف الثالثة ذات العلاقة.

المعايير

1	المتطلبات العامة (General Requirements)
الهدف	تصميم حلول "الكشف عن تهديدات الشبكات والاستجابة لها" بشكل آمن واستخدامها بشكل مناسب عند الحاجة.
المخاطر المحتملة	قد يؤدي الخطأ في ضبط إعدادات حلول "الكشف عن تهديدات الشبكات والاستجابة لها" إلى تقويض فرصة التعرف على التهديدات، ويؤدي إلى سرقة المعلومات والإفصاح عنها والوصول غير المصرح به إليها.
الإجراءات المطلوبة	
1-1	يجب أن تجمع حلول "الكشف عن تهديدات الشبكات والاستجابة لها" استخدام تقنيات علوم البيانات وتعلم الآلة والتحليل السلوكي مع معلومات التهديدات الاستباقية محكمة التنظيم، وذلك من أجل تحديد غرض استخدام الشبكة والكشف عن السلوكيات الضارة والمشبوهة بشكل آني أو شبه آني -بشكل مستقل عن التطبيقات وفي حالات الاستخدام المشفَّر للشبكة- وتقديم المساعدة في الاستجابة اليدوية في تتبع التهديدات والحوادث، باستعمال الأتمتة.
2-1	يجب أن تربط حلول "الكشف عن تهديدات الشبكات والاستجابة لها" بين معلومات التهديدات الاستباقية والتهديدات المحلية بغرض منع المهاجمين من إصابة الكثير من الضحايا بنفس البرمجيات الضارة.

3-1	تنفيذ حلول "الكشف عن تهديدات الشبكات والاستجابة لها" بمنهجيات مختلفة (المستشعرات المدمجة والمستشعرات السلبية - الجدول أ).
4-1	تقييد الوصول المادي إلى حلول "الكشف عن تهديدات الشبكات والاستجابة لها" ومنحه للموظفين المصرح لهم فقط (إسناد الحد الأدنى من الصلاحيات والامتيازات لمختلف مديري النظام).
5-1	تقييد حق الوصول الإداري إلى واجهة إدارة حلول "الكشف عن تهديدات الشبكات والاستجابة لها" ومنحه لمجموعة محدودة من مديري النظام.
6-1	فصل بطاقات واجهة الشبكة غير المستخدمة عن أي شبكة من الشبكات.
7-1	يجب أن تدعم حلول "الكشف عن تهديدات الشبكات والاستجابة لها" استخدام البروتوكول السادس IPv6 والبروتوكول الرابع IPv4 لمعالجة الشبكة وتحديد قواعد الأمن وسياسة استخدام الشبكة.
8-1	تثبيت كل التحديثات الأمنية لحلول "الكشف عن تهديدات الشبكات والاستجابة لها" عند إصدارها من المورّد ووفقًا لسياسة إدارة التغييرات.
9-1	يجب أن تستخدم جميع قنوات الاتصالات الإدارية شبكة إدارية مخصصة أو اتصالات شبكة الإدارة شرط أن تكون موثقة ومشفّرة باستخدام وحدات التشفير المعتمدة وفقًا لمتطلبات إدارة دورة الحياة الرئيسية التي حددها معيار التشفير الوطني (National Cryptography Standard).
10-1	يجب مزامنة إعدادات الوقت الخاصة بحلول "الكشف عن تهديدات الشبكات والاستجابة لها" مع خوادم زمنية موثوقة تتمتع بالصلاحيات المناسبة.
2	مراقبة استخدام الشبكة (Traffic monitoring)
الهدف	ضبط إعدادات حلول "الكشف عن تهديدات الشبكات والاستجابة لها" بشكل سليم وإدارتها بشكل آمن للكشف عن التهديدات السيبرانية والسلوكيات غير الطبيعية على الشبكات الخاضعة للمراقبة.
المخاطر المحتملة	قد يؤدي الخطأ في ضبط إعدادات حلول "الكشف عن تهديدات الشبكات والاستجابة لها" إلى تداعيات خطيرة مثل الإخفاق في تحليل استخدام الشبكة والإخفاق في التعرف على التهديدات، وهي أمور قد تفضي إلى تسريب البيانات أو تعرض مؤسسات شريكة أو عملاء الجهة للهجوم.
الإجراءات المطلوبة	

1-2	أن تتوصل حلول "الكشف عن تهديدات الشبكات والاستجابة لها" بشكل مستمر إلى الغرض الكامن وراء استخدام الشبكة حتى في الحالات التي تكون فيها نتائج البرمجيات الخبيثة غير مرئية. وهكذا، يمكن توفير الحماية دون التطفل على البيانات.
2-2	أن تحدد حلول "الكشف عن تهديدات الشبكات والاستجابة لها" نموذج أساسي للسلوك الطبيعي للشبكة وأن ترسل تنبيهات إلى الفرق الأمنية بشأن أي حالات استخدام مشبوه للشبكة خارج الحدود الطبيعية.
3-2	أن تربط حلول "الكشف عن تهديدات الشبكات والاستجابة لها" السلوكيات الضارة بعنوان بروتوكول إنترنت محدد وأن تجري التحليلات الجنائية اللازمة لتحديد كيفية انتشار التهديدات أفقيًا في البيئة الأمنية.
4-2	أن توفر حلول "الكشف عن تهديدات الشبكات والاستجابة لها" إمكانية الرؤية للعديد من البيئات السحابية العامة والخاصة.
5-2	أن تتمكن حلول "الكشف عن تهديدات الشبكات والاستجابة لها" من تحليل الاستخدام المشفَّر للشبكة دون فك تشفيره والكشف عن التهديدات التي تحاول التخفي تحت غطاء الاستخدام المشفَّر للشبكة.
6-2	أن تتعرف حلول "الكشف عن تهديدات الشبكات والاستجابة لها" على روابط الإنترنت والتطبيقات (استنادًا إلى التوقيعات) وعناوين بروتوكولات الإنترنت ومنافذ TCP/UDP.
7-2	أن توفر حلول "الكشف عن تهديدات الشبكات والاستجابة لها" إمكانية التحقق من الالتزام بمعايير بروتوكولات الإنترنت وأن تمنع استخدام الشبكة للأنشطة غير الملتزمة.
8-2	أن يكون فريق الاستجابة للحوادث قادرًا على الاستعلام عن قاعدة البيانات باستعمال قائمة الموارد/الهجمات "المتاحة دائمًا" أو "المرفوضة دائمًا" والتي تحققت منها حلول "الكشف عن تهديدات الشبكات والاستجابة لها" أثناء مراقبة استخدام الشبكة.
3	الكشف عن استخدام الشبكة وتسجيله (Traffic detection and logging)
الهدف	أن تعمل حلول "الكشف عن تهديدات الشبكات والاستجابة لها" على مراقبة ومعالجة استخدام الشبكة بشكل آمن بغرض حفظ أي نشاط مشبوه وإخطار فريق الاستجابة للحوادث بأي حادث جديد غير معروف.
المخاطر المحتملة	قد يؤدي عدم تهيئة الإعدادات بشكل سليم للكشف عن استخدام الشبكة إلى انتشار البرمجيات الضارة بسهولة والتعرض لمحاولات التصيّد الإلكتروني وتسريب المعلومات. قد تؤدي تهيئة إعدادات حلول "الكشف عن تهديدات الشبكات والاستجابة لها" بشكل غير سليم إلى عدم كفاية الإجراءات للحدّ من الحوادث الأمنية الجديدة المحتملة في المستقبل.

الإجراءات المطلوبة	
1-3	أن تكشف حلول "الكشف عن تهديدات الشبكات والاستجابة لها" عن التهديدات (مثل الحالات غير المألوفة من الوصول عن بعد، أو فحص المنافذ، أو استخدام بروتوكولات إنترنت مقيَدة أو منافذ مقيَدة أو غير ذلك) بشكل آني مع استخدام نماذج سلوكية دائمة التعلم تستند إلى تقنية تعلم الآلة.
2-3	يجب أن تستخدم حلول "الكشف عن تهديدات الشبكات والاستجابة لها" وسائل متقدمة للكشف عن التهديدات وتقليل الوقت المطلوب للاستقصاء عنها عبر جمع البيانات الوصفية والتعرف على الخصائص الفريدة للسلوكيات المشبوهة والضارة، وذلك من أجل تحديد اختراقات الشبكة على نحو موثوق حتى في الحالات التي تكون فيها الأدوات أو البرمجيات الخبيثة أو الهجمات مجهولة تمامًا.
3-3	يجب أن تعمل حلول "الكشف عن تهديدات الشبكات والاستجابة لها" على جمع وإثراء البيانات الوصفية بمرئيات متعمقة وسياق يتيح لها كشف وإيقاف مجموعة واسعة من سيناريوهات الهجوم في وقت مبكر وبصفة مستمرة.
4-3	يجب أن تنفذ حلول "الكشف عن تهديدات الشبكات والاستجابة لها" نماذج خوارزمية مباشرةً على استخدام الشبكة بغرض الكشف عن السلوكيات الهجومية الكامنة، ثم إثراء تلك البيانات تلقائيًا باستعمال مصادر ثانوية (مثل سجلات المصادقة ومعلومات التهديدات الاستباقية).
5-3	يجب أن تعثر حلول "الكشف عن تهديدات الشبكات والاستجابة لها" على دلائل على المهاجمين ممن يستخدمون اتصالات مخفية ضمن جلسة ويب مشفَّرة ببروتوكول SSL أوTLS. يجب أن تكشف حلول "الكشف عن تهديدات الشبكات والاستجابة لها" عن طبقات الاتصالات الإضافية المخفية حال وجودها، وذلك عبر تحليل التذبذبات الضئيلة في بروتوكولات الإنترنت، مثل بروتوكول نقل النص التشعبي (HTTPS) ونظام أسماء النطاقات (DNS).
6-3	يجب أن تحدد حلول "الكشف عن تهديدات الشبكات والاستجابة لها" مجموعة متنوعة من سلوكيات القيادة والتحكم، بما في ذلك محاولات محاكاة سلوك المتصفح واستعمال الأنفاق المخفية والاتصالات بين الأقران وتحديثات البرمجيات الضارة، بالإضافة إلى مجموعة واسعة من أساليب التخفي مثل برنامج تور (TOR).
7-3	يجب أن تعمل حلول "الكشف عن تهديدات الشبكات والاستجابة لها" بصفة مستمرة على المراقبة وإرسال تنبيهات بشأن أي حدث وصول ذي امتيازات غير مألوف (يؤدي تعقيد عملية إدارة الامتيازات والصلاحيات إلى احتمال وقوع أخطاء في الإعدادات).

اختر التصنيف

الإصدار <1.0>

8-3	يجب أن تقسم حلول "الكشف عن تهديدات الشبكات والاستجابة لها" المعلومات المجمَّعة إلى قسمين، وهما قسم معلومات المستخدم وقسم المعلومات التشخيصية المخصصة للأغراض الإدارية.
9-3	يجب أن تعمل حلول "الكشف عن تهديدات الشبكات والاستجابة لها" على تحليل الحوادث المسجَّلة وأن تضع خططًا باستخدام تقنيات تعلم الآلة والذكاء الاصطناعي لتجنب تلك الحوادث في المستقبل.
10-3	يجب أن تعمل حلول "الكشف عن تهديدات الشبكات والاستجابة لها" على جمع بيانات الحوادث في قاعدة بيانات مخصصة. ويجب أن يتضمن كل سجل معلوماتٍ عن الفئات المحددة من الحوادث، مثل رسائل بريد التصيّد الإلكتروني والروابط الضارة والمشبوهة وغيرها.
11-3	يجب تحديث قاعدة البيانات المخصصة لمعلومات التهديدات الاستباقية خلال الوقت الفعلي من أجل الإعداد لمواجهة الهجمات الحادثة في المؤسسات المحلية.
12-3	يجب أن تعمل حلول "الكشف عن تهديدات الشبكات والاستجابة لها" على تصفية كل المكونات المنقولة عبر الشبكة، مثل رسائل بريد التصيّد الإلكتروني والروابط الضارة والمشبوهة وغيرها. ويجب أن تكون حلول "الكشف عن تهديدات الشبكات والاستجابة لها" متوافقة مع متطلبات معيار الحماية من البرمجيات الضارة المطبق في <اسم الجهة>.
13-3	يجب أن تبلّغ حلول "الكشف عن تهديدات الشبكات والاستجابة لها" المستخدمين بالإجراءات المتخذة (لا سيما الطلبات المحجوبة أو الملفات المحجوبة) عبر صفحات ويب للاستجابة قابلة للتهيئة والإعداد.
14-3	يجب أن تستخدم حلول "الكشف عن تهديدات الشبكات والاستجابة لها" تدفقات البيانات الأمنية الواردة من الجهات الوطنية الموثوقة مثل فريق وطني للاستجابة لحوادث أمن الكمبيوتر (CSIRT).
4	الإشعارات والاستجابة التلقائية (Automatic response and notification)
الهدف	أن تستخدم حلول "الكشف عن تهديدات الشبكات والاستجابة لها" تقنيات علوم البيانات وتعلم الآلة من أجل الكشف عن التهديدات الأمنية المستقبلية وتحليلها وحماية الأنظمة منها.
المخاطر المحتملة	قد تكون حلول "الكشف عن تهديدات الشبكات والاستجابة لها" غير فعالة في منع الحوادث المستقبلية والحدّ من مخاطرها، ما لم تتسم بمزايا التحليل السليم للأنشطة وتقديم تنبيهات لحظية إلى فرق الاستجابة للحوادث.

الإجراءات المطلوبة	
1-4	يجب أن تكشف حلول "الكشف عن تهديدات الشبكات والاستجابة لها" باستمرار عن أنشطة الشبكة بغرض الكشف عن الهجمات القائمة، حتى يحظى المحللون الأمنيون بوقت أطول للمبادرة بالبحث عن التهديدات واستقصاء الحوادث بنجاح أكبر.
2-4	يجب أن تسرّع حلول "الكشف عن تهديدات الشبكات والاستجابة لها" وقت الاستجابة عبر تكامل المرئيات الأمنية ومشاركتها مع حلول "الكشف عن تهديدات النقاط النهائية والاستجابة لها" (EDR) ونظام "إدارة سجلات الأحداث ومراقبة الأمن السيبراني" (SIEM) و"أدوات التنسيق الأمني والأتمتة والاستجابة" (SOAR).
3-4	يجب أن تحظر حلول "الكشف عن تهديدات الشبكات والاستجابة لها" الوصول غير المصرح به لمنع حالات الوصول إلى المعلومات الجوهرية التي قد تسفر عن تطوير الهجمات أو انتهاك بيانات حساسة.
4-4	يجب أن تبلغ حلول "الكشف عن تهديدات الشبكات والاستجابة لها" فورًا عن الهجمات المحجوبة أو التي تم الحدّ من مخاطرها.
5-4	يجب أن تجمع حلول "الكشف عن تهديدات الشبكات والاستجابة لها" الأحداث ومعلوماتها في قاعدة بياناتها، على أن تشمل الأحداث غير الطبيعية المسجَّلة والهجمات التي تم التصدي لها من قبل للأغراض المستقبلية.
6-4	يجب أن تحدد الجهة سيناريوهات تنفيذ مختلفة لتتبعها حلول "الكشف عن تهديدات الشبكات والاستجابة لها" بغرض الحماية من تهديدات الخصوم، بما يشمل على سبيل المثال لا الحصر: إزالة التهديدات والحدّ من مخاطرها عبر عزل الأنظمة المتأثرة بالتهديد، وكشف ومنع انتشار الروابط الضارة والمشبوهة ورسائل بريد التصيّد الإلكتروني (تستند عمليات الكشف إلى قاعدة البيانات المحلية الخاصة بمعلومات التهديدات الاستباقية).
7-4	يجب أن تجمع حلول "الكشف عن تهديدات الشبكات والاستجابة لها" كل أنواع السجلات من موارد <اسم الجهة>.
8-4	يجب أن تكون حلول "الكشف عن تهديدات الشبكات والاستجابة لها" متوافقة مع متطلبات معيار إدارة ومراقبة سجل الأحداث المعتمد في <اسم الجهة>.
9-4	يجب تهيئة إعدادات حلول "الكشف عن تهديدات الشبكات والاستجابة لها" بحيث تقتصر على إرسال السجلات المحددة فقط إلى نظام السجلات المركزي باستخدام بروتوكول SYSLOG وصيغ السجلات CEF أو LEEF أو RFC 5425، على سبيل المثال.

10-4	يجب أن تشتمل حلول "الكشف عن تهديدات الشبكات والاستجابة لها" على المعلومات التالية، كحد أدنى: ● تاريخ الجلسة ووقت إجرائها ● عنوان برتوكول الإنترنت المصدري ● بيانات تسجيل دخول المستخدم ● بروتوكول الإنترنت للهدف ● التدابير المتخذة ● سياسة استخدام الشبكة المعمول بها

الجدول "أ" - منهجيات استخدام حلول "الكشف عن تهديدات الشبكات والاستجابة لها" (NDR)

توجد منهجيتان رئيسيتان لاستخدام حلول "الكشف عن تهديدات الشبكات والاستجابة لها":

- المستشعرات المدمجة - توفر قدرات استجابة مباشرة.
- المستشعرات السلبية - تعتمد على عمليات التكامل.

المستشعرات المدمجة	تعتمد هذه الطريقة على وضع حلول "الكشف عن تهديدات الشبكات والاستجابة لها" مباشرة في مسار شريحة الشبكة، مما يسمح بالتفتيش السريع لنشاط استخدام الشبكة والتخلص الآني من أنشطة استخدام الشبكة غير الطبيعية أو الضارة أو المشبوهة.
المستشعرات السلبية	يتمحور خيار المستشعرات السلبية حول وضع حلول "الكشف عن تهديدات الشبكات والاستجابة لها" داخل الشبكة (عادةً ما تكون مدمجة مع نظام "إدارة سجلات الأحداث ومراقبة الأمن السيبراني" والحلول السحابية العامة والخاصة، وغيرها) واستخلاص البيانات الوصفية من اللقطات المسجَّلة، ومن ثمَّ إرسالها للتحليل.

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

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>.