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 الحماية من التهديدات المستمرة المتقدمة(APT)

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

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

جدول المراجعة

معدل المراجعة	التاريخ لآخر مراجعة	تاريخ المراجعة القادمة
مره واحدة كل سنة	اضغط هنا لإضافة تاريخ	اضغط هنا لإضافة تاريخ

اختر التصنيف

الإصدار <١,٠>

قائمة المحتويات

الغرض

الغرض من هذا المعيار هو تحديد متطلبات الأمن السيبراني التفصيلية المتعلقة بالكشف عن التهديدات المستمرة المتقدمة والحماية منها. حيث سيساعد اتباع هذه المتطلبات على الحدّ من مخاطر الأمن السيبراني والحماية من التهديدات الداخلية والخارجية من أجل الحفاظ على توافر وسلامة وسرية الأصول التقنية لدى <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

يغطي هذا المعيار جميع الأصول التقنية والمعلوماتية الخاصة ب<اسم الجهة>، وينطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

المعايير

١	إعدادات البيئة الأمنية (Security environment configuration)
الهدف	ضمان نشر الآليات الأمنية (security mechanisms) بنجاح لحماية البيئة من التهديدات المستمرة المتقدمة (APT) من أجل الكشف عن جميع التهديدات واتخاذ تدابير الحماية منها ومنعها.
المخاطر المحتملة	في حالة عدم وجود مركز عمليات أمنية (SOC) مشغل ومُدار بشكل سليم، تصبح موارد <اسم الجهة> عرضة للتهديدات المستمرة المتقدمة (APT)، مما قد يكون له عواقب وخيمة على الالتزام واستمرارية الأعمال لدى <اسم الجهة>، وقد يؤدي إلى وقوع حوادث أمنية محتملة جديدة بسبب الهجمات الناتجة عن مجموعات التهديدات المستمرة المتقدمة.
الإجراءات المطلوبة	
١-١	يجب على <اسم الجهة> تنفيذ خدمة المعلومات الاستباقية بشأن التهديدات السيبرانية (Threat Intelligence Service) لتحديد الهجمات التي تسمح بالوصول غير المصرح به إلى الشبكة لفترة زمنية طويلة دون اكتشافها.
١-٢	يجب على <اسم الجهة> التحقيق في الطرق والأساليب المستخدمة خلال الهجمات المنفذة من مجموعات التهديدات المستمرة المتقدمة (APT) المعروفة.

١-٣	يجب على <اسم الجهة> التأكد من أن إعدادات التسجيل في كل نظام تحتوي على سمات تسمح بتحديد سلوكيات معينة (مثل مستوى الخطورة، واسم المستخدم ذي الصلة، واسم المضيف، والوقت المستغرق، والأوامر المنفذة، وغيرها من البيانات ذات الصلة)، ويجب توضيحها جميعها في قواعد الارتباط الخاصة بنظام إدارة المعلومات والأحداث الأمنية (SIEM).
١-٤	يجب على <اسم الجهة> وضع وتحديث قائمة بأنواع الحوادث التي قد تؤكد أو تنفي الارتباط بالتهديدات المستمرة المتقدمة (APT). ويجب أن تشمل هذه القائمة كحدٍ أدنى جميع الحوادث ذات الصلة بالوصول غير المصرح به أو الإصابة بالبرمجيات الضارة.
٢	تأكيد التهديدات المستمرة المتقدمة (Confirmation of APT)
الهدف	يجب التحقق من جميع الحوادث الأمنية التي تقع في بيئة <اسم الجهة> من حيث اتصالها بالتهديدات المستمرة المتقدمة (APT).
المخاطر المحتملة	يمكن أن يؤدي تجاهل الدلائل على وجود التهديدات المستمرة المتقدمة (APT) إلى استمرار وجود ممثلي التهديدات وقد يؤدي ذلك إلى سرقة المعلومات والإفصاح عنها أو الوصول غير المصرح به إليها .
الإجراءات المطلوبة	
٢-١	يجب <اسم الجهة> التحقيق بعناية في كل أنواع الحوادث المدرجة لتأكيد أو نفي وجود أي دلالة على تهديدات مستمرة متقدمة (APT) في تلك الحادثة. وقد تم توضيح الطرق التي تستخدمها مجموعات التهديدات المستمرة المتقدمة (APT) في الجدول "أ" وذلك وفقًا لإطار تكتيكات الخصم وتقنياته ومعرفته العامة (MITRE Attack) .
٢-٢	يجب على <اسم الجهة> تنفيذ آليات لتحليل العينات بشكل آمن وتحديد مدى ارتباطها بالتهديدات المستمرة المتقدمة، باستخدام نوعين حديثين من برامج مكافحة الفيروسات (Antivirus) أو تقنيات وآليات الكشف عن التهديدات في الأجهزة الطرفية والاستجابة لها (EDR) ومحركات تقنية الحماية المعزولة (sandbox engines) (يمكن إسناد هذه المهمة إلى مقدم خدمات مدارة إذا لزم الأمر).
٢-٣	يجب على <اسم الجهة> تحديد كل مؤشرات الاختراق (IoCs) المتعلقة بالحادثة الذي تم تحليلها. ويوضح الجدول "ب" أمثلة على مؤشرات الاختراق المحتملة.

٢-٤	يجب على <اسم الجهة> توفير بيئة معزولة لإتلاف الملفات الخبيثة التي تم تحليلها للتعرف على جميع الإجراءات التي تقوم بها البرمجيات الضارة وتحديد مؤشرات الاختراق الجديدة المحتملة. ويجب أن تكون هذه البيئة في جزء مخصص من الشبكة وأن يتم نشرها على مجموعات خوادم مخصصة تتم مراقبتها بعناية عن طريق الحلول الأمنية. ويعتبر حل تقنية الحماية المعزولة (Sandbox) من الأجزاء المهمة في هذه البيئة. (يمكن إسناد هذه المهمة إلى مقدم خدمات مدارة إذا لزم الأمر).
٢-٥	يجب على <اسم الجهة> التحقق من جميع مؤشرات الاختراق التي تم رصدها في قاعدة بيانات المعلومات الاستباقية عن التهديدات. جميع روابط الإنترنت وعناوين بروتوكول الإنترنت، ودوال الاختزال (Hash) للملفات المشبوهة، جميعها قد تكون حدثت بواسطة ممثل التهديد في وقت سابق، ويمكن لفريق مركز العمليات الأمنية في <اسم الجهة> تحديد ما إذا كان ممثل التهديد المعني من مجموعات التهديدات المستمرة المتقدمة المعروفة .
٢-٦	يجب على <اسم الجهة> التحقق من الطرق والأساليب المستخدمة من جانب ممثل التهديد مع فريق الاستجابة لحوادث الأمن السيبراني على المستوى الوطني (CSIRT) إذا كانت مجموعة التهديدات المستمرة المتقدمة المحددة تنفذ الهجمات حاليًا في جهة أخرى في نفس قطاع الأعمال الذي تعمل فيه <اسم الجهة>.
٣	الحدّ من الهجمات (Attack mitigation)
الهدف	بعد النجاح في الكشف عن التهديدات المستمرة المتقدمة وتأكيد وجودها، من الضروري الحدّ من المخاطر عن طريق مشاركة المعلومات عن الهجوم مع فريق الاستجابة لحوادث الأمن السيبراني على المستوى الوطني (CSIRT).
المخاطر المحتملة	في حالة عدم الحدّ من المخاطر وعدم مشاركة المعلومات عن خصائص الهجوم بشكل مناسب، فقد تتمكن مجموعات التهديدات المستمرة المتقدمة من نشر البرمجيات الضارة والتصيد الاحتيالي وتسريب المعلومات بسهولة.
الإجراءات المطلوبة	
٣-١	يجب على <اسم الجهة> التحقيق في جميع الأحداث السابقة المجمعة لتحديد الطرق المستمرة التي استخدمها ممثل التهديد المكتشف.
٣-٢	يجب على <اسم الجهة> مشاركة المعلومات بشأن الهجوم مع فريق الاستجابة لحوادث الأمن السيبراني على المستوى الوطني وعلى مستوى قطاع الأعمال.
٣-٣	يجب على <اسم الجهة> مراقبة أنظمتها الداخلية لتحديد جميع الأجهزة الطرفية والخوادم المصابة وعزلها .

٣-٤	يجب على <اسم الجهة> تحليل كل نظام مصاب لاتخاذ الإجراءات اللازمة للحدّ من المخاطر أو استعادة البيانات من النسخة الاحتياطية بعد إزالة البيانات المصابة .
٣-٥	بعد الحدّ من التهديدات على نظام معين، يجب على <اسم الجهة> مراقبة سلوكه لتحديد مدى نجاح إجراءات الحدّ من التهديدات .
٣-٦	يجب على <اسم الجهة> أن تضع في الاعتبار أنه بالرغم من اتخاذ الإجراءات اللازمة لاستعادة النظام، إلا أنه يجب تحليله في كل مرة يتم فيها اكتشاف مؤشر اختراق جديد يتعلق بالتهديدات المستمرة المتقدمة التي تم تحليلها .
٤	معايير أخرى (Other Standard Controls)
الهدف	يعتمد الأمن السيبراني ل<اسم الجهة> بالكامل على بناء البيئة الأمنية وفقًا لأفضل الممارسات والتزامًا بالمعايير والسياسات ذات العلاقة .
المخاطر المحتملة	في حالة عدم التزام <اسم الجهة> بجميع المعايير والمتطلبات الإلزامية المطبقة، فقد يعرضها ذلك إلى زيادة حادة في التهديدات في المجالات المشمولة ضمن نطاق المعايير المذكورة أدناه .
الإجراءات المطلوبة	
٤-١	يجب تطبيق المعايير التالية للكشف عن التهديدات المستمرة المتقدمة والوقاية منها بفعالية وكفاءة: ١. تسجيل الأحداث وسجلات التدقيق ٢. إدارة ومراقبة سجل الأحداث ٣. الكشف عن تهديدات النقاط النهائية والاستجابة لها ٤. الكشف عن تهديدات الشبكات والاستجابة لها ٥. تحليل سلوكيات المستخدمين ٦. إدارة المعلومات والأحداث الأمنية ٧. اختبار الاختراق ٨. حماية تطبيقات الويب ٩. إدارة الثغرات ١٠. منع فقدان البيانات

الجدول "أ" - التكتيكات المستخدمة خلال الهجمات وفقًا لإطار تكتيكات الخصم وتقنياته ومعرفته العامة (MITRE Attack)

مرحلة تكتيكات الهجوم	الوصف
الاستطلاع	تجمع مجموعة الاختراق البيانات التي ستُستخدم عند التخطيط للإجراءات المستقبلية. وتشير هذه المرحلة إلى التكتيكات التي تتبعها مجموعات الاختراق للحصول على المعلومات التي يمكن استخدامها لمساعدتها في الاستهداف، سواءً بشكل مباشر أو غير مباشر. ومن الأمثلة على تلك المعلومات تفاصيل البنية التحتية والعاملين في الإدارة المعرضة للهجوم.
تطوير الموارد	تحاول مجموعات الاختراق جمع الموارد لمساعدتها في العمليات .وتقوم مجموعات الاختراق بإنشاء أو شراء أو اختراق أو سرقة الموارد (البنية التحتية أو الحسابات أو القدرات) التي يمكن استخدامها لتمكين الاستهداف في إطار طرق تطوير الموارد.
الوصول الأولي	تحاول مجموعات الاختراق الوصول إلى شبكة الجهة .ويشتمل الوصول الأولي على عدد من المنهجيات التي تستخدم مجموعة متنوعة من متجهات الدخول للوصول إلى الشبكة. ويعتبر التصيّد الاحتيالي المستهدف واستغلال الثغرات الأمنية في خوادم الويب العامة من الطرق المستخدمة للوصول إلى الشبكة. وقد يسمح الدخول الأولي الذي تحققه مجموعات الاختراق باستدامة الوصول (مثل، الحسابات الصحيحة واستخدام الخدمات الخارجية عن بعد).
التنفيذ	يحاول الخصم تشغيل شفرة برمجية خبيثة. ويُشار إلى التقنيات التي تؤدي إلى تشغيل شفرة برمجية يتحكم فيها الخصم على نظام محلي أو بعيد باسم "التنفيذ." وعادةً ما يتم دمج تقنيات تنفيذ الشفرة البرمجية الخبيثة مع تقنيات التكتيكات الأخرى لتحقيق أهداف أوسع نطاقًا، مثل استكشاف الشبكة أو سرقة البيانات.
الاستمرارية	تحاول مجموعات الاختراق الحفاظ على الوصول الذي حققته، وتستخدم استراتيجيات الاستمرارية للحفاظ على الوصول إلى الأنظمة رغم إعادة تشغيلها وتغيير بيانات هويات الدخول وغير ذلك من التغييرات. وتشمل تقنيات الاستمرارية تغيير أو اختراق الشفرة البرمجية الشرعية أو إضافة شفرة برمجية عند التشغيل، إلى جانب إجراء أي تعديلات على صلاحيات الوصول أو الإجراءات أو الإعدادات بحيث تحتفظ مجموعات الاختراق بسيطرتها على الأنظمة.
تصعيد الامتيازات	تحاول مجموعات الاختراق الحصول على صلاحيات وصول ذات امتيازات أعلى. وتستخدم لذلك استراتيجيات تصعيد الامتيازات (Privileged Escalation) للحصول على تصاريح ذات مستوى أعلى على النظام أو الشبكة. وتستطيع في كثير من الأحيان الحصول على صلاحيات وصول دون امتيازات إلى الشبكة واستكشافها، لكنه يحتاج إلى تصاريح ذات امتيازات أعلى لإتمام مهامها المخططة. ومن الاستراتيجيات الشائعة لذلك استغلال العيوب في النظام والإعدادات الخاطئة والثغرات الأمنية.
المراوغة الدفاعية	تحاول مجموعات الاختراق تفادي اكتشافها. ويُقصد بالمراوغة الدفاعية الاستراتيجيات التي تستخدمها مجموعات الاختراق للتهرب من الاكتشاف أثناء الاختراق. ومن الأمثلة على تقنيات المراوغة الدفاعية، إلغاء تثبيت أو تعطيل

اختر التصنيف

الإصدار <١,٠>

	البرمجيات الأمنية أو تعتيم/تشفير البيانات والنصوص. وتستخدم مجموعات الاختراق العمليات الموثوقة ويسيئون استعمالها لإخفاء برمجياتهم الضارة.
الوصول إلى بيانات هويات الدخول	تحاول مجموعات الاختراق سرقة أسماء المستخدمين وكلمات مرورهم. ويُشار إلى تقنيات سرقة بيانات الاعتماد، مثل أسماء المستخدمين وكلمات مرورهم، بـ " الوصول إلى بيانات هويات الدخول." ويعتبر رصد لوحة المفاتيح (Keylogging) واختراق بيانات هويات الدخول (Credential dumping) من طرق الحصول على بيانات هويات الدخول. ومن خلال استخدام بيانات هويات الدخول الأصلية، يمكن لمجموعات الاختراق الوصول إلى الأنظمة، مما يجعل اكتشافها أكثر صعوبةً ويتيح لهم إنشاء حسابات جديدة لتحقيق أهدافهم.
الاستكشاف	تحاول مجموعات الاختراق التأكد من محيط الشبكة والأنظمة. ويشير الاستكشاف إلى الطرق التي قد تستخدمها مجموعات الاختراق لمعرفة المزيد عن النظام والشبكة الداخلية. وتساعد هذه الاستراتيجيات مجموعات الاختراق في مراقبة محيط الشبكة والأنظمة وتوجيه أنفسهم قبل اتخاذ القرار بشأن كيفية الاستجابة. كما أنها تتيح للخصوم استكشاف العناصر التي يمكنهم التأثير عليها والمكوّنات المحيطة بنقطة دخولهم لمعرفة ما إذا كان ذلك قد يساعدهم في تحقيق هدفهم الحالي. وغالبًا ما يتم تحقيق هدف جمع المعلومات بعد هذا الاختراق باستخدام تقنيات نظام التشغيل الأصلي.
الحركة الجانبية	تحاول مجموعات الاختراق التنقل داخل محيط الشبكة والأنظمة. وتستخدم طرق الحركة الجانبية للوصول إلى الأنظمة المتصلة بالشبكة عن بُعد والتحكم فيها. ومن المتطلبات الشائعة لمجموعات الاختراق كي تحقق هدفها الأساسي استكشاف الشبكة لتحديد هدفها، ثم الوصول إليه. وغالبًا ما يستلزم الوصول إلى هدفه الالتفاف حول العديد من الأنظمة والحسابات. وللقيام بالحركة الجانبية، قد تقوم مجموعات الاختراق بتثبيت أدوات الوصول عن بُعد الخاصة بها أو استخدام بيانات هويات دخول صالحة باستخدام قدرات الشبكة ونظام التشغيل الأصلي، أيهما كان متخفيًا بدرجة أكبر.
الجمع	تحاول مجموعات الاختراق جمع البيانات ذات الصلة بالهدف. ويشير جمع البيانات إلى الاستراتيجيات التي قد تستخدمها مجموعات الاختراق لجمع المعلومات وكذلك إلى المصادر التي تُجمع منها المعلومات ذات الصلة بتحقيق أهدافها. وبعد الحصول على البيانات، غالبًا ما تكون الخطوة التالية هي سرقتها (استخراجها). وهناك العديد من المصادر المستهدفة الشائعة، من بينها أنواع الأقراص المختلفة والمتصفحات والصوت والفيديو والبريد الإلكتروني. وتعتبر لقطات الشاشة ومُدخلات لوحة المفاتيح من التقنيات الشائعة لجمع البيانات.
القيادة والتحكم	تحاول مجموعات الاختراق الاتصال بالأنظمة المصابة للتحكم فيها، وقد تستخدم طرق القيادة والتحكم للاتصال بأجهزة الكمبيوتر الخاضعة لسيطرتها داخل الشبكة المصابة. وللتهرب من الاكتشاف، تحاول مجموعات الاختراق في العادة محاكاة حركة مرور البيانات الطبيعية والمتوقعة. وبناءً على بنية الشبكة وتدابير الحماية لدى الضحية، يمكن لمجموعات الاختراق تحقيق القيادة والتحكم بطرق مختلفة ذات مستويات متفاوتة من التخفي.

اختر التصنيف

الإصدار <١,٠>

الاستخراج	تحاول مجموعات الاختراق سرقة المعلومات. ويُقصد الاستخراج الطرق التي يمكن للمتسللين استخدامها لسرقة البيانات من الشبكة. وغالبًا ما تقوم مجموعات الاختراق بضغط البيانات في حزم بعد جمعها للتهرب من الاكتشاف أثناء التخلص منها. ومن الأمثلة على ذلك ضغط البيانات وتشفيرها. ومن التقنيات الشائعة أيضًا نقل البيانات من الشبكة المستهدفة باستخدام قناة القيادة والتحكم الخاصة بالخصم أو أي قناة بديلة، وكذلك فرض قيود على حجم البيانات المرسلة.
التأثير	تحاول مجموعات الاختراق تعديل أو تعطيل أو تدمير البيانات والأنظمة. تستخدم مجموعات الاختراق منهجيات التأثير (مثل تدمير البيانات أو التلاعب بها) لتعطيل التوافر أو تقويض سلامة البيانات من خلال تعديل عمليات الأعمال والعمليات التشغيلية. وقد تبدو إجراءات الأعمال طبيعية في الظاهر، لكنها ربما تكون قد تم تعديلها لتتناسب مع أهداف مجموعات الاختراق. ويمكن أن يستخدم الخصم هذه الاستراتيجيات لتحقيق غرضه النهائي أو توفير غطاء لانتهاك السرية.

الجدول "ب" - أمثلة على مؤشرات الاختراق

مؤشرات الاختراق	الوصف
حركة مرور البيانات الصادرة غير العادية على الشبكة	تُعتبر الحالات غير الطبيعية في أنماط حركة المرور على الشبكة وأحجامها من أكثر علامات الاختراق الأمني شيوعًا. ورغم الصعوبة المتزايدة لمنع المتسللين من الدخول إلى الشبكة، إلا أنه قد يكون من الأسهل مراقبة حركة مرور البيانات الصادرة بحثًا عن مؤشرات الاختراق المحتملة. فعندما يحاول أحد المتسللين استخراج البيانات من الشبكة أو عندما ينقل أحد الأنظمة المصابة المعلومات إلى أحد خوادم القيادة والتحكم، يمكن اكتشاف حركة مرور البيانات الصادرة غير العادية على الشبكة.
النشاط من مناطق جغرافية غريبة	إذا كانت الأعمال مرتكزة في دولة معينة وحاول أحد المستخدمين الاتصال بالشبكة من موقع مختلف، فيجب التحقيق في الأمر. ومن المفترض أن تُظهر السجلات أي حساب يسجل الدخول من عناوين بروتوكول إنترنت متعددة خلال مدة زمنية قصيرة، لا سيما عندما يكون ذلك مقترنًا بوسم تحديد الموقع الجغرافي. وفي كثير من الأحيان، يكون هذا دليلاً على استخدام أحد المهاجمين لمجموعة من بيانات هويات الدخول المخترقة لتسجيل الدخول إلى الأنظمة السرية. تُعتبر مراقبة عناوين بروتوكول الإنترنت الموجودة على الشبكة والمواقع التي صدرت منها من الطرق المتيسرة للكشف عن الهجمات السيبرانية قبل أن تتمكن من إحداث ضرر حقيقية للجهة.
أنشطة غير مبررة من جانب حسابات المستخدمين ذات الامتيازات	في الهجمات السيبرانية المعقدة، مثل التهديدات المستمرة المتقدمة، من الطرق الشائعة اختراق حسابات المستخدمين ذات الامتيازات المنخفضة ثم تصعيد الامتيازات والتصريحات أو توجيه الهجوم نحو حسابات ذات امتيازات أعلى. وعندما يلاحظ مسؤولو الأمن سلوكيات مشبوهة من حسابات المستخدمين ذات

اختر التصنيف

الإصدار <١,٠>

	الامتيازات، فقد يكون ذلك دليلاً على وجود هجمات داخلية أو خارجية على أنظمة وبيانات الجهة.
ارتفاع كبير في حجم قراءة قاعدة البيانات	تخزن معظم الجهات بياناتها السرية والشخصية في قاعدة بيانات، وبالتالي، عادةً ما تكون قواعد البيانات هدفًا رئيسيًا للمهاجمين. لذلك، يمثل الارتفاع في حجم قراءة قاعدة البيانات مؤشرًا وجيهًا على محاولة أحد المهاجمين اختراق البيانات.
زيادة حالات الفشل في التحقق من الهوية	في حالة الاستيلاء على الحسابات، يستخدم المهاجمون تقنيات الأتمتة للتحقق من الهوية باستخدام بيانات هويات الدخول المسروقة. وقد يشير المعدل المرتفع لمحاولات التحقق من الهوية إلى أن أحد الأشخاص يستخدم بيانات اعتماد مسروقة ويحاول العثور على حساب يتيح له الوصول إلى الشبكة.
زيادة الطلبات على الملفات المهمة	يضطر المهاجم الذي لا يمتلك حسابًا ذي امتيازات لاستخدام طرق مختلفة لإيجاد ثغرة يصل منها إلى الملفات. وعندما يجد المهاجمون دلالات على أن إحدى محاولات الاستغلال قد تنجح، فإنهم عادةً ما يستخدمون طرقًا بديلة مختلفة لتنفيذها. فعلى سبيل المثال، من غير الطبيعي أن يقوم مستخدم أو عنوان بروتوكول إنترنت واحد بطلبات أكثر من المعتاد بعشر مرات.
التغييرات المشبوهة في الإعدادات	يمكن أن يؤدي تغيير إعدادات الملفات والخوادم والأجهزة إلى إتاحة منفذ خلفي آخر للمهاجم كي يصل إلى الشبكة. كما أن التغييرات يمكن أن تضيف أيضًا ثغرات تستطيع البرمجيات الضارة استغلالها.
مؤشرات على هجمات حجب الخدمة الموزعة (DDoS)	تقع هجمات حجب الخدمة الموزعة (DDoS) عندما تحاول جهة خبيثة إيقاف تشغيل أي خدمة من خلال إغراقها بحركة مرور البيانات والطلبات من شبكة من جهاز متحكّم فيه يُطلق عليه اسم شبكة البوت (Botnet). وغالبًا ما تُستخدم هجمات حجب الخدمة الموزعة كوسائل تمويه لإخفاء هجمات أخرى أكثر ضررًا. ومن الدلائل على هجمات حجب الخدمة الموزعة: بطء أداء الشبكة، وعدم توافر المواقع الإلكترونية، وتعطل جدار الحماية، وعمل الأنظمة الخلفية بأقصى طاقتها لأسباب غير معروفة.

الأدوار والمسؤوليات

١- **مالك المعيار:** <رئيس الإدارة المعنية بالأمن السيبراني>.

٢- **مراجعة المعيار وتحديثه:** <الإدارة المعنية بالأمن السيبراني>.

٣- **تنفيذ المعيار وتطبيقه:** <الإدارة المعنية بتقنية المعلومات>

٤- **قياس الالتزام بالمعيار:** <الإدارة المعنية بالأمن السيبراني>.

اختر التصنيف

الإصدار <١,٠>

التحديث والمراجعة

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

الالتزام بالمعيار

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

٢- يجب على كافة العاملين في <اسم الجهة> الالتزام بهذا المعيار.

٣- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في <اسم الجهة>.