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 هجمات حجب الخدمة الموزعة (DDoS Attacks)

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. 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	عُدّل 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 للحماية من هجمات حجب الخدمة الموزعة (DDoS) في <اسم الجهة> وستساعد قدرة <اسم الجهة> على تطبيق الضوابط المحددة في معيار الحماية من هجمات حجب الخدمة الموزعة (DDoS) في الحفاظ على توافر وسلامة وسرية معلومات <اسم الجهة> وأصولها.

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 أفضل الممارسات المتبعة لدى <اسم الجهة> في نشر واستخدام حل الحماية من هجمات حجب الخدمة الموزعة (DDoS)، وينطبق على جميع الأصول وجميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>

المعايير

1	المتطلبات العامة (General Requirements)
الهدف	نشر حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) بشكل آمن واستخدامه بشكل مناسب عند الحاجة.
المخاطر المحتملة	قد يؤدي الخطأ في ضبط إعدادات حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) إلى عدم توفر خدمات الأعمال المقدمة للعملاء والخدمات الداخلية للشركة.
الإجراءات المطلوبة	
1-1	أن يقوم حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) بتوفير اتفاقية لمستوى الخدمة تنص على مدة مضمونة للحدّ من الهجمات (TTM). وهذا المتطلب مهم بشكل خاص عند نشر الحل كخدمة.
2-1	أن يوفر حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) الحماية لحزمتي بروتوكول الإنترنت الإصدار الرابع (IPv4) وبروتوكول الإنترنت الإصدار السادس (IPv6)على شبكة <اسم الجهة>.
3-1	أن يكون هناك اتساق في وقت تشغيل التطبيق والتوافر بالنسبة لحل الحماية من هجمات حجب الخدمة الموزعة (DDoS).

اختر التصنيف

الإصدار <1.0>

4-1	أن يوفر حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) الحماية للشبكات ولخوادم نظام أسماء النطاقات (DNS) والمواقع الإلكترونية المتاحة للجمهور والمستضافة في بيئة تقنية المعلومات وبروتوكولات الإنترنت الفردية لدى <اسم الجهة>.
5-1	أن يوفر حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) حماية متعددة الطبقات من الهجمات على طبقات الشبكة والتطبيقات ومن الهجمات الكمّية وغير الكمّية، إلى جانب التغطية الكاملة لهجمات حجب الخدمة الموزعة المعتمدة على بروتوكول طبقة المنافذ الآمنة (SSL) / بروتوكول أمن طبقة النقل (TLS).
6-1	أن يكون لجميع مديري نظام تقنية المعلومات لدى <اسم الجهة> المحددين في مبادئ إدارة صلاحيات الوصول، والذين يحتاجون إلى الوصول إلى سجلات هجمات حجب الخدمة الموزعة (DDoS)، صلاحية وصول إلى قاعدة بيانات السجلات.
7-1	إتاحة نشر حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) بمختلف المنهجيات - الجدول "أ ".
8-1	تثبيت جميع التحديثات الأمنية لحل الحماية من هجمات حجب الخدمة الموزعة (DDoS) وفقًا لعملية إدارة التحديثات والإصلاحات.
9-1	أن تقوم جميع قنوات الاتصالات الإدارية باستخدام شبكة مخصصة للإدارة أو اتصالات عبر شبكة الإدارة بحيث تكون موثقة ومشفّرة باستخدام وحدات التشفير المعتمدة وفقًا لمعيار التشفير الوطني (National Cryptography Standard) ومعايير التشفير الداخلية المطبقة لدى <اسم الجهة>. ويجب توفير الحماية في حالة الوصول إلى وحدة التحكم الإدارية كطريقة لنشر هجمات حجب الخدمة الموزعة كخدمة (DDoS as a Service).
10-1	وضع خطة للاستجابة لهجمات حجب الخدمة الموزعة (DDoS) والحدّ منها وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة.
11-1	على <اسم الجهة> تدريب العاملين فيها بصفة دورية لضمان معرفتهم بكيفية اختيار الخدمة المناسبة للحدّ من الهجمات، مع قياس فعالية التدريب بناءً على مراجعة مؤشرات الأداء الرئيسية سنويًا.
2	الوقاية من الهجمات (Attack prevention)
الهدف	أن يمنع حل الحماية من هجمات حجب الخدمة الموزعة (DDoS)، الذي تم ضبط إعداداته بشكل صحيح وإدارته بشكل آمن، محاولات شن تلك الهجمات على البنية التحتية لـ <اسم الجهة> .

المخاطر المحتملة	قد يؤدي الخطأ في ضبط إعدادات حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) إلى عواقب وخيمة، مثل حجب حركة مرور البيانات المشروعة وحجب الخدمة.
الإجراءات المطلوبة	
1-2	على <اسم الجهة> تحديد جميع الأصول المتاحة من الشبكة العامة وحمايتها، باستخدام حل الحماية من هجمات حجب الخدمة الموزعة (DDoS)، لضمان قدرتها على الاستجابة بفعالية لهجمات حجب الخدمة/حجب الخدمة الموزعة.
2-2	تخصيص حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) بما يتناسب مع خصائص القطاع الذي تعمل فيه <اسم الجهة>.
3-2	أن يوفر حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) تقارير ولوحات تحكم للهجمات التي تم منعها والإجراءات المتخذة بشأنها.
4-2	أن يوفر حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) حماية متعددة الطبقات، بحيث يحمي طبقة الشبكة وطبقة التطبيقات عند نشره مع جدار حماية تطبيقات الويب (WAF).
5-2	أن يستخدم حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) المعلومات الأمنية المقدمة من المؤسسات الوطنية الموثوقة، مثل الهيئة الوطنية للأمن السيبراني (NCA).
3	الكشف عن الهجمات والتنبيه بها والحدّ منها (Attack detection, alerting and mitigation)
الهدف	أن يكتشف حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) الحالات غير الطبيعية وأن يحدّ من الهجمات باستخدام أسلوب التصفية والتقييد.
المخاطر المحتملة	قد تؤدي عدم كفاية عمليات الكشف عن الهجمات إلى انتشار البرمجيات الضارة وحجب الخدمة وتسرب المعلومات.
الإجراءات المطلوبة	
1-3	على <اسم الجهة> تحديد مؤشرات أداء رئيسية لرصد مدى فعالية حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) والتوجهات المتعلقة بهذا الحل.
2-3	أن يكون بإمكان حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) إيقاف انتشار هجمات حجب الخدمة/حجب الخدمة الموزعة ومنح حدوث المزيد من الأضرار للنظام .

3-3	أن يَستخدم حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) الأتمتة من أجل الحد من الهجمات الناشئة بشكل سريع.
4-3	أن يتيح حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) تكوين رؤية واضحة آنية حول تهديدات حجب الخدمة الموزعة، مع إمكانية إعداد التقارير وإنشاء الروابط بين الهجمات من خلال تحليلات الهجمات أو التكامل مع نظام إدارة المعلومات والأحداث الأمنية (SIEM).
5-3	أن يصدر عن حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) إشعارات فورية بالهجمات.
6-3	أن يخطر حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) المستخدمين بالإجراءات المتخذة والهجمات التي تم منعها والحد منها.
7-3	ضبط إعدادات التنبيهات بحيث تصدر في بداية الهجوم وفي نهايته وخلاله، وذلك باستخدام مقاييس مخصصة للهجمات.
8-3	أن يستخدم حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) تقنيات التعلّم الآلي والذكاء الاصطناعي لمنع التهديدات الجديدة.
9-3	ضبط إعدادات حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) لإرسال سجلات محددة فقط إلى نظام السجلات المركزي باستخدام بروتوكول سجل النظام (syslog) وبتنسيق الحدث العام (CEF) أو التنسيق الموسع لسجل الحدث (LEEF) أو تنسيق (RFC 5425) المحدد للسجلات.
10-3	أن يحدد حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) عنوان بروتوكول إنترنت معين للسلوك الخبيث، مع إجراء التحليلات الجنائية لتحديد كيفية انتقال التهديدات من جانب إلى آخر داخل البيئة الأمنية.
11-3	أن يراقب حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) نشاط الشبكة باستمرار لرصد أي حدث غير طبيعي في حركة مرور البيانات، مثل النمو غير المعتاد في إنتاجية الشبكة أو استخدام موارد الشبكة بدرجة أعلى من المعتاد.
4	معايير أخرى (Other Standards)
الهدف	ضبط إعدادات حل الحماية من هجمات حجب الخدمة الموزعة (DDoS) بشكل آمن ونشره واستخدامه بشكل مناسب وفقًا لأفضل الممارسات والتزما بالمعايير والسياسات ذات العلاقة بالبيئة الأمنية.

المخاطر المحتملة	قد يؤدي عدم التزام <اسم الجهة> بجميع المعايير والمتطلبات الإلزامية المطبقة إلى تعرضها إلى زيادة حادة في التهديدات في المجالات التي تختص المعايير المذكورة أدناه بتغطيتها .
الإجراءات المطلوبة	
1-4	تطبيق المعايير التالية فيما يتعلق بحلول الحماية من هجمات حجب الخدمة الموزعة (DDoS): 1. إدارة هويات الدخول والصلاحيات 2. النسخ الاحتياطي والتعافي من الكوارث 3. التشفير 4. تسجيل الأحداث وسجلات التدقيق 5. الأمن المادي 6. الإعدادات والتحصين الآمن 7. إدارة ومراقبة سجلات الأحداث

الجدول "أ" - منهجيات نشر حل الحماية من هجمات حجب الخدمة الموزعة (DDoS)

المنهجية	الوصف
الحماية من هجمات حجب الخدمة الموزعة كخدمة (DDoS as a Service)	تطبيق حلول مقدمي الخدمات. وعادةً ما يتم تنفيذ منهجية "الحماية من هجمات حجب الخدمة الموزعة كخدمة" من خلال إعادة توجيه حركة مرور البيانات على الشبكة إلى مركز معالجة (scrubbing center) خارجي.
داخل الموقع (الأجهزة)	نشر الحل على شبكة <اسم الجهة>، ويتم ذلك من خلال تركيب الأجهزة وتوصيلها بالشبكة.
المنهجية الهجينة (Hybrid)	تجمع هذه المنهجية بين نشر الحل كخدمة ونشره داخل الموقع بهدف الحد من الهجمات الكمية على مقربة من مصدر الهجوم قدر الإمكان، مع الحد من هجمات حجب الخدمة الموزعة (DDoS) على محيط شبكة <اسم الجهة> باستخدام موارد مركز المعالجة الخاصة بالخدمة السحابية/مزود خدمة الإنترنت إذا كانت هجوم حجب الخدمة الموزع يتجاوز قدرات الأجهزة الموجودة داخل الموقع .

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> و<الإدارة المعنية بالأمن السيبراني>.

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 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.

اختر التصنيف

الإصدار <1.0>

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>.