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 أمن البيئة الافتراضية

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. 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	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 <١,٠>

قائمة المحتويات

اختر التصنيف

الإصدار <١,٠>

الغرض

الغرض من هذا المعيار هو تحديد متطلبات الأمن السيبراني التفصيلية المتعلقة بالبيئة الافتراضية في <اسم الجهة>. حيث أن البيئة الافتراضية هي عملية إنشاء وإدارة نظام حاسوبي افتراضي في بيئة محاكاة افتراضية.

تمت مواءمة هذه المتطلبات مع متطلبات الأمن السيبراني الصادرة عن 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) وضوابط الأمن السيبراني للحوسبة السحابية (CCC-1:2020) وغيرها من المتطلبات التشريعية والتنظيمية ذات العلاقة.

النطاق

يغطي هذا المعيار جميع الأصول المعلوماتية والتقنية الخاصة ب<اسم الجهة> وينطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة> والأطراف الثالثة ذات العلاقة.

المعايير

١	أمن المضيف (Host Security)
الهدف	إدارة المضيف المستخدم للبيئة الافتراضية بشكل آمن واستخدامه بشكل مناسب عند الحاجة.
المخاطر المحتملة	قد يكون لاختراق المضيف تداعيات أمنية جسيمة على كافة البيئات الافتراضية وقد يتسبب في سرقة المعلومات والكشف عنها والوصول غير المصرح به إليها.
الإجراءات المطلوبة	
١-١	تثبيت جميع التحديثات الأمنية على نظام تشغيل المضيف (إن وُجد) بمجرد إصدارها من المورد. ويجب إزالة جميع التطبيقات غير الضرورية باستثناء مراقب الأجهزة الافتراضية.
١-٢	أن يتوافق نظام تشغيل المضيف مع متطلبات معيار إدارة ومراقبة سجل الأحداث المعتمد في <اسم الجهة>، ويجب أن يجمع خصيصًا الأحداث المتعلقة بمحاولات تسجيل الدخول الناجحة والفاشلة لواجهات الإدارة في ملف سجلات التدقيق.
١-٣	أن يقتصر الوصول المادي إلى الخادم على الموظفين المصرح لهم فقط (الحد الأدنى من الصلاحيات لمختلف مديري النظام).
١-٤	تقييد وصول مديري النظام إلى واجهة إدارة مراقب الأجهزة الافتراضية.

١-٥	حماية جميع قنوات الاتصال الإدارية التي تستخدم شبكة إدارة مُخصصة أو شبكة الاتصالات الإدارية من إساءة الاستخدام، مع مراعاة المصادقة والتشفير باستخدام وحدات التشفير بما يتوافق مع المعايير الوطنية للتشفير.
١-٦	قطع اتصال الأجهزة المادية غير المستخدمة عن نظام المضيف.
١-٧	قطع اتصال وحدات التحكم غير المستخدمة في واجهة الشبكة عن جميع الشبكات.
١-٨	مزامنة نظام المضيف مع خوادم زمنية موثوقة تتمتع بالصلاحيات المناسبة.
١-٩	استخدام أجهزة داعمة لبيئة التشغيل المُقاسة حصرًا لإنشاء الثقة بين الأجهزة ومراقب الأجهزة الافتراضية.
١-١٠	أن تدعم الأجهزة بيئة التشغيل المُقاسة بقدرات قياس التشفير وأجهزة التخزين القائمة على المعيار.
١-١١	أن يستوفي عزل العمليات الدائرة في الأجهزة الافتراضية ما يلي من إرشادات: • يجب موازنة الأوامر أو الإرشادات ذات الصلاحيات من نظام تشغيل ضيف إلى معالج المضيف للحفاظ على مدير الآلات الافتراضية/مشغل الأجهزة الافتراضية كوحدة تحكم بالموارد الافتراضية. • يجب حماية سلامة وظيفة إدارة الذاكرة لمضيف مراقب الأجهزة الافتراضية من الهجمات السيبرانية مثل تجاوز سعة التخزين المؤقت وتنفيذ التعليمات البرمجية غير المصرح بها، وخاصةً في جداول الترجمة اللازمة لإدارة الوصول إلى الذاكرة بواسطة آلات افتراضية متعددة. • يجب أن تضمن خوارزميات تخصيص الذاكرة أن الأحمال على جميع الآلات الافتراضية قادرة على أداء وظائفها. • يجب أن تضمن خوارزميات تخصيص وحدة المعالجة المركزية أن الأحمال على جميع الآلات الافتراضية قادرة على أداء وظائفها.
١-١٢	إدارة ومراقبة جميع الأدوات الأمنية لأنظمة تشغيل الضيف بطريقة محددة مسبقًا وفقًا لهذا المعيار.
١-١٣	تطبيق الآليات التالية للوقاية من هجمات القناة الجانبية: • إلغاء تفعيل تعدد العمليات المتزامنة (SMT) • عدم استخدام إلغاء نسخ الذاكرة (إن أمكن) • استخدام معالجات مع ذاكرة تخزين موقتة حصرية (إن أمكن)، وتفعيل خاصية التوزيع العشوائي لمخطط مساحات العناوين.

اختر التصنيف

الإصدار <١,٠>

١-١٤	أن تتبع عملية ترحيل البيئة الافتراضية للمضيف بين البيئات المادية أو الافتراضية جميع متطلبات الأمان الواردة في هذا المعيار.
٢	أمن مراقب الأجهزة الافتراضية (Hypervisor Security)
الهدف	ضبط إعدادات استخدام مراقب الأجهزة الافتراضية في <اسم الجهة> بشكل مناسب وإدارتها بشكل آمن.
المخاطر المحتملة	مراقب الأجهزة الافتراضية هو الأساس لكل بنية تحتية افتراضية، وقد ينتج عن أي خطأ في ضبط إعداداته إلى سرقة المعلومات والكشف عنها والوصول غير المصرح به إليها.
الإجراءات المطلوبة	
١-٢	أن تتبع <اسم الجهة> أفضل الممارسات في إدارة نظام التشغيل المادي، مثل المزامنة الزمنية، وإدارة السجلات، والتحقق من الهويات، والوصول عن بعد، وغيرها.
٢-٢	الحصول على صور تثبيت مراقب الأجهزة الافتراضية يجب أن يكون من مصادر موثوقة فقط.
٣-٢	تركيب مراقب الأجهزة الافتراضية على خوادم معدنية (bare metal) لتجنب وجود ثغرات محتملة في نظام تشغيل المضيف.
٤-٢	تثبيت جميع التحديثات على مراقب الأجهزة الافتراضية خلال فترة زمنية محددة في <اسم الجهة> بعد إصدارها من قبل المورد.
٥-٢	أن يقوم مدراء النظام بمراقبة مراقب الأجهزة الافتراضية بعناية باستخدام أدوات أمنية متخصصة لأي مؤشرات على وجود اختراق.
٦-٢	أن يوفر مراقب الأجهزة الافتراضية واجهة افتراضية لبيئة التشغيل المقاسة في الأجهزة بناء على (MLE).
٧-٢	تنفيذ جميع عمليات تثبيت مراقب الأجهزة الافتراضية مركزيًا في المؤسسة باستخدام نظام إدارة البيئة الافتراضية المؤسسي (EVMS).
٨-٢	ضبط إعدادات المعيار الذهبي المؤسسية لمراقب الأجهزة الافتراضية لتستوعب مختلف أنواع أحمال العمل والتجمعات من خلال نظام إدارة البيئة الافتراضية للمؤسسة. يجب أن تغطي إعدادات المعيار الذهبي الجوانب التالية كحدٍ أدنى: • وحدة التحكم المركزية • الذاكرة • التخزين

اختر التصنيف

الإصدار <١,٠>

	• تحصين عرض نطاق الشبكة ونظام تشغيل المضيف (إذا استدعت الحاجة)
٢-٩	يجب عزل جميع أنظمة التشغيل للمضيف بشكل كامل (ماديًا ومنطقيًا) عن حدث مراقب الأجهزة الافتراضية.
٣	أمن نظام تشغيل الضيف (Guest OS Security)
الهدف	إدارة وتحديث نظام تشغيل الضيف بشكل آمن لضمان استقلاليته عن الأنظمة الأخرى باستخدام التغليف وطرق الأمان التقليدية بسبب وصوله المباشر إلى الشبكة.
المخاطر المحتملة	إذا تم اختراق نظام تشغيل الضيف على نظام افتراضي مستضاف، فمن المحتمل أن يتسبب نظام التشغيل الضيف في إلحاق الضرر بالأنظمة الأخرى على نفس مراقب البيئة الافتراضية، مما قد يؤدي إلى سرقة المعلومات والكشف عنها والوصول غير المصرح به إليها.
الإجراءات المطلوبة	
٣-١	أن تتبع <اسم الجهة> أفضل الممارسات في إدارة نظام التشغيل المادي، مثل مزامنة التوقيت، وإدارة السجلات، والتحقق من الهويات، والوصول عن بعد، وغيرها.
٣-٢	تثبيت جميع التحديثات على نظام تشغيل الضيف بشكل فوري. تحتوي جميع أنظمة التشغيل الحديثة على مزايا تقوم تلقائيًا بالتحقق من التحديثات وتثبتها.
٣-٣	إجراء نسخ احتياطي لمحركات الأقراص الافتراضية المستخدمة من قبل نظام التشغيل الضيف بشكل منتظم باستخدام نفس السياسة الخاصة بإعداد النسخ الاحتياطية المستخدمة لأجهزة الحاسوب غير الافتراضية في <اسم الجهة>.
٣-٤	على كل نظام تشغيل ضيف، يجب قطع الاتصال مع الأجهزة الافتراضية غير المستخدمة (تحديدًا محركات الأقراص الافتراضية ومحولات الشبكة الافتراضية).
٣-٥	استخدام حلول مصادقة منفصلة لكل نظام تشغيل ضيف ما لم يكن هناك سبب محدد لاشتراك نظامي تشغيل ضيفين في بيانات الاعتماد. ويجب الحصول على موافقة المصادقة لفترة زمنية محدودة فقط.
٣-٦	لا يجب ربط الأجهزة الافتراضية لنظام تشغيل الضيف إلا مع الأجهزة المادية المناسبة على نظام المضيف، مثل الروابط بين وحدات التحكم في واجهة الشبكة الافتراضية والمادية.
٣-٧	ألا يصل نظام تشغيل الضيف إلا إلى موارده الخاصة فقط ويجب ألا يصل إلى موارد أنظمة تشغيل الضيف الأخرى أو أي موارد غير مخصصة لاستخدام البيئة الافتراضية.

٨-٣	تقييد أداء نظام تشغيل الضيف لمنع حالات الكشف غير المصرح به عن المعلومات.
٤	أمن البنية التحتية الافتراضية (Virtualized Infrastructure Security)
الهدف	ضمان المواصفات المناسبة للبنية التحتية الافتراضية في المنطقة المؤمنة.
المخاطر المحتملة	قد يتسبب الخطأ في ضبط إعدادات البنية التحتية الافتراضية أو أي انتهاك لها في عواقب وخيمة يمكن أن تسفر عن سرقة المعلومات أو الإفصاح عنها أو الوصول غير المصرح بها إليها.
الإجراءات المطلوبة	
١-٤	أن يقتصر الوصول إلى الأجهزة الافتراضية على نظام تشغيل الضيف الذي سيستخدمها.
٢-٤	أن يقوم مدراء النظام بتطبيق ضابط الوصول إلى الأجهزة الافتراضية، خاصةً التخزين والشبكات، ومراقبته بصرامة باستخدام أدوات أمنية متخصصة.
٣-٤	استخدام مبدلات الشبكة الافتراضية التي تدعم الشبكة المحلية الافتراضية (VLAN) وقدرات جدار الحماية لتوفير إمكانية فصل وعزل حركة البيانات على الآلات الافتراضية.
٤-٤	تركيب أجهزة الأمن الإضافية (المادية أو الافتراضية) لفحص وضبط وتهيئة ومراقبة اتصالات الشبكة على الآلات الافتراضية في موقع مركزي.
٥-٤	استخدام أدوات إدارة إعدادات الآلات الافتراضية لمراقبة وإدارة إعدادات كل شبكة للآلات الافتراضية على مدار دورة حياتها.
٦-٤	لا يجب استخدام محاكاة الأجهزة المادية إلا عندما يكون التعقيد قابلًا للإدارة (على سبيل المثال، وحدة تحكم المضيف بالناقل التسلسلي للبيانات).
٧-٤	تعيين حدود الموارد لعرض نطاق الشبكة وعرض نطاق الإدخال والإخراج (مثل سرعات قراءة/كتابة الأقراص) لكل شبكة افتراضية لمنع هجمات حجب الخدمة.
٥	أمن البيئة الافتراضية لسطح المكتب (Desktop Virtualization Security)
الهدف	إدارة وتنظيم استخدام البيئة الافتراضية لسطح المكتب بصرامة باستخدام نهج الحد الأدنى من الصلاحيات.
المخاطر المحتملة	عند استخدامها، تعد بيئة سطح المكتب الافتراضية أساسية للعمليات اليومية واي خطأ في ضبط الإعدادات او خرق قد يتسبب بانتهاك سياسة الامن السيبراني لدى الجهة والكشف عن المعلومات.

اختر التصنيف

الإصدار <١,٠>

الإجراءات المطلوبة	
٥-١	تحديد السيناريوهات التي تتطلب تطبيق الإجراءات الأمنية من خلال حلول افتراضية مدارة وتلك التي لا تتطلب إدارة مركزية. على سبيل المثال، إذا تمت إتاحة بيئة سطح المكتب الافتراضية للموظفين الذين يعملون من المنزل، فلن تتطلب أجهزة الحاسوب الخاصة بهم ضوابط أمنية صارمة على عكس تلك التي توفر الوصول إلى قواعد البيانات الداخلية أو المواقع الإلكترونية.
٥-٢	أن تستخدم <اسم الجهة> حلول البيئة الافتراضية التي تتيح نشر نظام تشغيل الضيف على سطح المكتب المدار على أجهزة الحاسوب غير المدارة.
٥-٣	تثبيت جميع التحديثات على نظام تشغيل الضيف على أجهزة الحاسوب غير المدارة متى يقوم المورّد بإصدارها.
٥-٤	أن يكون مستخدمو أنظمة تشغيل الضيف المُدارة التي يستخدمها العديد من المستخدمين على دراية بأن أي تغييرات أجراها مستخدم من المستخدمين يجوز أن يتم نشرها مرة أخرى على الصورة الرئيسية، ثم تظهر على الصور التي يستخدمها المستخدمون الآخرون.
٦	معايير أخرى (Other Standards)
الهدف	ضبط إعدادات البيئة الافتراضية بشكل آمن واستخدامها بشكل مناسب عند الحاجة.
المخاطر المحتملة	إذا كانت <اسم الجهة> لا تلتزم بجميع المعايير والمتطلبات المعمول بها والإلزامية، فقد يؤدي ذلك إلى سرقة المعلومات والوصول غير المصرح به إليها والكشف عنها.
الإجراءات المطلوبة	
٦-١	تطبيق المعايير التالية فيما يتعلق بالبيئة الافتراضية: ١. نموذج معيار أمن الخوادم ٢. نموذج معيار أمن الشبكات ٣. نموذج معيار إدارة هويات الدخول والصلاحيات ٤. نموذج معيار إدارة النسخ الاحتياطية والاسترجاع ٥. نموذج معيار التشفير ٦. نموذج معيار الأمن المادي ٧. نموذج معيار الإعدادات والتحصين الآمن ٨. نموذج معيار إدارة ومراقبة سجل الأحداث ٩. نموذج معيار الحماية من البرمجيات الضارة

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> و<الإدارة المعنية بالأمن السيبراني>.

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

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة المعيار سنويًا 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

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>.