Trellix

ملخص الحل

ضوابط الأمن السيبراني بالهيئة الوطنية للأمن السيبراني (NCA) في المملكة العربية السعودية

الاستفادة من Trellix® لتحقيق مرونة الأمن السيبراني والتوافق مع الضوابط

تتوافق شركة Trellix، الرائدة في مجال الأمن السيبراني، مع رؤية المملكة العربية السعودية لتحقيق أمن سيبراني قوي على المستوى الوطني، وقد بدأ استخدام الحلول التي تقدمها شركة Trellix في المملكة العربية السعودية منذ عقدين ماضيين لحماية بعض المؤسسات الرئيسية في جميع القطاعات في المملكة فيما يتعلق بأمان نقاط النهاية وأمان الشبكات والبيانات، وذلك من خلال النظام الأساسي للأمان الشامل المدعوم بالذكاء الاصطناعي التوليدي، ولأنها شريك موثوق به، تدعم Trellix التحول الرقمي المتطور في المملكة من خلال ضمان حصول المؤسسات والجهات الحكومية على حلول متطورة.

تؤدي **الهيئة الوطنية للأمن السيبراني (NCA)** في المملكة العربية السعودية دورًا محوريًا في حماية البنية التحتية الحيوية للمملكة والشركات والمواطنين من التهديد المتزايد للهجمات الإلكترونية، وهذه الهيئة هي السلطة المركزية للأمن السيبراني في المملكة العربية السعودية، وتعمل على وضع أطر العمل والسياسات والمبادئ التوجيهية لتعزيز الوضع الأمني للكيانات العامة والخاصة. تعزز Trellix التزامها من خلال تمكين التوافق مع معايير الهيئة الوطنية للأمن السيبراني وضمان الصمود ضد التهديدات الإلكترونية المتطورة باستمرار.

تربط هذه الوثيقة مجموعة منتجات Trellix بجميع ضوابط التحكم الثلاثة التي وضعتها الهيئة الوطنية للأمن السيبراني، وهي ضوابط الأمن السيبراني الأساسية (ECC) وضوابط الأمن السيبراني للأنظمة المهمة (CSCC) وضوابط الأمن السيبراني للبيانات (DCC) لتكون المرجع للمؤسسات في المملكة العربية السعودية.

ما ضوابط ECC وCSCC وDCC التي وضعتها الهيئة الوطنية للأمن السيبراني بالسعودية؟

وضعت الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية ثلاثة أطر عمل لضوابط الأمن السيبراني لتعزيز البنية التحتية الرقمية في البلاد:

ضوابط الأمن السيبراني الأساسية (NCA ECC): إطار عمل أساسي مصمم لتعزيز أمن المؤسسات من خلال تنفيذ تدابير الأمن السيبراني الأساسية، مثل إدارة الأصول والتحكم في الوصول والاستجابة للحوادث.

ضوابط الأمن السيبراني للأنظمة المهمة (NCA CSCC): تهدف هذه الضوابط إلى حماية الأنظمة المهمة والضرورية لتقديم الخدمات الحيوية، وتركز على إدارة المخاطر وأمان الوصول وحماية البنية التحتية للمعلومات الحيوية.

ضوابط الأمن السيبراني للبيانات (NCA DCC): تركز هذه الضوابط على ضمان حماية البيانات الحساسة طوال دورة حياتها، بما في ذلك التصنيف والتشفير والتحكم في الوصول، بما يتماشى مع المتطلبات التنظيمية والقانونية.

ما المؤسسات والقطاعات التي تنطبق عليها ضوابط ECC وCSCC وDCC التي وضعتها الهيئة الوطنية للأمن السيبراني؟

تنطبق أطر عمل الهيئة الوطنية للأمن السيبراني على مجموعة واسعة من المنظمات في جميع أنحاء المملكة العربية السعودية، بما في ذلك:

- الجهات الحكومية: القطاعات التي تدير البيانات الحساسة والخدمات الحيوية
- مقدمو البنية التحتية الحيوية: قطاعات الطاقة والنقل والرعاية الصحية
- منظمات القطاع الخاص: الصناعات مثل الاتصالات والخدمات المصرفية والتصنيع، وخاصة تلك التي تتعامل مع البيانات الحساسة أو الخدمات الأساسية
- مقدمو الخدمات الرقمية: العروض الخاصة بخدمات الحوسبة السحابية والبرمجيات وتقنيات المعلومات

يعد تحقيق التوافق ضروريًا لضمان سلامة النظام البيئي الرقمي للمملكة وموثوقيته ومرونته.

لماذا نستخدم حلول Trellix لضوابط ECC وCSCC وDCC التي وضعتها الهيئة الوطنية للأمن السيبراني بالسعودية؟

توفر Trellix مجموعة واسعة من حلول وخدمات الأمن السيبراني التي تتوافق مع أطر عمل ECC وCSCC وDCC التي وضعتها الهيئة الوطنية للأمن السيبراني مع الالتزام بالمعايير الدولية مثل NIST Cybersecurity Framework وISO27001.

التغطية الشاملة: تعالج حلول وخدمات Trellix مجالات مهمة، بما في ذلك أمان نقاط النهاية وحماية الشبكات وأمان البيانات.

النهج المتكامل: توفر أدوات مثل Trellix ePolicy Orchestrator (ePO) إدارة مركزية، وهذا يضمن تحقيق سلسل للتوافق مع الضوابط.

التحليل الذكي للتهديدات المتقدمة: من خلال الاستفادة من إمكانات Trellix في الكشف عن التهديدات، يمكن للمؤسسات أن تتغلب دومًا على أي التهديدات الناشئة.

حلول Trellix المتوافقة مع ضوابط ECC وCSCC وDCC للهيئة الوطنية للأمن السيبراني

الفئة	المنتج	الوصف	ضوابط الهيئة الوطنية للأمن السيبراني
أمان نقاط النهاية	Trellix Endpoint Security	يوفر هذا المنتج حماية متعددة الطبقات في وكيل واحد للأجهزة عبر البيئات المحلية والسحابية وغير المتصلة، ويتم إدارتها من خلال وحدة تحكم واحدة.	ECC: 2-3-3 CSCC: 2-3-1-1 & 2-1-3-2
	Trellix Endpoint Detection and Response (EDR)	يوفر هذا المنتج إمكانات الكشف عن التهديدات والاستجابة الاستباقية لتحديد التهديدات واحتوائها بسرعة.	CSCC: 2-11-1-3
	Trellix Application and Change Control	يضمن هذا المنتج تشغيل التطبيقات المصرح بها فقط على الأجهزة، وهذا يقلل من خطر تشغيل البرامج الضارة.	CSCC: 2-3-1-1 & 2-1-3-2 & 8-1-3-2 & 1-1-3-2
	Trellix Mobile Security	يعمل هذا المنتج على تأمين الأجهزة المحمولة ضد التهديدات، وذلك يضمن حماية البيانات وتحقيق التوافق.	ECC: 2-6-3 DCC: 2-3-1-1 & 2-1-3-2 & 3-1-3-2

نبذة مختصرة عن الحلول

الفئة	المنتج	الوصف	ضوابط الهيئة الوطنية للأمن السيبراني
أمان نقاط النهاية	Trellix Device Control	تساعد إدارة الأجهزة الشاملة في التحكم في البيانات السرية التي يتم نسخها إلى أجهزة التخزين القابلة للإزالة وحظرها، بما في ذلك تقنية البلوتوث.	ECC: 2-3-3-2
	Trellix Policy Auditor	يعمل هذا المنتج على أتمتة وتبسيط عمليات تدقيق التوافق والتصحيح وتكوين الأمان عبر بيئات المؤسسة.	ECC: 3-3-3-2 CSCC: 1-1-2-1 & 1-1-2-2 & 1-4-1 & 6-1-3-2 & DCC: 1-1-2-2
	Trellix ePolicy Orchestrator (ePO)	يعمل هذا المنتج على أتمتة وتبسيط عمليات تدقيق التوافق والتصحيح وتكوين الأمان عبر بيئات المؤسسة.	CSCC: 1-1-1-2
	خدمة تقييم الاختراق	تعمل هذه الخدمة على إبراز التهديدات النشطة داخل بيئتك لتحديد البرامج الضارة والأوامر والتحكم عن بُعد من المعلومات التي تم جمعها من نقاط النهاية، وتتم مطابقة ذلك مقابل أداء نقاط النهاية الخاصة بك مع نظام المعالجة ومحتوى التحليل الذكي الإلكتروني المخصص من Trellix.	ECC: 3-3-3-2 & 3-3-2 CSCC: 2-1-3- 2 & 2-1-3-2 & 1-2-3-1 & 8-1-3-2 & 3-1-11-2 & 1-1-2-1 & 6-1-3-2 & 1-4-1 & 1-1-2-2 & DCC: 1-1-2-2
أمان الشبكات	Trellix Network Security	يعمل هذا المنتج على اكتشاف التهديدات المتقدمة والحركة الجانبية وسلوك الشبكة المشتبه به في الوقت الفعلي ويمنع كل هذه التهديدات.	ECC: 8-3-5-2 CSCC: 5-1-4-2
	Trellix Network Forensics	يحدد هذا المنتج مجموعة واسعة من الحوادث الأمنية بشكل أسرع ويعمل على حلها باستخدام تسجيل بيانات الشبكة واسترجاعها دون فقد للبيانات باستخدام التحليل المركزي والتمثيل المرئي.	
	Trellix Intrusion Prevention System	يفحص هذا المنتج كل حركات المرور على الشبكة لمنع الهجمات الجديدة وغير المعروفة باستخدام تقنيات الكشف والمحاكاة المتقدمة بدرجة عالية من الدقة والأداء.	ECC: 9-3-5-2 & 6-3-5-2
	خدمة الاستجابة للحوادث والكشف عن الأدلة	تساعد هذه الخدمة في التعامل مع حوادث أمان الشبكات و/أو أجهزة الكمبيوتر، مثل عمليات اختراق أجهزة الكمبيوتر وانتشار الفيروسات على نطاق واسع، وغيرها من الأحداث غير المقبولة التي تهدد فعالية المؤسسة وسمعتها وأصولها الملموسة.	ECC: 9-3-5-2 & 8-3-5-2 & 6-3-5-2 CSCC: 5-1-4-2
أمان البريد الإلكتروني	Trellix Email Security	يحمي هذا المنتج البريد الإلكتروني من التصيد الاحتيالي والبرامج الضارة، وغيرها من التهديدات.	ECC: 4-3-4-2 & 1-3-4-2
	Trellix IVX for Enterprise Applications	يوفر هذا المنتج حماية شاملة عبر قنوات الاتصال المختلفة بالمؤسسة.	ECC: 2.4.3.5 & 4-3-4-2 & 1-3-4-2
	خدمة تقييم مرونة برامج الفدية الضارة (RRA)	تستفيد هذه الخدمة من تحليل برامج الفدية الضارة لتقييم الضوابط الموجودة لتحديد الثغرات والقدرات اللازمة للتعامل مع حوادث برامج الفدية الضارة.	ECC: 2.4.3.5 & 4-3-4-2 & 1-3-4-2
أمان البيانات	Trellix Data Loss Prevention Endpoint Complete	يمنع هذا المنتج عمليات نقل البيانات غير المصرح بها وتسريبها عبر قنوات مختلفة.	CSCC: &1-6-2 DCC: 2-1-4-2 & 1-1-4-2
	Trellix Data Loss Prevention Network Prevent	يعمل هذا المنتج على منع المستخدمين من مشاركة المعلومات غير المصرح بمشاركتها عبر الشبكات.	ECC: 2.5.3.3

Trellix

نبذة مختصرة عن الحلول

الفئة	المنتج	الوصف	ضوابط الهيئة الوطنية للأمن السيبراني
أمان البيانات	Trellix Data Encryption	يعمل هذا المنتج على تشفير البيانات الحساسة في حالة السكون وفي حالة النقل.	ECC: 2-8-3 CSCC: 2-7-1 DCC: 2-5-1
	Trellix Database Security	يراقب هذا المنتج قواعد البيانات ويعمل على حمايتها من التهديدات والوصول غير المصرح به.	ECC: 2-10-3 CSCC: 2-2-8-1 & 2-9-1-1
	خدمة تقييم أمان البيانات وتطوير برنامج حماية البيانات	تبدأ هذه الخدمة باستخدام ورشة عمل حماية البيانات للتوصل إلى تعريف عالمي متعدد الوظائف للبيانات المهمة المعروفة لديك وفهم المتطلبات التنظيمية لأمن البيانات وحمايتها، بعد ذلك يتم تصميم برنامج حوكمة يتضمن الإدارة الشاملة لسرية البيانات وسلامتها وتوفرها مع مستويات تصنيف محددة وسياسات ومعايير وإجراءات السليمة تشكل الأساس لإستراتيجية منع فقد البيانات الفعالة.	CSCC: 2-6-1 & 2-7-1 & 2-2-8-1 & 2-9-1-1 DCC: 2-4-1-1 & 2-4-2 & 2-5-2 ECC: 2.5.3.3 & 2-8-3 & 2-10-3
حلول إدارة المعلومات والأحداث الأمنية في مركز العمليات الأمنية	Trellix Enterprise Security Manager	يعمل هذا المنتج على إجراء عمليات إدارة فعالة ومبسطة للمعلومات الأمنية والأحداث وفقًا لأساس شامل.	ECC: 2-12 CSCC: 2-11
	خدمة تكوين الفرق الحمراء	تجمع هذه الخدمة عناصر الاحتيال الاجتماعي واختبار الاختراق للحصول على نظرة ثاقبة عن كيفية عمل البيئة في سيناريو الهجوم الفعلي. يمكن تصميم سيناريوهات الهجوم لمحاكاة أنواع معينة من الجهات الفاعلة في التهديدات (الهواة والمجموعات المنظمة والمجرمون الإلكترونيون) باستخدام تقنيات تقليدية وغير تقليدية لاختبار القدرة على الصمود ضد الاختراقات وتسريب البيانات والاحتيال والهجوم الداخلي والتجسس المؤسسي والاختراق الفعلي، وما إلى ذلك.	ECC: 2-12 CSCC: 2-11
التحليل الذكي للتهديدات	Trellix Threat Intelligence Exchange	يعمل هذا المنتج على تحويل بنية الأمان التحتية إلى نظام تعاوني.	ECC: 2.13.3.5
	خدمة تقييم نضج التحليل الذكي للتهديدات وتطوير الممارسات	تساعد هذه الخدمة في تحديد أصحاب المصلحة الرئيسيين والجهات الفاعلة، ثم إجراء مقابلات مع هذه الجهات المحددة لفهم النضج الحالي لبرنامج CTI الخاص بك، وتأثيرات CTI العمودية على الأعمال والمبادئ الأساسية ذات الصلة. وبعد ذلك، يمكن تحديد ممارسات التحليل الذكي للتهديدات لتعزيز وجهة نظرك عن سياق التهديدات، وهذا يساعد في تحقيق الحماية والكشف والاستجابة الفعالة.	ECC: 2.13.3.5
حماية الملفات	Trellix File Protect (FX)	يكتشف هذا المنتج البرامج الضارة الموجودة في مشاركات الملفات على الشبكة ومستودعات المحتوى ويعمل على إزالتها، وهذا يمنع الانتشار الجانبي للتهديدات داخل المؤسسة.	ECC: 2-3-3-1 CSCC: 2-3-1-2
	خدمة مراجعة تكوين الضوابط في الأمن السيبراني	تراجع هذه الخدمة إعدادات تكوين أمان التحكم ويساعد في التحقق منها يدويًا في كل الأنظمة مع التأكد من أنها تتوافق مع أفضل ممارسات الصناعة والمبادئ التوجيهية والتوصيات الأمنية.	ECC: 2-3-3-1 CSCC: 2-3-1-2

ضوابط الأمن السيبراني بالهيئة الوطنية للأمن السيبراني (NCA) في المملكة العربية السعودية

نبذة مختصرة عن الحلول

الفئة	المنتج	الوصف	ضوابط الهيئة الوطنية للأمن السيبراني
أمان عالي المستوى	الوكيل	يعمل هذا على مراقبة الوصول إلى المعلومات الحساسة والتحكم فيه.	ECC: 2-5-3-3
	خدمة تقييم أمان تطبيقات الويب وتطبيقات الهاتف المحمول وواجهة برمجة التطبيقات	تعمل هذه الخدمة على استخدم منهجية شاملة أثناء تقييمات أمان تطبيقات الويب وتطبيقات الهاتف المحمول وواجهة برمجة التطبيقات التي تشمل سيناريوهات الاختبار وتتراوح من اختبار "الصندوق الأسود" دون معرفة إلى اختبار "الصندوق الأبيض" ذي الوصول الكامل. وهذا يشمل النهج التكراري للعديد من نماذج التقييم، مثل الفحص السريع والتقييم الكامل وقائمة أعلى عشرة أخطار أمنية وفقًا لمؤسسة OWASP ونموذج الصندوق الرمادي الذي يلبي احتياجات عملك، إلى جانب عملية Trellix المخصصة التي تتكون من أكثر من 100 فحص.	ECC: 2-5-3-3
	خدمة مراجعة تكوين السحابة	تبدأ هذه الخدمة بإجراء عمليات فحص على مستوى الشبكة للتأكد من أن البنية الأساسية تم تكوينها بشكل مناسب ولا يوجد بها أي مشكلات متعلقة بالأمان، وتستهدف هذه العمليات نظام تشغيل الخادم وبرامج خادم الويب. بعد ذلك، يتم إجراء عمليات فحص يدوية للتحقق من نتائج الفحص ومحاولة تحديد المشكلات الإضافية، ثم الانتقال إلى مراجعة التكوين اليدوي لجميع الخدمات السحابية الموجودة في البنية التحتية الخاصة بك.	ECC: 2-5-3-3

تشكل أطر العمل الثلاثة إستراتيجية شاملة لتعزيز النظام البيئي للأمن السيبراني في المملكة العربية السعودية وتمكين الكيانات من التوافق مع أهداف التحول الرقمي لرؤية المملكة 2030.

من خلال الحلول المصممة خصيصًا والشراكات الإستراتيجية، تلتزم Trellix بتأمين الاقتصاد الرقمي في المملكة العربية السعودية وتعزيز الفضاء الإلكتروني الأكثر أمانًا والمساهمة في تحقيق رؤية المملكة الطموحة 2030.

لمزيد من المعلومات، يرجى الرجوع إلى www.trellix.com.