

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

Leverage Trellix® لمرونة الأمن السيبراني والتوافق

تتسجم شركة Trellix، الرائدة في مجال الأمن السيبراني، انسجامًا عميقًا مع رؤية المملكة العربية السعودية لتحقيق الأمن السيبراني الوطني القوي. ولأكثر من عشرين عامًا، عملت Trellix في المملكة العربية السعودية ووفّرت الحماية للمؤسسات الأساسية عبر كل القطاعات.

من خلال **مجموعة منتجاتها لخدمات الأمان الشاملة المدعومة بالذكاء الاصطناعي**، توفر Trellix خدمات الحماية الفعالة عبر البيانات ونقاط النهاية والشبكات. وباعتبارها شريكًا موثوقًا به، تدعم Trellix التحول الرقمي المتسارع في المملكة من خلال ضمان حصول المؤسسات والجهات الحكومية على حلول متطورة.

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

صُمم هذا المستند للمؤسسات العاملة في المملكة العربية السعودية، وهو يقارن مجموعة منتجات Trellix بثلاثة أطر عمل للهيئة الوطنية للأمن السيبراني: ECC وCSCC وDCC.

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

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

- **ضوابط الأمن السيبراني الأساسية (ECC) التي وضعتها الهيئة الوطنية للأمن السيبراني:** 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 (CSCC) التي وضعتها الهيئة الوطنية للأمن السيبراني:** تهدف إلى حماية الأنظمة المهمة والضرورية لتقديم الخدمات الحيوية. تركز هذه الضوابط على إدارة المخاطر، وأمان الوصول، وحماية البنية التحتية للمعلومات الحيوية.
- **ضوابط الأمن السيبراني للبيانات (DCC) التي وضعتها الهيئة الوطنية للأمن السيبراني:** تركز على ضمان حماية البيانات الحساسة طوال دورة حياتها، بما في ذلك التصنيف والتشفير والتحكم في الوصول، بما يتماشى مع المتطلبات التنظيمية والقانونية.

من يتأثر بضوابط ECC وCSCC وDCC التي وضعتها الهيئة الوطنية للأمن السيبراني؟

تتطبق أطر عمل الهيئة الوطنية للأمن السيبراني على مجموعة واسعة من المؤسسات 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.
 - **مؤسسات القطاع الخاص:** الصناعات مثل الاتصالات، والخدمات المصرفية، والتصنيع، وخاصة تلك التي تتعامل مع البيانات الحساسة أو الخدمات الأساسية.
 - **مزودو الخدمات الرقمية:** العروض الخاصة بخدمات الحوسبة السحابية والبرمجيات وتكنولوجيا المعلومات.
- يعد 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 إطار عمل الأمن السيبراني NIST وISO 27001.

- **التغطية الشاملة:** تعالج حلول وخدمات Trellix مجالات مهمة، بما في ذلك أمان نقاط النهاية، وحماية الشبكة، وأمان البيانات.
- **النهج المتكامل:** توفر أدوات مثل Trellix ePolicy Orchestrator (ePO) إدارة مركزية، مما يُبسط جهود الامتثال.
- **استخبارات التهديدات السيبرانية المتقدمة:** من خلال الاستفادة من رؤية Trellix وقدرات الكشف عن التهديدات، يمكن للمؤسسات أن تظل متقدمة على التهديدات الناشئة.

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

الغنة	المنتج	الوصف	ضوابط الهيئة الوطنية للأمن السيبراني
أمان نقاط النهاية	Trellix Endpoint Security	يوفر حماية متعددة الطبقات في وكيل واحد للأجهزة عبر البيانات المحلية والسحابية وغير المتصلة، ويتم إدارتها من خلال وحدة تحكم واحدة.	ECC: 3-3-2 CSCC: 2-1-3-2 & 1-1-3-2
	Trellix Endpoint Detection and Response (EDR)	يوفر إمكانيات الكشف عن التهديدات والاستجابة الاستباقية لتحديد التهديدات واحتوائها بسرعة.	CSCC: 3-1-11-2
	Trellix Application and Change Control	يضمن تشغيل التطبيقات المصرح بها فقط على الأجهزة، مما يقلل من خطر تنفيذ البرامج الضارة.	CSCC: 1-1-3-2 & 8-1-3-2 & 1-2-3-1
	Trellix Mobile Security	يعمل على تأمين الأجهزة المحمولة ضد التهديدات، مما يضمن حماية البيانات والتوافق.	ECC: 3-6-2 DCC: 3-1-3-2 & 2-1-3-2 & 1-1-3-2
	Trellix Device Control	تساعد إدارة الأجهزة الشاملة في التحكم في البيانات السرية التي يتم نسخها إلى أجهزة التخزين القابلة للإزالة وحظرها، بما في ذلك عبر تقنية البلوتوث.	ECC: 2-3-3-2
	Trellix Policy Auditor	يعمل على أتمتة وتبسيط عمليات تدقيق التوافق والتصحيح وتكوين الأمان عبر بيئات المؤسسة.	ECC: 3-3-3-2 CSCC: 6-1-3-2 & 1-4-1 & 1-1-2-2 & 1-1-2-1 DCC: 1-1-2-2
	Trellix ePolicy Orchestrator (ePO)	يعمل على أتمتة وتبسيط عمليات تدقيق التوافق والتصحيح وتكوين الأمان عبر بيئات المؤسسة.	CSCC: 1-1-1-2

نبذة مختصرة عن الحلول

الفئة	المنتج	الوصف	ضوابط الهيئة الوطنية للأمن السيبراني
أمان نقاط النهاية	خدمة مراجعة تكوين ضوابط الأمن السيبراني	تعمل على مراجعة إعدادات تكوين الأمان والتحقق منها يدوياً على كل نظام والتأكد من أنها تتوافق مع أفضل ممارسات الصناعة والمبادئ التوجيهية والتوصيات الأمنية.	ECC: 3-3-3-2 CSCC: 6-1-3-2 & 1-4-1 & 1-1-2-2 & 1-1-2-1 DCC: 1-1-2-2
	خدمة تقييم الكشف عن الاختراقات	يرصد التهديدات النشطة داخل بيئتك ويُحدِّد البرامج الضارة والأوامر والتحكم عن بُعد من المعلومات التي تم جمعها من نقاط النهاية. ويُقارن ذلك بملوك نقاط النهاية الخاصة بك باستخدام نظام المعالجة ومحتوى التحليل الذكي السيبراني المخصص من Trellix.	ECC: 3-3-3-2 & 3-3-2 CSCC: 1-1-2-2 & 2-1-3-2 & 1-2-3-1 & 8-1-3-2 & 3-1-11-2 & 1-1-2-2 & 1-1-2-1 1-4-1 & 6-1-3-2 DCC: 1-1-2-2
	Trellix Network Security	يعمل على اكتشاف ومنع التهديدات المتقدمة، والحركة الجانبية، وسلوك الشبكة المشتببه به في الوقت الحقيقي.	ECC: 8-3-5-2 CSCC: 5-1-4-2
أمان الشبكة	Trellix Network Forensics	يعمل على تحديد وحل مجموعة واسعة من الحوادث الأمنية بشكل أسرع باستخدام تسجيل بيانات الشبكة واسترجاعها دون فقدان البيانات باستخدام التحليل المركزي والتصورات.	
	Trellix Intrusion Prevention System	يعمل على فحص كافة حركة 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 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 & 6-3-5-2 & 8-3-5-2 CSCC: 5-1-4-2
أمان البريد الإلكتروني	Trellix Email Security	يعمل على حماية اتصالات البريد الإلكتروني من التصيد الاحتيالي، والبرامج الضارة، وغيرها من التهديدات.	ECC: 4-3-4-2 & 1-3-4-2
	Trellix IX for Enterprise Applications	يوفر حماية شاملة عبر قنوات الاتصال المختلفة بالمؤسسة.	ECC: 2.4.3.5 & 4-3-4-2 & 1-3-4-2
	خدمة تقييم مرونة برامج الغدية الضارة (RRA)	تستفيد من تحليل برامج الغدية الضارة لتقييم الضوابط الموجودة لتحديد الثغرات والقدرات اللازمة للتعامل مع حوادث برامج الغدية الضارة.	ECC: 2.4.3.5 & 4-3-4-2 & 1-3-4-2
أمان البيانات	Trellix Data Loss Prevention Endpoint Complete	يمنع 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	يمنع المستخدمين من مشاركة المعلومات غير المصرح بها عبر الشبكات.	ECC: 2.5.3.3
	Trellix Data Encryption	يضمن تشفير البيانات الحساسة أثناء السكون وأثناء النقل.	ECC: 3-8-2
			CSCC: 1-7-2 DCC: 1-5-2

نبذة مختصرة عن الحلول

الفئة	المنتج	الوصف	ضوابط الهيئة الوطنية للأمن السيبراني
أمان البيانات	Trellix Database Security	يعمل على مراقبة قواعد البيانات وحمايتها من التهديدات والوصول غير المصرح به.	ECC: 3-10-2 CSCC: 1-1-9-2 & 8-1-2-2
		خدمة تقييم أمان البيانات وتطوير برنامج حماية البيانات	CSCC: 1-1-9-2 & 8-1-2-2 & 1-7-2 & 1-6-2 DCC: 1-5-2 & 2-1-4-2 & 1-1-4-2 ECC: 3-10-2 & 3-8-2 & 2.5.3.3
		أبدأ بورشة عمل حماية البيانات للتوصل إلى تعريف عام متعدد الوظائف لبياناتك المهمة المعروفة، وفهم المتطلبات التنظيمية لحماية البيانات وأمانها. ثم يُبنى برنامج حوكمة يتضمن الإدارة الشاملة لسرية البيانات وسلامتها وتوافرها مع مستويات تصنيف محددة وسياسات ومعايير وإجراءات سليمة والتي تشكل الأساس لاستراتيجية فعالة لمنع فقدان البيانات.	
حلول إدارة معلومات وأحداث الأمان في مركز العمليات الأمنية	Trellix Enterprise Security Manager	يعمل على إجراء إدارة فعالة ومبسطة لمعلومات وأحداث الأمان من أساس شامل.	ECC: 12-2 CSCC: 11-2
		خدمة تقييم الأمان	ECC: 12-2 CSCC: 11-2
		تقدم تقييمات مستقلة تكشف عن مدى تعرض المؤسسة الحقيقي لمخاطر الأمن السيبراني. ويحدد اختبار الاختراق الخارجي نقاط الضعف في الأنظمة المتصلة بالإنترنت التي قد تُمكن من الوصول غير المصرح به أو اختراق البيانات. ويقم اختبار الاختراق الداخلي المخاطر من داخل الشبكة، بما في ذلك الحركة الجانبية وزيادة الامتيازات. ويتم تقديم النتائج بأسلوب واضح، ويركز على احتياجات العمل، مع توصيات مُرتبة حسب الأولوية لتعزيز المرونة وتوجيه الاستثمار الاستراتيجي.	
خدمة تكوين الفرق الحمراء		تجمع هذه الخدمة عناصر من الهندسة الاجتماعية 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 التهديد (المتحمسون والمجموعات المنظمة ومجرمو الإنترنت) باستخدام تقنيات تقليدية وغير تقليدية لاختبار مرونتك ضد الاختراقات، تسريب البيانات، الاحتيال، الهجوم الداخلي، التجسس المؤسسي والاختراق الفعلي وما إلى ذلك.	ECC: 12-2 CSCC: 11-2
التحليل الذكي للتهديدات	Trellix Threat Intelligence Exchange	يعمل على تحويل البنية التحتية الأمنية إلى نظام تعاوني.	ECC: 2.13.3.5
		خدمة تقييم نضج التحليل الذكي للتهديدات وتطوير الممارسات	ECC: 2.13.3.5
		حدد أصحاب المصلحة الرئيسيين والجهات الفاعلة، ثم قم بإجراء مقابلات مع أصحاب المصلحة والجهات الفاعلة المحددة لفهم التطور الحالي لبرنامج التحليل الذكي للتهديدات السيبرانية الخاص بك، وتأثيرات التحليل الذكي للتهديدات السيبرانية المباشرة على الأعمال، والمبادئ الأساسية ذات الصلة. وبعد ذلك، قم بوضع ممارسات التحليل الذكي للتهديدات الخاصة بك لتعزيز وجهة نظرك حول مشهد التهديدات، مما يتيح لك الحماية والكشف والاستجابة الفعالة.	
حماية الملفات	Trellix File Protect (FX)	يعمل على اكتشاف وإزالة البرامج الضارة الموجودة في مشاركات الملفات على الشبكة ومستودعات المحتوى، مما يمنع الانتشار الجانبي للتهديدات داخل المؤسسة.	ECC: 1-3-3-2 CSCC: 2-1-3-2
		خدمة مراجعة تكوين ضوابط الأمن السيبراني	ECC: 1-3-3-2 CSCC: 2-1-3-2
		تعمل على مراجعة إعدادات تكوين الأمان والتحقق منها يدويًا على كل نظام والتأكد من أنها تتوافق مع أفضل ممارسات الصناعة والمبادئ التوجيهية والتوصيات الأمنية.	

نبذة مختصرة عن الحلول

الفئة	المنتج	الوصف	ضوابط الهيئة الوطنية للأمن السيبراني
	الوكيل	يعمل على المراقبة والتحكم في الوصول إلى المعلومات الحساسة.	ECC: 3-3-5-2
	خدمة تطوير تقييم بنية الثقة الصفرية (ZTA) والاستراتيجية وخارطة الطريق	تستبدل بنية الثقة الصفرية (ZTA) النموذج المحيطية القديمة بالتحقق المستمر لتعزيز مرونة المؤسسة. تبدأ المشاركة بتقييم الوضع الحالي، يليه استراتيجية بنية الثقة الصفرية (ZTA) المتوافقة مع الأعمال، ووضع خارطة طريق للتنفيذ المرحلي. يعتمد هذا النهج على ثلاثة مبادئ: التحقق الواضح، وتقليل امتيازات الوصول، وافترض حدوث اختراق من خلال التجزئة والحماية القوية للبيانات.	ECC: 3-3-5-2
Skyhigh Security	خدمة تقييم أمان تطبيقات الويب وتطبيقات الهاتف المحمول وواجهة برمجة التطبيقات	تعمل هذه الخدمة على استخدام منهجية شاملة أثناء تقييمات أمان تطبيقات الويب وتطبيقات الهاتف المحمول وواجهة برمجة التطبيقات، والتي 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 وفقاً لمؤسسة OWASP ونموذج الصندوق الرمادي الذي يلي احتياجات عمك، إلى جانب عملية Trellix الخاصة والتي تتضمن أكثر من 100 فحص.	ECC: 3-3-5-2
	خدمة مراجعة تكوين السحابة	أبدأ بإجراء عمليات فحص على مستوى الشبكة للتأكد من أن البنية الأساسية تم تكوينها بشكل مناسب وأنها خالية من مشكلات الأمان لخدمة مراجعة تكوين السحابة. تستهدف عمليات الفحص هذه نظام تشغيل الخادم وبرامج خادم الويب. بعد ذلك، تابع من خلال إجراء عمليات فحص يدوية للتحقق من نتائج الفحص ومحاولة تحديد المشكلات الإضافية. بعد ذلك، انتقل إلى المراجعة اليدوية للتكوين لجميع الخدمات السحابية الموجودة في البنية التحتية لديك.	ECC: 3-3-5-2

تشكل أطر العمل الثلاثة استراتيجية 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 خصيصاً والشراكات الاستراتيجية، تلتزم Trellix بتأمين الاقتصاد الرقمي في المملكة العربية السعودية، وتعزيز الفضاء الإلكتروني الأكثر أماناً، والمساهمة في الرؤية الطموحة للمملكة 2030.

لمعرفة المزيد، الرجاء زيارة www.trellix.com.