نشرة تعريفية عن خدمات الأمن السيبراني المقدمة من سمارت أوربيت

سمارت أوربيت لخدمات وحلول الأمن السيبراني

SOITC
شركة سمارت اوربيت لتقنية المعلومات
Smart Orbit Information Technology Company

رؤية VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

سمارت أوربيت

لـخدمـات الأمـن السـيبرانـي

تأسست سمارت أوربيت لتوظيف الحلول المتقدمة وتقديم أفضل الخدمات الاستشارية في مجال الأمن السيبراني. من خلال فريق من خبراء الأمن السيبراني البارزين الذين سبق لهم العمل في مختلف مجالات الأمن السيبراني وحصلوا على شهادات متقدمة في الأمن السيبراني والعديد من الشهادات، كما سبق لهم العمل باستخدام العديد من المنتجات الأمنية في مختلف مراحل منهجية الدفاع في العمق، وتعاملوا مع حوادث أمن سيبراني نتجت عن تهديدات خبيثة متطورة.

SMART ORBIT

رؤيـــة VISION 2030

المملكة العربية السعودية

KINGDOM OF SAUDI ARABIA

SMART ORBIT

VISION رؤيـــة 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

رؤية سمارت أوربيت

أن نكون موفر خدمات الأمن السيبراني المفضل في المملكة العربية السعودية.

رسالة سمارت أوربيت

نشر التوعية، وتوظيف الحلول المتقدمة، وتقديم أفضل الخدمات الاستشارية في مجال الأمن السيبراني.

قيم سمارت أوربيت

الريادة في الابتكار

نلتزم في سمارت أوربيت بتقديم حلول مبتكرة للتغلب على التحديات التي تواجه عملاءنا؛ فنحن نعتبر هذه التحديات الجديدة والمعقدة فرصًا لابتكار واستكشاف حلول جديدة.

الإخلاص لعملائنا

نلتزم في سمارت أوربيت بتقديم خدمات أمن سيبراني تلبي احتياجات عملائنا وتمهد الطريق لنجاح أعمالهم لأننا نؤمن أن التحديات التي تواجههم تواجهنا والتغلب عليها نجاح لهم ولنا.

SMART ORBIT

رؤيـــة VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

قيم سمارت أوربيت

تنمية مهارات الموظفين

تنمو سمارت أوربيت بنمو موظفيها، ولذلك نلتزم بتزويد موظفينا بأحدث المهارات والمعارف في مجال الأمن السيبراني لنحافظ على مكانتنا المتقدمة في هذا المجال الذي يتطور باستمرار.

تمرير المعارف

نحرص سمارت أوربيت على تمرير مهارات فريقنا ومعرفته إلى عملائنا، كما نلتزم برد الجميل للمجتمع من خلال تقديم خدمات تزود العامة بالمهارات الأساسية للحفاظ على الأمن السيبراني.

SMART ORBIT

رؤية VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

رؤية VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

خدماتنا السيبرانية

خـدمـات تـقييـم الأمن السيبراني

تقييم أمن الاستضافة السحابية

هل تحتفظ بكامل البنية التحتية الرقمية الخاصة بمؤسستك أو ببعضٍ منها في الاستضافة السحابية؟ هل تعلم ما إن كنت تتبع أفضل معايير الأمن المتعلقة بالاستضافة السحابية؟ هل عليك أن تلتزم بمعايير أو لوائح أمنية معينة تتعلق باستضافة البيانات في السحابة؟

من خلال خدمة تقييم أمن الاستضافة السحابية التي تقدمها سمارت أوربيت، سنستعرض حالة أمن البنية التحتية للسحابة الخاصة بك سواء كانت مستضافة محليًا أو دوليًا، وستتأكد من أنك تمارس أفضل ممارسات الأمن السيبراني لاستضافة البنية التحتية في السحابة. وبنهاية هذه الخدمة، سنزودك بتقريرٍ مفصلٍ بالحالة الأمنية الخاصة ببنيتك التحتية المستضافة في السحابة، وسيحتوي التقرير على توصيات تهدف لتحسين حالة الأمن السيبراني الخاص بالبنية التحتية للسحابة.

رؤيـــة VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

خـدمـات تـقييـم الأمن السيبراني

تقييم أمن الشبكات

يبحث المهاجمون باستمرار عن طريق يعبرون من خلاله لأصول مؤسستك المعلوماتية، وغالبًا ما يتضمن هذا الطريق العبور خلال شبكتك. تتكون الشبكات من عدد هائل من الأجهزة والخوادم التي تلبي احتياجات عملك ومتطلباته، ولذلك من الضروري جدًا ضمان تطبيق ضوابط الأمن السيبراني الأساسية لحماية شبكتك.

من خلال خدمة تقييم أمن الشبكات التي تقدمها سمارت أوربيت سنقيم دفاع مؤسستك ضد التهديدات التي تستهدف شبكتها، إذ صممنا منهجيتنا في تقييم أمن الشبكات للحماية ضد التهديدات المستجدة بناءً على منهجية الدفاع في العمق، وسنساعدك للوصول إلى أعلى درجات حماية شبكتك من خلال مراجعة البيانات وجمعها من الموجهات (Routers)، أو المبدلات (Switches)، أو جدران الحماية (Firewalls)، أو الخوادم الوسيطة (Proxy)، أو نظام كشف التسلل (IDS)، أو نظام منع التسلل (IPS)، أو أي أجهزة أخرى مرتبطة بالشبكة، ومن ثم سنقارن جميع البيانات بالممارسات الأمنية الرائدة وسنوظف خبرات فريقنا لتفسير النتائج والتعرف على الضوابط الأمنية التي تفتقدها مؤسستك. وعند نهاية التقييم، سنقدم لك أهم النصائح التي من شأنها أن تحسن من الحالة الأمنية لشبكتك.

رؤيـــة VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

خـدمـات تـقييـم الأمن السيبراني

تقييم أمن الأجهزة

أجهزة المستخدمين هي الغاية النهائية لأي هجمات سيبرانية؛ إذ إن وجود جهاز واحد متضرر في مؤسستك قد يؤدي إلى آثار خطيرة متتالية تعيق عملك. تمدك خدمة تقييم أمن الأجهزة التي تقدمها سمارت أوربيت بتصور شامل يوضح لك الضوابط والإمكانيات المتعلقة بحماية أجهزة مؤسستك، كما تقدم لك هذه الخدمة توصيات أمنية مفصّلة لتضمن أن أجهزة مؤسستك محمية بالطريقة المناسبة. علاوة على ذلك، سنتعرف من خلال الخدمة على المخاطر التي قد تحدث لأجهزة مؤسستك، ومن ثم سنضع خطة عمل لتخفيف ضرر هذه الأخطار حسب ما تمليه الممارسات الأمنية الرائدة.

رؤيـــة VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

خـدمـات تـقييـم الأمن السيبراني

تقييم مدى الالتزام بمعايير الأمن السيبراني

هل تتعامل مع بيانات الدفع الخاصة بزبائنك أو تخزنها؟ هل تتعامل مع بينات طبيّة حساسة خاصة بمرضاك؟ هل تتعامل مع مستندات حكومية سرية وحساسة من الواجب الحفاظ عليها في مكان آمن؟ أو هل تحتاج إلى تحقيق الالتزام بمعايير أمن معلومات دولية أو عالمية؟ أم هل تحتاج إلى الامتثال بمعايير NCA's ECC-1, SAMA, PCI DSS, NIST, ISO/IEC 27002, GDPR, HIPAA أو أي معايير أو إرشادات أمنية ولا تعلم من أين تبدأ أو من تستشير؟

من خلال خدمة تقييم مدى الالتزام بمعايير الأمن التي تقدمها سمارت أوربيت، سنقيم البنية التحتية الرقمية الخاصة بمؤسستك، وسنحدد الفجوات التي تفصل بينك وبين تلك المعايير والمجهودات المطلوبة لسد هذه الفجوات، وسنكون معك لنرشدك طوال رحلتك في سبيل تحقيق الامتثال بالمعايير التي تريدها.

رؤيـــة VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

خـدمـات تـقييـم الأمن السيبراني

تقييم أمن استضافة البريد الإلكتروني

هل تعلم ما إن كانت إعداداتك الأمنية مناسبة لاستضافة البريد الإلكتروني سواء كانت الاستضافة في مركز بياناتك أو في السحابة؟ هل تحتاج إلى الالتزام بإرشادات أمنية معينة تتعلق بالبريد الإلكتروني؟ هل تعلم أن 90% من الانتهاكات الأمنية تبدأ من رسائل البريد الإلكتروني؟
من خلال خدمة تقييم أمن البريد الإلكتروني التي تقدمها سمارت أوربيت، سنستعرض و نقييم إعدادات بريدك الإلكتروني. سنتأكد من أن الوصول إلى البريد الإلكتروني الخاص بمؤسستك لا يتم إلا من خلال أفضل الممارسات الأمنية، كما سنحرص على أن يكون تواصل مؤسستك مع المزودين والعملاء آمنًا للغاية. وبنهاية تقديم الخدمة، سنسلمك تقريرًا مفصلًا يوضح حالة الأمن الخاصة بالحل المستخدم لاستضافة البريد الإلكتروني قبل إجراء الخدمة. إضافة إلى ذلك، سيحتوي التقرير على توصيات تهدف إلى تحسين حالة أمن البريد الإلكتروني الخاص بمؤسستك.

رؤيـــة VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

خدمات التوعية بالأمن السيبراني

الوسائط المتعددة للتوعية بالأمن السيبراني

تدرك سمارت أوربيت الحاجة للاستفادة من قنوات التواصل المختلفة لزيادة مستوى الوعي بالأمن السيبراني لدى موظفيك بفعالية، إذ أنّ استخدام قنوات تواصل مختلفة أمر أساسي لضمان تفاعل موظفيك المتواصل مع البرنامج، ولهذا ستنتج سمارت أوربيت مقاطع فيديو مبتكرة، وملصقات، وخلفيات سطح مكتب، وخلفيات شاشات توقف جذابة وفعّالة لإيصال رسائل الأمن السيبراني المطلوبة، وستلقي تلك الرسائل الضوء على موضوعات مختلفة متعلقة بالأمن السيبراني.

رؤية VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

خدمات التوعية بالأمن السيبراني

دورات الأمن السيبراني الإلكترونية

توفير دورة أمن سيبراني إلكترونية مكون أساسي من استراتيجيات التوعية بالأمن السيبراني الخاصة بمؤسستك. تتيح الدورات الإلكترونية لكل موظف أن ينهي التدريب حسب الوقت المتاح له شخصيًا، ولتضمن سمارت أوربيت حصول موظفيك على أقصى فائدة ممكنة من الدورات الإلكترونية فإنها ستقدم لك حلول تعلم تفاعلية إلكترونية مصممة وفقًا لاحتياجات مؤسستك الأمنية.

رؤيـــة VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

خدمات التوعية بالأمن السيبراني

التوعية بمخاطر التصيد الإلكتروني (اختبارات التصيد)

يستهدف عدد هائل من هجمات التصيّد الإلكتروني موظفي الشركات والمؤسسات، وندرك في سمارت أوربيت الخطر المحتمل من نقطة الضعف هذه لدى عملائنا، ولذا نقدم برنامجًا مخصصًا لتوعية موظفيهم بالتصيد الإلكتروني. يهدف البرنامج إلى تحسين قدرة الموظفين على التعرف على رسائل التصيد الإلكترونية، كما يُصمم البرنامج ليلبي احتياجات مؤسستك ويلائم مستوى الوعي لديها.

رؤيـــة VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

خدمات التوعية بالأمن السيبراني

تقييم مستوى الوعي بالأمن السيبراني

إدراك مستوى الوعي بالأمن السيبراني لمؤسستك أمر محوري لتصميم وتطبيق برنامج توعية فعّال، ولذا تجري سمارت أوربيت دراسة مخصصة لتقييم مستوى وعي الموظفين في مؤسستك، ومن ثم تستخدم نتائج الدراسة لاستحداث المنهجية الأمثل لتصميم البرنامج.

رؤية VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

خـدمـات التـحقـيق الـجنائــي الرقمي والاستجابة للحوادث

تقييم جاهزية الاستجابة للحوادث

تفتقر العديد من المؤسسات إلى المعرفة والمهارات اللازمة للتعامل مع حوادث الأمن السيبراني، ويقفون حائرين لو تعرضوا لإحداها، وقد يترتب على ذلك ضياع العديد من فرص العمل الثمينة وساعات العمل والعائدات المادية عند التعرض لمثل هذه الحوادث. علاوة على ذلك، يتعذر التحقيق في العديد من حوادث الأمن السيبراني، إضافةً إلى انعدام إمكانية العثور على المسبب الرئيسي للحادثة مما قد يؤدي إلى تكرار وقوع نفس الحادثة.

من خلال خدمة تقييم جاهزية الاستجابة للحوادث التي تقدمها سمارت أوربيت سنتأكد من أن مؤسستك مؤهلة للتعامل مع حوادث الأمن السيبراني عند حدوثها، إذ سيزود فريق الشركة مؤسستك بخطة استجابة للحوادث جاهزة للاستخدام عند الحاجة، وستضمن لك الخطة أقل الأضرار الممكنة لحوادث الأمن السيبراني. إضافة إلى ذلك، سنتأكد من أن جميع البيانات اللازمة للتحقيق في الحادثة عند وقوعها قد استُحدِثت وحفظت في مخزن الكتروني مركزي آمن؛ إذ إن هذه السجلات أساسية لتحديد المسبب الرئيسي للحادثة.

رؤيـــة VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

خـدمـات التـحـقـيـق الـجـنـائــي الرقـمـي والاستجابة للحوادث

التعاقد المسبق للاستجابة للحوادث

عند وقوع حوادث الأمن السيبراني، يجهل الكثير من أصحاب الأعمال ما الذي يتوجب عمله في هذه الحالة أو بمن يستنجدون، وقد يتوقف عملهم أيامًا دون معرفة كيفية الاستجابة المناسبة للحادثة.

ولهذا، تقدم سمارت أوربيت خدمة التعاقد المسبق للاستجابة للحوادث لتكون ملاذك عند وقوع الحوادث الأمنية. تضمن لك هذه الخدمة تواجد سمارت أوربيت أثناء وقوع أي حادثة خلال مدة زمنية يتفق عليها الطرفان مسبقًا، كما تضمن لك أن يساعدك فريق سمارت أوربيت في تنفيذ خطة الاستجابة للحادثة ويقدم لك توصيات بما يجب عمله للتعافي من آثار الحادثة بأسرع ما يمكن.

رؤيـــة VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

خـدمـات التـحقـيق الـجنائــي الرقمي والاستجابة للحوادث

تقييم الاختراق

هل أنت متأكد من أن بيئتك الرقمية آمنة 100%؟ هل تعلم ما إن كانت البنية التحتية الرقمية الخاصة بمؤسستك غير مخترقة؟

من خلال خدمة تقييم الاختراق التي تقدمها سمارت أوربيت، سنجرد أصول مؤسستك الرقمية ونراجع سجلات الشبكة والأجهزة بدقة لتحديد ما إن كانت تحتوي على أي نشاطات مشبوهة، وسنخبرك عن أي سجلات مفقودة يجب عليك استحداثها وحفظها. وبناءً على مراجعة السجلات، سنجري مراجعة جنائية لعينة تمثيلية من أجهزة مؤسستك للكشف عن أي مؤشرات اختراق.

وبنهاية الخدمة، سنقدم لك تقريرًا مفصلًا يوضح لك النشاطات التي أداها فريقنا أثناء إجراء التقييم ونتائج الخدمة بالإضافة إلى مجموعة من التوصيات.

رؤيـــة VISION
2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

خدمات اختبار الاختراق

اختبار اختراق تطبيقات الويب

يزداد اعتماد المؤسسات على تطبيقات الويب يومًا بعد يوم. ويفضل مطورو البرمجيات تطوير واجهات ويب لتطبيقاتهم لإتاحة فرصة التنقل وزيادة المرونة الشخصية. ومع وفرة تطبيقات الويب مؤخرًا، أصبحت ثغرات تطبيقات الويب أهدافًا مغرية بالنسبة للمهاجمين ليتسللو إلى شبكات المؤسسات ويسرقوا بياناتها الحساسة. ولهذا، من المهم جدًا اكتشاف الثغرات الأمنية في تطبيقات الويب وإزالتها متى ما وجدت.

سيتعرف خبراء سمارت أوربيت من خلال خدمة اختبار اختراق تطبيقات الويب على ثغرات تطبيقات الويب الخاصة بمؤسستك وسيحاولون استغلالها باستخدام أحدث الأساليب والتقنيات، كما سيصمم الخبراء اختبار الاختراق وفقًا لمواصفات تطبيقات الويب الخاصة بمؤسستك. علاوة على ذلك، ولمضاعفة مدى استفادتك من الخدمة، سيزودك فريقنا أيضًا بالمستندات التقنية المطلوبة التي تتيح لك الحصول على نفس النتائج مرة أخرى.

رؤية VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

خدمات اختبار الاختراق

اختبار اختراق الشبكات

يبحث المهاجمون باستمرار عن طريق يعبرون من خلاله لأصول مؤسستك المعلوماتية، وغالبًا ما يتضمن هذا الطريق العبور خلال شبكتك. تتكون الشبكات من عدد هائل من الأجهزة والخوادم لتلبية احتياجات عملك ومتطلباته، ولذلك من الضروري جدًا ضمان تطبيق ضوابط الأمن السيبراني الأساسية لحماية شبكتك.

سيجري فريق الخبراء الأمنيين في سمارت أوربيت اختبار اختراق يشمل كامل شبكتك لتقييم مدى قدرتها على التعافي. سيحلل الاختبار نقاط ضعف شبكتك وعيوبها التقنية وثغراتها الأمنية بالضبط كما قد يفعل مهاجم خبيث في الهجمات الحقيقية. ويمكن لفريقنا إجراء اختبارات الاختراق خارج محيط الأمن الخارجي أو داخله. ويكمن الهدف الأساسي من هذه الاختبارات في تقديم تصور يوضح مدى كفاءة نظامك في الصمود في وجه الهجمات. وبنهاية إجراء الاختبارات، سيسلمك فريق سمارت أوربيت تقريرًا يوضح جميع الثغرات وأخطاء الإعدادات المكتشفة في شبكتك، كما سيقدم لك الفريق خطة عمل لمعالجة النتائج. علاوة على ذلك، ولمضاعفة مدى استفادتك من الخدمة، سيزودك فريقنا أيضًا بالمستندات التقنية المطلوبة التي تسمح لمديري شبكتك الحصول على نفس النتائج مرة أخرى.

رؤيـــة VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

خدمات اختبار الاختراق

محاكاة الهجمات السيبرانية

على الرغم من أن الانتهاكات السيبرانية تُخلف آثارًا فتاكة، إلا أنها بمثابة فرصة رائعة لتحديد مكامن الضعف في البنية التحتية الرقمية لمؤسستك. تتيح لك سمارت أوربيت من خلال خدمة محاكاة الهجمات السيبرانية فرصة التعرف على نقاط ضعف الأمن السيبراني في مؤسستك دون خوض المتاعب التي تخلفها الانتهاكات الأمنية الحقيقية.

نختبر في هذه الخدمة حصانة مؤسستك في وجه الهجمات الإلكترونية الحقيقية من خلال محاكاة الأساليب والتقنيات والإجراءات التي يستخدمها خصوم حقيقيون؛ ففريقنا في سمارت أوربيت يستطيع توظيف العديد من أنواع الهجمات السيبرانية بناء على خبرته في تحليل هجمات حقيقية وقعت في السابق، كما سيصمم الفريق نوع المحاكاة حسب الهجمات التي قد تحدث لمؤسستك وذلك بالنظر إلى نظام الدفاع السيبراني المستخدم لحماية المؤسسة. وعند انتهاء المحاكاة، يقدم لك فريق العمل في سمارت أوربيت تقريرًا شاملًا يبين ما استغله الفريق لتنفيذ الهجمة، وسيشمل التقرير كذلك خطة عمل لمعالجة الثغرات التي اكتشفها الفريق أثناء تنفيذ الخدمة.

رؤيـــة VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

في سمارت أوربيت
أمنك السيراني هو أهم أولوياتنا

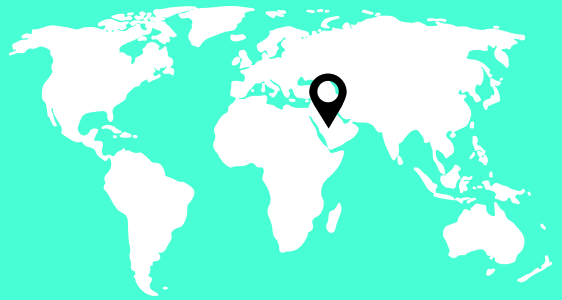
الـرئيـس الـتنفيذي

أنـس الـزبـن

رؤيـة VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

رؤيـــة VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

شكرا لكم



www.soitc.com.sa

info@soitc.com.sa

+966 55 571 1764 | +966 11 262 8358

soitcsa

شركة سمارت اوربيت
لتقنية المعلومات

Smart Orbit Information
Technology Company