نظام الأمن الأساسي لاستدامة
المؤسسة الصناعية والتحول الرقمي

النظام الأساسي للأمن الإلكتروني الصناعي من Kaspersky

واجهوا المستقبل بأمان kaspersky

تتعامل المؤسسات الصناعية مع الأمن الإلكتروني في مختلف البنى التحتية المتعلقة بتكنولوجيا المعلومات والتكنولوجيا التشغيلية. كما تمتلك أغلب الشركات بالفعل مقاييس اكتشاف واستجابة مدروسة في شبكات الشركة، ولكن عندما يتعلق الأمر بالتكنولوجيا التشغيلية فإنها تعتمد عادة على نهج قديم معزول. أصبحت الشركات الصناعية "رقمية" بشكل متزايد، وتستثمر المزيد والمزيد في التقنيات الذكية، وأنظمة الأتمتة الجديدة، كما تتبنى أيضًا عملية التحول الرقمي. ويعمل ذلك بالفعل على إزالة الفجوة التقليدية بين تكنولوجيا المعلومات وبيئات التكنولوجيا التشغيلية - فجوة لطالما تم استخدامها لمنع التهديدات الإلكترونية من الوصول إلى الأتمتة الصناعية وأنظمة التحكم.

التعرض للهجوم من البرامج الضارة

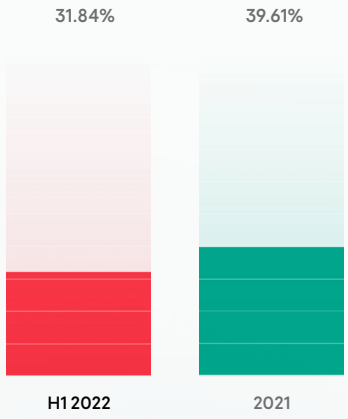
منذ بداية عام 2022، تعرض حوالي 30% تقريبًا من أجهزة الكمبيوتر التابعة لمجموعة أنظمة التحكم الصناعية لهجوم البرامج الضارة - أقل بنسبة 10% تقريبًا عن العام الماضي

فريق الاستجابة لطوارئ الكمبيوتر التابع لمجموعة أنظمة التحكم الصناعية لدى Kaspersky، يونيو 2022

ربما تكون هدفًا - لكن لا تكن ضحية.

لا تحتاج إلى أن تكون هدفًا لتصبح ضحية لانتهاكات الفجوة الهوائية العرضية أو الإصابة بالبرامج الضارة. قد يتسبب محرك أقراص واحد، أو هاتف خلوي، أو بريد إلكتروني احتيالي، أو برامج الفدية الضارة التي تدخل إلى بيئة الأمن الإلكتروني الصناعية في التأثير بشكل خطير على الأعمال الأساسية للشركة. وفي نفس الوقت، قد تتمكن مجموعة قرصنة متحفزة من اختراق شبكات التكنولوجيا التشغيلية وتتسبب في حدوث أضرار جسيمة للمعدات، أو العمليات، أو الإنتاج، أو السلامة والجودة، أو سرقة معلومات ذات قيمة.

فيما يلي النسب المئوية لأجهزة الكمبيوتر التابعة لأنظمة التحكم الصناعية التي تم فيها حظر الكائنات الضارة منذ بداية عام 2022



الأمن الإلكتروني الأساسي للتكنولوجيا التشغيلية

حماية نقطة النهاية

للأنظمة المستقلة والأنظمة المتصلة. يُساعد الحل الآمن والمختبر في إنفاذ السياسات الأمنية، ودعم الامتثال، وإجراء عمليات التدقيق الأمنية، وإدارة المخزون، وتنفيذ مهام التصحيح الجزئي، وجمع القياسات الدقيقة عن بُعد مثل مستشعر نقطة النهاية

حماية الشبكة

لرؤية الاتصالات، واكتشاف التهديدات، وإدارة الأصول. يتحكم نظام كشف الاختراق وتحليل نسبة استخدام الشبكة في كفاءة إعدادات جدار الحماية، وتقسيم الشبكة، والامتثال لاستخدام الشبكة كما يساعد في تقديم استجابة يدوية آمنة

برامج التدريب

للموظفين لتقليل الحوادث وخفض معدل العامل البشري (الخطأ البشري) إلى الحد الأدنى

الخدمات المتخصّصة

للتحقيق في البنية التحتية لإجراء تحليلات الخبراء أو التخفيف من حد تأثير الحادث

ماذا تُقدم شركة Kaspersky

يعمل النظام الأساسي للأمن الإلكتروني الصناعي من Kaspersky (KICS) للتقنيات المتكاملة محليًا، جنبًا إلى جنب مع مجموعة التدريبات والخدمات الاحترافية على تلبية جميع احتياجات الأمن الإلكتروني للمؤسسات الصناعية ومشغلي البنية التحتية الحيوية.

يُعد النظام الأساسي عنصرًا أساسيًا في نظام الاتصال المشترك الفريد للمؤسسات الصناعية التي تشتمل على:

- أفضل حلول الشركات في فئتها من **Kaspersky** والتي تقدم نقطة التقاء بين تكنولوجيا المعلومات والتكنولوجيا التشغيلية والمزايا المتعددة لنهج المورد الواحد
- توفر حلول متخصّصة متنوعة للأمن المادي الإلكتروني، وأمن إنترنت الأشياء الصناعي، وتعلم الآلة، ومساحة العمل الآمنة عن بُعد، وغيرها المزيد من المزايا غير المحدودة والقابلة للتوسع

التقدير العالمي

حازت شركة Kaspersky على جائزة أفضل شركة عالمية لعام 2020 المُقدمة من Frost and Sullivan بناء على تحليل سوق الأمن الإلكتروني (التكنولوجيا التشغيلية/ الأمن الإلكتروني الصناعي) الصناعي العالمي

في استطلاع الرأي العالمي السنوي المتعلق **بالتصميم والإنشاء الافتراضي**، كانت Kaspersky هي أفضل مورد في مجال الأمن الإلكتروني، بناء على التصنيفات الإجمالية من جانب أكثر من 250 متخصصًا مؤهلًا في مجتمع الأتمتة الصناعية

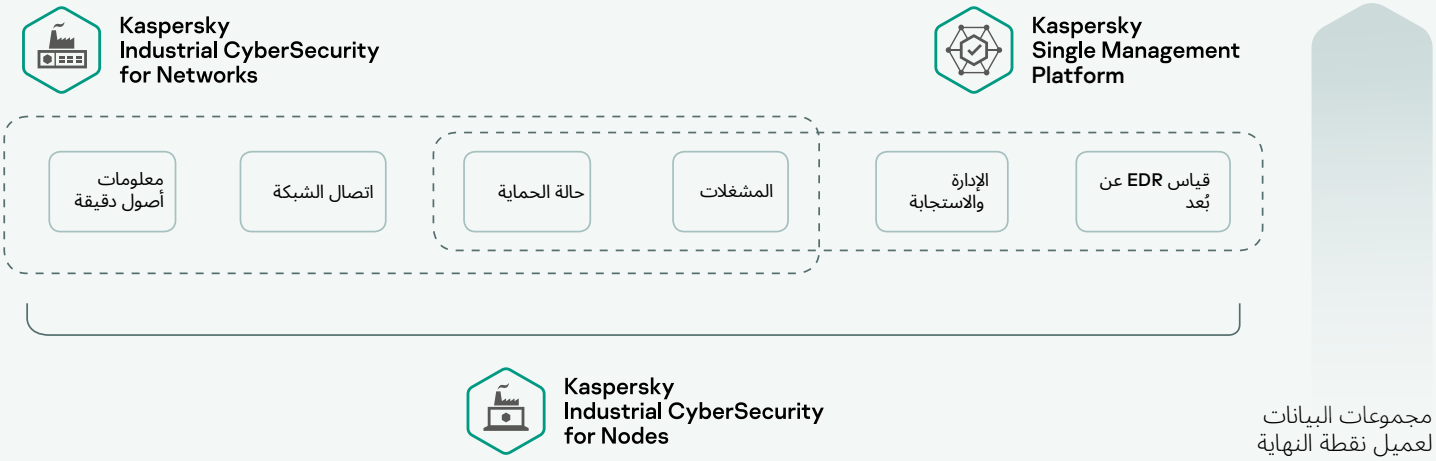
يُعد النظام الأساسي للأمن الإلكتروني الصناعي من Kaspersky رائدًا في الفئات التالية:

- أمن نقطة نهاية التكنولوجيا التشغيلية
- مراقبة شبكة التكنولوجيا التشغيلية ورؤيتها
- اكتشاف الحالات الشاذة والاستجابة للحوادث وإعداد التقارير
- خدمات أمن التكنولوجيا التشغيلية

المنتجات

يمثل **KICS** النظام الأساسي للأمن الإلكتروني للتكنولوجيا التشغيلية المُصمم لتقديم الحماية الشاملة للمكونات الأساسية لنظام التحكم والأتمتة الصناعية على كافة المستويات. يوفر التكامل السلس بين مكونات النظام الأساسي رؤية كاملة لأنظمة الأتمتة وشبكات التكنولوجيا التشغيلية المتعددة الموزعة جغرافيًا، ما يقدم تجربة محسّنة للعملاء، والوعي بالموقف، والمرونة في الانتشار.

عند استخدامهما معًا، يرى المستخدم الصورة بشكل أكبر وسياق أوسع نطاقًا: سلسلة من الحوادث على الشبكة ومستوى نقطة النهاية، ومعلمات الأصول الدقيقة، واتصالات الشبكة، وخرائط المخططات حتى من القطاعات التي لا يتوفر بها انعكاس نسبة استخدام الشبكة وغير ذلك.



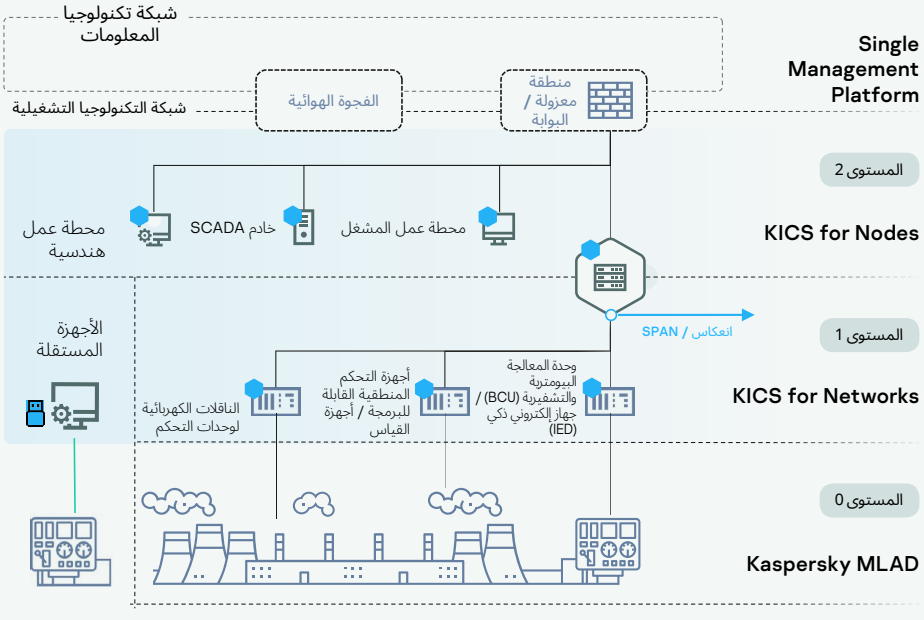
مجموعات البيانات
لعميل نقطة النهاية

يُعد KICS for Nodes برنامج حماية نقطة الحماية واكتشافها والاستجابة لها مع الامتثال لعمليات التدقيق ووظيفة مستشعر نقطة النهاية.

صُمم KICS for Networks لتحليل نسبة استخدام الشبكة المتعلقة بالتكنولوجيا التشغيلية واكتشافها والاستجابة لها.

يوفر Single Management Platform واجهة EDR متقدمة وقابلية توسع سريعة في مواقع متعددة.

هيكل الحل



تحت الحماية بواسطة منتجات Kaspersky

وظائف إضافية

يُقدم الحل وظائف إضافية متنوعة. تُمكّن تقنية **التحقق النشط** للشبكة من التجميع السريع والدقيق لمخططات الشبكة وإعدادات الأصول. تساعد وظيفة **تدقيق نقطة النهاية** في ضمان الامتثال لسياسة الأمن، ويتضمن ذلك على سلامة الإعدادات الحالية، والسيطرة على نقاط الضعف. تُساعد طريقة تقديم **جهاز الفحص المحمول** لبرنامج KICS for Nodes في وضع أفضل الممارسات لعمليات التدقيق المستقلة وتأمين الأجهزة المعزولة. **يُعد Machine Learning for Anomaly Detection** نظام الكشف المبكر عن الحالات الشاذة متعمقًا في العملية التكنولوجية.

Kaspersky Industrial CyberSecurity for Networks

المزايا

اكتشاف الأصل
تعريف الأصل الخامل للتكنولوجيا التشغيلية والمخزون

الفحص الدقيق للحزم
تحليل في الوقت الحقيقي تقريبًا لقياس العمليات التقنية عن بُعد

التحكم في تكامل بيانات الشبكة
اكتشاف المضيفين والتدفقات غير المصرح بهم في الشبكة

نظام كشف الاختراق
إرسال التنبيهات الخاصة بأنشطة الشبكة الضارة

التحكم بالأوامر
أوامر الفحص عبر البروتوكولات الصناعية

التكامل الخارجي
يضيف تكامل واجهة برمجة التطبيقات المرنة قدرات الكشف والمنع

Machine learning for anomaly (detection (MLAD
يكتشف الحالات الشاذة الإلكترونية أو المادية من خلال القياس عن بُعد في الوقت الحقيقي والتنقيب في البيانات القديمة (الشبكة العصبية المتكررة)

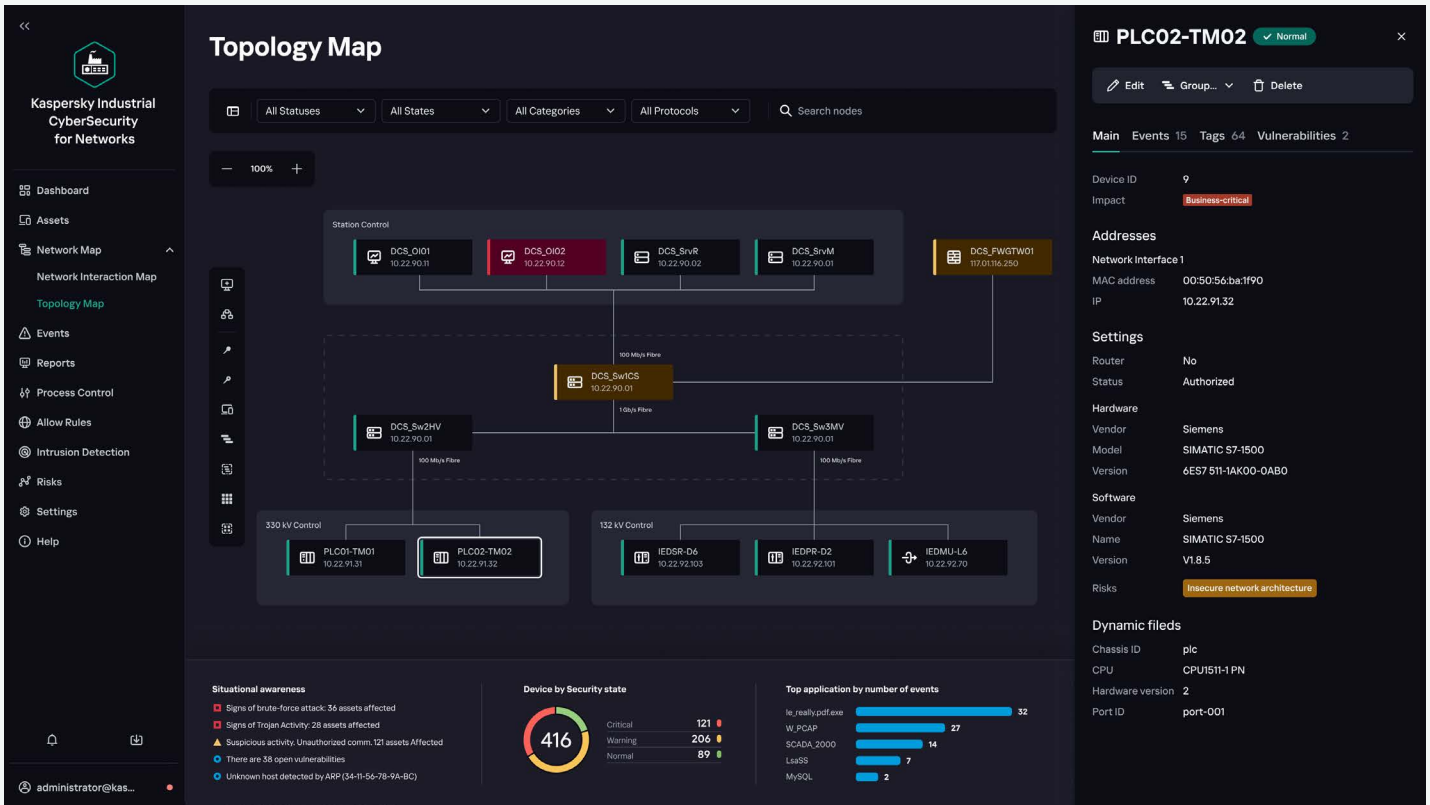
إدارة نقاط الضعف
قاعدة بيانات خاصة بنقاط الضعف قابلة للتحديث في الأجهزة الصناعية تخضع لإدارة فريق الاستجابة لطوارئ الكمبيوتر التابع لمجموعة أنظمة التحكم الصناعية لدى Kaspersky

تحليل نسبة استخدام الشبكة الخاصة بالتكنولوجيا التشغيلية واكتشافها والاستجابة لها. رؤية واضحة للمخاطر من خلال مراقبة نسبة الاستخدام السلبية، والتحقق النشط، ومستشعرات نقطة النهاية.

يكتشف الحالات الشاذة والاقتحام داخل شبكات أنظمة التحكم الصناعية في مراحلها المبكرة ويضمن اتخاذ الإجراءات اللازمة لمنع أي تأثير سلبي على العمليات الصناعية.

حل يتوافق مع الأجهزة يُمكنه التكامل سريعًا وبصورة مثالية في عمليات التوريد القائمة، ومع سياسات التكامل والضمان الخاصة بعملائنا.

الواجهة



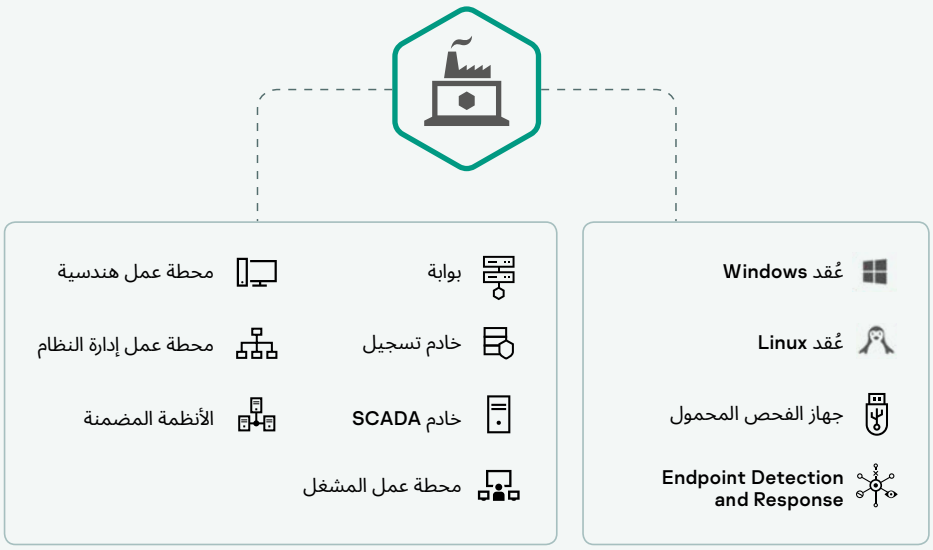
Kaspersky Industrial CyberSecurity for Nodes

صُمم KICS for Nodes خصوصًا للمتطلبات القاسية الخاصة بأنظمة الأتمتة الموزعة: البيئات المختلطة والمعقدة، والوقت الممتد في التشغيل، وحالات الاستخدام المستقلة والمتصلة، وحالات المعالجة والصيانة المجانية، وأولوية التحكم في إمكانية التوافر مهما كلف الأمر

يتمتع بالدرجة الصناعية، فقد تم اختبار واعتماد حماية نقطة النهاية واكتشافها والاستجابة لها. حل ذو تأثير منخفض ومتوافق ومستقر لأنظمة التشغيل **Linux**، و **Windows**، والأنظمة المستقلة.

حماية نقطة النهاية الصناعية واكتشافها والاستجابة لها

يحمي جميع نقاط النهاية لنظام حديث ورقمي تتم إدارته وتوزيعه باستخدام الأتمتة. يكشف عن مستويات جديدة من رؤية الحوادث في عملية التحليل للسبب الجذري. يقوم العامل بتجميع قياسات نقطة النهاية عن بُعد لإنشاء عرض مرئي واضح ومفصل لمدى تقدم الحادث في محطات العمل، والخوادم، والبوابات، ونقاط النهاية الأخرى، ما يُطمئِن مسؤولي نظام الأتمتة بأنه قد تم التعامل مع الحادث بشكل كامل ولن يحدث مجددًا.



الفوائد

تأثير منخفض
على الأجهزة المحمية للحصول على أفضل أداء للنظام

متوافق
مع أجهزة الكمبيوتر منخفضة الأداء من الأجيال السابقة، والأنظمة من Windows XP SP2 وحتى Windows Server 2003 SP1 فى الأعلي

دورة حياة ممتدة
تصل إلى ترخيص لمدة 5 سنوات ودعم ممتد

أداء وظيفي كامل
لجميع أجهزة سطح المكتب والخوادم من MS وأنظمة تشغيل Windows المضمّنة

التوزيع النمطي
خيارات مرنة وإعدادات آمنة غير متداخلة

يغطي البنى التحتية المختلطة
أنظمة تشغيل Windows، وLinux، والمتغيرات المحمولة

جهاز الفحص المحمول لنظام KICS for Nodes
يفرض سياسة الأمن الإلكتروني على الماكينات المستقلة، أو أنظمة الأتمتة، أو المعدات التي لا يمكن تثبيت البرنامج الأمني عليها. إلمام غير محدود بالحالة ورؤية التكنولوجيا التشغيلية حتى من خلال البنية التحتية المستقلة.

حل دون تثبيت
يُمكن تنشيط KICS for Nodes على عدد من محركات الأقراص الإضافية لجهاز الفحص المحمول. يساعد النظام الأساسي على عمليات فحص متزامنة عند الطلب على أجهزة متعددة خلال تشغيل نوافذ الصيانة، لتجميع بيانات نقطة النهاية وتنظيمها في تقرير موجز ملائم.

الامتثال للسياسة التنظيمية والداخلية
يُجري جهاز الفحص المحمول لنظام KICS for Nodes فحوصات الامتثال لمكافحة البرامج الضارة على الأجهزة التي يُمكنها الوصول إلى موقع التكنولوجيا التشغيلية، ويتضمن ذلك أجهزة الكمبيوتر الخاصة بالمتعاقدين الخارجيين. كما تتمتع ببصمة تشغيلية منخفضة للغاية ولا تتداخل مع الحلول الأمنية القائمة.

الفوائد

وعي بالموقف

إدارة الأنظمة/ السياسة

سلسلة القتل الإلكتروني والاستجابة لها

إعداد التقارير والإخطار

دمج **SIEM**

تكامل **HMI / MES**

Kaspersky Single Management Platform

يُعد **Single Management Platform** حلًا مركزيًا لإدارة الأمن لتوزيع الأمن على البنية التحتية للتكنولوجيا التشغيلية بشكل كامل، مع توفير خريطة بجميع الأصول الموزعة جغرافيًا والمدعومة بالأحداث، وتحليلات الحوادث وغير ذلك المزيد. يُعزز كفاءة الفرق الأمنية للتكنولوجيا التشغيلية وتكنولوجيا المعلومات المختلطة. وهو مكان تجتمع فيه جميع الضوابط الأمنية حيث تعمل في تناغم، ما يوفر استجابة سريعة ودقيقة.

الخدمات المتخصّصة

تُشكل مجموعة خدماتنا جزءًا مهمًا من قائمة حلول **KICS**. نوفر دورة كاملة لخدمات الأمن، بدءًا من تقييمات الأمن الإلكتروني في القطاع الصناعي ووصولًا إلى الاستجابة للحوادث

> ولقد منحتنا خبراتهم في مجال الأمن الإلكتروني لمجموعة أنظمة التحكم الصناعية، وكفاءتهم المهنية، وحلولهم للأمور المعقدة، مقارنة بموردينا الآخرين، قيمة رائعة وضمنت تقديم مستقبل باهر لإستراتيجية الأمن الخاصة بشركتنا.
>
> أوندريج سيكورا،
> مدير التحكم في العمليات والأتمتة لدى شركة Plzeňský Prazdroj

تقييم الأمن الإلكتروني في القطاع الصناعي

تقييم الأمن الإلكتروني في القطاع الصناعي: تُقدم **Kaspersky** تقييمًا للأمن الإلكتروني الصناعي بالحد الأدنى من التدخل، ويتضمن ذلك اختبار الاختراقات الخارجية والداخلية، وتقييم أمن التكنولوجيا التشغيلية، وتقييم أمن حلول الأتمتة. كما يُقدم خبراء **Kaspersky** رؤى مهمة فيما يتعلق بالبنية التحتية للشركة وتقديم التوصيات بشأن كيفية تعزيز وضع الأمن الإلكتروني في نظام التحكم الصناعي.

> ومن خلال الممارسة واكتساب المعرفة من فريق عمل Kaspersky، لقد عملنا على رفع مستوى الحماية لدينا ضد تهديدات الأمن الإلكتروني.
>
> يو تات مينغ،
> الرئيس التنفيذي لدى شركة PacificLight

المعلومات المتعلقة بالتهديدات

تساعد التحليلات الحديثة التي جمعها خبراء **Kaspersky** في تعزيز حماية العميل من التهديدات الإلكترونية الصناعية المستهدفة. وتُقدم باعتبارها موجزات تكنولوجيا المعلومات أو تقارير مخصصة، بحيث تلبي الاحتياجات الخاصة بالعميل بما يتوافق مع المعلمات الإقليمية، والصناعية، ومعلمات برنامج أنظمة التحكم الصناعية.

الاستجابة للحوادث

في حال وقوع حادث، يعمل خبراء **Kaspersky** على تجميع البيانات والبرامج الضارة وتحليلها، وإعادة بناء الجدول الزمني للحادث، وتحديد المصادر والدوافع المحتملة، ووضع خطة معالجة تفصيلية. وتشتمل الخطة على التوصيات المتعلقة بإزالة البرامج الضارة من أنظمة العميل والعودة إلى الحالة السابقة قبل تطبيق إجراءاتها الضارة.

التدريب والتوعية

> لقد كانت Kaspersky أفضل شركة يُمكنها توفير التدريب المتعلق بمهارات الأمن الإلكتروني الصناعي الاحترافي لمجموعة أنظمة التحكم الصناعية الخاصة بنا
>
> سورن إيجيديه كنودسن،
> الرئيس التقني

تدريب التوعية بالأمن الإلكتروني الصناعي

تدريب تفاعلي في الموقع وعبر الإنترنت وألعاب السلامة الإلكترونية للموظفين الذين يعملون مع الأنظمة الحاسوبية الصناعية ومديريهم. يكتسب المشاركون رؤى جديدة بشأن مشهد التهديدات الحالي ووجهات الهجوم التي تستهدف البيئات الصناعية على وجه الخصوص، واكتشاف سيناريوهات عملية، واكتساب مهارات السلامة الإلكترونية.

برامج تدريب الخبراء

تستهدف الدورات التدريبية لاختبار اختراقات أنظمة التحكم الصناعية والتحاليل الرقمية لأنظمة التحكم الصناعية المتخصصين في مجال الأمن الإلكتروني. يكتسب المشاركون جميع المهارات المتقدمة اللازمة لإجراء اختبارات الاختراق والتحليلات الرقمية الشاملة في البيئات الصناعية.

نظام اتصال مشترك لحلول متخصّصة

Kaspersky IoT Infrastructure Security

تعمل على حماية إنترنت الأشياء على مستوى البوابة بناء على نهج المناعة الإلكترونية المُقدم من Kaspersky.

معرفة المزيد

Kaspersky Antidrone

يعمل على حماية المجال الجوي من الطائرات دون طيار في المنشآت بأي حجم

معرفة المزيد

Kaspersky Secure Remote Workspace

الأداء الوظيفي للبنية التحتية الرقيقة الخاصة بالعميل إلى جانب المناعة الإلكترونية

معرفة المزيد

Kaspersky Security CAD

النمذجة الرقمية لنظم أمن المعلومات لمراحل التصميم والتشغيل

معرفة المزيد

Kaspersky Machine Learning for Anomaly Detection

نظام الكشف المبكر عن الحالات الشاذة في العمليات التقنية الصناعية

معرفة المزيد

Kaspersky Industrial CyberSecurity

معرفة المزيد

www.kaspersky.com