Kaspersky Industrial CyberSecurity

منصة XDR للأمان الشامل
للمؤسسات الصناعية

واجهوا المستقبل بأمان kaspersky

التهديدات الإلكترونية التي يواجهها نظام التحكم الصناعي والمؤسسات الصناعية

يتشكل الواقع الجديد لأصحاب ومشغلي البنى التحتية الصناعية عن طريق الاهتمام المتزايد لنشطاء القرصنة بأنظمة الأتمتة، والمتطلبات التنظيمية العالية، وتقارب تكنولوجيا المعلومات والتكنولوجيا التشغيلية، وارتفاع تنوع الهجمات الإلكترونية في القطاع الصناعي (زيادة بنسبة 50% تقريبًا في النصف الأول من عام 2023، مقارنة بالنصف الثاني من عام 2022، وفقًا لإحصائيات فريق Kaspersky ICS CERT).

يؤدي ظهور التقنيات الرقمية، الذي يُنظر إليه عادة كأمر جيد، إلى محو الفجوة بين بيئات تكنولوجيا المعلومات والتكنولوجيا التشغيلية التي كانت تُستخدم لحماية الأخيرة من مجرمي الإنترنت. وبينما قد يؤثر محرك أقراص محمول واحد في حالة إدخاله إلى بيئة نظام التحكم الصناعي بشكل خطير على الأعمال الأساسية للشركة، فإن أي مجموعة قرصنة لديها حافز تستطيع اختراق شبكات التكنولوجيا التشغيلية وتتسبب في أضرار كبيرة و/أو تسرق معلومات ذات قيمة. وإلى جانب معايير الأتمتة التي تتطور من خلال التوصيات المشتركة إلى المتطلبات التشريعية والحاجة المتزايدة لمشاركة أفضل الممارسات وكذلك إدارة المخاطر، فإن هذا يجعل الأمن الإلكتروني للمؤسسات الصناعية يمثل تحديًا هائلاً.

يتوقع فريق Kaspersky ICS CERT أن تواجه المؤسسات من الصناعات التالية هجمات إلكترونية بوتيرة متزايدة:

النفط والغاز والمواد الكيميائية

تجعل القيمة العالية للبيانات والأنظمة التي تتحكم فيها هذه المؤسسات منها هدفًا جذابًا لبرامج طلب الفدية والجهات الخبيثة التي تسعى إلى تعطيل العمليات أو التلاعب بالأسعار.

التصنيع الصناعي رفيع المستوى

تؤدي هذه الشركات أدوارًا مجتمعية في غاية الأهمية وتمتلك بيانات قيمة يمكن استغلالها لتحقيق مكاسب مالية، مما يؤدي إلى التسبب في أضرار جسيمة على المستوى الاقتصادي وعلى مستوى السمعة.

المعادن والفلزات والتعدين

يتم استهداف صناعة المعادن والفلزات والتعدين بسبب مواردها القيمة وتأثيرها المالي وسلاسل التوريد المترابطة.

الطاقة والشبكة والمرافق

يعد الدور الرئيسي الذي تلعبه الطاقة والشبكة والمرافق في حياتنا اليومية السبب الرئيسي للهجمات التي تهدف إلى خلق الفوضى أو ممارسة النفوذ.

التعرض للهجوم من البرامج الضارة

منذ بداية عام 2023، تعرض حوالي 35% من أجهزة الكمبيوتر التابعة لمجموعة أنظمة التحكم الصناعية لهجوم البرامج الضارة - أقل بنسبة 5% تقريبًا عن العام الماضي

Kaspersky ICS CERT،
أكتوبر 2023

معرفة المزيد

ستشمل الأهداف الأساسية لهجمات التهديدات المتقدمة المستمرة ما يلي:

أصحاب ومشغلي البنية التحتية الحرجة

تواجه المؤسسات الحكومية أو العامة ذات الأهمية الإستراتيجية عواقب محتملة أكبر بكثير من التدخل في العمليات

الجهات الصناعية رفيعة المستوى

من مصنع واحد إلى عدة مصانع على نطاق وطني أو دولي، تشارك هذه الشركات في عمليات عالية المخاطر، تنطوي على تكاليف كبيرة للحوادث

يرتبط استقرار الإنتاج والعمليات التجارية، فضلاً عن حماية الأصول القيمة، ارتباطًا مباشرًا بالتنمية المستدامة للمؤسسات الصناعية ومرافق البنية التحتية الحيوية. وترتفع وتيرة الهجمات على الأنظمة الصناعية، خاصة نظام التحكم الصناعي (ICS) وSCADA. ومن ناحية أخرى، يبدو أن التهديدات الإلكترونية الحديثة التي تستهدف البيئات الصناعية محصنة ضد الحلول التقليدية.

بات أكثر أهمية من أي وقت مضى أن تختار شريكًا يمكنك الوثوق به، يتمتع بمعرفة عميقة بالتداخلات بين الأمن الإلكتروني الصناعي والخاص بالشركات والقدرة على توفير مجموعة كاملة من تقنيات الأمان المتطورة.

تعرف على المزيد عن التكتيكات والتقنيات والإجراءات الشائعة للهجمات ضد المؤسسات الصناعية

معرفة المزيد

تقنيات أمان نظام التحكم الصناعي المتقدمة

Kaspersky Industrial CyberSecurity (KICS) عبارة عن منصة أصلية للاكتشاف والاستجابة الموسعة (XDR) للمؤسسات الصناعية، تم تصميمها واعتمادها خصيصًا لحماية معدات التكنولوجيا التشغيلية والأصول والشبكات المهمة من التهديدات الإلكترونية. وتحتوي المنصة على تقنيات متكاملة تعمل على تأمين المكونات الأساسية لنظام الأتمتة والتحكم الصناعي على كل المستويات. يُعد KICS for Nodes برنامج حماية نقطة الحماية واكتشافها والاستجابة لها مع الامتثال لعمليات التدقيق ووظيفة مستشعر نقطة النهاية. وصُمم KICS for Networks لتحليل حركة استخدام شبكة التكنولوجيا التشغيلية واكتشافها والاستجابة لها. وتم دمج وظيفة الإدارة المركزية على مستوى الموقع، التي تعد ضرورية لتوسيع نطاق عمليات أمان التكنولوجيا التشغيلية إلى حجم كبير من البنى التحتية الصناعية الكبيرة والمتنوعة والموزعة جغرافيًا، في المنصة.

يوفر التكامل السلس عبر مكونات النظام الأساسي رؤية كاملة لأنظمة الأتمتة وشبكات التكنولوجيا التشغيلية المتعددة الموزعة جغرافيًا، ما يقدم تجربة محسّنة للعملاء، والوعي بالموقف، والمرونة في الانتشار. ومن خلال الاكتشاف والاستجابة الموسعة، تتيح منصة KICS التقارب بين تكنولوجيا المعلومات والتكنولوجيا التشغيلية وتوفر العديد من المزايا للمورد الفردي.

تتيح منصة KICS XDR Platform للمستخدمين رؤية الصورة بشكل أكبر وسياق أوسع نطاقًا: سلسلة الحوادث على الشبكة ومستوى نقطة النهاية، ومعلمات الأصول الدقيقة، واتصالات الشبكة، وخرائط المخططات حتى من القطاعات التي لا يتوفر بها انعكاس حركة استخدام الشبكة وغير ذلك.

مستشعر نقطة النهاية

- حالة الحماية
- تدقيق الأمان
- اتصالات الشبكة
- نقل القياس عن بعد للمضيف
- مراقبة المعدات
- الاستجابة للحوادث

نقاط تطبيق المنصة

تقارب بيئات التكنولوجيا التشغيلية وتكنولوجيا المعلومات

منطقة معزولة / البوابة

بيئة تكنولوجيا المعلومات

بيئة التكنولوجيا التشغيلية

Kaspersky Industrial CyberSecurity for Nodes

- بوابة ICS
- محطة العمل الهندسية
- خادم SCADA
- محطة عمل المشغل

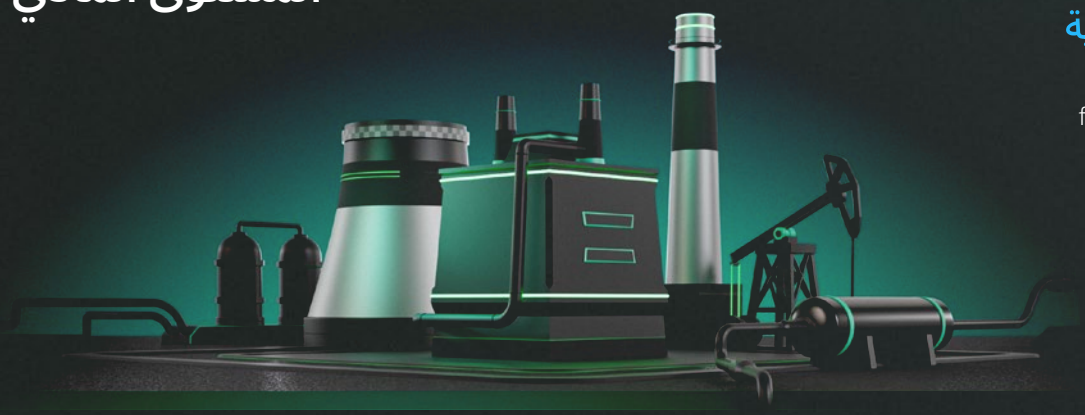
معدات الشبكة

SPAN

Kaspersky Industrial CyberSecurity for Networks

- جهاز إلكتروني ذكي (IED)
- وحدة صندوق التحكم (BCU)
- نظام حماية المرحل والسلامة (SIS)
- وحدات التحكم المنطقية القابلة للبرمجة (PLC)
- العُقد المعزولة (الفحص اليدوي باستخدام جهاز الفحص المحمول في KICS)

المستوى المادي



الاكتشاف المبكر للحالات الشاذة والتحليلات التنبؤية

يعد Kaspersky Machine Learning for Anomaly Detection (Kaspersky MLAD) نظامًا مبتكرًا يستخدم شبكة عصبية لمراقبة مجموعة واسعة من بيانات القياس عن بعد في الوقت نفسه. ويكتشف أخطاء المعدات والأخطاء البشرية، مما يساعد على منع الفشل والحوادث، ويتعرف على تصرفات الموظفين غير المعتادة أو عمليات المعدات كعلامات على هجوم متخصص أو تخريب، ويجمع بين اكتشاف الحالات الشاذة والتحليل التنبؤي لحالة المعدات ودورة حياتها.

معرفة المزيد

محمي بواسطة منتجات Kaspersky

KICS for Networks

Kaspersky Industrial CyberSecurity for Networks

حل خاص على مستوى البروتوكول لمراقبة الشبكات الصناعية وتحليل حركة المرور، يتم شحنه كبرنامج أو كجهاز افتراضي.

يتعرف KICS for Networks على الحالات الشاذة والاختراقات في نظام التحكم الصناعي في مرحلة مبكرة، ويوضح كيفية تطور الهجوم عبر الشبكة وفي العُقد (سلسلة التدمير في EDR والقياس عن بعد)، ويضمن اتخاذ الإجراءات اللازمة لمنع أي تأثير سلبي على العمليات الصناعية .

يساعد الحل على اكتشاف المخاطر وتصنيفها بناءً على البيانات الواردة من الثغرات الأمنية واتصالات الشبكة، بالإضافة إلى دور الأصول المختلفة، لمنع وقوع الحوادث.

الفوائد

جرد الأصول

الجرد التلقائي للأصول وجمع البيانات باستخدام الطرق السلبية والإيجابية لجمع البيانات

جرد الشبكة والتصوير المرئي

- خريطة اتصالات الشبكة
- مخطط التركيب البنيوي للشبكة

تقييم الثغرات الأمنية والمخاطر

- إدارة الثغرات الأمنية والمخاطر الخاصة بالتكنولوجيا التشغيلية
- التسجيل التلقائي وتحديد الأولويات
- توصيات معالجة المخاطر

اكتشاف الحالات الشاذة في الشبكة

التحكم في سلامة الشبكة مع مراقبة انحراف خط الأساس واكتشاف أنشطة الشبكة الضارة والمشبوهة

التحكم في عمليات التكنولوجيا التشغيلية والفحص العميق للحزم (DPI)

- استخراج بيانات الحمولة الصناعية
- التحكم في العمليات في الوقت الحقيقي
- التحكم في القيادة الصناعية
- مراقبة عملية التكنولوجيا التشغيلية المتقدمة بواسطة Kaspersky MLAD

التكامل وتبادل البيانات

- المعلومات المركزية
- التكامل مع Kaspersky وأنظمة الجهات الخارجية أو أنظمة العملاء (IEC104 وOPC وCEF وSyslog والموصلات المستندة إلى واجهة برمجة التطبيقات)

الامتثال المركزي تدقيق عقد الشبكة الصناعية

يقدم KICS for Networks تدقيقًا مركزيًا لعُقد الشبكة الصناعية، بما في ذلك التدقيق المستند إلى العميل (عبر KICS for Nodes) والتدقيق بدون عميل لأجهزة الشبكات ونقاط النهاية للبحث عن الثغرات الأمنية والامتثال لمعايير الصناعة OVAL* وXCCDF**.

- دعم أي قواعد بيانات متوافقة مع معيار OVAL خاصة بجهة خارجية أو مخصصة
- قاعدة بيانات الثغرات الأمنية في نظام SCADA المضمن بواسطة فريق ICS CERT
- إتاحة جميع التقارير وبيانات الأصول في مكان واحد - قاعدة أصول KICS for Networks
- مخزن محمي لبيانات اعتماد العُقد
- التدقيق الأمني المركزي الآلي لنظام التشغيل Windows وعُقد Linux وأجهزة الشبكة
- التدقيق في الامتثال. محرر كامل الوظائف لفحوصات الامتثال والمعلمات

* لغة الثغرات الأمنية والتقييم المفتوحة (OVAL)
** تنسيق وصف قائمة التحقق من التكوين القابل للتوسيع (XCCDF)

KICS for Nodes

Kaspersky Industrial CyberSecurity for Nodes

حل حماية نقطة النهاية واكتشافها والاستجابة من الدرجة الصناعية والخاضع للاختبارات والمعتمد. حل ذو تأثير منخفض ومتوافق ومستقر لأنظمة التشغيل Linux وWindows والأنظمة المستقلة.

يحمي KICS for Nodes جميع نقاط النهاية في نظام حديث ورقمي تتم إدارته وتوزيعه باستخدام الأتمتة. يجمع الحل القياس عن بُعد لإنشاء عرض مرئي واضح ومفصل لمدى تقدم الحادث في محطات العمل والخوادم والبوابات ونقاط النهاية الأخرى، ما يُطمئن مسؤولي نظام الأتمتة بأنه قد تم التعامل مع الحادث بشكل كامل ولن يحدث مجددًا.

يفرض جهاز الفحص المحمول في KICS for Nodes سياسة الأمن الإلكتروني على الماكينات المستقلة، أو أنظمة الأتمتة، أو المعدات التي لا يمكن تثبيت برامج الأمان عليها. ومع بصمة تشغيلية منخفضة للغاية، لا تتداخل مع حلول الأمان الموجودة.

- حل بدون تثبيت يوفر أفضل وعي بالظروف ورؤية التكنولوجيا التشغيلية حتى لبنية تحتية مستقلة.
- يسمح لك بإجراء عمليات الفحص عند الطلب على أجهزة متعددة أثناء فترات الصيانة في وقت واحد، ويوفر تقارير سهلة.
- ينفذ فحوصات امتثال المعدات التي تصل إلى موقع التكنولوجيا التشغيلية لمكافحة البرامج الضارة، بما في ذلك أجهزة الكمبيوتر الخاصة بمقاولي الجهة الخارجية.

- التحكم في الأجهزة
- التحكم في سلامة الملفات
- التحكم في سلامة وحدة التحكم المنطقية القابلة للبرمجة (PLC)
- الحماية ضد التشفير
- منع الاستغلال
- منع تهديدات الشبكة
- أداة فحص سجل Windows
- التحكم في شبكة Wi-Fi
- إدارة جدار الحماية
- مراقبة التسجيل
- تدقيق الأمان
- عميل EDR
- مستشعر نقطة النهاية (التكامل مع KICS for Networks)

- عُقد Windows
- عُقد Linux
- جهاز الفحص المحمول
- عميل التدقيق

- البوابة
- خادم التسجيل
- خادم SCADA
- محطة عمل المشغل
- محطة العمل الهندسية
- محطة عمل إدارة النظام
- الأنظمة المضمنة

الفوائد

تأثير منخفض

- تأثير منخفض على الأجهزة المحمية للحصول على أفضل أداء للنظام
- لا يلزم إعادة التشغيل للتثبيت أو التحديث أو الترقية
- توافر وضع الاكتشاف فقط
- استهلاك موارد النظام القابل للضبط

التوافق

- دعم أنظمة التشغيل القديمة بدءًا من Windows XP SP2 وWindows Server 2003 SP1
- التوافق مع بائعي أنظمة الأتمتة الصناعية
- جهاز فحص محمول كخيار لا يحتاج إلى تثبيت

الحماية الموسعة

- الحماية من البرامج الضارة وبرامج طلب الفدية وثغرات الاستغلال
- تحليل السجل
- التحكم في جدار الحماية
- تكنولوجيا EDR لنظام التحكم الصناعي المدمجة
- تحديثات قاعدة بيانات المعزولة عن الشبكات غير الآمنة

النشر المعياري

- خيارات مرنة وإعدادات آمنة غير متداخلة مصممة للتكنولوجيا التشغيلية
- بنية معيارية تسمح باختيار مكونات الحماية المطلوبة فقط

دعم وحدة التحكم المنطقية القابلة للبرمجة (PLC)

- Siemens SIMATIC S7-300, S7-400, S7-400H, S7-1500, S7-1200, SIPROTEC 4
- Schneider Electric Modicon M340, M580
- الأجهزة المعتمدة على CODESYS V3
- Fastwel CPM723-01

التدقيق

- تدقيق الشامل للأمان والامتثال معتمد على المعايير المفتوحة للغة OVAL

الأمن الإلكتروني الموحد عبر القطاعات الصناعية والشركات في مؤسستك

ترتفع وتيرة الهجمات على الأنظمة الصناعية، خاصة نظام التحكم الصناعي (ICS) وSCADA. وبات أكثر أهمية من أي وقت مضى أن تختار شريكًا يمكنك الوثوق به، يتمتع بمعرفة عميقة بالتداخلات بين الأمن الإلكتروني الصناعي والخاص بالشركات والقدرة على توفير مجموعة كاملة من التقنيات المتطورة للأمن الإلكتروني الصناعية وللشركات.

Kaspersky XDR الأداة المثالية لبناء بيئة عمل آمنة وخالية من التهديدات. ويسهل توافقها مع مجموعة متنوعة من منتجات الأمان إنشاء مساحة إلكترونية آمنة، مما يوفر خيارات خاصة بالصناعة لأعمالك ويحميها من أي تهديد، مهما كان كبيرًا أو صغيرًا. وتتيح خيارات التكامل في Kaspersky XDR توفير رؤية موحدة وشاملة للتهديدات، وتزويد فريق الأمان لديك بجميع الأدوات والبيانات التي يحتاجونها لحماية أعمالك من التهديدات الحالية والمحتملة.

معرفة المزيد

عوامل فعالية Kaspersky XDR

الفهم السياقي للخصائص والمتطلبات والأنظمة المتخصصة والبروتوكولات والاعتبارات التشغيلية الفريدة

تكامل مع نظام التحكم الصناعي يتيح الرؤية الشاملة والتحليل لحركة مرور الشبكة الصناعية وسلوك النظام

معلومات التهديدات الخاصة بالتكنولوجيا التشغيلية للاستفادة من خبرة Kaspersky في مجال الحماية من تهديدات البيئة الصناعية

التخصيص والتكوين لتكييف الحل مع متطلبات تحمل المخاطر المحددة وبنية الشبكة واحتياجات الامتثال التنظيمي

بائع واحد لتحقيق أقصى استفادة من دعم البائع وتعاونه، بما في ذلك توفير التحديثات والتصحيحات في الوقت المناسب

تقارب تكنولوجيا المعلومات والتكنولوجيا التشغيلية مع Kaspersky Hybrid XDR

الأمن الإلكتروني لتكنولوجيا المعلومات

معرفة المزيد

الأمن الإلكتروني للتكنولوجيا التشغيلية

معرفة المزيد

حدود البيئة

أكثر من 26 عامًا من الخبرة ذات المستوى العالمي وكم هائل يقاس بالبيتابايت من بيانات التهديدات

ICS CERT

ICS-CERT — قسم دولي خاص لأبحاث أمان التكنولوجيا التشغيلية / إنترنت الأشياء

خبرة راسخة في مجال أمان تكنولوجيا المعلومات / التكنولوجيا التشغيلية حصلت على العديد من الجوائز وحققت العديد من الإنجازات

أكثر من 100 شهادة لقابلية التشغيل البيني مع حلول موردي الأتمتة

فعالية التكنولوجيا الراسخة، والامتثال للمعايير والمتطلبات

عملاء في جميع أنحاء العالم

ROSATOM NORNICKEL EuroChem

NLMK TATNEFT ROSSETI Wintershine

alperia PacificLight КазМунайГаз AGC

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Networks

معرفة المزيد

#kaspersky
#bringonthefuture

me.kaspersky.com