Kaspersky OT CyberSecurity

نظام بيئي للأمن الإلكتروني المادي
للمؤسسات الصناعية

واجهوا المستقبل بأمان kaspersky

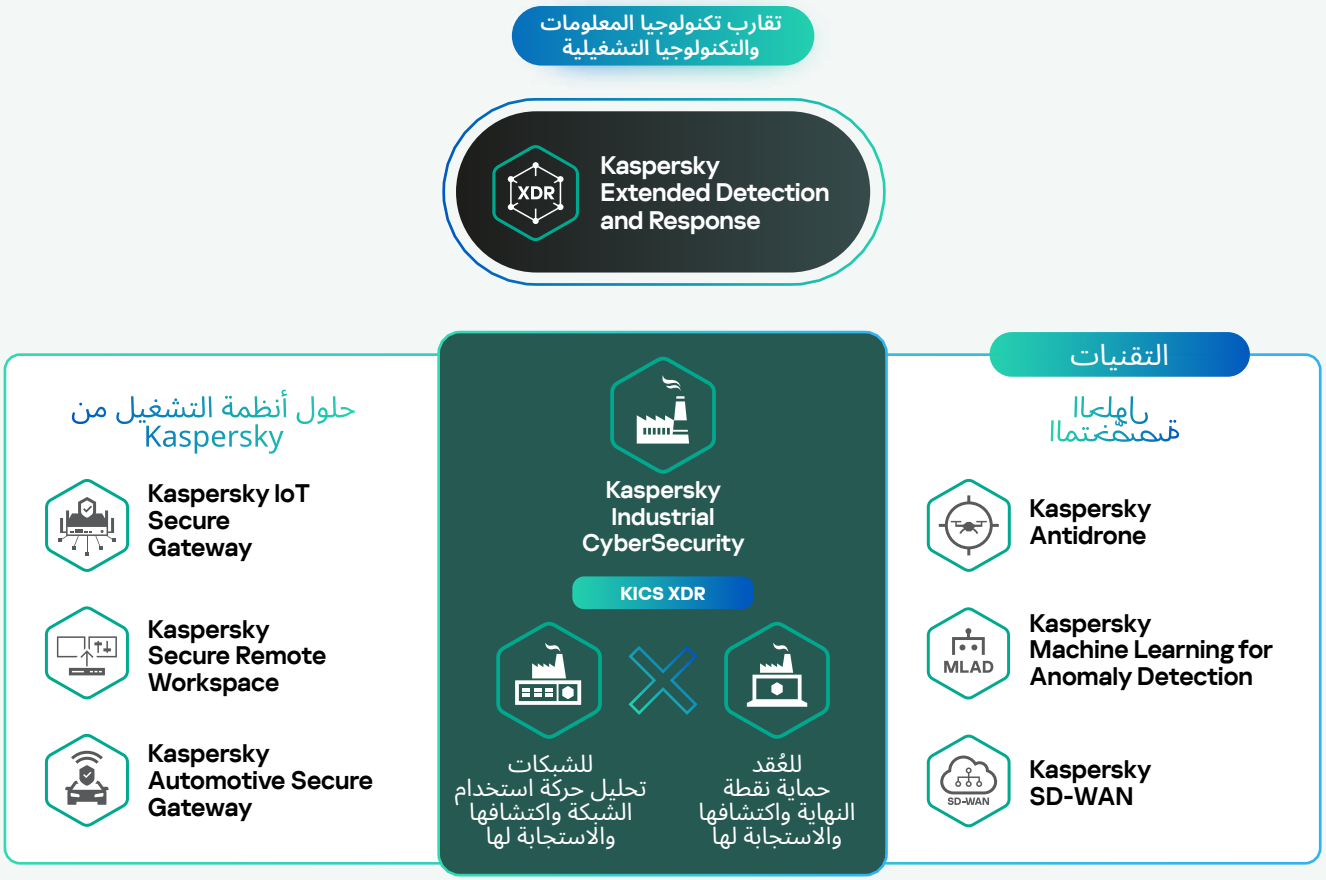
Kaspersky OT CyberSecurity

مفهوم السلامة الصناعية الموحد

التقنيات
مجموعة قوية من حلول الأمان الصناعي الخاضعة للاختبار والمتوافقة والمعتمدة

المعرفة
تحليلات موثوقة للتهديدات وتدريب شامل على الأمن الإلكتروني الصناعي

الخبرة
مجموعة كاملة من الخدمات المهنية للأمن الإلكتروني الصناعي الشامل



Kaspersky OT CyberSecurity

تقارب تكنولوجيا المعلومات والتكنولوجيا التشغيلية

Kaspersky Extended Detection and Response

Kaspersky IoT Secure Gateway

Kaspersky SD-WAN

Kaspersky Industrial CyberSecurity

للعُقد
حماية نقطة النهاية واكتشافها والاستجابة لها

للشبكات
تحليل حركة استخدام الشبكة واكتشافها والاستجابة لها

KICS XDR

4 Industry 4.0 & IIoT

3 IT systems

2 Monitoring & Control

1 Automation & Protection

0 Technological process

Kaspersky Secure Remote Workspace

Kaspersky Machine Learning for Anomaly Detection

Kaspersky Antidrone

Kaspersky Automotive Secure Gateway

الخبرة

الاكتشاف	الخدمة المدارة	الاستجابة
تقييم أمن نظام التحكم الصناعي (ICS) من Kaspersky	Kaspersky Incident Response	Kaspersky Managed Detection and Response

المعرفة

النظافة الإلكترونية	المعلومات المتعلقة	التدريب
Kaspersky Security Awareness	معلومات التهديدات لأنظمة التحكم الصناعية (ICS) من Kaspersky	تدريبات خبراء فريق Kaspersky ICS CERT

تفضل بزيارة موقع الويب

Kaspersky Industrial CyberSecurity

XDR

التكنولوجيا

منصة XDR الأصلية لحماية أنظمة الأتمتة

- تكتشف التهديدات الخفية والحالات الشاذة والثغرات الأمنية ومحاولات التسلل قبل وقت طويل من أن تصبح خطيرة على عملياتك
- معتمدة من قبل بائعي الأتمتة والجهات التنظيمية
- لا يوجد تأثير سلبي على العمليات التقنية. يمنع الضرر غير المقبول
- تُسهل إدارة البنية التحتية المعقدة والموزعة للأتمتة والاستجابة للحوادث
- تساعد في تخفيف المخاطر والاحتفاظ بسجل للانتهاكات

مميزات منصة XDR

تغطية شاملة لأنظمة الأتمتة والتحكم الصناعي (IACS). حماية أجهزة الكمبيوتر التي تعمل بنظام Linux أو Windows أو أجهزة الكمبيوتر المعزولة أو التابعة لجهات خارجية، بالإضافة إلى اكتشاف الحالات الشاذة والتهديدات في الشبكة.

التدقيق الأمني النشط و/أو السلبي لنقاط النهاية والشبكات. الإدارة المركزية للمخاطر وسياسة الأمان والأصول على جميع مستويات أنظمة الأتمتة والتحكم الصناعي (IACS).

أنظمة متميزة ورؤية الشبكة. التحقيق وإعادة بناء سلسلة التدمير بأكملها. التصوير المرئي لتطور الحادث عبر الشبكات الصناعية والعُقد المختلفة.

الشراء من شريك | طلب عرض توضيحي | صفحة البيانات

ics.kaspersky.com

تفضل بزيارة موقع الويب

Kaspersky Extended Detection and Response

التكنولوجيا

الأمن الإلكتروني الموحد عبر القطاعات الصناعية والشركات في مؤسستك

من خلال التكامل الوثيق مع Kaspersky Extended Detection & Response، تتيح منصة Kaspersky Industrial CyberSecurity سيناريوهات جديدة تتضمن تفاعلات مع حلول الجهات الخارجية، مع إمكانات تحقيق واستجابة محسنة. وتساعد المنصة أيضًا على حماية أعمالك ليس فقط في البيئات الصناعية، لكن أيضًا في الأماكن التي تتداخل فيها البيئات الصناعية وبيئات الشركات. وقد تحقق ذلك بفضل التنسيق الوثيق مع مجموعة الأمن الإلكتروني لتكنولوجيا المعلومات الأفضل في فئتها من Kaspersky.

بهذه الطريقة، تستطيع فرق الأمان تكوين صورة شاملة لتطور الحادث وتحديد أسبابه الجذرية لمنع وقوع حوادث مماثلة في المستقبل.

أمثلة الاستجابة مع KICS:

- ✔ تغيير تصريح العقدة
- ✔ عزل العقدة والعملية
- ✔ الفحص لمكافحة الفيروسات وتحديث قواعد بيانات مكافحة الفيروسات
- ✔ تشغيل المهام

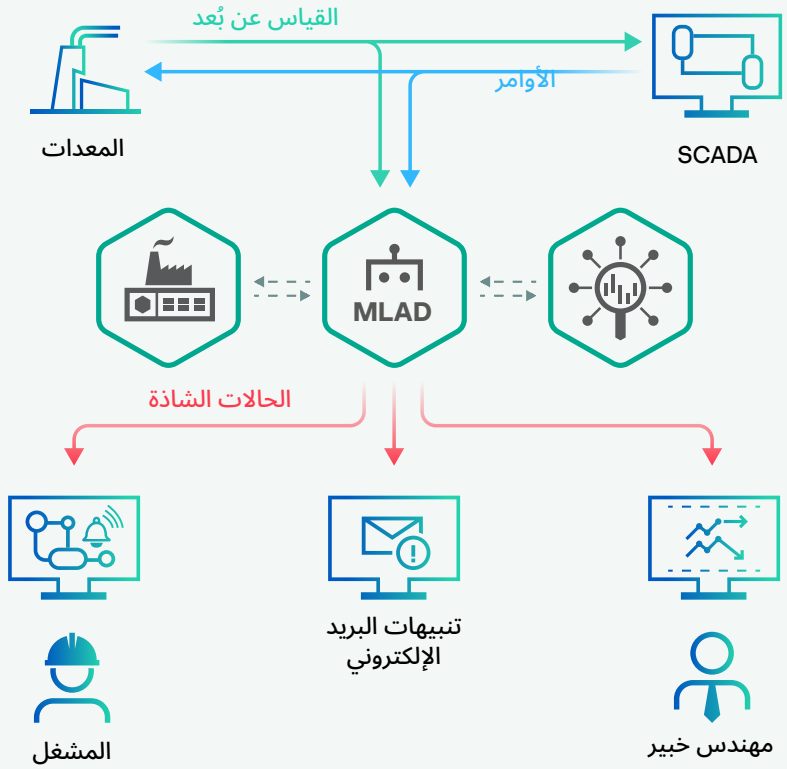
اتصل بنا صفحة البيانات

تفضل بزيارة موقع الويب

MLAD

Kaspersky
Machine learning
for Anomaly Detection

التكنولوجيا



الاكتشاف المبكر للحالات الشاذة والتحليلات التنبؤية

- يكتشف أخطاء المعدات والأخطاء البشرية قبل أن تصبح خطيرة بوقت طويل، مما يساعد على منع الفشل والحوادث
- يحدد إجراءات الموظف غير المعتادة أو عمليات المعدات كعلامات على هجوم أو تخريب متخصص
- يجمع بين اكتشاف الحالات الشاذة والتحليل التنبؤي لحالة المعدات ودورة حياتها

النظام البيئي والذكاء الاصطناعي

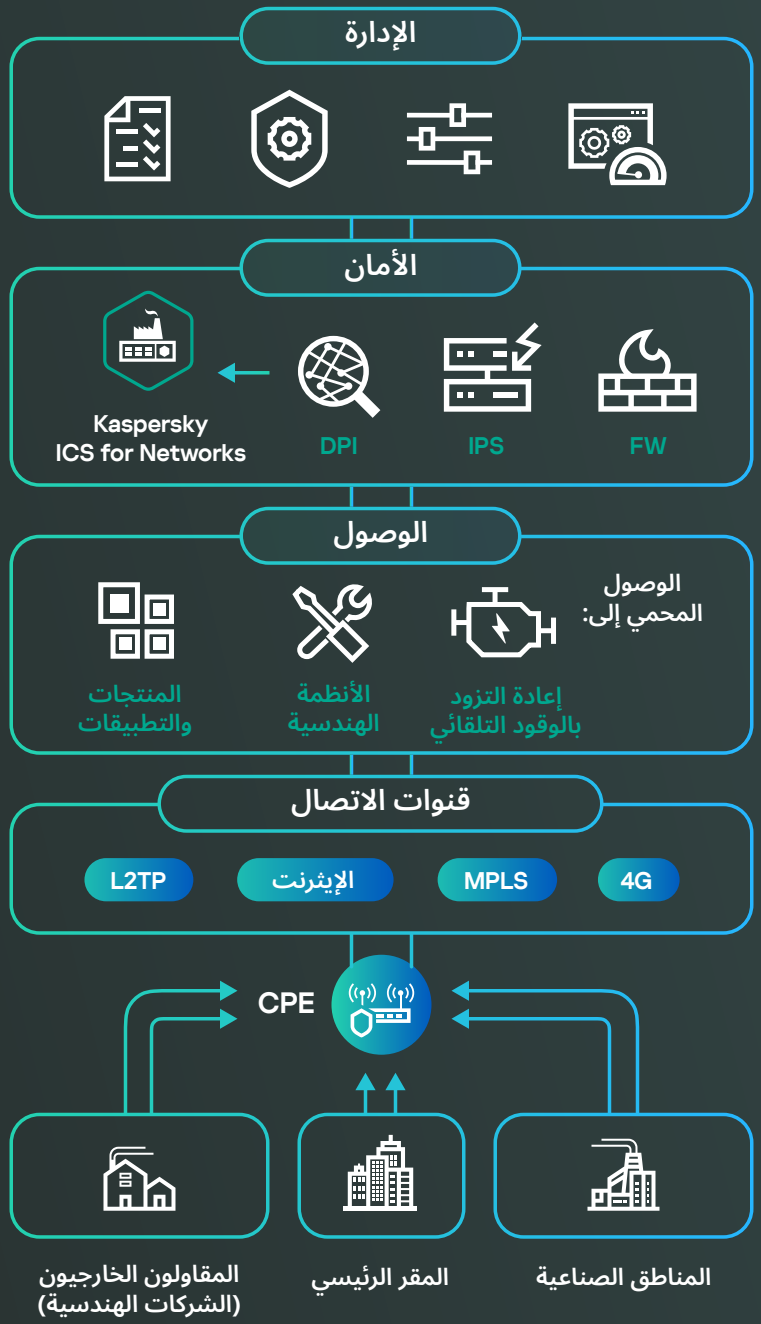
التكامل مع KICS for Networks وKUMA: يتلقى القياس عن بعد والأحداث من هذه الأنظمة ويرسل تنبيهات عن الحالات الشاذة المكتشفة

يطبق قواعد التشخيص على الأعراض المحددة مسبقًا للمشكلة، والتعلم الآلي لاكتشاف أي انحرافات عن سلوك المعدات العادي

يستخدم الذكاء الاصطناعي لتحليل القياس عن بُعد للعملية والأحداث المتعلقة بإجراءات الموظف

mlad.kaspersky.com

عملية التنفيذ دراسات الحالات اتصل بنا



تفضل بزيارة
موقع الويب

SD-WAN

Kaspersky SD-WAN

التكنولوجيا

ميزات Kaspersky SD-WAN:

- قابلية توسّع سهلة
- إدارة سهلة
- تحسين التكلفة
- أمان مركزي

حل واحد للشبكات الصناعية الموثوقة

يتيح Kaspersky SD-WAN للمؤسسات إنشاء شبكة قادرة على العمل في وجود أخطاء وموزعة جغرافيًا مع إدارة مركزية، بينما يضمن استمرارية عمليات الإنتاج. وتسمح لك بنية Kaspersky SD-WAN بدمج أدوات أمان Kaspersky وأدوات الجهات الخارجية بسهولة من خلال مدير وظائف الشبكة الافتراضية (VNFs).

باستخدام البنية التحتية للشبكة واسعة النطاق المحددة بالبرمجيات (SD-WAN) مع Kaspersky ICS for Networks، يمكنك تنظيم نظام مراقبة وحماية مركزي للعديد من المواقع الصناعية الموزعة.

اتصل بنا

تفضل بزيارة موقع الويب

Kaspersky Antidrone

التكنولوجيا

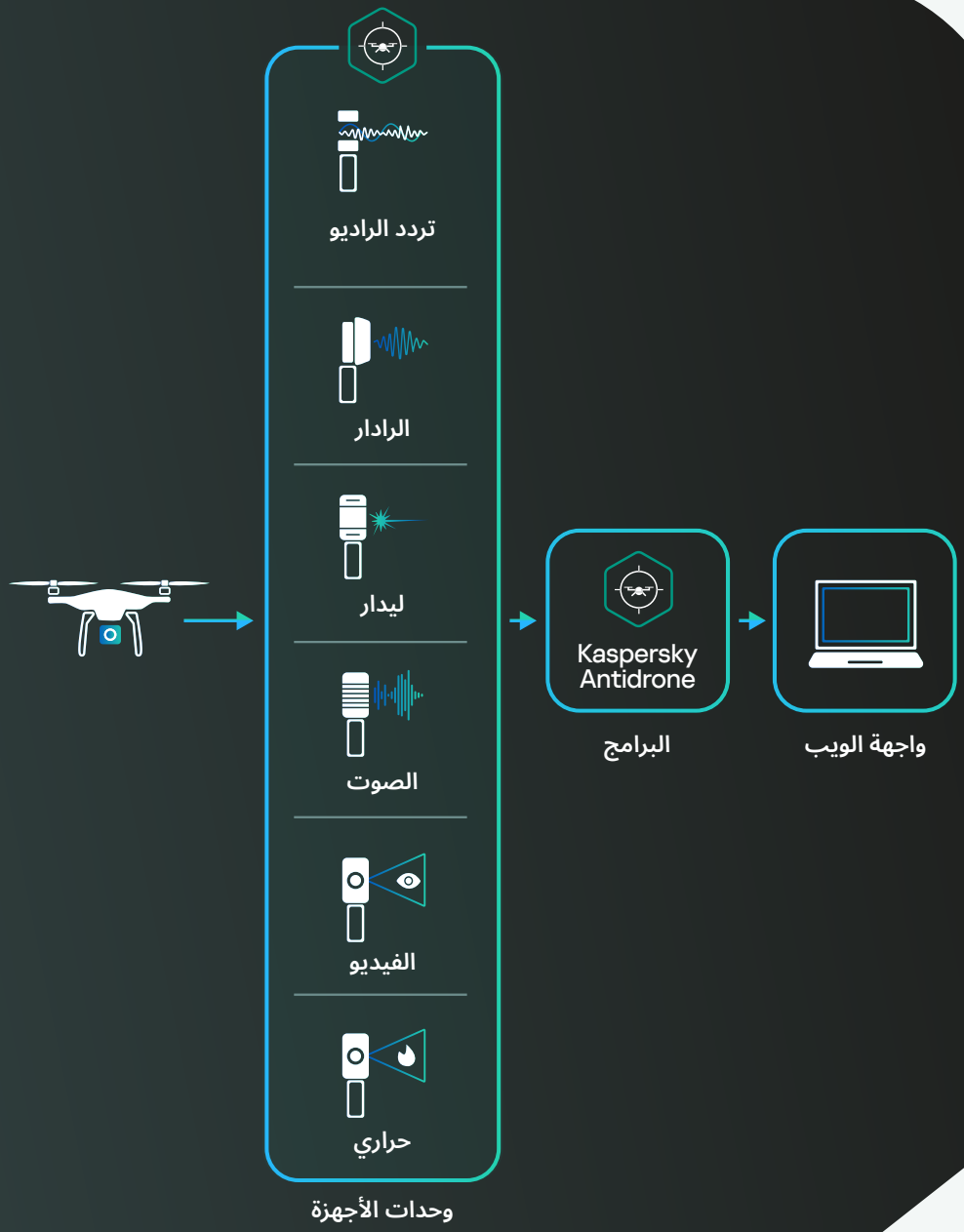
الميزات الرئيسية

- اكتشاف وتتبع الطائرات بدون طيار
- تصنيف الطائرات بدون طيار باستخدام الشبكات العصبية
- التشويش الاتجاهي ومتعدد الاتجاهات

مراقبة الطائرات بدون طيار وحل الدفاع

يقلل حل Kaspersky Antidrone من احتمالية توقف العمليات في المؤسسات الصناعية عن طريق منع الطائرات بدون طيار غير المصرح بها من دخول أراضيها. يفحص النظام تلقائيًا المجال الجوي ويكتشف الطائرات بدون طيار ويصنفها. ويتم عرض المعلومات حول ما يحدث في واجهة الويب. وفي حالة وجود تهديد، ومع الأذونات المناسبة، يستطيع المشغل تحييد الطائرة بدون طيار.

يعتبر حل Kaspersky Antidrone معياريًا ويمكن تطبيقه على المواقع الصناعية من أي حجم. ويدعم الحل أيضًا وضع التشغيل "صديق أو عدو"، مما يسمح للعملاء باستخدام طائراتهم بدون طيار وتجنب التدخل من خلال المركبات الجوية غير المشروعة وغير المأهولة.



طلب عرض توضيحي

صفحة البيانات

antidrone.kaspersky.com

تفضل بزيارة موقع الويب

Kaspersky IoT Secure Gateway

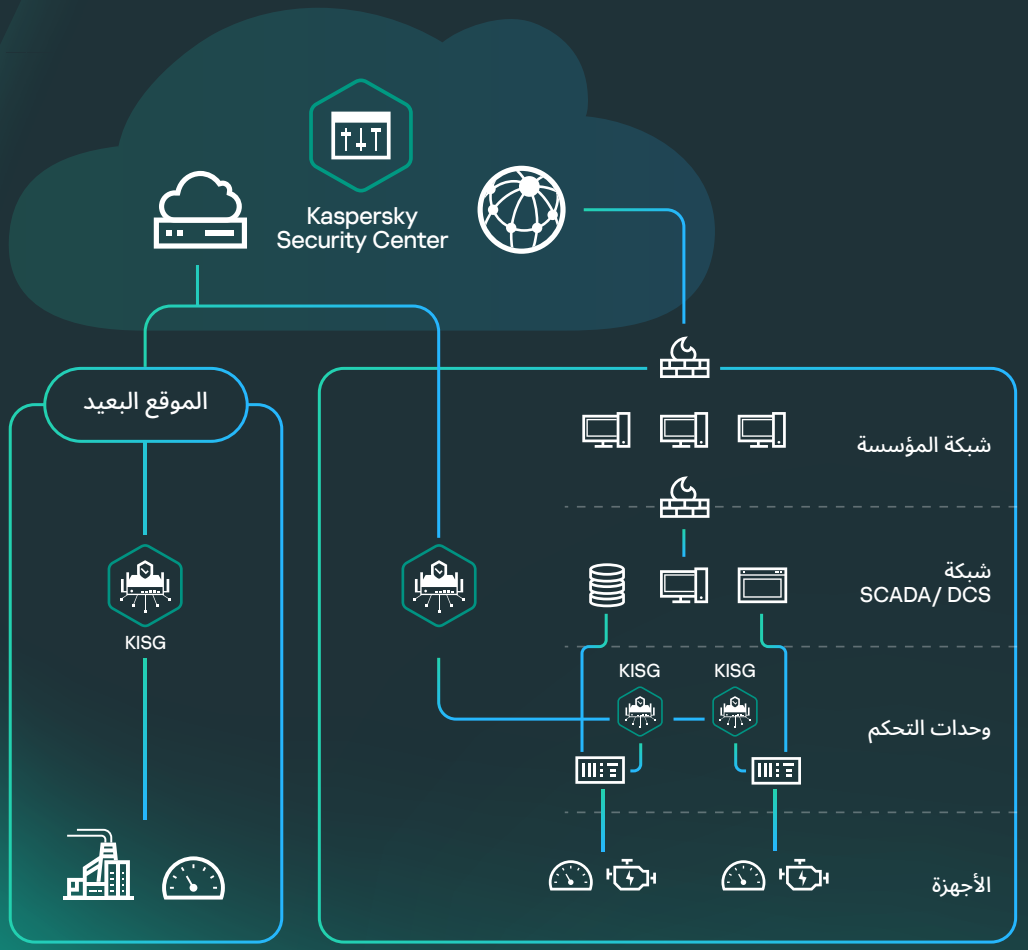
التكنولوجيا

الميزات الرئيسية

- جمع البيانات ونقلها بشكل آمن من أجهزة إنترنت الأشياء إلى المنصات الرقمية والسحابية
- يوفر Kaspersky Cyber Immunity المبني على نظام التشغيل KasperskyOS المقاومة "الأساسية" للغالبية العظمى من أنواع الهجمات الإلكترونية دون أدوات أمان إضافية
- شفافية البنية التحتية، وإدارة الأحداث المركزية، وتحسين الإنتاج

البيانات الموثوقة لتطوير الأعمال في الصناعة 4.0

يتكون الحل من أداة Kaspersky IoT Secure Gateways المستندة إلى KasperskyOS ووحدة تحكم الإدارة Kaspersky Security Center (KSC)). وتجمع البوابات البيانات وتنقلها بشكل آمن من المعدات إلى المنصات الرقمية والسحابية، مما يوفر معلومات أعمال عالية الجودة لتحسين الإنتاج ومنع الحوادث. وتتيح وحدة التحكم رسم خرائط للأحداث من مصادر مختلفة وإدارة ما يصل إلى 100,000 محطة عمل فعلية وافتراضية وسحابية.



aprotech

تتولى شركة Adaptive Production Technologies LLC (Aprotech)، إحدى الشركات التابعة لشركة Kaspersky) التطوير الفني والتجاري لهذا الحل.

اتصل بنا | طلب عرض توضيحي | صفحة البيانات

تفضل بزيارة
موقع الويب

Kaspersky
Secure Remote
Workspace

التكنولوجيا

تطبيق المنتج

المخاطر

محطات عمل المستخدمين من بين الأهداف الأكثر شيوعًا للهجمات الإلكترونية

الحل

يُعد Kaspersky Secure Remote Workspace (KSRW)) حلاً لإنشاء بنية تحتية مُدارة ووظيفية للعملاء رفيعي المستوى استنادًا إلى نظام التشغيل KasperskyOS ذي النواة الدقيقة الخاص بشركة Kaspersky.

البنية التحتية لحل
Cyber Immune Thin Client

يوفر Cyber Immune Thin Client، كجزء من Kaspersky Secure Remote Workspace، اتصالاً آمنًا بأجهزة سطح المكتب الافتراضية، بما في ذلك منطقة موثوقة لربط المستخدمين بالبنية التحتية الصناعية.

نظرة عامة على الحل طلب عرض توضيحي صفحة البيانات

تفضل بزيارة موقع الويب

Kaspersky Automotive Secure Gateway

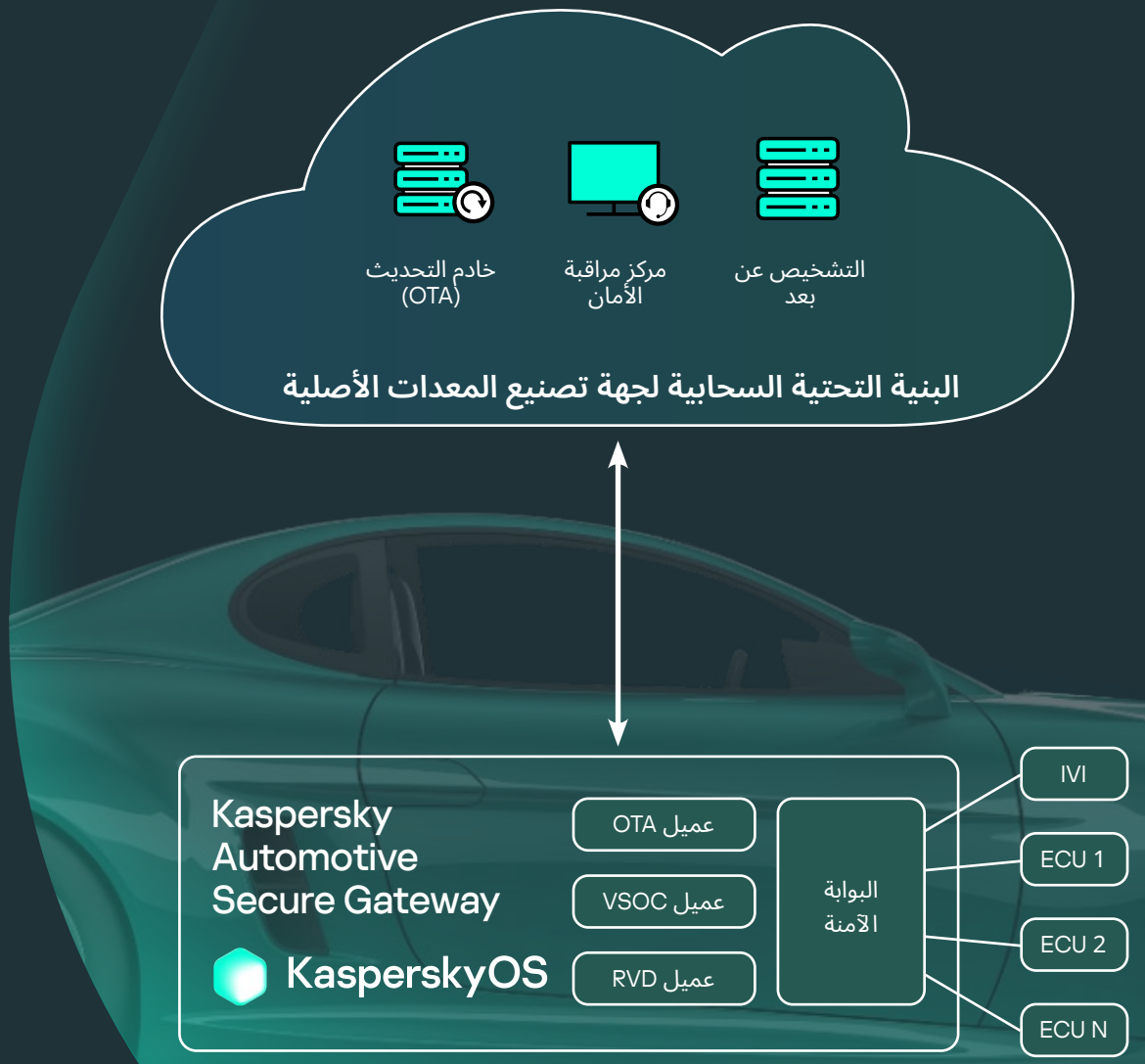
التكنولوجيا

حماية المركبات

- الوصول غير المصرح به
- الهجمات التي تستهدف وحدة التحكم الإلكترونية
- الهجمات عبر أنظمة المعلومات والترفيه في المركبات (IVI)
- تشخيص البرامج الخبيثة
- اختراق نظام التحديث
- الاتصالات وتدفقات البيانات غير الخاضعة للتحكم، وانقطاع الاتصالات

الفوائد الرئيسية

- حل آمن حسب التصميم
- يساعد على الامتثال للوائح الأمن الإلكتروني
- 4 في 1: بوابة متصلة، وبوابة أمان، وOTA-Master، وعميل VSOC
- التوافق مع ISO21434 وISO26262 وAUTOSAR Adaptive وUptane



AUTOSAR

صفحة البيانات اتصل بنا

تفضل بزيارة موقع الويب

المعرفة

فهم عميق لتهديدات الأمن الإلكتروني الصناعي والثغرات الأمنية لتقييم المخاطر بكفاءة، والاكتشاف الناجح للهجمات، والتحقيق في الحوادث، والاستجابة لها.

بدعم من الخبرة والتجربة التي لا تضاهى التي يتمتع بها فريق الاستجابة للطوارئ الإلكترونية لأنظمة التحكم الصناعية في Kaspersky، وهو أول فريق خاص للاستجابة للطوارئ الإلكترونية في مجال الأمن الإلكتروني الصناعي.

الميزات الرئيسية

- الاكتشاف السريع للتهديدات والقدرات التحليلية واسعة النطاق
- يزيد من فعالية التحقيقات وعمليات البحث عن التهديدات النشطة
- معلومات شاملة عن التهديدات والثغرات الأمنية لاتخاذ قرارات مستنيرة

تفوق على منافسيك من خلال الرؤية المتعمقة للتهديدات الإلكترونية التي تستهدف مؤسستك

المعلومات المتعلقة بالتهديدات
تدفقات البيانات التلقائية

موجزات بيانات تهديدات أنظمة التحكم الصناعية من Kaspersky

مجموعة من موجزات بيانات معلومات التهديدات التي يتم تحديثها بانتظام والمصممة خصيصًا لتلبية الاحتياجات المحددة للأمن الإلكتروني الصناعي

خدمة إعداد تقارير المعلومات المتعلقة بالتهديدات في أنظمة التحكم الصناعية (ICS) من Kaspersky

يوفر وعيًا أكبر بالحملات الضارة التي تستهدف المؤسسات الصناعية بالإضافة إلى معلومات عن الثغرات الأمنية الموجودة في أنظمة التحكم الصناعي الأكثر شيوعًا

Kaspersky Ask the Analyst

خدمة للعملاء لطلب توجيهات الخبراء والرؤى عن التهديدات المحددة التي يواجهونها أو يهتمون بها.

طلب عرض توضيحي نظرة عامة على الحل اتصل بنا

توفر خدمة موجز بيانات التهديدات من Kaspersky معلومات عن التهديدات في الوقت الحقيقي لمساعدة المؤسسات الصناعية على حماية شبكاتها وأنظمتها من التهديدات الإلكترونية. وتتضمن موجزات البيانات معلومات عن البرامج الضارة المعروفة، ومواقع ويب التصيد الاحتيالي، وأحدث الثغرات الأمنية وفيروسات الاستغلال، وأنواع أخرى من التهديدات الإلكترونية. وعند وضع هذه البيانات في سياق، يمكنها بسهولة أكبر كشف الصورة الأكبر واستخدامها للإجابة عن أسئلة من وماذا وأين ومتى التي تؤدي إلى التعرف على خصومك، وتجعلك تتخذ قرارات وإجراءات سريعة.

ما الذي تحصل عليه:

موجز بيانات تجزئات أنظمة التحكم الصناعية من Kaspersky

معلومات التهديدات الحديثة لأنظمة التحكم الصناعي والأنظمة الأخرى المستخدمة في التكنولوجيا التشغيلية لتبسيط وأتمتة اكتشاف الهجمات والتحقيق فيها في الوقت المناسب

#الوقاية

#الاكتشاف

#التحقيق

موجز بيانات الثغرات الأمنية في أنظمة التحكم الصناعية من Kaspersky

يتم اكتشاف البيانات التي يتم التحقق منها وتنقيحها عن الثغرات الأمنية في البرامج والأجهزة الخاصة بأنظمة التحكم الصناعي والأنظمة الأخرى المستخدمة في البيئات الصناعية، ويتم توفيرها بتنسيق يمكن قراءته آليًا

#الوقاية

#الاكتشاف

#التحقيق

موجز بيانات الثغرات الأمنية في أنظمة التحكم الصناعية بتنسيق OVAL

موجز يتم تحديثه بانتظام ويحتوي على تعريفات بلغة OVAL للاكتشاف الآلي للثغرات الأمنية المعروفة في أنظمة SCADA والبرامج الصناعية الأخرى

#الاكتشاف

اتصل بنا

المزيد من المعلومات عن الخدمة

تفضل بزيارة موقع الويب

Kaspersky ICS Threat Intelligence Reporting

المعرفة

توفر خدمة إعداد تقارير المعلومات المتعلقة بالتهديدات عن أنظمة التحكم الصناعية (ICS) من Kaspersky معلومات تفصيلية ووعيًا أكبر عن الحملات الضارة التي تستهدف المؤسسات الصناعية، وكذلك معلومات عن نقاط الضعف التي يتم العثور عليها في أنظمة التحكم الصناعية الشائعة والتقنيات المستخدمة فيها. وتساعد المعلومات التفصيلية المصممة خصيصًا للمؤسسات الصناعية العملاء على حماية الأصول المهمة، بما في ذلك مكونات البرامج والأجهزة وضمان سلامة واستمرارية العملية التقنية.

يتم تسليم التقارير عبر **Kaspersky Threat Intelligence Portal** أو يمكن الوصول إليها عبر واجهة برمجة التطبيقات (API).

ما الذي تحصل عليه:

تقارير التهديدات المستمرة المتقدمة

تقارير عن التهديدات المستمرة المتقدمة الجديدة وحملات التهديدات الكبيرة التي تستهدف المؤسسات الصناعية وتحديثات عن التهديدات النشطة.

بيئة التهديدات

تقارير عن التغييرات الكبيرة في عالم التهديدات لأنظمة تحكم الأفراد والعوامل القوية المكتشفة حديثًا وتؤثر على مستويات أمان أنظمة التحكم الصناعية وتعرض أنظمة التحكم الصناعية للتهديدات، ويشمل ذلك معلومات إقليمية وخاصة بكل بلد وصناعة.

الثغرات الأمنية التي تم العثور عليها

تقارير عن الثغرات الأمنية التي اكتشفتها Kaspersky في معظم المنتجات الشائعة المستخدمة في أنظمة التحكم المستمرة وإنترنت الأشياء في مجال الصناعة والبنى التحتية في مختلف الصناعات.

تحليل الثغرات الأمنية والحد منها

توفر التحذيرات التي نصدرها توصيات قابلة للتطبيق من خبراء Kaspersky للمساعدة على تحديد التهديدات والحد منها.

اتصل بنا

المزيد من المعلومات عن الخدمة

ما الذي تحصل عليه:

يكمل حل Kaspersky Ask The Analyst مجموعة Kaspersky Threat Intelligence الخاصة بنا. وعن طريق هذه الخدمة، يمكنك الاتصال بالخبراء للحصول على الدعم والمعلومات المفيدة عن التهديدات والثغرات الأمنية المحددة التي تواجهها أو تهتم بها. وباستخدام هذه البيانات، يمكنك تحسين دفاعاتك ضد التهديدات التي تستهدف مؤسستك ككل والبنية التحتية الصناعية الخاصة بك.

الفوائد الرئيسية

تعليمات تفصيلية من خبرائنا حول كيفية الاستجابة بسرعة للتهديدات والثغرات الأمنية

معلومات سياقية شخصية ومفصلة لإجراء تحقيقات فعالة

الوصول إلى كبار خبراء معلومات التهديدات، بما في ذلك خبراء الأمن الصناعي من فريق Kaspersky ICS CERT

اتصل بنا

المزيد من المعلومات عن الخدمة

***معلومات إضافية عن التقارير المنشورة:**

- معلومات عن الثغرات الأمنية في نظام التحكم الصناعي
- إحصائيات التهديدات الموجهة لنظام التحكم في العمليات والاتجاهات الجديدة حسب المنطقة والصناعة
- تحليل البرامج الضارة التي تستهدف نظام التحكم الصناعي
- المعلومات المتعلقة بالمتطلبات والمعايير التنظيمية

تفضل بزيارة موقع الويب

Kaspersky
Security Awareness

المعرفة

زيادة المعرفة الإلكترونية للموظفين

- مواد تدريبية تزود موظفيك بالمعرفة اللازمة عن أهم جوانب الأمن الإلكتروني الصناعي، مما يزيد من مستوى الوعي على جميع مستويات المؤسسة
- محاكاة الحماية التفاعلية من Kaspersky - تدريب قائم على الألعاب من خلال عمليات محاكاة الأعمال التي تتضمن عددًا كبيرًا من السيناريوهات عبر مختلف الصناعات: الطاقة الحرارية، والطاقة الكهرومائية، والنفط والغاز، والبتروكيماويات، والمنشآت البترولية، وما إلى ذلك.
- Kaspersky Automated Security Awareness Platform (ASAP) — وحدات تعليمية تفاعلية ومحاكاة لهجمات التصيد الاحتيالي مصممة لتعزيز السلوك الآمن على الإنترنت

المواضيع الرئيسية التي تم تناولها

- البريد الإلكتروني
- مواقع الويب والإنترنت
- كلمات المرور والحسابات
- وسائل التواصل الاجتماعي وبرامج المراسلة
- الأمن الإلكتروني الصناعي
- أمان الكمبيوتر الشخصي
- الأجهزة المحمولة
- البيانات السرية
- أمان البطاقات البنكية ومعيار أمان بيانات صناعة بطاقات الدفع (PCI DSS)
- التوجيه العام لحماية البيانات

[اتصل بنا](#) [جرّبه الآن](#) [كتالوج التدريب](#)

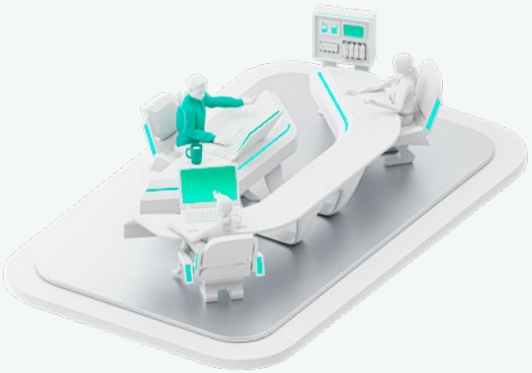
تفضل بزيارة موقع الويب

Kaspersky
ICS CERT
Expert Trainings

المعرفة

التعلم التطبيقي

تم تصميم برنامجنا التدريبي على نظام التحكم النصاعي خصيصًا للتأكد من أن متخصصي تكنولوجيا المعلومات (IT)، وتكنولوجيا العمليات (OT)، وأمان المعلومات (IS)، بالإضافة إلى المديرين والموظفين الآخرين، يمكنهم توسيع معرفتهم بالأمن الإلكتروني الصناعي واكتساب مهارات عملية متخصصة.



المهارات العملية من خبراء Kaspersky

- التحاليل الرقمية والاستجابة للحوادث
- استكشاف الثغرات الأمنية في أجهزة التكنولوجيا التشغيلية / إنترنت الأشياء والبرامج الصناعية
- برامج تدريبية متعددة الوظائف لخبراء تكنولوجيا المعلومات والتكنولوجيا التشغيلية ونظم المعلومات

[اتصل بنا](#) [كتالوج التدريب](#)

تفضل بزيارة موقع الويب

Kaspersky ICS Security Assessment

الخبرة

تحليل أمان بنيتك التحتية الصناعية

نهج شامل لتحديد الثغرات الأمنية ونقاط الضعف الأمنية في البنى التحتية الصناعية، بما في ذلك:

- سطح الهجوم
- مستوى أمان البنية التحتية للشبكة الصناعية ونظام التحكم بالتوزيع والأجهزة الصناعية
- مخاطر اختراق الأنظمة الحرجة

فحص المكونات الهامة

- حركة مرور الشبكة، بما في ذلك البروتوكولات الصناعية
- مكونات التحكم في العمليات: SCADA، وحدة التحكم المنطقية القابلة للبرمجة، العدادات الذكية، وما إلى ذلك.
- العناصر المادية لنظام التحكم الآلي في العمليات
- بنية الشبكة، بما في ذلك شبكات ACS

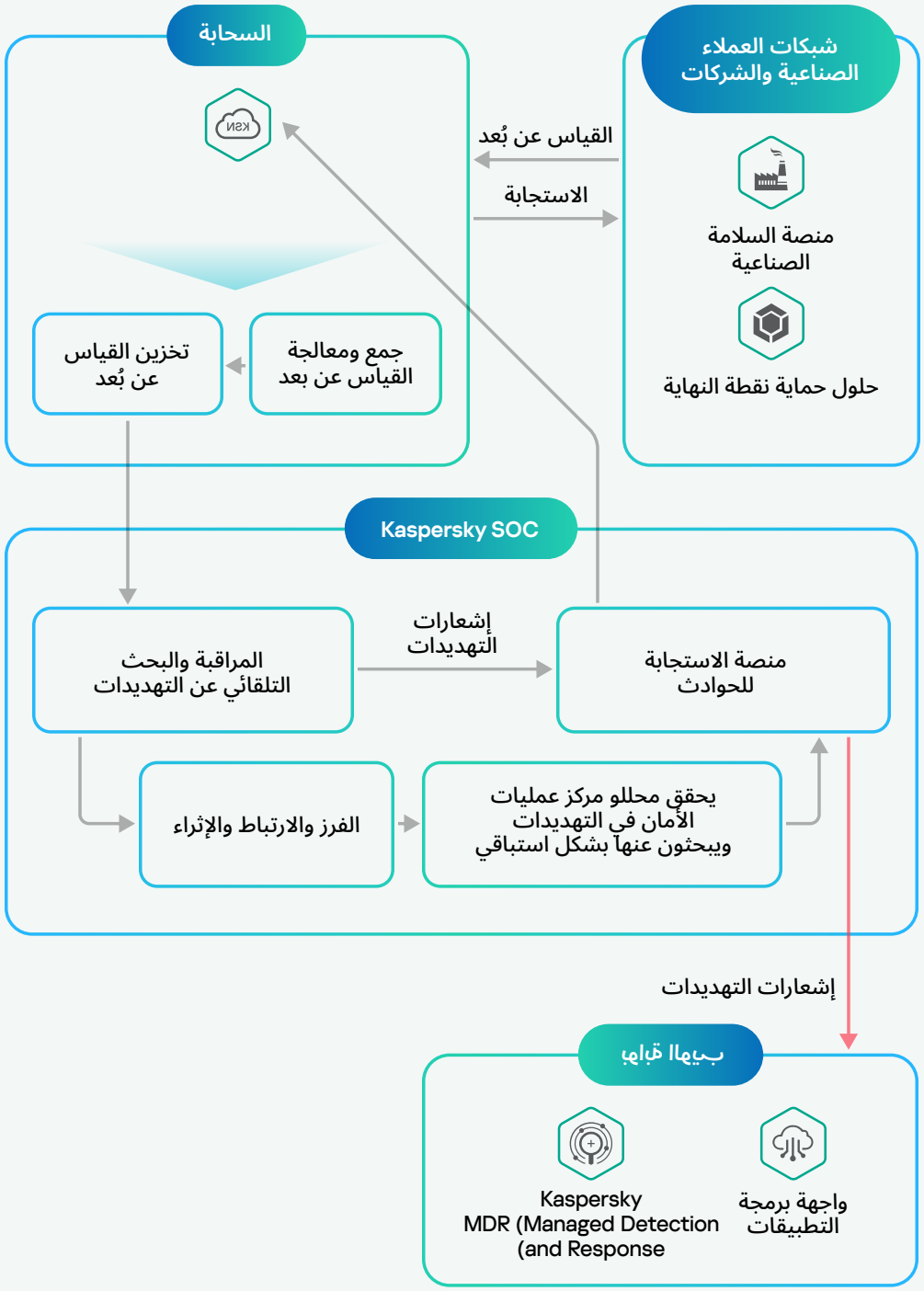
اتصل بنا

المزيد من المعلومات عن الخدمة

تفضل بزيارة موقع الويب

Kaspersky Managed Detection and Response

الخبرة



الميزات الرئيسية

- الاكتشاف الاستباقي للتهديدات: تساعد مؤشرات الهجوم الحاصلة على براءة اختراع في تتبع التهديدات غير المكتشفة داخل نظام التحكم
- الاستجابة الآلية والموجهة (مع توفر التحقيق الجنائي الكامل وتحليل البرامج الضارة عند الطلب)
- خبرة الأمن الإلكتروني لنظام التحكم الصناعي: مدعومة بواحد من أكثر فرق اكتشاف التهديدات الاستباقية نجاحًا وخبرة في الصناعة

ما الذي تحصل عليه:

- المطاردة المستمرة والاكتشاف والقضاء على التهديدات التي تستهدف مؤسستك الصناعية
- خفض تكاليف الأمان من خلال القضاء على الحاجة إلى توظيف خبراء جدد في مجال الأمن الإلكتروني
- جميع المزايا الرئيسية لمركز عمليات الأمان، دون الحاجة إلى إنشاء مركز داخل الشركة

ينتمي 25% من عملائنا المحميين إلى القطاع الصناعي

انظر تقرير MDR لمعرفة المزيد

اتصل بنا المزيد من المعلومات عن الخدمة

تفضل بزيارة موقع الويب

Kaspersky Incident Response

الخبرة

الاستجابة للحوادث

المخاطر

ثغرة أمنية واحدة تكفي لمجرمي الإنترنت للسيطرة على الأنظمة الصناعية بأكملها

الحل

- القضاء السريع على عواقب أي حادث من قبل فريق الاستجابة للطوارئ العالمي في Kaspersky
- تحليل أسباب ومصادر وعواقب الحادث
- عرض تفصيلي للبرامج الضارة المستخدمة
- دعم إضافي من فريق Kaspersky ICS-CERT

تكوين الخدمة

الاستجابة للحوادث:
التحقيق في التهديدات والقضاء عليها

التحليل الرقمي:
تحليل الأدلة الرقمية

تحليل البرامج الضارة:
احصل على عرض تفصيلي للملفات المستخدمة في الهجوم

[اطلب دليل الاستجابة للحوادث من فريق Kaspersky ICS-CERT]

[معرفة المزيد]

[اتصل بنا]

اكتشف اتجاهات علاقات المستثمرين في أبحاث فريق Kaspersky (Global Emergency Response Team (GERT.

الشريك الذي يمكنك الوثوق به

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

المزيد عن النظام البيئي للتكنولوجيا التشغيلية
المزيد عن النظام البيئي لتكنولوجيا المعلومات
اتصل بنا