Une plateforme de détection et de réponse étendue (XDR) pour la sécurité globale des entreprises industrielles.

Kaspersky Industrial CyberSecurity

kaspersky bring on the future

Attaque de programmes malveillants

Au premier trimestre 2024, trente incidents de cybersécurité au total ont été confirmés publiquement par les organisations touchées ou les responsables, le secteur manufacturier représentant 64,5 % de ces incidents.

Kaspersky ICS CERT, Juin 2024

En savoir plus

Paysage des menaces industrielles

La nouvelle réalité pour les propriétaires et les exploitants d'infrastructures industrielles est façonnée par des facteurs tels que l'intérêt croissant des hacktivistes pour les systèmes d'automatisation, les exigences réglementaires élevées, la convergence IT-OT et l'augmentation de la variété des cyberattaques dans le secteur industriel (au premier trimestre 2024, les solutions de Kaspersky ont bloqué des programmes malveillants de 10 865 familles différentes sur des systèmes d'automatisation industrielle).

La prolifération des technologies numériques, qui est généralement considérée comme une bonne chose, efface le fossé entre les environnements informatiques et techniques qui protégeait ces derniers des cybercriminels. Alors qu'une simple clé USB introduite dans l'environnement ICS peut sérieusement affecter les activités principales d'une entreprise, un groupe de pirates motivés peut pénétrer dans les réseaux OT, causer des dommages considérables et/ou voler des informations précieuses. Si l'on ajoute à cela l'évolution des normes d'automatisation, qui passent de simples recommandations à des exigences législatives, et la nécessité croissante de partager les meilleures pratiques et de gérer les risques, la cybersécurité des entreprises industrielles devient un formidable défi.

Kaspersky ICS CERT s'attend à ce que les organisations industries suivantes soient confrontées à des cyberattaques de plus en plus fréquentes :

Pétrole, gaz et produits chimiques

La numérisation de l'exploration, de l'extraction, du transport et du raffinage, un facteur concurrentiel clé pour ces entreprises, implique l'intégration de l'IIoT, des drones et des robots, le déploiement de la 5G, de la blockchain et des solutions de RV, ce qui élargit le paysage des actions malveillantes.

Fabrication de produits essentiels

Soucieuses d'améliorer leur rentabilité, ces entreprises déploient des technologies de pointe, développent la connectivité, exploitent le cloud et explorent des scénarios de convergence IT-OT, ce qui les expose de plus en plus à des menaces nouvelles et changeantes.

Minéraux, métaux et exploitation minière

Pierre angulaire d'une production manufacturière cruciale et d'importance nationale, cette industrie doit équilibrer ses dépenses tout en adoptant l'automatisation et les technologies numériques. Étant donné qu'elle intéresse à la fois les hacktivistes et les cyberattaquants de haut niveau, cette industrie ne peut pas faire de compromis en matière de cybersécurité.

Électricité, réseau et services publics

Les technologies numériques et émergentes sont indispensables pour favoriser la transition énergétique tout en préservant les infrastructures existantes, qui constituent toujours l'épine dorsale de la plupart des installations énergétiques. Pourtant, elles courent le plus grand risque et appellent des efforts supplémentaires en matière de cybersécurité.

Les attaques contre les systèmes industriels, en particulier les ICS et les SCADA, sont en augmentation. En attendant, les cybermenaces actuelles visant les environnements industriels semblent résister aux solutions conventionnelles. À ce titre, Kaspersky propose une approche globale pour ces industries. Sur notre site Internet, vous trouverez des témoignages de nos clients, des informations sur le paysage des menaces et des offres adaptées à des scénarios spécifiques.

Il n'a jamais été aussi important de choisir un partenaire en qui vous pouvez avoir confiance, qui maîtrise les liens entre la cybersécurité de l'industrie et celle des entreprises et qui est capable de fournir une gamme complète de technologies de pointe dans le domaine de la sécurité.

Voici les principales cibles des attaques APT :

Propriétaires et exploitants d'infrastructures critiques

Les organisations d'importance stratégique des secteurs du pétrole et du gaz, de la chimie, de l'énergie et des services publics sont confrontées à des conséquences potentielles très graves en cas d'interférence opérationnelle

Fabrication de produits essentiels

De la simple usine à l'échelle nationale ou internationale, ces entreprises, y compris celles des secteurs des métaux et des mines, de l'agriculture et de l'industrie manufacturière mondiale, s'engagent dans des opérations à haut risque impliquant des coûts d'incidents importants

Apprenez-en plus sur les attaques APT et financières contre les entreprises industrielles au cours du début de l'année 2024

En savoir plus

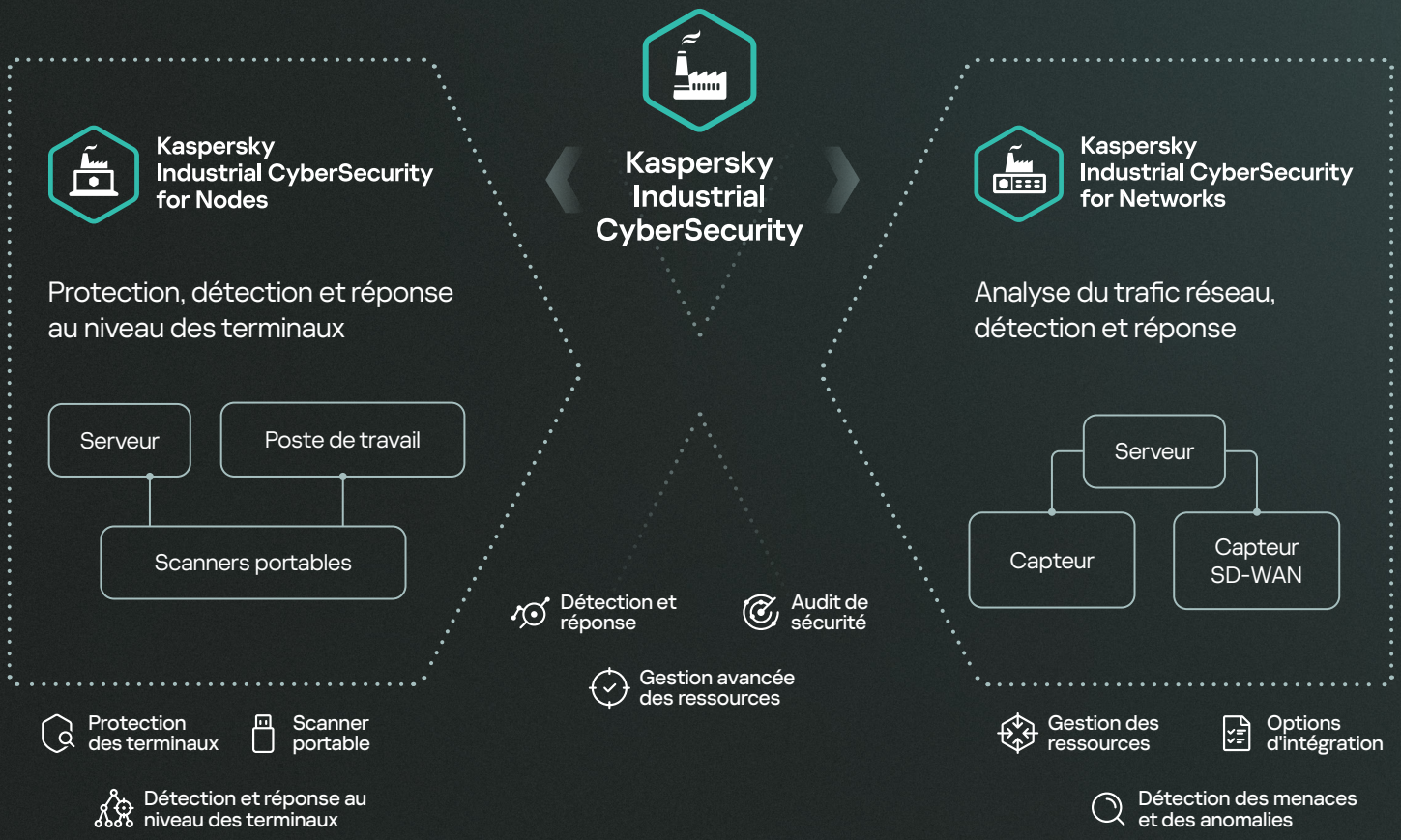
Technologies avancées de sécurité ICS

Dès lors que le fossé entre les environnements IT et OT, qui protégeait autrefois ces derniers des cybercriminels, devient de plus en plus étroit, il devient indispensable pour les propriétaires et les exploitants de systèmes cyberphysiques de disposer d'une solution de sécurité complète, de niveau entreprise et proposée par un seul fournisseur, afin de protéger les infrastructures critiques. **La plateforme XDR native de Kaspersky Industrial CyberSecurity (KICS)** comprenant les modules KICS for Networks et KICS for Nodes protège les systèmes et réseaux d'automatisation industrielle.

KICS for Networks est un produit d'analyse du trafic, de détection et de réponse qui assure la surveillance du réseau industriel, la détection des intrusions et la gestion des risques, tout en offrant une fonctionnalité d'audit centralisé des nœuds du réseau industriel afin de détecter les vulnérabilités et de vérifier la conformité aux normes de l'industrie.
KICS for Nodes offre une protection, une détection et une réponse de niveau industriel pour les terminaux, avec un audit de conformité basé sur OVAL*. Cette solution modulaire et peu encombrante est compatible avec Linux, Windows, les anciens systèmes, les systèmes autonomes et les contrôleurs programmables. La version du scanner portable protège les machines autonomes et les appareils de sous-traitants sans qu'il soit nécessaire de l'installer.

Combinés, ces composants forment la plateforme KICS XDR qui offre un inventaire centralisé des ressources, un système de gestion des risques et une fonction d'audit, permettant ainsi de faire évoluer la sécurité au sein d'une infrastructure diversifiée et distribuée via une plateforme unique avec un graphique complet des incidents, des analyses et bien plus.

La plateforme KICS XDR offre aux utilisateurs une vue d'ensemble et un contexte plus large : la chaîne des incidents au niveau du réseau et des terminaux, les paramètres précis des ressources, les cartes de communication et de topologie du réseau, même à partir de segments où la mise en miroir du trafic n'est pas encore disponible, et bien d'autres choses encore.



* Langage ouvert de vulnérabilité et d'évaluation (OVAL)

Points d'application de la plateforme

Convergence des environnements OT et IT

Environnement informatique

DMZ / GTW

Environnement OT

Kaspersky Industrial CyberSecurity for Nodes

- Poste de travail de l'opérateur
- Serveur SCADA
- Poste de travail de l'ingénieur
- Passerelle ICS

Équipement de réseau

SPAN

Kaspersky Industrial CyberSecurity for Networks

- Unité de contrôle de la baie (BCU)
- Appareil électronique intelligent (IED)
- Contrôleurs logiques programmables (PLC)
- Protection par relais et système de sécurité instrumenté (SIS)
- Nœuds isolés (vérification manuelle avec le scanner portable KICS)

Détection précoce des anomalies et analyse prédictive

Kaspersky Machine Learning for Anomaly Detection (Kaspersky MLAD) est un système innovant qui utilise un réseau neuronal pour surveiller simultanément un large éventail de données télémétriques. Il détecte les erreurs humaines et les défaillances des équipements, contribuant ainsi à prévenir les pannes et les accidents, il détecte les comportements d'employés ou les opérations d'équipement atypiques comme signes d'une attaque ciblée ou d'un sabotage, et il associe la détection d'anomalies à l'analyse prédictive de l'état des équipements et de leur cycle de vie.

En savoir plus

Niveau physique

Protégé par les produits Kaspersky

Kaspersky Industrial CyberSecurity for Networks

KICS for Networks

Solution de surveillance du réseau industriel et d'analyse du trafic. Permet une inspection approfondie des paquets (DPI) des protocoles industriels propriétaires. Livré sous forme de logiciel ou d'appliance virtuelle.

KICS for Networks identifie les anomalies et les intrusions dans l'ICS à un stade précoce, montre comment l'attaque se développe sur le réseau et dans les nœuds (chaîne d'élimination EDR et télémétrie), et veille à ce que les actions nécessaires soient prises pour éviter toute répercussion négative sur les processus industriels.

Gestion des ressources

Découverte des ressources
Découvrez mieux vos ressources grâce à une base de données des vulnérabilités, à la hiérarchisation des risques et au sondage actif sécurisé

Visibilité du réseau
Surveillez le trafic, créez des cartes topologiques et suivez l'état du réseau au fil du temps afin d'avoir une vue d'ensemble optimale

Outils d'analyse du trafic
Suivez et analysez les sessions réseau, en exportant et en stockant des données détaillées relatives au trafic

Avantages

- Spécialisé dans les applications et protocoles industriels. Prise en charge immédiate d'un large éventail de protocoles OT, d'appareils et d'attaques réseau + possibilité d'importation à partir de projets externes
- Règles prédéfinies pour la configuration de l'audit de sécurité
- Interface conviviale et rapports personnalisables
- Compréhension globale des risques dans toute l'infrastructure distribuée
- Collecte d'échantillons de trafic à partir de sources multiples : capteurs de réseau propres, capteurs SD-WAN, capteurs de terminaux et sondes portables

Écosystème et intégrations

Écosystème
Profitez des vastes possibilités de l'écosystème Kaspersky grâce à l'intégration des solutions suivantes et à notre approche unifiée de la cybersécurité, qui englobe divers produits :

- Kaspersky Next XDR Expert
En savoir plus

- Kaspersky IoT Secure Gateway (KISG)
En savoir plus

- Kaspersky Machine Learning for Anomaly Detection (MLAD)
En savoir plus

- Kaspersky SD-WAN (Software-Defined Wide Area Network)
En savoir plus

Gérez toutes les composantes de l'écosystème à l'aide d'une console unique

Intégrations tierces
Compatibilité transparente avec une multitude d'outils et de plateformes de sécurité externes

Détection des menaces et des anomalies

Détection d'intrusion
Détection par signature et moteur statistique qui détecte les tentatives de force brute ou d'analyse

Contrôle de l'intégrité du réseau
Le système analyse les interactions normales du réseau et signale tout écart

Détection des anomalies
Détecte les anomalies de base liées aux paquets et aux protocoles. Possibilité d'amélioration grâce à la MLAD

DPI des protocoles industriels
Maintient le processus et le contrôle de commande, et assure un suivi efficace des données télémétriques

Corrélation d'événements
Associe les événements de sécurité à la classification MITRE et à une chaîne d'exécution unique

Kaspersky Industrial CyberSecurity for Nodes

KICS for Nodes

Solution de protection, de détection et de réponse au niveau des terminaux, testée et certifiée, de qualité industrielle. Un produit à faible impact, compatible et stable pour Linux, Windows et les systèmes autonomes.

KICS for Nodes protège chaque terminal des systèmes d'automatisation numériques, gérés et distribués d'aujourd'hui. La solution collecte des données télémétriques pour créer une représentation visuelle claire et détaillée de l'évolution d'un incident sur les postes de travail, les serveurs, les passerelles et autres terminaux, ce qui permet de rassurer les administrateurs du système d'automatisation en leur indiquant qu'un incident a été entièrement traité et qu'il ne se reproduira plus.

Protection des terminaux

Prévention des menaces en temps réel
Analyses personnalisées et à la demande des disques amovibles et des zones critiques pour prévenir les exploits et protéger les fichiers

Contrôle de l'activité locale
Fonctions de contrôle des appareils et du Wi-Fi. Assurez l'intégrité du projet PLC pour favoriser la compréhension des activités locales

Contrôle de l'activité du réseau
Gérez les pare-feu de l'hôte et bloquez les sessions du réseau, afin de garantir la protection contre les menaces réseau

Surveillance du système
Vérifiez l'intégrité des fichiers, suivez l'accès au registre et détectez les menaces dans les journaux du système afin de préserver la sécurité du système d'exploitation

Détection et réponse au niveau des terminaux

Détection
Recherche d'indicateurs de compromission (IoC), fonctions complètes de surveillance et d'établissement de rapports

Réponse
Empêchez l'exécution, mettez en quarantaine/supprimez des fichiers, démarrez/arrêtez des processus, isolez des réseaux, et bien plus

- Nœuds Windows
- Scanner portable
- Nœuds Linux
- Agent d'audit

Scanner portable

Analyseur de programmes malveillants
Analyse anti-malware des équipements autonomes et de tous les ordinateurs utilisés sur le site industriel

Analyse OVAL
Appliquez votre stratégie de cybersécurité aux machines autonomes en procédant à des analyses manuelles de la vulnérabilité et au contrôle de la mise en conformité

Capture de paquets
Capturez et analysez le trafic réseau afin de mieux comprendre le fonctionnement des infrastructures isolées

Inventaire de base des ressources
Collectez des données complètes sur le matériel et les logiciels à l'aide d'une solution sans empreinte

Avantages

- Faible impact sur les appareils protégés, consommation de ressources réglable
- Compatibilité avec les systèmes d'exploitation existants et les fournisseurs de systèmes d'automatisation industrielle
- Configuration de base de la sécurité, ainsi que des options avancées pour protéger vos hôtes contre tout type de menace
- Déploiement modulaire et réglages non intrusifs
- PLC pris en charge : Siemens SIMATIC S7-300, S7-400, S7-400H, S7-1500, S7-1200, SIPROTEC 4 ; Schneider Electric Modicon M340, M580 ; appareils CODESYS V3 ; Fastwel CPM723-01
- Options de licence flexibles, de 1 mois à 5 ans
- Préréglages de configuration vérifiés et efficaces pour les ICS les plus courants

- Passerelle
- Serveur Historian
- Serveur SCADA
- Poste de travail de l'opérateur
- Systèmes embarqués
- Poste de travail pour la gestion des systèmes
- Poste de travail de l'ingénieur

La plateforme KICS et au-delà

Cybersécurité unifiée dans les secteurs industriels et commerciaux de votre entreprise

XDR OT native

Les principaux composants de Kaspersky Industrial Cybersecurity, KICS for Networks et KICS for Nodes sont conçus pour fonctionner harmonieusement au sein de notre écosystème, offrant ainsi une expérience unifiée et cohérente. Lorsqu'ils sont achetés ensemble, ils forment une plateforme XDR native qui offre des fonctionnalités supplémentaires intéressantes entre les produits.

Gestion avancée des ressources

Inventaire du matériel des terminaux
Visibilité complète de tous les appareils connectés de votre infrastructure, garantissant un suivi précis des ressources et améliorant la gestion de la sécurité

Inventaire des applications, des utilisateurs et des correctifs
Aperçu détaillé des déploiements de logiciels, de l'accès des utilisateurs et de l'état des correctifs dans votre environnement. Enrichissement des données pour une gestion appropriée et réduction des vulnérabilités potentielles

Surveillance du trafic au niveau des terminaux
Surveillance continue des flux de données à chaque terminal dans le but de détecter rapidement des tendances inhabituelles ou des menaces possibles, ce qui permet de réagir rapidement en cas d'activité suspecte

Audit de sécurité

Analyse des vulnérabilités
Analysez minutieusement vos ressources afin de déterminer les faiblesses en matière de sécurité, de mieux comprendre les risques, de pouvoir réagir rapidement et de renforcer votre position de sécurité dans son ensemble

Audit de conformité
Audit basé sur un agent et sans agent pour assurer la conformité avec les normes de l'industrie OVAL et XCCDF*. Un éditeur entièrement fonctionnel, une base de données de rapports centralisée, un coffre-fort numérique protégé pour les identifiants des nœuds et bien plus

Contrôle de la configuration
Assurez la sécurité des configurations des ressources, suivez de près les changements pour détecter les risques de sécurité et maintenez l'intégrité des données de base pour les ressources matérielles et logicielles

Détection et réponse

Détection
Identification améliorée et simplifiée des menaces grâce à la corrélation des événements entre l'hôte et le réseau, avec une vue unique de la chaîne d'exécution. Enrichissement des données d'alerte réseau pour une meilleure compréhension des incidents

Réponse
Atténuation robuste des menaces grâce à la prévention de l'exécution, à l'isolation des hôtes et à la mise en quarantaine des fichiers. Les intégrations transparentes de pare-feu améliorent davantage votre capacité à répondre rapidement et efficacement aux incidents de sécurité

XDR OT ouverte

Élargissez les fonctionnalités de vos solutions EDR avec un moteur de corrélation, des réponses automatisées et des connecteurs tiers. Améliorez votre plateforme KICS avec la solution Kaspersky XDR Core pour accéder aux fonctionnalités suivantes :

- Surveillance complète et corrélation des événements liés à la sécurité de l'information (SIEM), intégration avec différents systèmes
- Enrichissement et gestion de la Threat Intelligence

XDR IT-OT unique

Franchissez une nouvelle étape et profitez de la convergence ultime entre l'informatique et les technologies opérationnelles. Combinez votre plateforme KICS avec notre offre Kaspersky Next XDR Expert. Tirez parti des fonctionnalités de protection des terminaux les plus performantes de Kaspersky et bénéficiez des fonctionnalités suivantes :

- Un graphique d'enquête unique, des guides et la gestion des incidents par Kaspersky Single Management Platform
- Protection complexe de l'infrastructure informatique (IT XDR)

XDR Industrial

Kaspersky Industrial CyberSecurity

En savoir plus

Kaspersky Single Management Platform

XDR Corporate

Kaspersky Next XDR Expert

En savoir plus

* Format de description de liste de contrôle de configuration extensible (XCCDF)

27 ans d'expérience au niveau mondial et des pétaoctets de données sur les menaces

ICS CERT

ICS CERT – propre division internationale de recherche sur la sécurité OT / IdO

Expertise avérée dans le secteur IT et OT, avec de nombreuses récompenses et succès

Plus de 200 certificats de compatibilité avec les solutions de fournisseurs de systèmes d'automatisation

Efficacité technologique prouvée, respect des normes et des exigences

Des clients dans le monde entier

ROSATOM NORNICKEL EuroChem

NLMK TATNEFT ROSSETI Wintershine

alperia PacificLight КазМунайГаз AGC

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Networks

En savoir plus

www.kaspersky.fr

#kaspersky
#bringonthefuture