Une plateforme de sécurité pour la durabilité et la transformation numérique des entreprises industrielles

La Plateforme de Kaspersky Industrial CyberSecurity

kaspersky BRING ON THE FUTURE

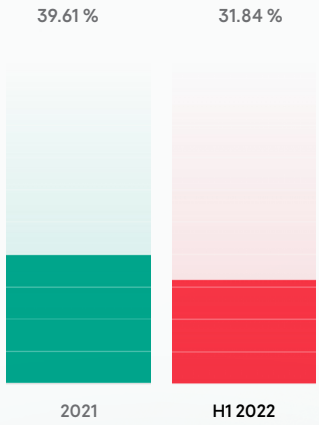
Victime d'une attaque de programme malveillant

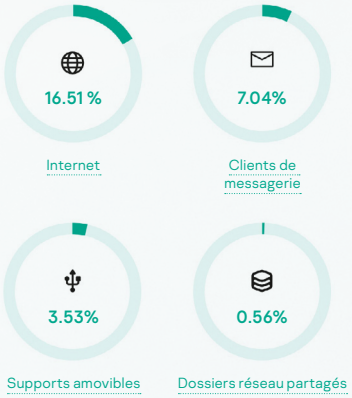
Depuis le début de l'année 2022, près de 30 % des ordinateurs équipés des ICS ont été attaqués par des logiciels malveillants, soit près de 10 % de moins que l'année précédente

Kaspersky ICS-CERT, Juin 2022

En savoir plus

Pourcentage d'ordinateurs équipés de ICS sur lesquels des objets malveillants ont été bloqués depuis le début de l'année 2022





Les entreprises industrielles abordent différemment les questions de cybersécurité dans leurs IT et OT (technologie opérationnelle). La plupart des entreprises disposent déjà de mesures de détection et de réaction bien rodées dans leurs réseaux d'entreprise, mais lorsqu'il s'agit d'OT, elles s'appuient généralement sur une approche désuète de type air gap. Les entreprises industrielles deviennent de plus en plus "numériques" et investissent davantage dans les technologies intelligentes, les nouveaux systèmes d'automatisation et l'adoption de la transformation numérique. Ainsi, elles éliminent le fossé traditionnel entre les IT et OT - un fossé qui empêchait autrefois les cybermenaces d'atteindre les systèmes d'automatisation et de contrôle industriels.

Vous êtes peut-être une cible — mais ne soyez pas une victime

Vous n'avez pas besoin d'être une cible pour être victime d'une violation accidentelle de l'air gap ou d'une attaque de logiciels malveillants. Une simple clé USB, un téléphone portable, un email de phishing ou un ransomware introduit dans l'environnement ICS peut sérieusement affecter les activités principales d'une entreprise. De même, un groupe de pirates motivés peut pénétrer dans les réseaux OT et causer des dommages considérables aux équipements, aux processus, à la production, à la sécurité et à la qualité, ou voler des informations précieuses.

La cybersécurité essentielle pour les OT

Protection des terminaux

pour les systèmes isolés et connectés. Une solution sûre et testée doit permettre de renforcer les politiques de sécurité, d'assurer la conformité, de réaliser des audits de sécurité, de gérer l'inventaire, d'appliquer les correctifs et de collecter des données télémétriques précises en tant que capteur d'extrémité

Protection réseau

pour la visibilité des communications, la détection des menaces et la gestion des actifs. Le système d'analyse du trafic réseau et de détection des intrusions contrôle l'efficacité des paramètres du pare-feu, de la segmentation du réseau et de la conformité de l'utilisation du réseau et permet de fournir une réponse manuelle fiable

Programmes de formation

pour les employés afin de réduire les accidents et de minimiser le facteur humain (erreur humaine)

Services d'experts

enquêter sur l'infrastructure, effectuer des analyses d'experts ou atténuer l'impact d'un incident.

Reconnaissance mondiale

Frost and Sullivan attribue à Kaspersky le prix de la meilleure entreprise mondiale de l'année 2020 sur la base de son analyse du marché mondial de la cybersécurité industrielle (OT/ICS)

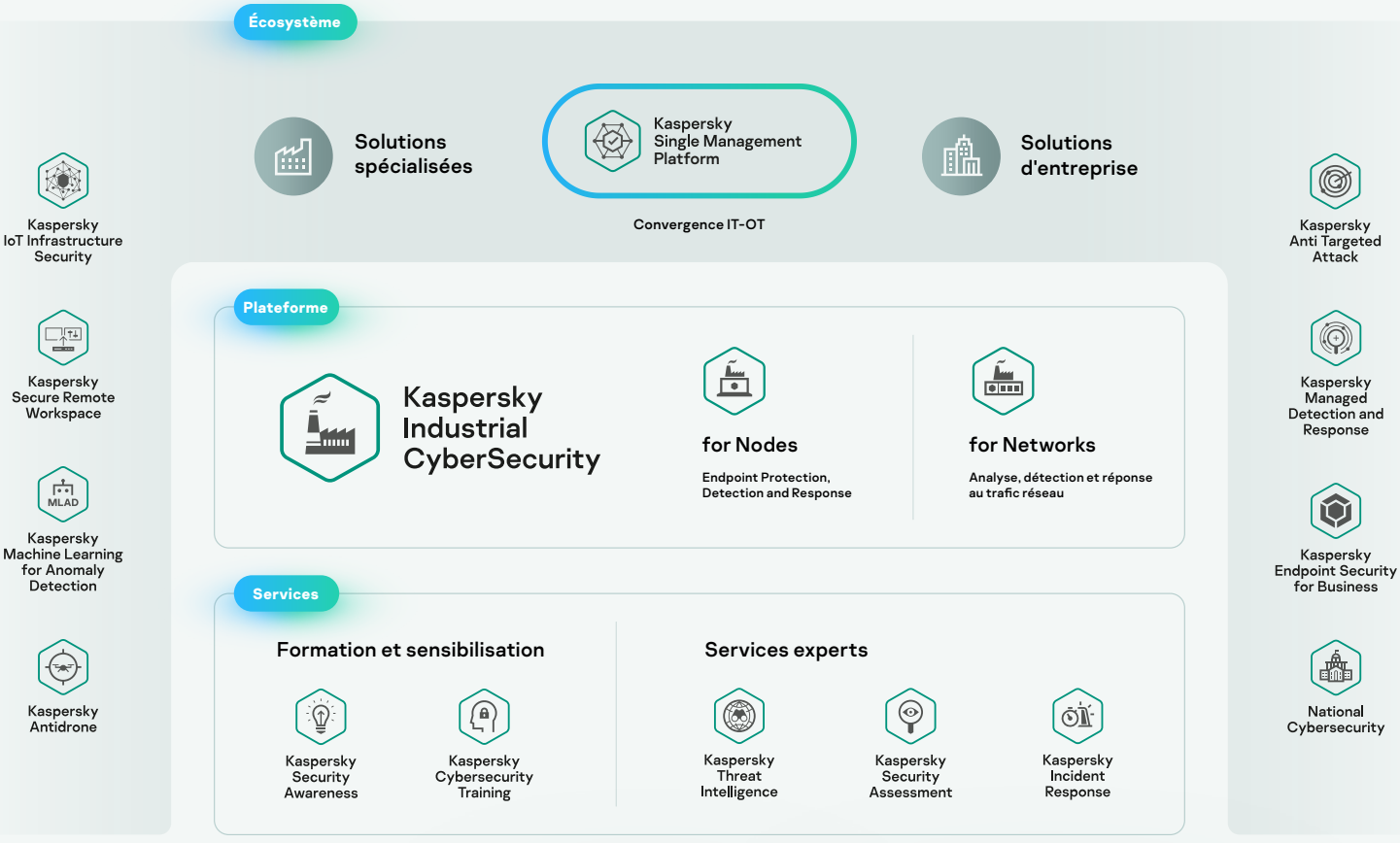
Dans l'enquête mondiale annuelle de **VDC**, Kaspersky a été le premier fournisseur dans la catégorie de la cybersécurité industrielle, sur la base des évaluations générales de plus de 250 professionnels qualifiés de la communauté de l'automatisation industrielle

Ce que propose Kaspersky

La plateforme de Kaspersky Industrial CyberSecurity (KICS), composée de technologies nativement intégrées, ainsi que notre portefeuille de formations et de services spécialisés, répondent à tous les besoins de cybersécurité des entreprises industrielles et des opérateurs d'infrastructures critiques.

La plateforme est un élément clé d'un écosystème unique pour les entreprises industrielles qui comprend :

- **Les meilleures solutions d'entreprise de Kaspersky, qui offrent une vraie convergence IT-OT et les multiples avantages d'une approche à fournisseur unique**
- **Diverses solutions spécialisées pour la sécurité cyber-physique, la sécurité industrielle IOT, l'apprentissage automatique, l'espace de travail à distance sécurisé et bien d'autres offrent une évolutivité illimitée et agile.**



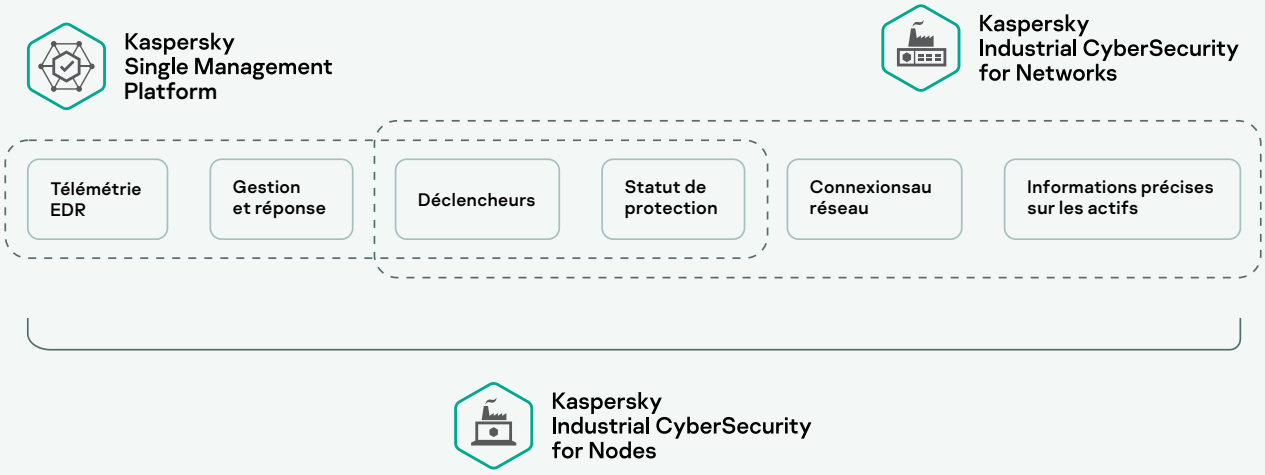
La plateforme de Kaspersky Industrial CyberSecurity est en tête dans les catégories suivantes :

- Sécurité des terminaux OT
- Visibilité et surveillance du réseau OT
- Détection des anomalies, réponse aux incidents et rapports
- Services de sécurité OT

Lorsqu'ils sont utilisés ensemble, l'utilisateur bénéficie d'une vue d'ensemble et d'un contexte plus large : chaîne d'incidents au niveau du réseau et des terminaux, paramètres précis des actifs, 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, etc.

Produits

KICs est une plateforme de cybersécurité OT conçue pour une protection complète des principaux composants des systèmes d'automatisation et de contrôle industriels à tous les niveaux. L'intégration transparente entre les composants de la plateforme offre une visibilité complète sur plusieurs réseaux OT et systèmes d'automatisation répartis géographiquement, ce qui permet d'améliorer l'expérience client, la connaissance de la situation et la flexibilité du déploiement.



KICS for Nodes est un logiciel de protection, de détection et de réponse aux terminaux avec des fonctionnalités d'audit de conformité et de capteur de terminaux.

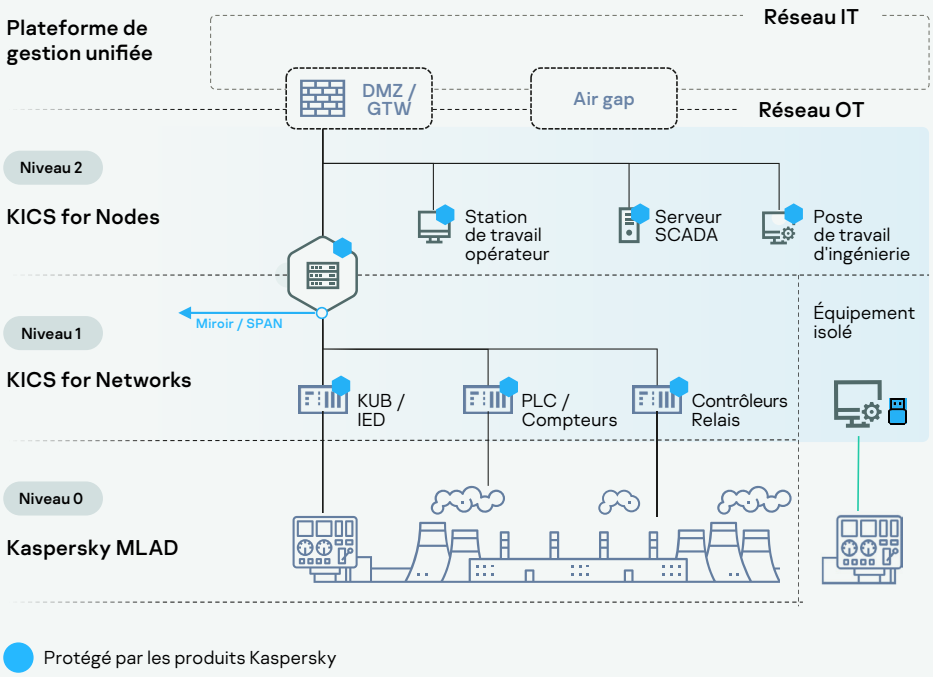
KICS for Networks est conçu pour l'analyse, la détection et la réponse au trafic réseau OT.

La plateforme de gestion unique offre une interface EDR avancée et une évolutivité rapide pour de nombreux sites.

Fonctionnalités supplémentaires

La solution offre de nombreuses fonctionnalités supplémentaires. La technologie Network **Active Polling** permet une collecte rapide et précise de la topologie du réseau et des paramètres des actifs. La fonction **Endpoint Audit** permet de garantir la conformité aux politiques de sécurité, notamment la sécurité des paramètres actuels, et de contrôler les vulnérabilités. La méthode de livraison **Scanner Portable** de KICS for Nodes permet d'établir les meilleures pratiques en matière d'audits de sécurité des équipements isolés et airgapped. **Le Machine Learning pour la détection d'anomalies** est un système de détection précoce des anomalies au cœur du processus technologique.

Architecture de la solution



Fonctionnalités

Découverte d'actifs
Identification et inventaire des actifs passifs d'OT

Inspection approfondie des paquets
Analyse en temps quasi réel de la télémétrie des processus techniques

Contrôle de l'intégrité du réseau
Détection des hôtes et des flux réseau non autorisés

Système de détection des intrusions
Envoi d'alertes sur les activités malveillantes du réseau

Contrôle de commande
Inspecte les commandes sur les protocoles industriels

Intégration externe
L'intégration flexible de l'API ajoute des capacités de détection et de prévention

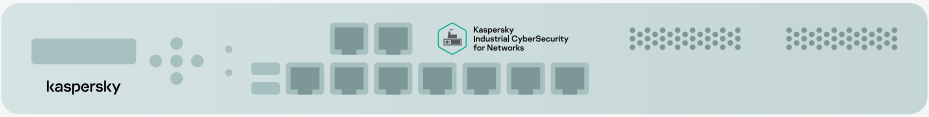
Machine Learning pour la détection d'anomalies (MLAD)
Recherche d'anomalies cybernétiques ou physiques grâce à la télémétrie en temps réel et à l'exploration de données historiques (réseau neuronal récurrent).

Gestion des vulnérabilités
Base de données actualisable des vulnérabilités des équipements industriels, alimentée par Kaspersky ICS CERT

Kaspersky Industrial CyberSecurity for Networks

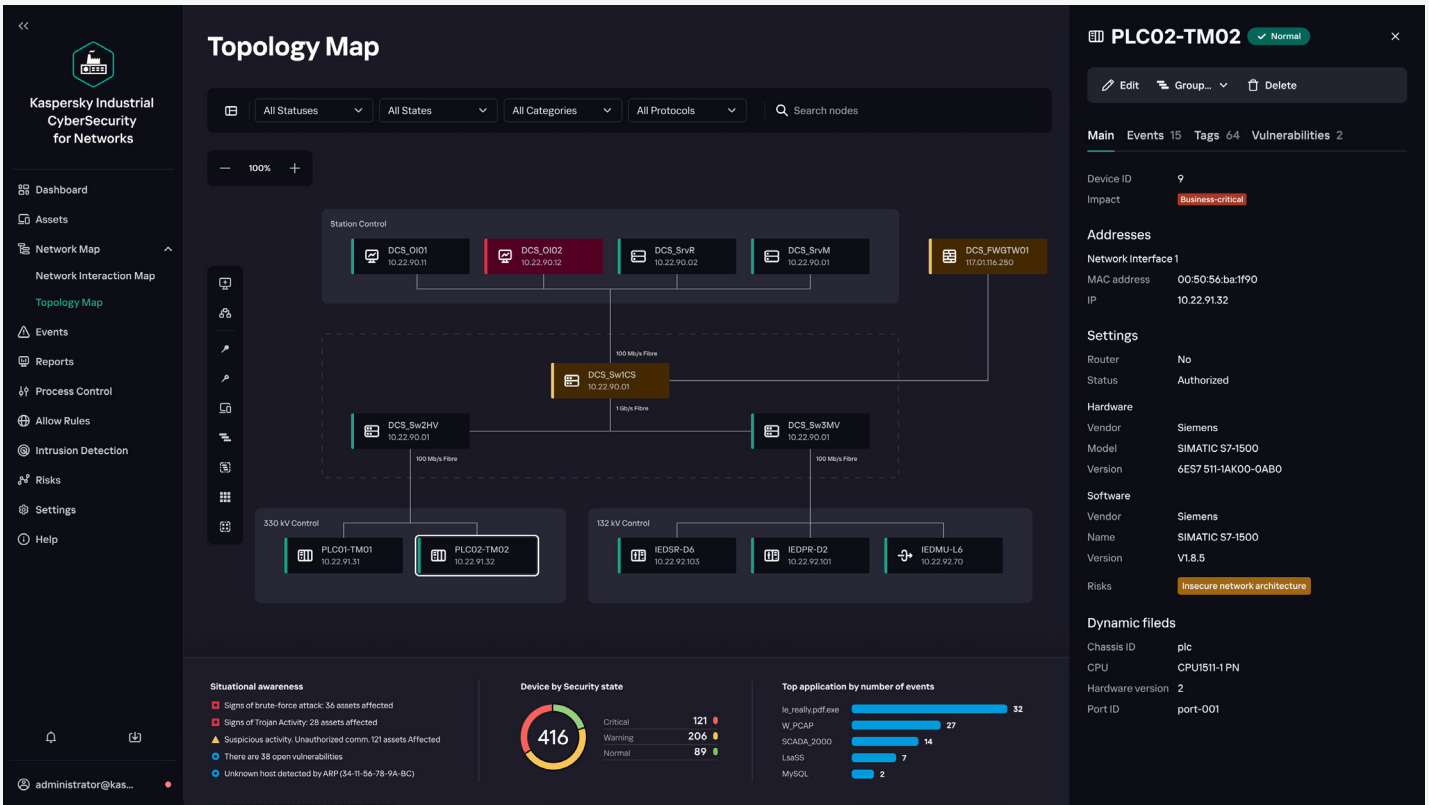
Analyse, détection et réponse au trafic du réseau OT. Une visibilité claire des risques grâce à la surveillance passive du trafic, à l'interrogation active et aux capteurs de terminaux.

Détecte très tôt les anomalies et les intrusions dans les réseaux ICS et veille à ce que les mesures nécessaires soient prises pour éviter tout impact négatif sur les processus industriels.



Une solution indépendante des appareils qui peut être intégrée rapidement et de manière optimale dans les processus d'approvisionnement, d'intégration et de garantie de nos clients.

Interface



KICs for Nodes a été spécialement conçu pour répondre aux exigences des systèmes d'automatisation distribués : environnements mixtes et complexes, durée de fonctionnement prolongée, cas d'utilisation isolés et connectés, instance assistée et sans maintenance et priorité à la disponibilité du contrôle à tout instant

Kaspersky Industrial CyberSecurity for Nodes

Endpoint Protection, Detection and Response de niveau industriel, testée et certifiée. Une solution à faible impact, compatible et stable pour Linux, Windows et les systèmes isolés.

Protection, détection et réponse des terminaux industriels

Protège chaque terminal d'un système d'automatisation moderne, numérique, géré et distribué. Il révèle de nouveaux niveaux de visibilité des incidents dans le processus d'analyse des causes profondes. L'agent collecte la télémétrie des terminaux 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, rassurant ainsi les administrateurs de systèmes d'automatisation sur le fait qu'un incident a été entièrement traité et ne se reproduira plus.

Avantages

Faible impact
sur un appareil protégé pour une meilleure performance du système

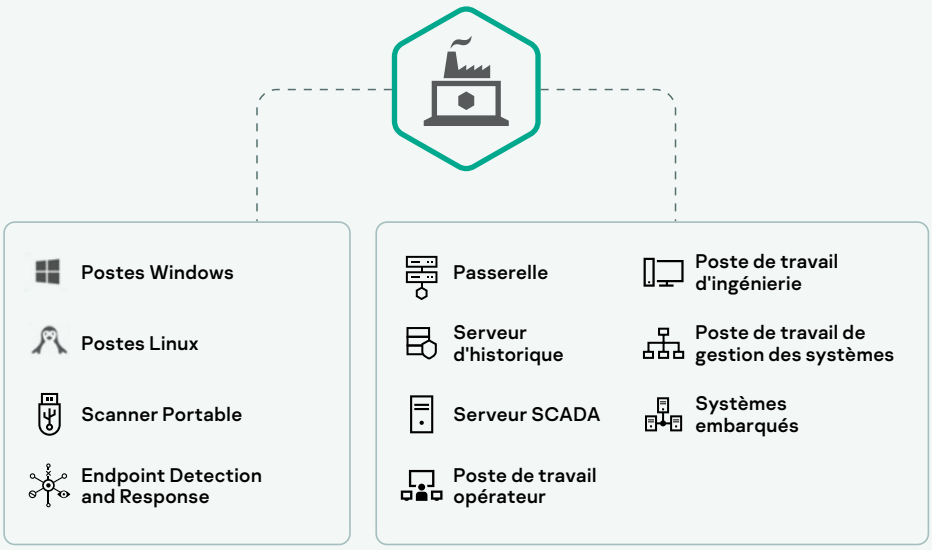
Compatible
avec les ordinateurs peu performants des générations précédentes, ainsi qu'avec les systèmes Windows XP SP2 et Windows Server 2003 SP1 et plus.

Cycle de vie prolongé
jusqu'à 5 ans de licence et de support étendu

Fonctionnalité complète
pour tous les systèmes d'exploitation Microsoft Windows, Windows Server et Windows Embedded

Déploiement modulaire
Options flexibles et réglages sécurisés non intrusifs

Couverture des infrastructures mixtes
Variantes Windows, Linux et Portable



Scanner portable KICS for Nodes
Applique une politique de cybersécurité aux machines isolées, aux systèmes d'automatisation ou aux équipements sur lesquels il est impossible d'installer un logiciel de sécurité. Connaissance ultime de la situation et visibilité de l'OT, même à partir d'une infrastructure isolée.

Solution sans installation
KICS for Nodes peut être activé sur un certain nombre de lecteurs flash Scanner Portable supplémentaires. Cela permet d'effectuer des analyses simultanées à la demande sur plusieurs machines pendant les fenêtres de maintenance, de recueillir des données sur les points d'extrémité et de les organiser dans un rapport de synthèse pratique.

Respect de la réglementation et des politiques internes
KICS for Nodes Scanner Portable effectue des contrôles de conformité anti-malware sur les équipements accédant à un site OT, y compris les ordinateurs des contractants tiers. Il a une très faible empreinte opérationnelle et n'interfère pas avec les solutions de sécurité existantes.

Avantages

Connaissance de la situation

Gestion des systèmes / politiques

Kill-chain et réponse

Génération de rapports et notifications

Intégration SIEM

Intégration IHM / MES

Kaspersky Single Management Platform

La plateforme de gestion unique est une solution de gestion de la sécurité centralisée pour l'orchestration de la sécurité de l'ensemble de l'infrastructure OT, avec une carte de tous les actifs géographiquement répartis enrichie d'événements, d'analyses d'incidents et plus encore. Il renforce l'efficacité des équipes de sécurité mixtes OT et IT. Un endroit où tous vos contrôles de sécurité fonctionnent en harmonie, permettant une réponse rapide et précise.

Services d'experts

Notre gamme de services constitue une partie importante du portefeuille KICS. Nous fournissons le cycle complet des services de sécurité, des évaluations de la cybersécurité industrielle à la réponse aux incidents.

> Leur expérience dans le domaine de la cybersécurité ICS, leur professionnalisme et la complexité de leur solution, en comparaison avec d'autres éditeurs, ont offert une grande valeur ajoutée et assuré un brillant avenir à la stratégie de sécurité de notre entreprise.
>
> Ondřej Sýkora,
> responsable C&A,
> Plzeňský Prazdroj

Industrial Cybersecurity Assessment

Industrial Cybersecurity Assessment : Kaspersky propose une évaluation de la cybersécurité industrielle peu invasive comprenant des tests de pénétration externes et internes, l'évaluation de la sécurité OT et l'évaluation de la sécurité des solutions d'automatisation. Les experts de Kaspersky fournissent des informations importantes sur l'infrastructure d'une entreprise et des recommandations sur la manière de renforcer la cybersécurité ICS.

Threat Intelligence

> En réalisant cet exercice et en profitant des connaissances de l'équipe de Kaspersky, nous avons renforcé notre protection contre les cybermenaces.
>
> Yu Tat Ming,
> PDG, PacificLight

Les analyses actualisées collectées par les experts de Kaspersky permettent de renforcer la protection du client contre les cyberattaques industrielles ciblées. Délivrées sous forme de flux TI ou de rapports personnalisés, elles répondent aux besoins spécifiques des clients en fonction des paramètres régionaux, sectoriels et logiciels ICS.

Réponse à incidents

En cas d'incident, les experts de Kaspersky collectent et analysent les données et les logiciels malveillants, reconstituent la chronologie de l'incident, déterminent les sources et les motivations possibles et élaborent un plan de remédiation détaillé. Ce plan inclut des recommandations pour neutraliser les logiciels malveillants des systèmes du client et annuler les actions malicieuses (automatic rollback)

Formation et sensibilisation

> Kaspersky était la meilleure entreprise pour offrir des compétences professionnelles en matière de cybersécurité industrielle pour notre groupe ICS.
>
> Søren Egede Knudsen, directeur technique

Formation à la cybersécurité industrielle

Formation interactive sur site et en ligne et jeux de cybersécurité pour les employés qui travaillent avec des systèmes informatiques industriels et leurs responsables. Les participants acquièrent de nouvelles connaissances sur le paysage actuel des menaces et les vecteurs d'attaque ciblant spécifiquement les environnements industriels, explorent des scénarios pratiques et acquièrent des compétences en matière de cybersécurité.

Programmes de formation d'experts

Les cours de formation aux tests de pénétration ICS et à la criminalistique numérique ICS sont destinés aux professionnels de la cybersécurité. Les participants acquièrent toutes les compétences avancées nécessaires pour réaliser des tests de pénétration complets ou des cyberdiagnostics dans des environnements industriels.

Ecosystème de solutions spécialisées

Kaspersky IoT Infrastructure Security

Protège l'Internet des objets (IoT) au niveau de la passerelle en s'appuyant sur l'approche Cyber Immunity de Kaspersky.

En savoir plus

Kaspersky Antidrone

Protège l'espace aérien des drones dans les installations de n'importe quelle taille

En savoir plus

Kaspersky Secure Remote Workspace

Une infrastructure client léger fonctionnelle avec Cyber Immunity

En savoir plus

Kaspersky Security CAD

Modélisation numérique des systèmes de sécurité de l'information pour les phases de conception et d'exploitation

En savoir plus

Kaspersky Machine Learning for Anomaly Detection

Système de détection précoce des anomalies dans les processus technologiques industriels

En savoir plus

www.kaspersky.fr

Kaspersky Industrial CyberSecurity

En savoir plus