Kaspersky Industrial CyberSecurity : présentation de la solution

kaspersky BRING ON THE FUTURE

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity : présentation de la solution

Introduction

Les sociétés industrielles du monde ont pour habitude d'aborder différemment la cybersécurité dans leurs réseaux IT et OT (« operational technology », technologies opérationnelles). La plupart des entreprises disposent déjà de mesures de réponse à incidents et de systèmes de détection d'attaques avancées au sein de leur structure. Cependant, elles ont tendance à s'appuyer sur une approche d'isolement physique (« air gap ») classique lorsqu'il s'agit de leurs réseaux OT. Les sociétés industrielles se tournent de plus en plus vers le numérique en investissant davantage dans les technologies intelligentes, les nouveaux systèmes d'automatisation et l'adoption de l'industrie 4.0. Ainsi, elles éliminent l'écart entre les environnements IT et OT en termes de protection contre les cybermenaces dangereuses pour les systèmes de contrôle industriels. Selon Kaspersky ICS CERT, le pourcentage d'ordinateurs en partage de connexion sur lesquels des objets malveillants ont été détectés a atteint 41,2 % au cours du premier semestre 2019[1].

Quelles sont ces menaces ?

Tout d'abord, elles incluent le risque d'une infection accidentelle par un programme malveillant classique. Il n'est pas nécessaire d'être une cible pour devenir une victime. Une simple clé USB ou un email de phishing avec un cheval de Troie bancaire ou un ransomware introduit involontairement dans l'environnement ICS peut sérieusement affecter le cœur de métier d'une entreprise. Même si les infections accidentelles ne sont pas sicourantes, un pirate motivé peut évidemment s'introduire dans les réseaux OT et causer des dommages considérables à une production ou à des équipements coûteux, ou encore voler des données sensibles.

Quelles sont les mesures de cybersécurité ICS appropriées ?

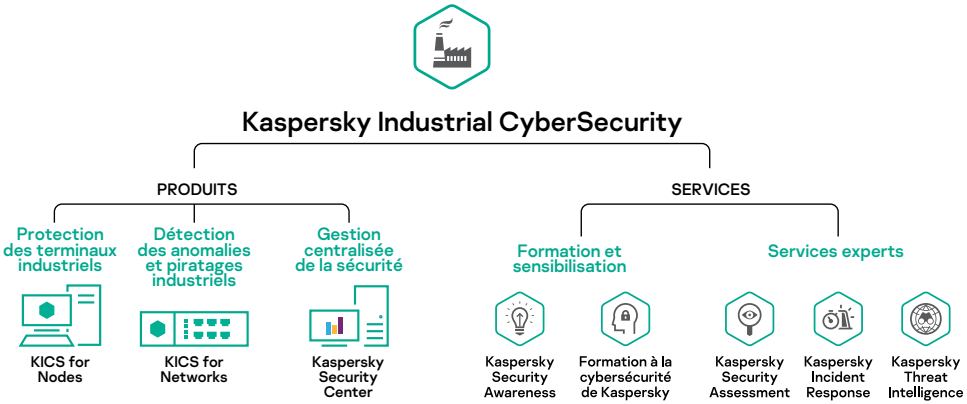
1. La protection des terminaux industriels pour éviter les infections accidentelles et entraver les intrusions motivées.
2. La surveillance du réseau OT et la détection d'anomalies pour identifier les actions malveillantes au niveau des automates programmables industriels (API).
3. Des programmes de formation pour les salariés afin de réduire le nombre d'accidents et de minimiser le facteur humain.
4. Des services d'experts dédiés pour étudier l'infrastructure, effectuer des analyses poussées ou réduire les effets d'un incident.

1 Threat landscape for industrial automation systems, 1er semestre 2019, Kaspersky ICS CERT

Qu'offre Kaspersky ?

Kaspersky répond à tous les besoins en cybersécurité des sociétés industrielles avec sa gamme Kaspersky Industrial CyberSecurity(KICS). KICS propose une approche holistique de la cybersécurité industrielle. En effet, la solution apporte une valeur ajoutée à n'importe quelle étape du processus de sécurité OT du client, des évaluations de la cybersécurité et de la formation aux technologies avancées et à la réponse aux incidents.

Composants Kaspersky Industrial CyberSecurity



En 2020, Kaspersky a été cité dans le rapport Gartner « Competitive Landscape: Operational Technology Security » (Paysage concurrentiel : sécurité des technologies opérationnelles)[2] comme "representative vendor" dans 4 catégories de produits, notamment :

- sécurité des terminaux OT ;
- visibilité et surveillance du réseau OT ;
- détection des anomalies, réponse aux incidents et rapports ;
- services de sécurité OT[2].

ARC Advisory Group souligne le fait que Kaspersky offre une alliance unique de Threat Intelligence, de Machine Learning et d'expertise humaine en phase avec une protection agile contre toutes sortes de menaces[3].

Par ailleurs, une étude de Forrester[4] démontre un retour sur investissement de 368 % pour une entreprise équipée de Kaspersky Industrial CyberSecurity ainsi que d'autres avantages tels que l'assistance d'experts et une tranquillité d'esprit assurée.

2 Gartner : Competitive Landscape: Operational Technology Security, mars 2020 https://ics.kaspersky.com/KICS-cited-in-Gartnercompetitive-landscape-OTsecurity

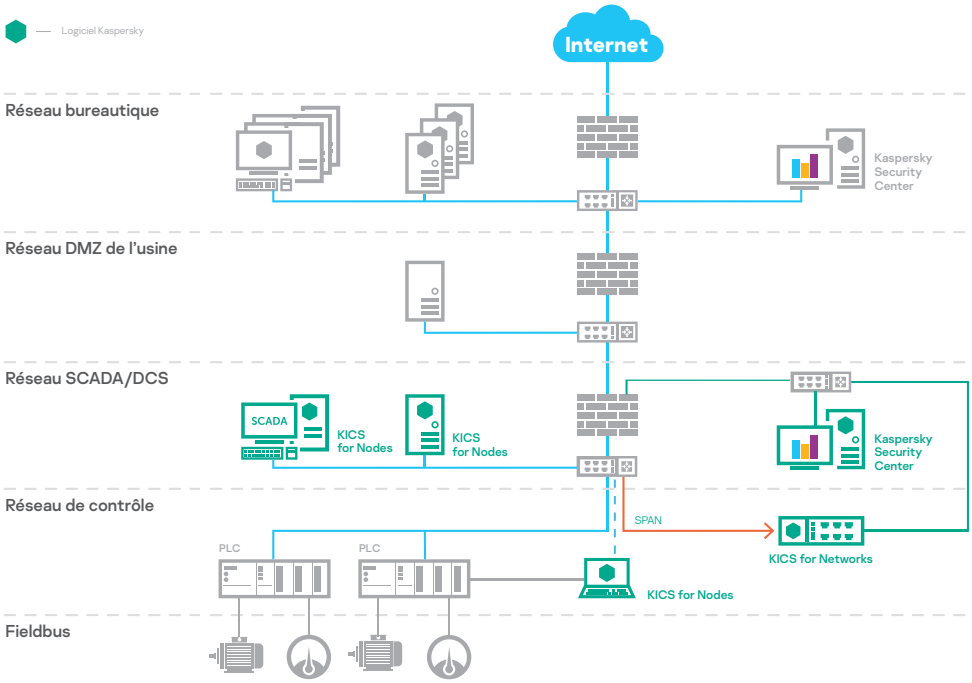
3 ARC Advisory : Kaspersky Moves Forward with Improved Cybersecurity Solutions, 2018

4 Forrester Research : The Total Economic Impact™ of Kaspersky Industrial CyberSecurity, April 2019. https://www.kaspersky.com/ forrester-tei-for-kics

Produits

Les produits KICS sont conçus pour sécuriser totalement les éléments industriels de votre société : KICS for Nodes est destiné aux terminaux industriels. De son côté, KICS for Networks surveille la sécurité des réseaux industriels.

Déploiement des produits Kaspersky Industrial CyberSecurity



KICS for Networks

KICS for Networks est une solutionde surveillance et de visibilité des réseaux OT proposée comme logiciel ou appliance virtuelle, connectée passivement au réseau ICS.

Avantages :

- ✓ **Détection des équipements réseau**
  Identification et Inventaire des équipements et des communications du réseau OT
- ✓ **Inspection approfondie des paquets d'informations**
  Analyse en temps quasi réel de la télémétrie des processus techniques
- ✓ **Contrôle de l'intégrité du réseau**
  Détection des hôtes et des flux de réseaux non autorisés
- ✓ **Système de détection des intrusions**Envoi d'alertes en cas d'activités malveillantes sur le réseau
- ✓ **Contrôle des commandes**
  Inspection des commandes de protocoles industriels
- ✓ **Systèmes externes**
  Capacités de détection externe par intégration d'API
- ✓ **Machine Learning au service de la détection des anomalies (MLDA)**
  Identification des violations de systèmes cyber ou physiques par le biais de la télémétrie en temps réel et de l'exploration de données historiques (réseau neuronal récurrent)

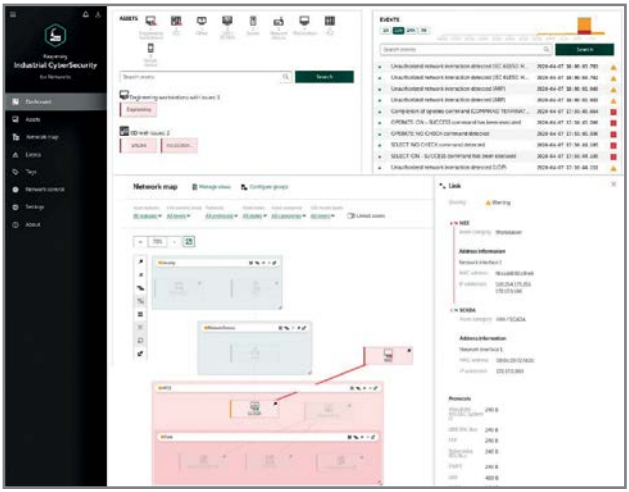
KICS for Network détecte les anomalies et les intrusions au sein des réseaux ICS dès qu'elles surviennent et s'assure que les actions nécessaires sont prises pour empêcher tout effet négatif sur les processus industriels.

KICS for Networks est une solution indépendante des applications, ce qui permet au client de choisir l'éditeur d'applications informatiques industrielles auquel il souhaite faire confiance.

L'interface KICS for Networks affiche un tableau de bord en temps réel et une carte des réseaux pour gérer les ressources et les événements de sécurité.

Exemple d'appliance KICS for Networks

Interface KICS for Networks



KICS for Nodes

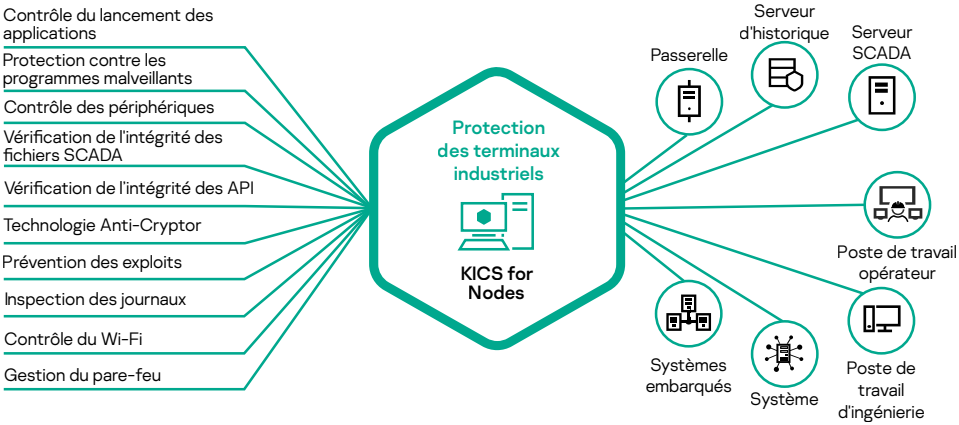
KICS for Nodes est un produit de sécurité des terminaux OT proposé comme logiciel pour Windows et Linux.

Avantages :

- ✓ **Impact minime sur l'appareil protégé**
- ✓ **Compatibilité optimale**
- ✓ **Protection avancée contre les programmes malveillants**
- ✓ **Contrôle de l'environnement**

KICS for Nodes a été spécialement conçu pour consommer un minimum de ressources. Construit sur des systèmes de sécurité et des systèmes embarqués, son architecture modulaire vous permet de simplement installer les composants de protection dont vous avez besoin. Les composants de protection peuvent être configurés en mode de prévention ou en mode de détection uniquement. Cette approche est parfaite pour les anciennes machines à faibles performances qui exigent un maximum de puissance informatique disponible.

Fonctionnalités KICS for Nodes et terminaux pris en charge



« Nous avons décidé de nous associer avec Kaspersky, car Kaspersky Industrial CyberSecurity peut être déployé pendant le déroulement de nos opérations et aussi car cette solution est compatible avec les systèmes de contrôle que nous utilisons. »

Jan Houben,
directeur d'usine chez
AGC Glass Germany GmbH

KICS for Nodes sécurise les nœuds industriels contre les différents types de cybermenaces susceptibles d'émerger des facteurs humains, de programmes malveillants génériques, d'attaques ciblées ou d'opérations de sabotage. KICS for Nodes est compatible avec l'ensemble des composants matériels et logiciels des systèmes d'automatisation industriels tels que SCADA, API et SNCC.

Kaspersky Security Center

Kaspersky Security Center est une solution de gestion centralisée de la sécurité. Elle offre un contrôle et une visibilité des couches industrielles sur plusieurs sites ainsi que des réseaux d'entreprises environnants.

Avantages :

- ✓ **Gestion des systèmes**
  - Collecte centralisée des données des systèmes
  - Déploiement centralisé du logiciel
  - Détection des vulnérabilités et gestion des correctifs
  - Fonctionnalités de gestion étendues
- ✓ **Gestion des politiques**
  - Une politique de sécurité centralisée
  - Planification et exécution des tâches à distance
- ✓ **Génération de rapports et notifications**
  - Enregistrement des évènements
  - Tableaux de bord et rapports
  - Notifications par sMS/email
- ✓ **INTÉGRATION SIEM**
  - Arcsight, Splunk, Qradar
  - Serveur Syslog
- ✓ **INTÉGRATION HMI**
- ✓ **INTÉGRATION de tableau de bord MES**
  - Niveau de sécurité et transmission d'informations vers UN HÔTE COMPATIBLE IEC 104 / OPC 2.0

Kaspersky Industrial CyberSecurity : services

Notre suite de services constitue une part importante de la gamme KICS : nous proposons des services de sécurité complets, de l'évaluation de la cybersécurité industrielle à la réaction en cas d'incident.

« 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

Services d'experts

- **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 offrent des informations importantes sur l'infrastructure d'une entreprise et donnent des recommandations sur la manière de renforcer la place de la cybersécurité ICS.
- **Threat Intelligence :** des analyses à jour recueillies par les experts de Kaspersky contribuent à améliorer la protection des clients contre les cyberattaques industrielles ciblées. Proposées sous forme de flux de Threat Intelligence ou de rapports personnalisés, elles répondent aux besoins spécifiques des clients en fonction des paramètres des logiciels ICS régionaux et industriels.

« En réalisant cet exercice et en tirant les enseignements des connaissances de l'équipe Kaspersky, nous avons renforcé notre protection contre les cybermenaces. »

Ya Tat Ming, CEO,
PacificLight.

- **Réponse aux incidents :** en cas d'incident de cybersécurité, nos experts collecteront et analyseront les données, reconstitueront la chronologie de l'incident, en détermineront les origines et causes probables et élaboreront un plan de résolution. En outre, Kaspersky propose un service d'analyse des programmes malveillants, dans le cadre duquel les experts de Kaspersky classeront les échantillons du programme malveillant transmis, analyseront ses fonctions et comportements et élaboreront des recommandations ainsi qu'un plan visant à le supprimer de vos systèmes et à annuler toute action malveillante.

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,
Chief Technical Officer,
Ezenta

- **Formation de sensibilisation à la sécurité informatique :** modules de formation interactifs sur site et en ligne, jeux autour de la cybersécurité pour les salariés en contact avec des systèmes industriels informatisés et leurs responsables. Les participants explorent des scénarios pratiques, acquièrent des compétences professionnelles en matière de cybersécurité et repartent avec un nouvel aperçu du paysage actuel des menaces et des vecteurs d'attaque ciblant spécifiquement l'environnement industriel. La formation sur site peut être personnalisée et adaptée sur 1 ou 2 jours.

- **Programme de formation pour spécialistes :** les modules de formation aux tests de pénétration ICS et Cyberdiagnostics ICS ont été créés pour les 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. La certification est incluse.

Pour en savoir plus sur KICS :
https://ics.kaspersky.fr/

#Kaspersky
#BringontheFuture

www.kaspersky.fr

IIC MEMBER industrial internet CONSORTIUM

ePC FOUNDATION MEMBER

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2018

* World Leading Internet Scientific and Technological Achievement Award à l'occasion de la 3e Conférence mondiale de l'Internet Conférence

** Prix spécial du China International Industry Fair (CIIF) 2016