KASPERSKY lab

Kaspersky Industrial CyberSecurity : présentation de la solution

www.kaspersky.com/ics
#truecybersecurity

Kaspersky Industrial CyberSecurity : présentation de la solution

Les attaques sur les systèmes industriels se multiplient

Non seulement les cyberattaques sur les systèmes de contrôle industriels se multiplient, mais leur présence est désormais indiscutable et ne tient plus de la spéculation[1]. 67 % des responsables de la sécurité informatique et des responsables sécurité des technologies opérationnelles (OT security managers) perçoivent la cybermenace pesant actuellement sur les SCI comme étant élevée ou critique, soit une hausse de plus de 43 % par rapport à l'an passé[2]. Depuis cinq ans, le risque d'interruption des activités et de perturbation de la chaîne d'approvisionnement occupe la première place des préoccupations au niveau mondial ; le risque de cyberincident est d'ailleurs la principale crainte qui émerge de cette tendance[3]. Pour les entreprises utilisant des systèmes industriels ou des systèmes d'infrastructure critiques, les risques n'ont jamais été aussi élevés. Les conséquences de la sécurité industrielle vont bien au-delà de la protection de l'entreprise et de sa réputation. De nombreux facteurs écologiques, sociaux et macroéconomiques importants sont à prendre en compte lorsqu'il s'agit de protéger les systèmes industriels contre les cybermenaces.

[1] PwC : Global State of Information Security 2015 (Bilan 2015 sur la sécurité de l'information)

[2] SANS 2016 State of ICS Security Survey (Sondage 2016 du SANS Institute sur le paysage de la sécurité des SCI)

[3] Allianz Risk Barometer 2017

Différences entre technologie opérationnelle et technologie de l'information

D'après la définition de la norme IEC 62443 relative à l'automatisation, un système de contrôle industriel (SCI) est un ensemble de logiciels, de matériels et de personnels susceptibles d'avoir un impact sur la sûreté, la sécurité et la fiabilité du fonctionnement d'un processus (technologique) industriel.

Les systèmes de contrôle industriels incluent, sans s'y limiter :

- Les systèmes de contrôle distribués (SCD), les automates programmables (API), les unités terminales distantes (RTU), les équipements électroniques intelligents (IED), les systèmes de télésurveillance et d'acquisition de données (SCADA) et les systèmes de diagnostic.
- Les interfaces internes, humaines, réseau ou machine utilisées en association afin d'assurer le contrôle, la sécurité et l'exécution de la fonctionnalité opérationnelle dans les processus continus, par lots, discrets ou autres.

D'un point de vue plus technique, toute infrastructure de système industriel peut être divisée en deux domaines :

- Technologie de l'information (systèmes informatiques) – systèmes nécessaires à la gestion des données dans un contexte commercial
- Technologie opérationnelle (systèmes TO) – systèmes nécessaires à la gestion des processus physiques et industriels de l'automatisation industrielle.

Les stratégies de sécurité informatique sont généralement axées sur la protection des données et visent les objectifs du modèle « C-I-D » : Confidentialité, Intégrité et Disponibilité des données. Au contraire, pour la plupart des systèmes TO, la cybersécurité ne concerne pas les « données », mais la continuité des processus technologiques. Ainsi, en termes de modèle C-I-D, la « disponibilité » est le principal objectif des stratégies de sécurité appliquées aux systèmes TO. Il s'agit là de la principale différence entre les besoins de la cybersécurité industrielle et ceux des autres systèmes : même la plus performante des solutions de cybersécurité informatique classique ne serait pas adaptée aux systèmes TO, car elle mettrait en péril la disponibilité (et, dans certains cas, l'intégrité) des processus.

Risques et menaces

En dépit d'une prise de conscience croissante de la prévalence des cyberattaques sur les systèmes de contrôle industriels, de nombreux modèles de sécurité informatique continuent de penser, bien que cela soit dépassé, que l'isolation physique des systèmes (en les isolant du réseau, par « air-gap ») et la « sécurité par l'obscurité » suffisent. Cela n'est pas le cas : à l'ère de l'industrie 4.0, la plupart des réseaux industriels non essentiels sont accessibles via Internet[4], que ce soit par choix ou non. D'après des recherches approfondies menées par l'ICS-CERT Kaspersky Lab et basées sur des données issues du réseau Kaspersky Security Network, les PC industriels sont régulièrement attaqués par les mêmes programmes malveillants génériques qui affectent les systèmes informatiques d'entreprise, notamment (mais pas exclusivement) par les coupables habituels que sont les chevaux de Troie, les virus et les vers. Au cours du second semestre 2016, à l'échelle mondiale, les produits Kaspersky Lab ont bloqué des tentatives d'attaques sur 39,2 % de tous les ordinateurs bénéficiant d'une protection Kaspersky Lab classés comme des composants d'infrastructure industrielle[5].

Bien qu'il ne soit pas spécifique aux systèmes industriels, le ver « Kido » (également appelé « Conficker ») a contraint une centrale nucléaire allemande à fermer pendant plusieurs jours en avril 2016, non pas en pénétrant directement dans son système de contrôle, mais en infectant le réseau bureautique adjacent.

Le ransomware est une autre menace croissante pour les SCI. La diversité des ransomwares s'est largement étendue entre 2015 et début 2017. L'émergence des ransomwares revêt une importance considérable pour le secteur industriel : de telles infections peuvent engendrer des répercussions significatives et endommager des systèmes critiques de diverses manières, faisant ainsi du SCI une cible potentielle particulièrement intéressante. Les attaques de ransomwares menées sur des systèmes SCADA au cours de l'année 2016 l'ont d'ailleurs prouvé. Le ransomware conçu pour attaquer les systèmes industriels peut avoir son propre objectif : au lieu de chiffrer les données, le programme malveillant peut prévoir de perturber les opérations ou de bloquer l'accès à une ressource clé.

Outre les menaces simples, la sécurité industrielle doit également lutter contre les programmes malveillants spécifiques aux SCI et contre les attaques ciblées : Stuxnet, Havex, BlackEnergy, PLC Blaster, Ladder Logic Bomb, Pin Control Attack... la liste s'allonge rapidement. Comme les attaques Stuxnet et BlackEnergy l'ont montré, il suffit d'une clé USB infectée ou d'un e-mail de phishing ciblé pour que les cybercriminels bien préparés pénètrent un réseau isolé.

De nombreuses attaques ciblant des complexes industriels sont lancées et propagées à la fois via les réseaux et via les SCI. Par exemple, au cours de l'attaque BlackEnergy sur le réseau électrique ukrainien en décembre 2015 qui a engendré de sévères coupures d'électricité, les pirates informatiques ont utilisé plusieurs vecteurs d'attaque. Tout d'abord, les identifiants d'accès au système SCADA ont été dérobés depuis l'environnement d'entreprise via une attaque de phishing. Les pirates informatiques ont par la suite commencé à couper le réseau électrique manuellement, puis ont inséré sur le réseau industriel un programme malveillant KillDisk qui a effacé ou remplacé les données figurant dans les fichiers systèmes essentiels, provoquant ainsi une panne de la machine de l'opérateur. En

[4] ICS and their online availability 2016 (Les SCI et leur disponibilité en ligne en 2016), Kaspersky Lab

[5] Threat Landscape for Industrial Automation Systems for H2 2016 (Le paysage des menaces contre les systèmes d'automatisation industriels au deuxième semestre 2016), ICS-CERT Kaspersky Lab

parallèle, le centre d'appels du service a subi une attaque DDoS afin d'empêcher que les clients ne signalent la panne.

Outre les programmes malveillants et les attaques ciblées, les organisations industrielles sont également confrontées à d'autres risques et menaces ciblant le personnel, les processus et les technologies, et le fait de sous-estimer ces risques peut avoir de graves conséquences. Kaspersky Lab développe des solutions et des services pour aider nos clients à combattre non seulement ces programmes malveillants et ces attaques ciblées, mais aussi de nombreux autres cyberincidents et facteurs de risques, notamment :

- Les erreurs commises par les sous-traitants ou les opérateurs SCADA (tierces parties)
- Les actions frauduleuses
- Le cybersabotage
- Les problèmes de conformité
- Le manque de connaissances et de données concrètes en matière d'analyse criminalistique

La nécessité de spécialiser la cybersécurité industrielle

Seuls les fournisseurs de cybersécurité qui comprennent la différence entre les systèmes industriels et les systèmes axés sur les données sont en mesure de proposer des solutions qui répondent aux besoins uniques des infrastructures et des systèmes de contrôle industriels. Forrester Research recommande aux organisations industrielles à la recherche d'un fournisseur de sécurité de « Rechercher une expertise spécifique à l'industrie ». Forrester poursuit en identifiant Kaspersky Lab comme étant l'un des rares fournisseurs disposant d'une véritable expertise dans le domaine.

Kaspersky Lab : un fournisseur de cybersécurité industrielle digne de confiance

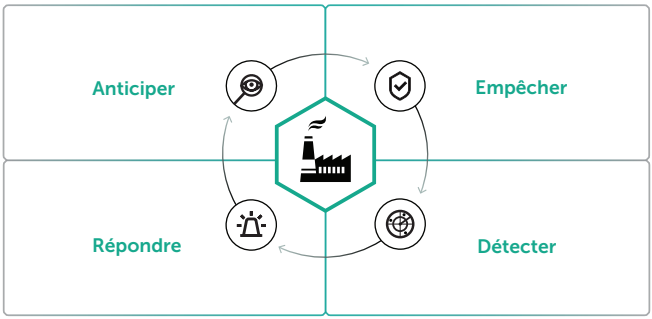
Leader reconnu dans la cybersécurité et la protection industrielle[6], Kaspersky Lab recherche et développe continuellement des solutions qui font bien plus que de contrer les menaces en constante évolution qui pèsent sur les infrastructures industrielles et critiques. De la gestion des opérations aux systèmes SCI, Kaspersky Lab joue un rôle majeur en aidant l'industrie, les organismes de réglementation et les agences gouvernementales à anticiper les changements qui surviennent dans le paysage des menaces et à se protéger contre les attaques.

Fournisseur de solutions de sécurité digne de confiance et partenaire des principales organisations industrielles qui s'appuient sur notre protection contre les programmes malveillants depuis des années, Kaspersky Lab collabore également avec les entreprises et les fournisseurs d'automatisation industrielle les plus reconnus, notamment Emerson, SAP, Siemens, Schneider Electric et Industrial Internet Consortium, afin d'établir des procédures spécialisées en matière de compatibilité, ainsi que des cadres de coopération qui protègent les environnements industriels des menaces existantes et nouvelles, notamment les attaques extrêmement ciblées.

[6] Gartner Market Guide for Operational Technology Security (Guide publié par Gartner sur la sécurité de la technologie opérationnelle), 2016

Kaspersky Lab a développé une gamme de solutions spécialisées permettant de répondre aux besoins spécifiques du marché de la cybersécurité industrielle : Kaspersky Industrial CyberSecurity (KICS). Ces solutions permettent de bénéficier d'une sécurité efficace contre les cybermenaces à tous les niveaux des SCI (serveurs SCADA, interfaces homme-machine, postes de travail des ingénieurs, API et connexion réseau industriel inclus), sans affecter la continuité des opérations ni la cohérence des processus technologiques.

En accord avec la stratégie de sécurité globale multi-niveaux de Kaspersky Lab, Kaspersky Industrial CyberSecurity fournit une combinaison de plusieurs méthodes de protection. Pour garantir de manière optimale la continuité et le fonctionnement sécurisé de votre entreprise, vous devez adopter une approche de la cybersécurité industrielle globale, de la prévision des vecteurs d'attaques potentielles grâce aux technologies de prévention et de détection industrielles spécialisées, à la neutralisation proactive d'un cyberincident.



L'architecture de sécurité évolutive

Les services Kaspersky Industrial CyberSecurity

Nous proposons des services de sécurité complets, de l'évaluation de la cybersécurité industrielle à la réaction en cas d'incident.

Connaissances (formation et veille stratégique)

- **Formations :** Kaspersky Lab propose des formations conçues pour les experts (responsables de la sécurité informatique et responsables sécurité des technologies opérationnelles) et les ingénieurs et opérateurs ICS. Au cours de ces formations, les participants en apprennent plus sur les cybermenaces qui les concernent, les grandes lignes de leur évolution et les méthodes les plus efficaces pour s'en protéger. Ces cours permettent également aux professionnels de la sécurité de renforcer encore davantage leurs compétences dans des domaines spécifiques, comme les tests de pénétration des SCI ou le cyberdiagnostic.

- **Programmes de sensibilisation :** Kaspersky Lab propose aux ingénieurs et aux responsables de la sécurité des formations sous forme de jeux permettant de prendre conscience des problèmes de cybersécurité relatifs à l'industrie, tout en développant les compétences nécessaires pour les neutraliser. Par exemple, Kaspersky Industrial Protection Simulation (KIPS) simule des cyberattaques sur des systèmes d'automatisation industriels, montrant ainsi les principaux problèmes associés à la mise en place de la cybersécurité industrielle.
- **Rapports de veille stratégique :** des rapports de veille stratégique à jour vous sont fournis par notre équipe dédiée « ICS Cyber-Emergency Response ».

Services d'experts

- **Évaluation de la cybersécurité :** pour les organisations préoccupées par le potentiel impact de la sécurité informatique et technologique sur les opérations, Kaspersky Lab propose une évaluation peu invasive de la cybersécurité industrielle. Il s'agit d'une première étape cruciale dans la mise en place des exigences en matière de sécurité à la lumière des besoins opérationnels, pouvant également fournir de nombreuses informations relatives aux niveaux de cybersécurité, sans avoir à déployer d'autres technologies de protection.
- **Intégration de la solution :** si les systèmes de contrôle industriels d'une entreprise disposent d'une architecture unique ou sont basés sur des composants matériels et logiciels personnalisés peu utilisés dans l'industrie, Kaspersky Lab peut adapter les outils de cybersécurité recommandés pour qu'ils fonctionnent avec ces systèmes. Ce service inclut la prise en charge des systèmes matériels et logiciels uniques (API et SCADA propriétaires inclus) et des protocoles de communication industriels.
- **Investigation sur les 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 Lab propose un service d'analyse des programmes malveillants, dans le cadre duquel les experts de Kaspersky Lab classeront les échantillons du programme malveillant transmis, analyseront ses fonctions et comportements et élaboreront des recommandations et un plan visant à supprimer ce programme malveillant de vos systèmes et à annuler toute action malveillante.

Kaspersky Industrial CyberSecurity : gestion centralisée de la sécurité

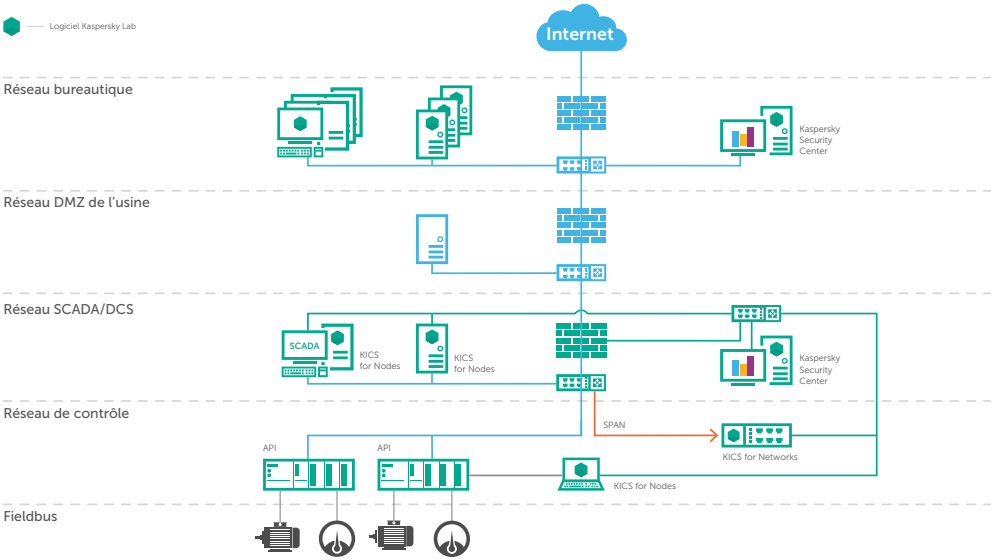
Kaspersky Security Center

Afin d'assurer les plus hauts niveaux de protection contre tous les vecteurs d'attaque, la sécurité industrielle de base doit être opérationnelle au niveau des postes et du réseau. Afin de garantir un contrôle optimal, une facilité de gestion et une bonne visibilité,

le contrôle de KICS se fait, comme pour toute technologie de protection Kaspersky Lab, via une console d'administration unique appelée Kaspersky Security Center. Cela permet :

- De bénéficier de la gestion centralisée des politiques de sécurité ; possibilité de définir différents paramètres de protection pour différents postes et groupes.
- De faciliter les tests des mises à jour avant leur déploiement sur le réseau, garantissant ainsi l'intégrité totale du processus.
- D'aligner l'accès basé sur les rôles avec les politiques de sécurité et les interventions urgentes.

Kaspersky Security Center garantit un contrôle facile et une visibilité, non seulement au niveau industriel sur plusieurs sites, mais également au niveau commercial, comme le montre l'image ci-dessous.



Kaspersky Security Gateway

KICS peut également envoyer des données concernant des événements spécifiques à d'autres systèmes, tels que des SIEM, des MES et des solutions de veille économique. Tous les événements et les anomalies détectés sont signalés aux systèmes tiers, notamment aux serveurs Syslog, SIEM, messageries et systèmes de gestion du réseau, en utilisant les protocoles CEF 2.0, LEEF et Syslog. Non seulement les solutions spécialisées de surveillance des réseaux industriels aident à détecter, à résoudre et à analyser les cyberattaques, mais elles contribuent également à la maintenance prédictive.

Intégration au sein des interfaces homme-machine (IHM)

La solution peut envoyer des notifications de sécurité directement aux IHM, ce qui fournit aux employés industriels les informations nécessaires pour réagir immédiatement et signaler le cyberincident.

Kaspersky Industrial CyberSecurity for Nodes

KICS for Nodes a été conçu pour lutter spécifiquement contre les menaces au niveau des opérateurs dans les environnements SCI. Il sécurise les serveurs SCI/SCADA, les IHM et les postes de travail des ingénieurs 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 SCD.

Facteurs de risques et menaces	Technologies Kaspersky Lab
Exécution de logiciels non autorisés	Listes blanches ; modes prévention ou détection seule (enregistrement plutôt que blocage)
Programmes malveillants	Moteurs sophistiqués de détection des programmes malveillants basés sur les signatures ; moteur de détection basé dans le Cloud qui utilise un Cloud public (KSN) ou un Cloud privé (KPSN) Kaspersky Lab
Cryptovirus, y compris les ransomwares	Technologie Anti-Cryptor
Attaques réseau	Pare-feu hébergé sur l'hôte
Connexion des appareils non autorisés	Contrôle des périphériques
Connexions sans fil non autorisées	Contrôle du réseau Wi-Fi
Imitation des programmes API	Vérification de l'intégrité des API
Spécificités des API : isolement (air-gap) ; faux positifs des processus/ logiciels des SCI, etc.	Mises à jour dignes de confiance, testées avec les logiciels des principaux fournisseurs industriels ; certification de produit par les principaux fournisseurs d'automatisation industrielle.

Listes blanches d'applications

La nature relativement statique des configurations des terminaux SCI signifie que les mesures de contrôle de l'intégrité sont bien plus efficaces que dans le cadre de réseaux dynamiques d'entreprise. Les technologies de contrôle de l'intégrité incluses dans KICS for Nodes permettent de :

- Contrôler l'installation et le démarrage des applications selon des politiques de listes blanches (bonne pratique pour les réseaux de contrôle industriel) ou de listes noires.
- Contrôler l'accès des applications aux ressources du système d'exploitation : fichiers, dossiers, base de registre, etc.
- Contrôler tous les types de fichiers exécutables qui s'exécutent dans un environnement Windows, à savoir : exe, dll, ocx, pilotes, ActiveX, scripts, interpréteurs de lignes de commande et pilotes en mode noyau.

- Mettre à jour les données sur la réputation des applications.
- Bénéficier de catégories d'applications pré-définies et définies par les clients pour gérer les listes d'applications contrôlées.
- Affiner le contrôle des applications pour différents utilisateurs.
- Bénéficier de modes de prévention ou de détection seule qui bloquent toutes les applications qui ne figurent pas sur la liste blanche ou, en mode « observation », qui autorisent ces dernières à s'exécuter tout en enregistrant cette activité dans le Kaspersky Security Center, où elle peut être évaluée.

Contrôle des périphériques

Gestion de l'accès des appareils amovibles, périphériques et bus informatiques selon la catégorie de l'appareil, sa famille et son identifiant.

- Prise en charge des approches par listes blanches et listes noires.
- Attribution granulaire des politiques par utilisateur et par ordinateur à un seul utilisateur/ordinateur ou à un groupe d'utilisateurs/d'ordinateurs.
- Mode prévention ou détection seule.

Pare-feu hébergé sur l'hôte

Configuration et application des politiques d'accès au réseau pour les postes protégés, tels que les serveurs, les interfaces homme-machine (IHM) ou les postes de travail. Les principales fonctionnalités comprennent :

- Le contrôle de l'accès aux réseaux et aux ports limités.
- La détection et le blocage des attaques réseau lancées à partir d'appareils internes, tels que les ordinateurs portables des sous-traitants, qui peuvent introduire des programmes malveillants qui essayent de scanner et d'infecter l'hôte dès qu'il se connecte au réseau industriel.

Contrôle du réseau Wi-Fi

Cela permet de surveiller tout tentative de connexion aux réseaux Wi-Fi non autorisés. La fonction de contrôle du réseau Wi-Fi repose sur la technologie de blocage par défaut, qui consiste à bloquer automatiquement les connexions à tout réseau Wi-Fi « non autorisé » dans les paramètres.

Vérification de l'intégrité des API

Cela permet de bénéficier d'un contrôle supplémentaire sur la configuration des API grâce à des vérifications périodiques de serveurs protégés par Kaspersky Lab. Les sommes de contrôle qui en résultent sont comparées aux valeurs « étalon » sauvegardées et tous les écarts sont signalés.

Protection avancée contre les programmes malveillants

Les meilleures technologies proactives de Kaspersky Lab en matière de détection et de prévention des programmes malveillants sont adaptées et repensées pour répondre aux exigences en termes de disponibilité des systèmes et d'utilisations de ressources. Notre protection avancée contre les programmes malveillants a été conçue pour fonctionner de manière efficace même dans les environnements statiques ou rarement mis à jour. La protection contre les programmes malveillants de Kaspersky Lab couvre toute une gamme de technologies, notamment :

- Détection des programmes malveillants basée sur les signatures.
- Détection à la demande et à l'accès.
- Détection en mémoire (programmes résidents).
- Détection des ransomwares via la technologie de lutte contre les programmes malveillants de chiffrement.
- Kaspersky Security Network (KSN) et Kaspersky Private Security Network (KPSN), qui permettent de bénéficier du meilleur service de détection des programmes malveillants.

Mises à jour de confiance

Afin de garantir que les mises à jour de sécurité de Kaspersky Lab n'aient aucun impact sur la disponibilité des systèmes protégés, des contrôles de compatibilité sont effectués avant la mise à jour de la configuration et des logiciels du système de contrôle des processus, ainsi que des composants et de la base de données. Les éventuels problèmes d'utilisation des ressources peuvent être résolus à l'aide de plusieurs scénarios différents :

- Kaspersky Lab effectue des tests de compatibilité des mises à jour de la base de données avec les logiciels du fournisseur SCADA dans le banc d'essai de Kaspersky Lab.
- Votre fournisseur SCADA effectue des contrôles de compatibilité.
- Kaspersky Lab contrôle les mises à jour de la base de données de sécurité pour vous : les images IHM, SCADA, poste de travail et serveur sont intégrées dans le banc d'essai de Kaspersky Lab.
- Les mises à jour de sécurité de Kaspersky Lab sont testées sur votre site et automatisées via le Kaspersky Security Center.

Kaspersky Industrial CyberSecurity for Networks

La solution de sécurité du réseau de Kaspersky Lab fonctionne au niveau du protocole de communication industriel (Modbus, pile IEC, ISO, etc.). Elle analyse le trafic industriel à la recherche d'anomalies grâce à une technologie DPI (inspection approfondie des paquets d'information) performante. Des fonctions de contrôle de l'intégrité du réseau et de détection d'intrusion sont également fournies.

Facteurs de risques et menaces	Technologies Kaspersky Lab
Apparition d'appareils non autorisés sur le réseau industriel	La fonction de contrôle de l'intégrité du réseau détecte les appareils nouveaux/inconnus
Apparition de communications non autorisées sur le réseau industriel	La fonction de contrôle de l'intégrité du réseau surveille les communications entre les appareils connus/inconnus
Commandes API malveillantes par : • L'opérateur ou un tiers (par ex. un sous-traitant) par erreur • Des actions (frauduleuses) menées de l'intérieur • Un pirate informatique/programme malveillant	La technologie DPI industrielle surveille les communications vers et en provenance des API et contrôle les valeurs des paramètres et des commandes du processus technologique.
Attaques réseau	Un système sophistiqué de détection des intrusions identifie tous les modèles d'attaque réseau connus, notamment l'exploitation des vulnérabilités des appareils et des logiciels industriels
Manque de données pour procéder à des analyses criminalistiques et à des investigations	Outils d'analyse criminalistique : surveillance et enregistrement sécurisé des activités suspectes des réseaux industriels et des attaques détectées

Inspection non intrusive du trafic sur le réseau industriel

KICS for Networks fournit une surveillance passive des anomalies du trafic réseau et de la sécurité du réseau, tout en restant invisible pour les potentiels pirates. Son installation est aussi simple que l'activation ou la configuration d'un miroir de port (port mirroring) ; l'intégration du dispositif logiciel/virtuel ou matériel au sein du réseau industriel existant est facilement réalisable via le port SPAN du commutateur ou de l'appareil TAP existant. KICS for Networks présente une architecture modulaire : ses capteurs peuvent être déployés indépendamment à partir d'une unité de commande centrale.

Technologie DPI industrielle pour la détection des anomalies

KICS for Networks permet aux industriels qui l'utilisent de bénéficier d'une plateforme de surveillance des données télémétriques et des flux de commande du contrôle des processus digne de confiance qui permet notamment :

- De détecter toute commande entraînant la reconfiguration d'un API ou la modification de l'état d'un API.
- De contrôler le paramétrage des processus technologiques.
- De se protéger contre les menaces extérieures tout en atténuant le risque d'interférence interne « avancée » provenant des ingénieurs, des sous-traitants SCADA ou de tout autre membre du personnel interne ayant directement accès aux systèmes.

Machine learning

Notre DPI industriel peut être configuré grâce à une approche standard basée sur des règles, mais il peut également détecter des anomalies au sein de processus industriels via un modèle de prévision puissant basé sur une mémoire LSTM. La fonctionnalité de machine learning optimise encore davantage la détection des anomalies industrielles, en permettant de repérer des incidents dans des réseaux industriels particulièrement complexes, aux reconfigurations fréquentes.

Contrôle d'intégrité du réseau pour la sécurité et l'inventaire des appareils

KICS for Networks permet d'identifier tous les appareils connectés au réseau par Ethernet, notamment les serveurs SCADA, les interfaces homme-machine, les postes de travail des ingénieurs, les API, les IED et les RTU. Tous les appareils nouveaux ou inconnus et leurs communications sont automatiquement détectés. Ceci permet aux équipes de sécurité d'élaborer leur propre inventaire sécurisé et fiable des appareils du réseau, au lieu d'utiliser des outils de gestion des appareils informatiques et technologiques potentiellement vulnérables, qui sont largement ciblés par les cybercriminels.

Outils d'investigation numérique

La solution de Kaspersky Lab permet aux industriels qui l'utilisent de bénéficier d'un système d'enregistrement sécurisé, doté d'outils pour effectuer des analyses de données et des analyses cybercriminalistiques. Ce système empêche également que des modifications ne soient apportées aux journaux du SCI.

Autres services pour Kaspersky Industrial CyberSecurity

Kaspersky Security Network

Kaspersky Security Network (KSN) est une architecture complexe, distribuée et basée dans le Cloud qui se charge de recueillir et d'analyser des renseignements sur les menaces de sécurité provenant de millions de postes du monde entier. Non seulement KSN détecte et bloque les nouvelles menaces et attaques de type « zero-day », mais elle permet également de localiser et de mettre sur liste noire les sources d'attaques en ligne, en fournissant des données sur la réputation des sites Web et des applications.

Toutes les solutions professionnelles Kaspersky Lab peuvent être connectées à KSN, y compris les solutions pour l'industrie. Les principaux avantages sont les suivants :

- Taux de détection élevés.
- Réduction du temps de réaction : les réactions traditionnelles basées sur les signatures prennent des heures, alors que KSN réagit en environ 40 secondes.
- Faibles taux de détection de faux positifs.
- Réduction de l'utilisation des ressources pour les solutions de sécurité sur site.

Kaspersky Private Security Network (KPSN)

Pour les entreprises ayant des problèmes de confidentialité des données très spécifiques, Kaspersky Lab a développé l'option Kaspersky Private Security Network. Elle permet de bénéficier de presque tous les avantages de KSN, sans toutefois envoyer d'information à l'extérieur du réseau.

KPSN peut être déployée au sein même du data center de l'entreprise. Les spécialistes informatiques en interne gardent ainsi le contrôle total de cette solution. Les installations locales de KPSN peuvent permettre de satisfaire aux exigences d'un pays en matière de conformité, ou de respecter toute autre législation spécifique à un secteur.

Principales fonctions de KPSN :

- Services de réputation des URL et des fichiers : les hashes MD5 des fichiers, les expressions régulières des URL et les comportements caractéristiques des programmes malveillants sont stockés et classés de manière centralisée, puis rapidement déployés chez le client
- Record Management System (RMS) : il arrive parfois que les logiciels de sécurité se trompent et classent par erreur des fichiers ou des URL comme étant fiables ou non fiables. RMS agit telle une barrière pour les faux positifs, en rectifiant les erreurs tout en effectuant des analyses en continu afin d'améliorer la qualité
- Informations et renseignements basés dans le Cloud.

Kaspersky® Industrial CyberSecurity

Kaspersky Industrial CyberSecurity est une gamme de technologies et de services conçus pour sécuriser les couches et composants technologiques de votre organisation (serveurs SCADA, interfaces HMI, postes de travail des ingénieurs, API, connexions réseau et ingénieurs), sans affecter la continuité des opérations ni la cohérence du processus technologique.

Pour en savoir plus, rendez-vous sur : **https://www.kaspersky.fr/enterprise-security/industrial**

Tout savoir sur la cybersécurité concernant les ICS :
https://ics.kaspersky.fr/
Actualités des cybermenaces : **www.viruslist.fr**

#truecybersecurity

www.kaspersky.fr

IIC MEMBER industrial internet CONSORTIUM

OPC® FOUNDATION MEMBER

CYBER SECURITY EXCELLENCE AWARDS ★ FINALIST ★ 2017

* « World Leading Internet Scientific and Technological Achievement Award » (prix du leader mondial en matière de réussite scientifique et technologique sur Internet) à la 3e World Internet Conference

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