KASPERSKY lab

KASPERSKY INDUSTRIAL CYBERSECURITY : PRÉSENTATION DE LA SOLUTION

www.kaspersky.fr/enterprise-security/industrial

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 2015[2].

En 2015, l'ICS-CERT a neutralisé 295 cyberincidents signalés impliquant des infrastructures critiques aux États-Unis, soit une hausse de plus de 20 % par rapport à 2014[3].

Depuis trois 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[4].

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.

Différences entre technologie opérationnelle et technologie de l'information

Le terme « système de contrôle industriel » (SCI) est utilisé pour décrire tous les systèmes automatisés qui contrôlent la production industrielle. Ce terme englobe une large palette d'ordinateurs, de dispositifs de commande propriétaires et d'architectures réseau utilisés pour contrôler les processus industriels dans divers secteurs. En règle générale, un SCI inclut des systèmes SCADA (télésurveillance et acquisition de données), des DCS (systèmes de contrôle distribués) et des API (automates programmables).

En ce qui concerne les systèmes des organisations, ces derniers peuvent être répartis dans deux catégories :

- Technologie de l'information : systèmes utilisés dans les entreprises classiques
- Technologie opérationnelle (TO) : systèmes utilisés pour l'automatisation industrielle.

De nombreuses stratégies en matière de sécurité informatique sont axées sur la protection des données et reposent sur le concept du modèle « C-I-D » : **Confidentialité**, **Intégrité** et **Disponibilité** des données. La plupart des systèmes TO donnent avant tout la priorité à la continuité ; la protection ne concerne pas les données, mais le processus : **Disponibilité**, **Intégrité** et **Confidentialité**, dans cet ordre. C'est ce qui distingue les besoins de l'industrie en matière de sécurité informatique ; même la meilleure solution de sécurité peut s'avérer inutile si elle met la disponibilité (dans certains cas, l'intégrité) des processus en péril.

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 ICS-CERT Monitor, novembre-décembre 2015

4 Allianz Risk Barometer 2015

RISQUES ET MENACES

En dépit de la prise de conscience croissante des cyberattaques sur les systèmes de contrôle industriel, 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 disponibles via Internet[5], que ce soit par choix ou non.

Une étude menée par Kaspersky Lab, basée sur les données provenant de Kaspersky Security Network, indique que la plupart des ordinateurs industriels sont infectés par le même programme malveillant simple, affectant ainsi les systèmes informatiques de l'entreprise, par exemple (sans toutefois s'y limiter) des coupables bien connus tels que les vers, les virus, les chevaux de Troie, les programmes potentiellement dangereux et indésirables (PUP) et autres failles ciblant les vulnérabilités du système d'exploitation Windows.

Bien qu'il ne soit pas spécifique à l'industrie, le ver Kido (également appelé Conficker) a non seulement été décelé dans des équipements médicaux critiques, mais il permettrait également d'ouvrir la voie à des attaques industrielles d'envergure. Kido est capable de surcharger complètement les réseaux et de suspendre les processus. Les techniques de sécurité industrielle traditionnelles ne peuvent neutraliser ces menaces de manière adéquate : une stratégie « d'isolement du réseau » (« air-gap ») ou de « sécurité par l'obscurité » ne tient pas compte du fait que les réseaux intelligents et les applications basées sur le Web rendent « les systèmes de contrôle industriels de plus en plus semblables à des ordinateurs grand public[6].

Le ransomware est une autre menace croissante pour les SCI. La diversité des ransomwares s'est largement étendue entre 2015 et début 2016. L'émergence du ransomware revêt une importance considérable pour le secteur industriel : de telles infections peuvent engendrer des répercussions significatives et endommager les systèmes de diverses manières, faisant ainsi du SCI une cible potentielle particulièrement intéressante. Le ransomware conçu pour attaquer les systèmes industriels peut avoir son propre objectif : au lieu de chiffrer les fichiers, 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 attaques ciblées et les programmes malveillants spécifiques des SCI : Stuxnet, Citadel, Energetic Bear/Havex, Miancha, BlackEnergy, Irongate, PLC Blaster ; et la liste s'allonge rapidement. Comme les attaques Stuxnet et Black Energy 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 spécifiques à l'industrie 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 parallèle, le centre d'appels du service a subi une attaque DDoS afin d'empêcher que les clients ne signalent la panne.

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

6 Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) : 'Can we learn from SCADA security incidents?' (Pouvons-nous apprendre des incidents de sécurité SCADA ?)

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 également avoir de graves conséquences. Kaspersky Lab a développé une gamme complète de technologies, de solutions et de services permettant à ses clients de combattre et de gérer bon nombre de ces risques, notamment :

- Erreurs commises par les sous-traitants ou les opérateurs SCADA (tierces parties)
- Actions frauduleuses
- Cybersabotage
- Conformité
- Manque de connaissances et de données concrètes pour l'analyse criminalistique des incidents
- Manque de signalement des incidents

La nécessité de spécialiser la cybersécurité industrielle

Seuls les fournisseurs de cybersécurité qui comprennent la différence entre les systèmes industriels et les systèmes standard des entreprises axés sur les activités commerciales sont en mesure de proposer des solutions qui répondent aux besoins uniques des infrastructures industrielles et des systèmes de contrôle industriel. Forrester Research recommande aux organisations industrielles à la recherche de fournisseurs de sécurité de « Rechercher une expertise spécifique à l'industrie[7] ». Forrester poursuit en identifiant Kaspersky Lab comme étant l'un des rares fournisseurs proposant des solutions de cybersécurité industrielle spécialisées et disposant d'une véritable expertise dans le domaine.

7 Forrester Research : S&R Pros Can No Longer Ignore Threats to Critical Infrastructure (Les professionnels des risques et de la sécurité ne peuvent plus ignorer les menaces qui pèsent sur l'infrastructure critique), par Rick Holland

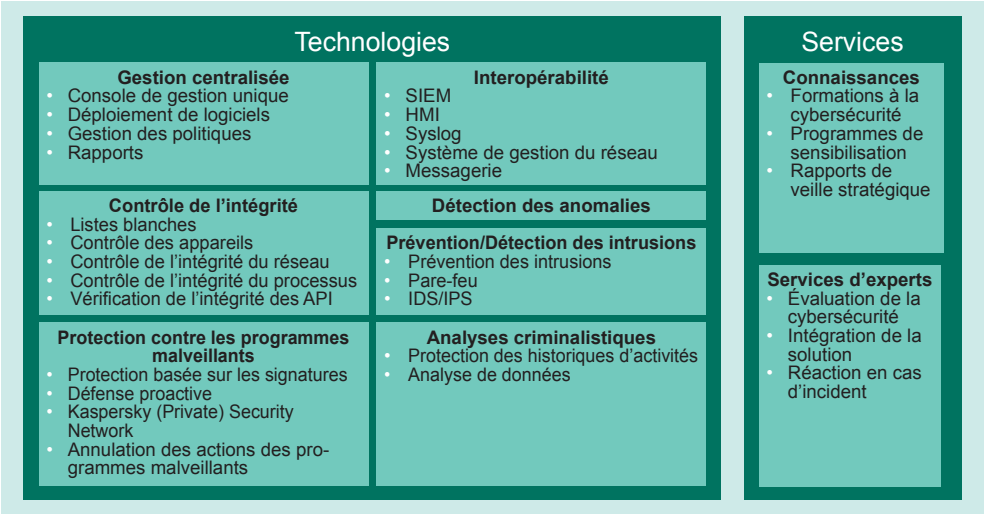
KASPERSKY LAB : UN FOURNISSEUR DE CYBERSÉCURITÉ INDUSTRIELLE DIGNE DE CONFIANCE

Leader reconnu dans la cybersécurité et la protection industrielle[8], 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 SCADA, 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 principales entreprises et les principaux fournisseurs d'automatisation industrielle, notamment Emerson, SAP, Siemens, Industrial Internet Consortium, pour 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 APT et les attaques extrêmement ciblées.

Kaspersky Lab développe une gamme de solutions spécialisées permettant de répondre aux besoins spécifiques du marché de la sécurité industrielle : Kaspersky Industrial CyberSecurity. Ces solutions permettent de bénéficier d'une sécurité efficace à tous les niveaux de l'industrie (serveurs SCADA, interfaces homme-machine, postes de travail, automates industriels programmables et connexion réseau inclus) contre les cybermenaces, sans affecter la continuité des opérations ni la cohérence du processus technologique.

En accord avec la stratégie de sécurité globale multi-niveaux de Kaspersky Lab, Kaspersky Industrial CyberSecurity fournit une combinaison de plusieurs types de protection. En complément des technologies et services prenant en charge chaque étape du cycle de sécurité, Kaspersky Industrial CyberSecurity offre une protection à l'appui du contrôle de l'intégrité, de la détection et de la prévention des intrusions, de la protection contre les programmes malveillants et de la détection des anomalies, entre autres.



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

KASPERSKY INDUSTRIAL CYBERSECURITY : SERVICES

Notre suite de services constitue une part importante de la gamme 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)

Formation à la cybersécurité : 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 la formation, les participants découvrent les cybermenaces qui les concernent et comment elles évoluent, ainsi que des méthodes efficaces pour s'en protéger.

Programmes de sensibilisation : Kaspersky Lab propose aux ingénieurs et responsables de la sécurité des jeux de formation 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 réelles sur des systèmes d'automatisation industrielle, montrant ainsi les principaux problèmes associés à la mise en place de la cybersécurité industrielle.

Rapports de veille stratégique : rapports de veille stratégique à jour préparés par les principaux experts de la cybersécurité, personnalisés selon les exigences des clients industriels.

Services d'experts

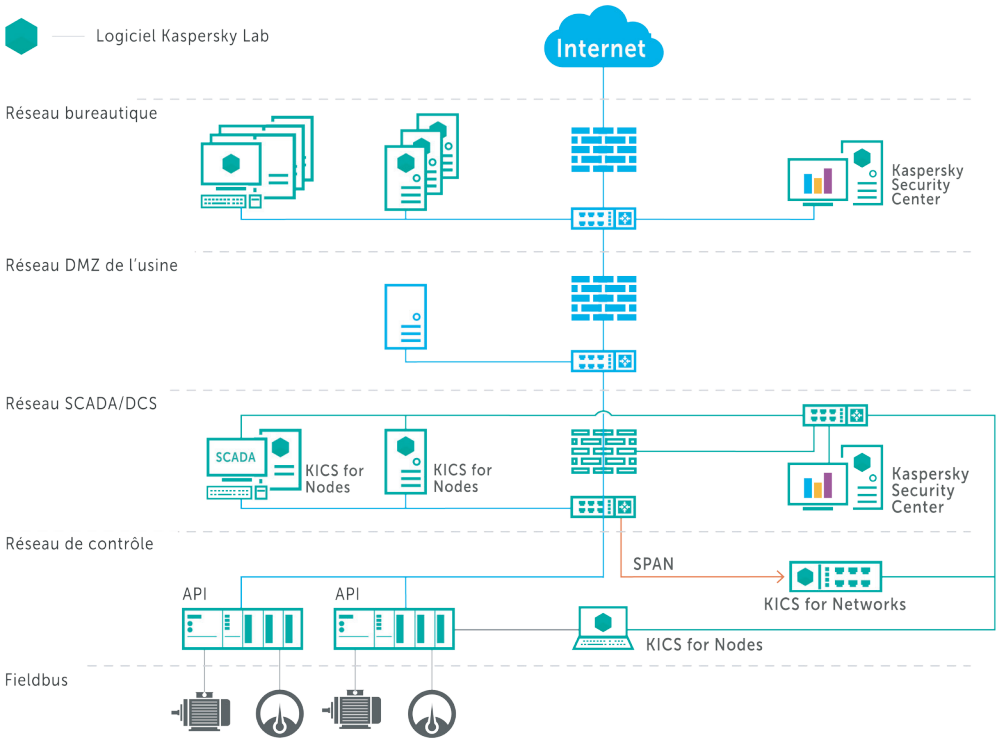
Évaluation de la cybersécurité : pour les organisations préoccupées par le potentiel impact de la sécurité informatique et technologique sur les opérations, Kaspersky Lab propose une évaluation peu invasive de la cybersécurité avant l'installation. Il s'agit d'une première étape cruciale dans la mise 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 industriel d'un client 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. Le service inclut la prise en charge des systèmes matériels et logiciels uniques (SCADA et API inclus) aux protocoles de communication de son réseau industriel.

Investigation sur les incidents : en cas d'incident de cybersécurité, nos experts collecteront et analyseront les données, reconstruiront la chronologie de l'incident, détermineront les éventuelles sources et raisons et élaboreront un plan visant à le résoudre. 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

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 de la visibilité, le contrôle de Kaspersky Industrial CyberSecurity se fait, comme pour chaque technologie de protection Kaspersky Lab, via une console d'administration unique, Kaspersky Security Center. Cette capacité de gestion centralisée garantit un contrôle facile et de la visibilité, non seulement au niveau industriel sur plusieurs sites, mais également au niveau commercial, comme le montre l'image ci-dessous.



KASPERSKY INDUSTRIAL CYBERSECURITY FOR NODES

Kaspersky Industrial CyberSecurity for Nodes a été spécialement conçu pour contrer les menaces dans les environnements SCI/SCADA. La solution fonctionne au niveau du serveur SCI/SCADA, de l'interface homme-machine et des postes de travail des ingénieurs pour fournir une sécurité optimale contre diverses cybermenaces dues à un facteur humain, des programmes malveillants simples, des attaques ciblées ou du sabotage. Elle est compatible avec l'ensemble des composants matériels et logiciels des systèmes industriels tels que SCADA, SCI et SCD.

Facteurs de risques et menaces	Technologies Kaspersky Lab
Exécution de logiciels non autorisés	Listes blanches ; modes prévention ou détection seule (pas de blocage, mais enregistrement de l'activité)
Programmes malveillants, zero-days inclus	Protection avancée contre les programmes malveillants : basée sur les signatures et proactive ; Protection automatique contre les Exploits et Kaspersky (Private) Security Network (KPSN)
Attaques réseau	Pare-feu hébergé sur l'hôte et Network Attack Blocker
Connexion des appareils non autorisés	Contrôle des appareils
Vulnérabilités logicielles	Évaluation des vulnérabilités
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 de confiance ; KPSN ; certification des principaux fournisseurs SCI ; coopération sur les listes blanches.

Contrôle de l'intégrité du matériel et des logiciels

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 Kaspersky Industrial CyberSecurity for Nodes comprennent :

Application Start-up Control et Application Privilege Control
Les mécanismes de contrôle des applications permettent entre autre 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 de l'accès aux appareils
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 et prévention des intrusions

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

Protection automatique contre les Exploits

Ceci permet de bénéficier d'une couche d'isolation qui protège les processus SCADA contre les modifications ou les injections de mémoire malveillante, telles que les charges utiles (Payload).

Vérification de l'intégrité des API

Permet de bénéficier d'un contrôle supplémentaire sur la configuration des API grâce à des vérifications périodiques de postes de travail ou de serveurs protégés par Kaspersky Lab. Les sommes de contrôle qui en résultent sont comparées aux valeurs « étalon » sauvegardées et 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 l'analyse des comportements, des signatures et heuristique
- Détection à la demande et à l'accès
- Détection en mémoire (programmes résidants)
- Détection des rootkits
- Kaspersky Security Network (KSN) et Kaspersky Private Security Network (KPSN) 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.

Évaluation des vulnérabilités

Fonctionnalité d'évaluation passive des vulnérabilités : détection et informations sur les vulnérabilités des logiciels sans interrompre les processus technologiques.

Contrôle, administration et déploiement centralisés

Kaspersky Industrial CyberSecurity for Nodes est déployé et géré via une console centralisée, ce qui 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 INDUSTRIAL CYBERSECURITY FOR NETWORKS

La solution de sécurité du réseau de Kaspersky Lab fonctionne au niveau de la couche logique du contrôle des processus, en analysant et inspectant les sources de trafic, tout en contrôlant l'intégrité du réseau industriel et des processus de contrôle industriel. Un ensemble intégré de technologies complémentaires forment un moteur de détection efficace des anomalies.

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	Surveillance des communications vers et en provenance des API et contrôle des valeurs des paramètres et des commandes du processus technologique.
Les opérateurs manquent de données sur les incidents de cybersécurité	Alerte l'opérateur (via l'intégration d'une interface HMI) des modifications suspectes ou malveillantes apportées aux paramètres du processus technologique.
Manque de données pour procéder à des analyses criminalistiques et à des investigations.	Outils d'analyse criminalistique : surveillance et enregistrement sécurisé des activités des réseaux industriels.

Inspection passive du trafic sur le réseau industriel : Effective Security Monitoring

Kaspersky Industrial CyberSecurity for Networks effectue des analyses passives des anomalies du trafic réseau, tout en restant invisible aux yeux des éventuels cybercriminels. Son installation est aussi simple que l'activation ou la configuration d'un miroir de port (Port mirroring) ; son intégration est facilement réalisable via le port SPAN du commutateur ou de l'appareil TAP existant.

Architecture hiérarchique, un seul point de contrôle

Les capteurs du trafic sur le réseau passivement connectés au segment du réseau contrôlé via le port SPAN ou l'appareil TAP sont gérés via une seule unité de contrôle qui permet de bénéficier des fonctionnalités suivantes :

- Récupération et stockage des données d'évènements provenant de tous les capteurs : utilisez-les pour réagir en cas d'incident et procéder à des investigations ou à des analyses criminalistiques
- Signalement de tous les évènements et anomalies aux systèmes tiers, notamment aux serveurs Syslog, SIEM, messageries et systèmes de gestion du réseau, en utilisant le protocole SNMP
- Surveillance de l'état général des systèmes
- Gestion via Kaspersky Security Center ou l'interface locale.

Surveillance digne de confiance du contrôle des processus industriels

La solution de Kaspersky Lab 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 toutes les commandes permettant de modifier l'état de l'API, notamment STOP, PAUSE, changer le programme API, changer le micrologiciel API
- De contrôler les algorithmes et les paramètres 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.

Intégrité du réseau et visibilité sur les appareils

Kaspersky Industrial CyberSecurity 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 technique, les API 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.

Analyses criminalistiques

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 criminalistiques. Ce système empêche également que des modifications ne soient apportées aux activités du système.

AUTRES SERVICES POUR LES PRODUITS DE CYBERSÉCURITÉ KASPERSKY : 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'attaque 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.

Pour en savoir plus sur Kaspersky Industrial CyberSecurity, rendez-vous sur :
www.kaspersky.fr/enterprise-security/industrial

KASPERSKY lab