Maîtriser les points faibles des systèmes OT

Les outils de cybersécurité conventionnels pour la gestion de la vulnérabilité et de la configuration ne connaissent pas les menaces qui pèsent sur les systèmes de contrôle et de commande industriels. Un flux de données (data feeds) standardisé et spécifique à l'OT peut être utile. Bernhard Aregger de BOLL Engineering explique dans une interview comment cela fonctionne.

Systèmes OT et cybersécurité – où en est-on?
Tout comme les systèmes informatiques, les systèmes de technologie opérationnelle (OT), dont les serveurs SCADA (supervisory control and data acquisition) et les systèmes de contrôle et d'automatisation industriels (IACS), ne sont pas à l'abri des cyberattaques, comme le montre régulièrement la pratique, y compris dans la région du DACH (Allemagne, Autriche et Suisse). Les cyberattaques utilisent les points faibles de ces systèmes pour s'infiltrer et causer des dégâts. Et de telles vulnérabilités sont loin d'être rares: la National Vulnerability Database (NVD) de l'autorité américaine de normalisation NIST recense des milliers de failles de sécurité dans les logiciels d'automatisation industrielle.

Quel est le problème par rapport aux systèmes informatiques?
Les outils courants de gestion des vulnérabilités et des configurations utilisent les recherches des fabricants et les données d'incidents collectées, également appelées «threat intelligence», pour identifier et neutraliser les vulnérabilités ou fournir des suggestions pour les corriger. Ces outils connaissent parfaitement les vulnérabilités des systèmes informatiques. En revanche, il y a un manque général de la threat intelligence sur les systèmes OT avec leurs protocoles en partie propriétaires et très spécifiques. Il faut donc des solutions qui connaissent également le monde OT et qui disposent des données correspondantes.

Bernhard Aregger, sales specialist chez BOLL, est notamment responsable des produits de Kaspersky.

Comment les solutions de sécurité traitent-elles les données relatives aux vulnérabilités?
Les informations sur les vulnérabilités parviennent aux outils de sécurité entre autres sous la forme de flux de données lisibles par machine. Ces informations peuvent provenir de la threat intelligence du fabricant de l'outil, mais aussi d'autres sources. Il existe un standard open source appelé OVAL (open vulnerability and assessment language) pour la transmission d'informations sur les vulnérabilités entre différents outils et services de sécurité.

Comment utiliser concrètement de tels flux de données?
Les flux de données OVAL peuvent être intégrés dans des solutions de gestion des vulnérabilités compatibles à →

l'aide d'interprètes OVAL open source et fournissent des informations détaillées sur les vulnérabilités détectées, généralement dans un format XML. Ces informations comprennent par exemple la description, le nom et la version du logiciel concerné, ainsi que le degré de gravité et le score CVSS. En outre, ces flux peuvent contenir des instructions sur la manière de limiter les dommages.

Tout cela paraît bien théorique – les flux de données OVAL liés à l'OT existent-ils vraiment?
Oui, un exemple est le Kaspersky Industrial OVAL Feed for Windows. Il est basé sur des données provenant de différentes sources officielles telles que NVD, MITRE et US-CERT, mais aussi de fournisseurs de sécurité et d'OT ainsi que de communautés d'utilisateurs. Les propres recherches de l'équipe ICS-Cert de Kaspersky complètent ces informations provenant de sources tierces. L'équipe analyse toutes les données et recherche les éventuelles informations erronées qui pourraient entraver l'identification et l'évaluation correctes des vulnérabilités.

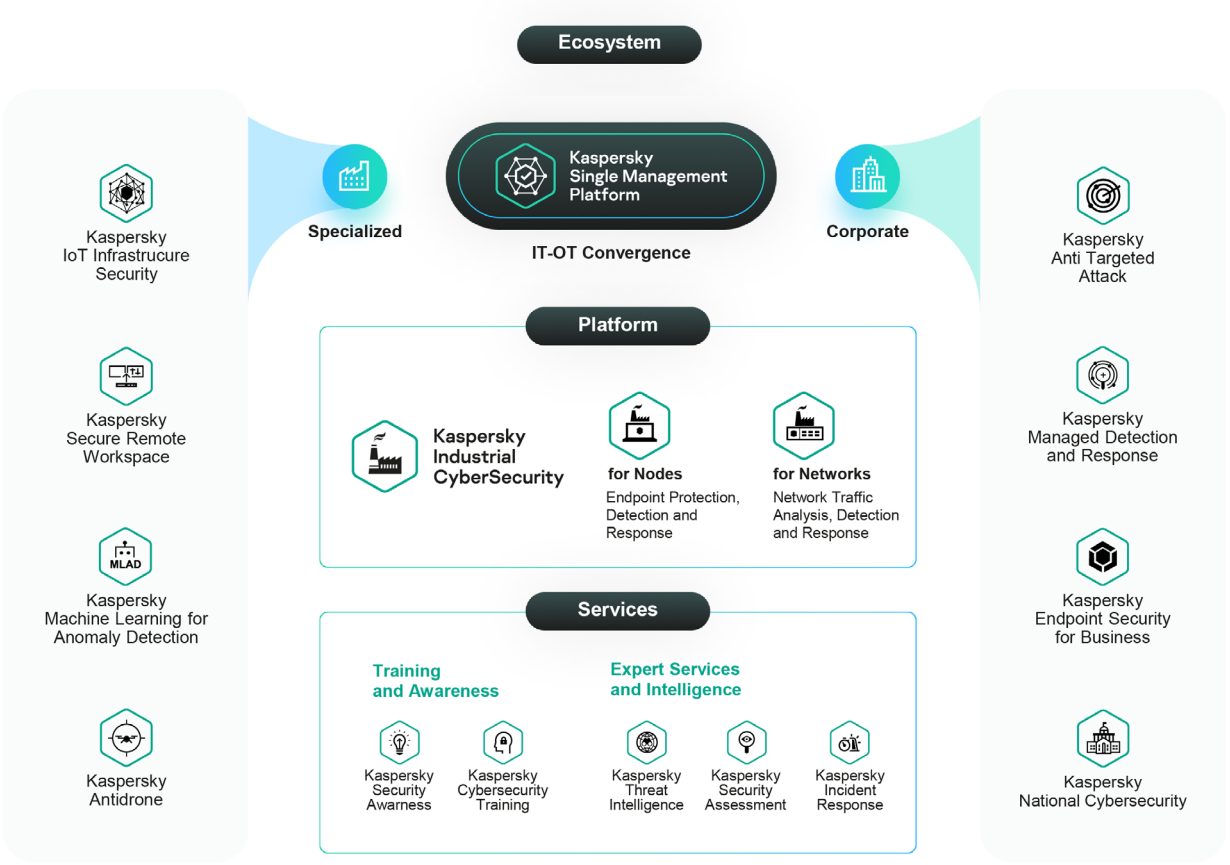
Quels sont les systèmes OT couverts par le flux de données?
Le flux de données prend en compte les produits OT de fabricants leaders mondiaux tels que Siemens, Schneider Electric, Yokogawa et Emerson. D'autres systèmes peuvent être ajoutés en fonction des besoins des clients. Les mesures de limitation des dommages recommandées dans le flux de données se basent sur l'expérience de l'équipe ICS-Cert et suivent les recommandations du fournisseur OT ou SCADA concerné.

Et quelles solutions s'entendent avec OVAL?
C'est tout naturellement que la solution KICS de Kaspersky (Kaspersky Industrial CyberSecurity) entre en jeu. Industrial OVAL Feed for Windows fait partie intégrante de cette plateforme de sécurité complète spécialisée dans l'OT, qui couvre pratiquement tous les aspects des produits de surveillance, de contrôle et d'automatisation industriels – des systèmes SCADA aux éléments de contrôle comme les PLC. OVAL est en outre soutenu par plusieurs autres fournisseurs. Citons par exemple Red Hat, qui prend directement en charge les définitions OVAL dans Enterprise Linux, et Cisco.

BOLL
IT Security Distribution

BOLL Engineering SA
Jurastrasse 58
5430 Wettingen

Tél. 056 437 60 60
info@boll.ch
www.boll.ch



→ **boll.ch/kaspersky**