JIRIKADERABEK - FOTOLIA

Cybelius mise sur une approche globale de la sécurité des environnements industriels

Créée en juillet 2017 comme une spin-off d'un spécialiste de l'ingénierie des systèmes industriels, la jeune pousse française avance avec une sonde dédiée, une offre de services, et une armoire dédiée à la sécurisation des échanges en IT et OT.

Valéry Marchive, Rédacteur en chef

Publié le: **31 janv. 2018**

Cybelius compte parmi ces jeunes pousses qui ambitionnent d'aider à sécuriser les systèmes informatiques industriels (ICS/Scada). Vincent Nicaise, son directeur marketing, revendique d'ailleurs une spécificité : venir du monde de l'industrie, des automatismes, et non pas de la cybersécurité IT. De fait, Cybelius s'apparente à une spin-off de FPC Ingénierie, un spécialiste de l'informatique et de la sûreté des installations industrielles. C'est là qu'est née la sonde CyPres sur la base de laquelle s'est fondé Cybelius en juillet 2018. Les deux entreprises font partie du groupe Stellis. Vincent Nicaise explique qu'il s'agissait de donner sa propre autonomie à l'activité cybersécurité industrielle.

SUITE DE L'ARTICLE CI-DESSOUS

CyPres est donc une sonde réseau centrée sur le monde industriel. Elle est bien sûr capable de découvrir des anomalies sur la base du trafic observé, comme tout système de détection d'intrusion (IDS), mais elle est capable d'aller bien loin en plongeant dans l'analyse des protocoles utilisés dans les systèmes industriels.

Une sonde aux règles taillées sur mesure

Vincent Nicaise explique que Cybelius accompagne ses clients dans le déploiement de sa sonde. Le but est de restituer les tables d'échanges entre les automates, ainsi qu'entre les automates et la supervision, pour en retirer des règles de détection taillées sur mesure. Cette approche doit permettre d'assurer une comparaison entre ce qui est prévu côté supervision, et ce qui se produit réellement sur le terrain, pour éviter, par exemple, des altérations comme dans un scénario de type Stuxnet.

Vincent Nicaise revendique là un positionnement « à mi-chemin entre la cybersécurité et la détection de dérive de processus ». Il souligne que Cybelius travaille actuellement avec Inria à l'adaptation d'algorithmes d'apprentissage automatique pour ajouter à cela une couche de détection de dérive comportementale.

L'accompagnement des clients

Cybelius met également à profit sa sonde pour son offre de services : elle permet de cartographier les flux. Et ce n'est pas un luxe : « neuf fois sur dix, les cartographies ne sont pas à jour ». L'entreprise a d'ailleurs développé, en interne, une méthode d'analyse de risque associant la cybersécurité à la sûreté de fonctionnement, voire à la sûreté physique et à la gestion de la malveillance.

Cybelius a en outre profité du Forum International de la Cybersécurité (FIC), qui se déroulait fin janvier à Lille, pour annoncer la signature d'un partenariat avec GFI Informatique. Dans le cadre de celui-ci, il sera possible d'exploiter des données remontées dans le système de gestion des informations et des événements de sécurité (SIEM) par d'autres systèmes, comme les badgeuses, pour générer des alertes, par exemple lorsqu'une personne se connectant en interne à la supervision est censée… avoir quitté les lieux.

Mais Cybelius a aussi un autre produit dans sa manche : CyFence, une armoire pouvant embarquer à la carte une dizaine de services. Vincent Nicaise la décrit comme une DMZ encadré par deux pare-feu, l'un côté système d'informatique bureautique (IT) et l'autre côté système d'information industriel (OT). C'est donc entre les deux que les services sont produits. Et l'éventail est large.

Et la sécurisation des échanges

CyFence peut ainsi héberger un serveur de déploiement des mises à jour des antivirus pour l'OT. Celles-ci peuvent être testées sur des copies de systèmes de production hébergés sur des machines virtuelles – toujours dans l'armoire. Cette dernière peut gérer les accès distants pour la télémaintenace, avec VPN, et authentification sur la base d'une réplique de l'annuaire IT, et contrôle temporel des accès.

L'armoire peut également servir de zone de dépôt tampon, que ce soit pour la remontée de données de production vers l'IT, ou pour la mise à disposition de données spécifiques pour l'OT – données de programmation, nouveaux firmwares, etc. Ces capacités de stockage peuvent également être mises à profit pour stocker, à des fins de sauvegarde et d'aide à la reprise d'activité, des logiciels de stations de travail, des programmes d'automates ou encore des données de configuration. Et le tout avec possibilité de suivi de versions. Bien sûr, les journaux d'activité de tous les services produits sur l'armoire peuvent être remontés à un SIEM.

Mais les capacités de virtualisation de l'armoire peuvent également être mises à profit pour virtualiser des postes d'ingénierie, de supervision ou de programmation. Un bénéfice dans certains environnements, souligne Vincent Nicaise, où il n'est pas rare de trouver un même poste utilisé à plusieurs de ces fins.

Et évidemment, la sonde CyPres peut être déployée dans l'armoire. Cette dernière peut profiter d'un stockage et d'une alimentation redondants ; l'armoire elle-même peut être déployée en redondance. Et optionnelle, là où la criticité en justifie le coût, il est possible d'intégrer des diodes unidirectionnelles.

Sur le même sujet

Petit guide spécial Ransomware
–LeMagIT

Des systèmes critiques au coeur des enjeux de cyberdéfense
–LeMagIT

Information Sécurité n°6 : Orchestration et Automatisation
–LeMagIT

L'utilisateur, éternel maillon faible de la cybersécurité
–VMware

Pour approfondir sur Cyberdéfense

Cybelius et Sesame IT préparent leur sonde réseau durcie pour IT et OT

Par: Valéry Marchive

Cisco dote les équipements industriels d'une intelligence serveurs

Par: Yann Serra

Systèmes industriels : Gatewatcher embarque le moteur de détection de Nozomi

Par: Valéry Marchive

Les 3 points de sécurité à prendre en compte sur un SD-WAN

Par: Kevin Tolly