IT for Business

Big data et IA accélèrent la convergence des réseaux IT, ceux de l'informatique de gestion, et OT, ceux des objets industriels. Ce mouvement de fond impose plus de collaboration entre les directions industrielles et les DSI sur la cyber. Une démarche indispensable avant de penser à des SOC communs IT et OT.

La convergence IT/OT *bute à la porte du SOC*

Le modèle d'une informatique industrielle totalement isolée a vécu. La démarche Industrie 4.0 impose au contraire de plus en plus d'échanges de données avec l'extérieur. Une telle transformation s'accompagne d'une montée en flèche du risque d'attaque : en 2024, le spécialiste de la sécurité dans le cloud Zscaler a bloqué 45% de plus de malwares visant l'IoT qu'un an auparavant.

Le rapport 2024 de l'observatoire de la convergence IT-OT NXO et Cisco dressait aussi un constat plutôt alarmant : 75% des décideurs déclaraient que leur niveau de connaissance sur ce sujet était partielle ou très faible, et 34% seulement estimaient que leurs réseaux industriels OT étaient bien définis dans leur organisation. Franck Bonnard chez NXO a toutefois noté une amélioration ces derniers mois : *«Nous avons observé une accélération de la prise en compte des problématiques cyber de l'OT par les DSI. Ceux-ci s'emparent du sujet car les métiers ont besoin de données pour mesurer et améliorer les performances de leurs processus et mettre en œuvre les IA.»*

Dans un tel contexte, quelle organisation cyber adopter ? Pour Sabri Khemissa, cofondateur de Fortress Cybersecurity, il y a trois grandes catégories d'organisations. *«Il y a celles où la DSI va progressivement prendre en charge la cybersécurité des installations. Une autre approche est d'étendre le périmètre d'action du RSSI. Sa position est un peu ambivalente, car il doit protéger des ressources qui ne sont pas sous la responsabilité de la DSI, tout en lui reportant parfois... Enfin, il y a des cas où la direction industrielle se saisit elle-même du sujet cyber.»* Vincent Nicaise, responsable des partenaires industriels et de l'écosystème chez Stormshield, confirme : *«Dans certains contextes, les usines restent maîtresses de la cybersécurité, car elle fait partie de la sûreté de fonctionnement qui est de leur ressort. C'est un vrai enjeu, car elles ont les budgets.»*

Si les acteurs montent en compétence sur l'OT, la convergence des SOC IT et OT n'est pas encore à l'ordre du jour : *«Ils sont de natures très différentes»*, explique Khalil Bajnati, SOC/CSIRT leader chez Serma Safety & Security, filiale du groupe industriel Serma, qui développe des offres de SOC OT mises en œuvre sur les entités industrielles du groupe, avant de les proposer à des tiers. L'intégration IT/OT va donc devoir faire entrer des experts avec des compétences industrielles dans les SOC. Comment savoir en effet que sur tel ou tel système SCADA, modifier un simple paramètre de vitesse de rotation ou de déplacement peut avoir des conséquences graves et endommager une machine ? L'IA pourrait assez rapidement apporter des éléments de réponse à ce type de questionnement. Mais la convergence des SOC prendra plus de temps.

ALAIN CLAPAUD

TÉMOIN **Franck Bonnard,** consultant connectivité et cybersécurité des environnements convergés IT-OT chez NXO

Mettre la cybersécurité à hauteur d'atelier

«La priorité est de mettre la cybersécurité à hauteur d'atelier. Les DSI doivent faire l'effort d'amener des solutions simples et opérables par les métiers avec un certain degré d'autonomie. Le contre-exemple, c'est la mise en œuvre d'un bastion qui reste compliquée et ne peut se faire sans la DSI. Or la solution doit être exploitable directement par les métiers. Il ne faut pas devoir appeler un administrateur réseau pour créer un accès un dimanche soir à 23h pour l'intervenant qui doit dépanner une machine et reprendre la production !»