Numéro 02

Mars 2020

CYBELIUS REVIEW

INDUSTRIAL CYBER SOLUTIONS

La **Cybelius Review** : votre rendez-vous en cybersécurité industrielle

L'humain dans la cybersécurité industrielle

Cybelius Review

Une étude menée par nos experts en cybersécurité industrielle.

Ce second numéro a été réalisé par *Frédéric Planchon,* fondateur et CEO de Cybelius.

Prochaines publications

- Numéro 3 : Les promesses mesurées de l'AI en cybersécurité industrielle
- Numéro 4 : La fascination de la menace

Introduction

La technicité du sujet – **la cybersécurité des systèmes industriels** - focalise l'attention sur les mesures techniques de protection des systèmes. Cependant tous les référentiels sont clairs : les mesures organisationnelles sont aussi importantes. Ce terme recouvre l'action des humains, qu'il s'agisse de simples utilisateurs du système, des administrateurs, des concepteurs. Et, de même qu'un outil et l'humain qui s'en sert forment un couple dont l'efficacité dépend des deux, la solidité de la sécurité dépend bien de la cohérence entre mesures techniques et mesures organisationnelles.

Il est intéressant d'analyser le rôle des humains, cette réflexion doit - entre autres - permettre de développer des outils de sécurité qui leur sont mieux adaptés. En allant dans le sens d'une ergonomie de la sécurité, on améliorera l'efficacité des systèmes de défense.

L'humain dans la cybersécurité industrielle

Le facteur humain

Lorsqu'un humain est dans une chaine d'action, le facteur humain doit être pris en compte. Le domaine a plusieurs décennies. Dès qu'une action doit être entreprise, la question de la bonne information de l'acteur, de sa capacité à les comprendre, à les intégrer, et à faire les bons choix est fondamentale. Ce n'est pas pour rien que les drones sont toujours pilotés : les automatismes ont des limites, notamment leur domaine de validité. Tout automaticien a un jour été confronté à la combinatoire des entrées sur son algorithme, et la réduction de cette combinatoire est une condition de réalisation de l'automatisme lui-même.

A ce sujet les tentatives actuelles avec l'intelligence artificielle présentent un prolongement intéressant. Là où l'automate va devoir formaliser son algorithme, l'AI pourra intégrer la diversité des situations sans la modéliser, et sans même la formaliser.

Et pourtant cela ne vient pas à bout de la combinatoire initiale : les données en nombre suffisant, non biaisées, et qui permettraient une inférence correcte des situations non présentes en apprentissage, cela n'existe pas. Mais ceci sera l'objet d'un autre article.

Il a très tôt été montré que la limite des automatismes n'est pas compensée entièrement par l'humain. Ce dernier sait traiter de situations non prévues, ou hors combinatoire. Mais il ne sait pas traiter toutes les données à la vitesse d'une machine. Il a besoin de synthèse, de temps, et d'une forme d'environnement de réflexion – action, choses étrangères à une machine. Le stress est un déformant majeur de cet environnement, par exemple, qui conduit à mal analyser les situations et faire de mauvais choix. Cela a notamment été le cas à Fukushima.

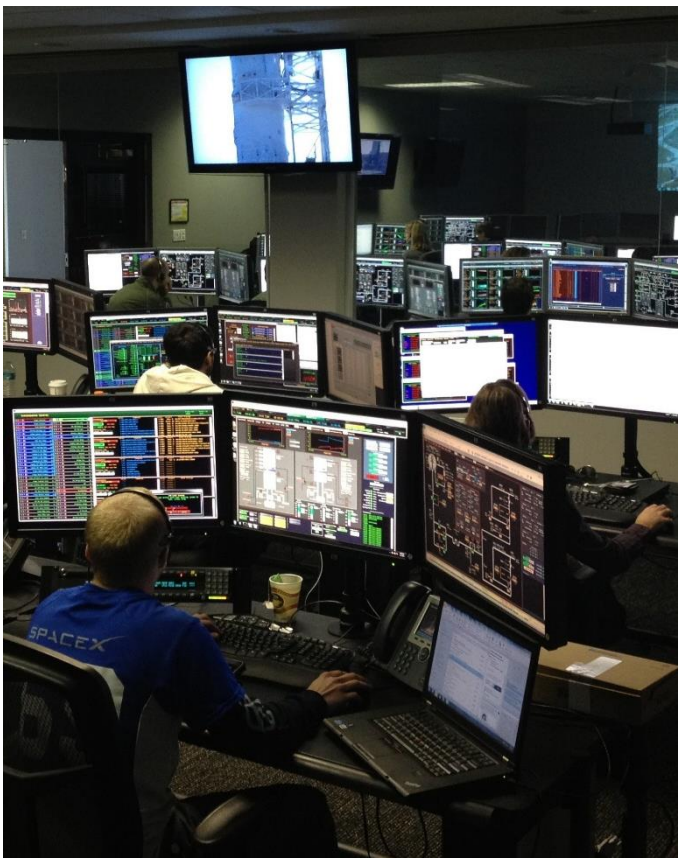
L'humain lorsqu'il est être acteur ou décisionnaire, doit avoir des automatismes dans les situations connues qui requièrent une réponse univoque et rapide : c'est l'entraînement. Il doit aussi pouvoir évaluer les situations pour pouvoir comprendre que la réponse automatique n'est pas la bonne : c'est la conscience de la situation. Enfin il doit dépasser ce que lui présente les instruments, pour appréhender la situation avec d'autres éléments : notamment son expérience, ses sens, sa connaissance du contexte.

L'expérience permet de se rendre compte qu'un instrument ne donne pas la bonne information, soit par une incohérence avec d'autres données, soit parce que physiquement il y a quelque chose d'invraisemblable. Les sens renseignent sur la réalité, qu'un système informatique représente, mais ignore (ce qui rend possible l'écart). La connaissance du contexte permet de plonger chaque situation au sein d'une sorte de méta-situation qui valide ou invalide la réponse usuelle. Une intervention de maintenance sur un équipement communicant peut amener à des informations diffusées tout à fait fausses, en cours d'essai par exemple. Dans ce dernier cas, soit le système est bien fait et le mode essai est activé et invalide les données, soit il est mal fait et seul l'humain peut corriger cette erreur.

En revanche, on peut submerger un humain, l'alimenter en informations fausses, biaiser ses outils, enfin prendre sa place numérique, son rôle au sein d'un système. Ces quatre formes d'attaque sont au cœur de la cybersécurité.

Cybersécurité et réalité

A la base, un système industriel représente numériquement un process et donne les moyens d'agir sur lui. Il s'agit d'un ensemble de données, dont une partie est liée à une réalité physique et temporelle : les informations captées et les ordres émis. La transformation d'une réalité physique en donnée numérique est un maillon terrible de la chaîne. On passe du réel au numérique. C'est très apparent précisément dans la réalité virtuelle, qui est une sorte de rétroaction du numérique vers le réel ; mais c'est vrai d'une simple acquisition de position de vanne ou de disjoncteur.



La cybersécurité n'existe que dans le champ du système numérique.

La menace spécifique aux systèmes industriels concerne la réalité physique.

L'humain est entre les deux :

- L'exploitant vit dans la réalité de son process
- L'administrateur et l'informaticien ne connaissent que le système numérique.

Une illustration de cette dissociation se trouve dans le cas si fréquent (hélas) de la panne provoquée par un système informatique. Lors du debug, l'informaticien ayant compris le problème annonce que c'était normal, au sens que l'informatique a bien fait ce qu'on lui a programmé de faire. Mais cette normalité-là est incompatible avec la normalité de la réalité, qui est que les choses doivent fonctionner.

On se trouve là au fondement de la méfiance, voire de la critique, des exploitants et même des automaticiens envers les informaticiens, et, « pire » qu'eux, les spécialistes en cybersécurité. Ces derniers se concentrent sur leur système informatique, pour son bon fonctionnement, pour son intégrité. Mais ce qu'il effectue, son objet, cela ne les concerne finalement pas beaucoup.

L'exploitant lui a besoin d'un contrôle-commande qui fonctionne. Pour cela il n'a que faire des technologies proposées. Si on lui représente son process, les informations doivent être exactes. S'il envoie une commande, elle doit arriver rapidement à destination et être effective dans le monde réel, et il lui est relativement indifférent qu'elle passe par de la communication cryptée ou des ondes courtes.

L'approche IT de la cybersécurité n'est pas confrontée à cette situation, l'ensemble des acteurs – et l'ensemble des actions – restent dans le monde informatique. Ceci explique, en partie, pourquoi l'approche cyber IT ne se transpose pas aisément au monde OT.

Le jeu d'acteurs

On a donc besoin

- **D'humains complémentaires aux systèmes informatiques**, qui puissent dépasser leurs limites des situations qu'ils savent traiter ;
- **D'opérateurs et exploitants concentrés sur le réel**, et d'informaticiens concentrés sur l'outil informatique qu'est le contrôle-commande.

Et par nature, les interventions des humains dépendent du nombre d'information, de son expérience, de sa connaissance du contexte global. Cela amène à une moins bonne réponse automatique, mais une meilleure réponse dans les cas d'exception.

Le système informatique peut être attaqué pour lui-même, mais aussi pour déstabiliser l'humain avec les quatre facteurs cités plus haut : le submerger de données, fausser ses informations, biaiser ses outils, usurper sa place.

Enfin, et peut-être surtout, il faut voir qu'une attaque est toujours un acte émanant d'une personne, a minima dans son intention, et presque toujours dans son exécution. Même si on peut s'attendre à des attaques de plus en plus automatisées (et l'AI dans ce cadre ouvre des perspectives assez effrayantes), il s'agit actuellement d'un « jeu » d'attaque –défense organisé, piloté, orchestré par des personnes. La créativité et l'évolutivité extraordinaire des techniques d'attaque sont le fait de personnes.

Comment progresser avec ces éléments pour bâtir une défense supérieure à l'attaque ?

Et pour rendre les choses un peu moins simples, il convient d'ajouter que si l'humain peut être malveillant, il peut aussi être maladroit, et parfois … absent. La tendance au dépostage des postes de conduite va de pair avec une astreinte évoluée, mais cette dernière est aujourd'hui pensée en termes de sûreté de fonctionnement uniquement.

Tant qu'un système industriel ne sera pas relié à un **SIEM**, il y a peu de chance que les alertes cyber soient traitées – pour la simple raison qu'elles n'existeront pas.

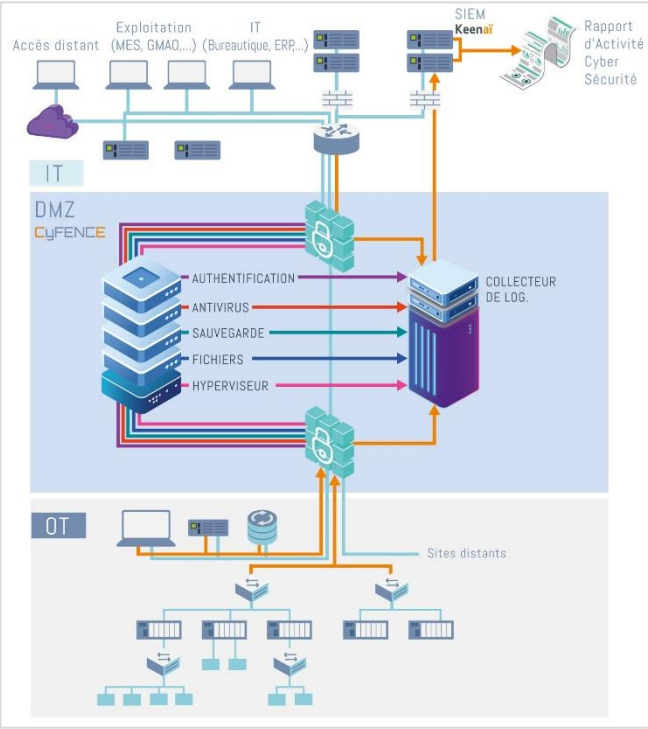
Mais le SIEM est un outil du monde informatique seul et ne sait pas traiter du monde réel, c'est quelque chose qui n'existe même pas au bout de ses logs et alertes.

Approche Cybelius

Nous estimons que la bonne réponse consiste à combiner les bonnes pratiques des deux mondes.

Pour **l'analyse de risque**, il nous parait impératif de pouvoir relier des causes cyber (des attaques de tout type) à des problèmes fonctionnels ; plus exactement, à s'intéresser essentiellement aux attaques qui peuvent avoir un effet fonctionnel. Celles qui n'en ont pas sont en effet bénignes, au seul bémol de l'exfiltration de données confidentielles. Il y en a peu dans un contrôle-commande, sauf si celui-ci effectue du comptage à but contractuel.

C'est la raison pour laquelle notre **méthode d'analyse de risque** a un acronyme qui finit par RO pour Risques Opérationnels.



Concernant la mise en sécurité, et notre produit **CyFENCE**, celui-ci est une interface entre les deux mondes. Côté haut, on est dans le monde IT avec le déploiement et l'administration des services de sécurité. Côté bas, on est proche du terrain et dans le monde physique, là où les actions peuvent engendrer un effet souhaité … ou pas sur le process. La partie OT est à la main des exploitants et automaticiens, la partie IT est à la main des DSI.

Ce check-point entre les deux mondes se double par ailleurs d'une capacité d'alerte IT avec l'offre récente « **CyFENCE & SIEM Services** ». Basiquement, les syslogs collectés par **CyFENCE**, qui sont très nombreux, sont collectés et traités par le SIEM de notre partenaire **Gfi**, **Keenaï**. Ce dernier effectue les actions suivantes :

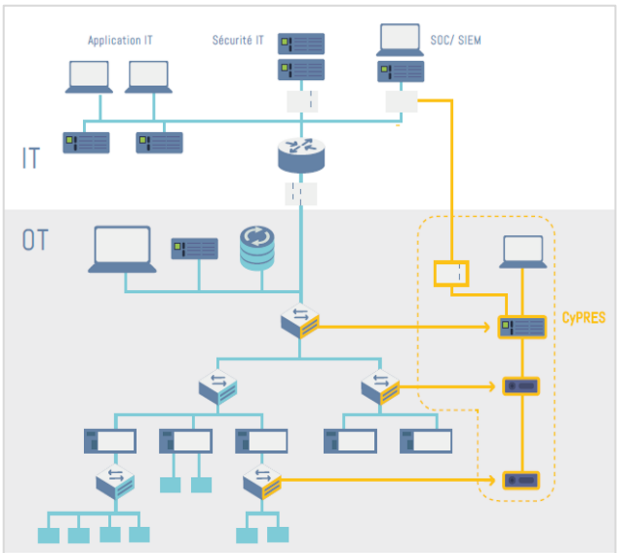
- **La collecte des événements produits par les équipements et applications :** firewalls, antivirus, serveurs web, applications métier, systèmes de détection d'intrusions, …
- **La centralisation et le stockage des événements issus des modules de collecte**,
- **La normalisation, l'analyse et la corrélation des événements de sécurité,**
- **La présentation synthétique** (tableaux de bords, statistiques, ...) **de la sécurité du SI,**
- **L'envoi d'alarmes pour notifier des incidents de sécurité.**

Si la génération d'alerte correspond à ce qu'on trouve usuellement dans le monde IT, la production de rapport est effectuée par rapport aux mesures de sécurité industrielle. Outre la permanence du système et le suivi de ses évolutions propres, le rapport contient les nouvelles vulnérabilités apparues sur ses composantes, l'activité d'accès distant, les authentifications réussies et refusées, les fichiers transférés. Tout cela correspond à des actes d'exploitation, en principe ; en donner une visibilité au monde IT permet justement de vérifier qu'il n'y a pas fraude et intrusion.

Notre sonde **CyPRES** a été pensée depuis sa conception initiale pour rapprocher les deux mondes et notamment intégrer l'exploitant dans la chaine de la cybersécurité.

- Par rapport aux problèmes de submersion d'information, les alertes de **CyPRES** ont un niveau de regroupement appelé Diagnostic, qui agglomère une quantité plus ou moins grande de symptômes ;
- Par rapport aux informations fausses, la contextualisation joue un grand rôle. Un contexte pour **CyPRES** est constitué d'un état donné du process, en termes de fonctionnalités actives ; d'un état du contrôle-commande, dans ses modes de fonctionnement (et incluant donc le mode essai) ; d'un état des personnes qui y sont connectées. Cet ensemble d'information, malgré une combinatoire très riche, est très facile à appréhender pour un humain et l'exploitant est alors le mieux placé pour valider, sur un diagnostic, l'origine malveillante ou non du problème ;
- Pour ce qui est des outils faussés et, de manière similaire, d'une identité usurpée, l'heuristique comportementale de **CyPRES** permet de détecter des actions non légitimes, au sens de leur cohérence process, de leur cohérence contextuelle, et demain au sens de leur cohérence temporelle.

Ainsi est-il possible de mettre en place avec **CyPRES** une véritable fonction de levée de doute, effectuée par l'exploitant, avec tous les outils pour analyser un problème. Cette capacité devrait permettre d'alerte bien plus rapidement la DSI sur un acte malveillant.



CyPRES : protection organique
Technologies spécifiques Cyber OT

Le duo **CyFENCE – CyPRES** permet même d'obtenir les traces de l'intrusion, les modifications apportées au système, les effets de l'attaque sur le système de contrôle-commande, avant même que ces effets ne descendent jusqu'au process lui-même. **CyPRES** a besoin de l'exploitant pour produire cette valeur, et l'exploitant sans **CyPRES** est aveugle sur les intrusions. La DSI est alertée par les syslogs de **CyPRES**, grâce aux syslogs collectés et traités.

Cette réponse est encore à améliorer. Dans tous les cas, pour Cybelius comme pour toutes les solutions techniques et technologiques, on n'arrivera à rendre la défense plus forte que l'attaque que par le couple humain – outil. Notre ambition est d'intégrer les hommes du réel, du contrôle-commande, dans ce couple, car on bénéficie là d'une force considérable, et spécifique au monde industriel.