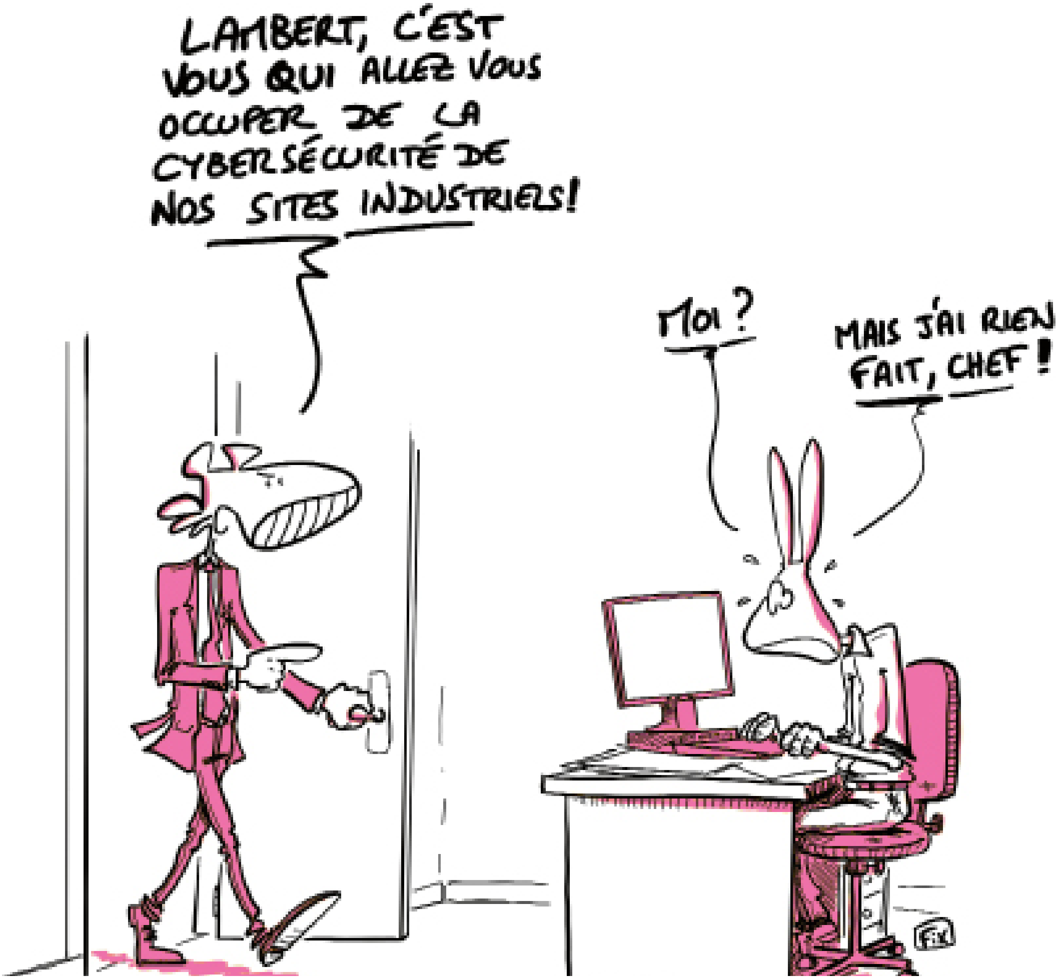
Volet 4

L'analyse de risques dans les systèmes industriels... ...en deux heures chrono

CESIN
Club des Experts de la Sécurité de l'Information et du Numérique
contact@cesin.fr - www.cesin.fr



Les mots de la présidente

Les entreprises ont besoin de cybersécurité pour protéger leurs activités, leurs données mais aussi pour s'inscrire dans les exigences de confiance vis-à-vis des solutions numériques, qu'ont désormais les utilisateurs internes et externes, clients et partenaires, au-delà d'une expérience utilisateur de qualité.

La cybersécurité est en train de vivre une évolution majeure qui prend en compte d'un côté l'évolution croissante des menaces et de l'autre la transformation des architectures, des solutions numériques et des organisations qui les conçoivent.

Ceux qui conduisent la cybersécurité ont besoin de partager des pratiques, des méthodes, des expériences et des informations. La compréhension des risques et le renseignement sur les menaces sont essentiels. La diversité des métiers et des organisations des membres du CESIN est une opportunité pour des échanges et un travail en réseaux fructueux. Cette coopération est l'ambition du CESIN, elle s'opère dans la confiance et la convivialité. Elle se veut pragmatique et efficace, au service des membres et de leur entreprise. Elle constitue un réel atout dans les stratégies de défense.

Les Labs sont un des outils que le CESIN met à disposition de ses membres. Réunis en petit groupe de travail de 10/15 personnes, les membres entreprennent une démarche exploratoire, de recherche ou d'approfondissement d'une question ciblée. Ils partagent leur expérience pour répondre à une problématique précise et dans un délai convenu. Les résultats produits par les labs peuvent prendre différentes formes et sont mis à disposition de l'ensemble des membres.

Nous sommes désolés

Ton chef, le COMEX ou même le Conseil d'Administration t'ont demandé une analyse de risques des systèmes de contrôles industriels pour justifier ta feuille de route cybersécurité (ou même avant de parler de cette feuille de route).

Pas de panique !

Avant de relire l'excellente documentation sur EBIOS Risk Manager de l'ANSSI, nous allons te présenter une approche pragmatique et rapide, issue des expériences et des cicatrices des membres du LAB industriel du CESIN. Elle te permettra de mener cette analyse de risques en deux heures chrono, ou en tout cas en moins de temps qu'il ne te faudrait pour écrire un cahier des charges et sélectionner un prestataire.

Cerise sur le gâteau : cette approche fonctionne aussi bien au niveau macroscopique d'une organisation qu'au niveau d'une usine en particulier.

Etape 1

Évènements redoutés et leurs conséquences : Pense DICT[1] , parle métier (45')

Lorsque tu discutes avec un sachant métier (un patron d'usine, un responsable de ligne d'activité dans une direction technique...), parle-lui d'événements redoutés métiers (mais pas de disponibilité, d'intégrité, de confidentialité, ni de traçabilité) et de leurs conséquences (impacts). Ne parle pas de DICT car dans l'industrie, personne ne sait ce que c'est (ou ça veut dire autre chose[2]) :

- Pour cerner les enjeux de disponibilité, tu parleras du coût d'un arrêt de production (perte de chiffre d'affaires, pénalités contractuelles, coûts de production alternative, masse salariale non productive...)...

- Au lieu d'intégrité, tu parleras de la qualité du produit, du respect du processus industriel, de sa conformité à une exigence (sanitaire, alimentaire, contractuelle...), de risque de casse machine (avec indisponibilité en conséquence), de risque de fonctionnement dangereux (avec risque potentiel pour les personnes)...

- La confidentialité deviendra la protection des savoir-faire (recettes, méthodes, analyses, comptage...) et la valorisation des données notamment au bénéfice des concurrents...

- La traçabilité, qui n'existe pas dans tous les métiers, s'exprimera sous forme de numéros de lot, de dates limites de consommation, de la traçabilité de l'origine des composants...

[1] Disponibilité, Intégrité, Confidentialité, Traçabilité.

[2] En France, la Déclaration d'Intention de Commencement de Travaux (DICT) constitue une mesure obligatoire du droit français à prendre préalablement à l'exécution de tous travaux effectués à proximité d'ouvrages critiques (tq transport ou de distribution d'électricité, de gaz, d'eau, …) afin de prévenir l'ensemble des exploitants de réseaux de l'imminence de travaux et d'éviter tout risque d'accident et d'atteinte aux ouvrages et aux personnes. Cette obligation légale est dictée par des impératifs de sécurité liés à la densité d'infrastructures dans le sous-sol des zones agglomérées ou industrielles.

Quelques exemples :

- Combien vous coûte une minute, une heure, une journée, une semaine d'arrêt de production ? Est-ce difficile de remettre l'usine en service après un arrêt prolongé, en particulier si l'arrêt n'était pas planifié ?

- Pouvez-vous vendre vos yaourts s'ils sont trop ou pas assez sucrés ? Que se passera-t-il si une partie des ingrédients manque dans votre préparation chimique ?

- Est-ce grave si vos concurrents accèdent à vos données de production et de maintenance/défaillance ou connaissent la recette de votre produit ?

- Est-ce grave si l'emballage de vos biscuits porte une date limite de consommation déjà dépassée ou fausse, à la sortie de la chaine de production ?

La bonne nouvelle, c'est qu'il est très probable que les sachants métier connaissent parfaitement leurs événements redoutés, parce qu'ils ont déjà été identifiés dans une analyse de risques métiers (type AMDEC ou HAZOP).

Ne vise pas l'exhaustivité. Un événement redouté à 10 k€ n'aura pas beaucoup d'importance en regard d'un événement redouté à 10 M€.

Inutile également de tenter une conversion des impacts en euro, si elle n'est pas déjà disponible. Les événements redoutés les plus graves parleront d'eux-mêmes.

Tu peux également mettre en avant les coûts cachés liés au redémarrage/à la remise en état de l'installation qui s'est arrêtée brutalement. Plus l'installation est ancienne/complexe, plus le redémarrage/ la remise en état risquent de prendre du temps et de coûter de l'argent.

Si tu as du temps, n'hésite pas à te rapprocher de la personne qui gère les contrats d'assurance dommage. Elle connait forcément le coût d'arrêt d'une usine. Attention : cette perte d'exploitation est généralement calculée sur 12 mois, il faudra ramener ce coût au temps de redémarrage d'un système de contrôle industriel en prenant en compte sa complexité.

Etape 2

Origine cyber d'un événement redouté (45')

Pour déterminer si un évènement redouté peut avoir comme origine une attaque cyber, quatre questions suffisent, mais il est nécessaire d'interroger quelqu'un ayant une bonne connaissance du procédé industriel. Un automaticien sera parfaitement adapté, mais le patron de l'usine, le responsable de ligne d'activité dans une direction technique ou même le responsable du processus industriel qui viennent de répondre à tes questions pourraient également faire l'affaire.

Question 1
L'événement redouté peut-il être produit directement ou indirectement par un composant qui est piloté par au moins un actionneur, et cet actionneur est-il lui-même piloté par au moins un système programmable ?
Exemple : l'explosion d'un four peut être produite par une suralimentation en combustible et l'injecteur du combustible est piloté par un automate.

Question 2
L'événement redouté peut-il être la conséquence d'une réaction humaine inappropriée ou d'une absence de réaction humaine (causée par une information erronée ou absente en provenance d'un ou plusieurs capteurs interrogés par un ou plusieurs systèmes programmables) ?
Exemple : l'opérateur appuiera sur le bouton d'arrêt d'urgence de l'usine si la supervision lui indique une température supérieure au seuil critique dans le four ou à l'inverse, n'appuiera pas, alors qu'il aurait dû, parce que la supervision lui affiche une température normale bien que le four soit sur le point d'exploser.

Si la réponse est non aux questions 1 et 2, cet événement redouté ne peut pas, a priori, être la conséquence d'une cyber-attaque. Dans ce cas, ignore les questions 3 et 4 et passe directement à l'événement redouté suivant.

Question 3
Un dispositif de protection permet-il d'éviter l'événement redouté, d'une façon totalement automatique et indépendante de tout système programmable ? *Exemple : une soupape mécanique permet d'évacuer une surpression dans le four. Attention : le dispositif doit être vraiment autonome. Il ne doit pas dépendre d'une réaction humaine, qui pourrait être négativement influencée par une information erronée en provenance de la supervision.*

Les automates de sécurité ne sont pas des dispositifs de protection contre une cyber-attaque, puisqu'ils sont programmables. Une redondance d'automate n'est pas non plus un dispositif de protection contre une cyber-attaque.

Question 4
Si oui, ce dispositif de protection a-t-il été testé en condition réelle ou simulée ? *Exemple : chaque année, un détecteur d'hydrocarbure est déposé , plongé dans un bidon contenant du carburant, puis reposé, pour vérifier qu'une alarme remonte vers la supervision.*

Si la réponse est oui aux questions 3 et 4, cet événement redouté pourrait être la conséquence d'une cyber-attaque, mais un mécanisme non débrayable empêcherait l'événement de se produire. Passe à l'événement redouté suivant.

Si la réponse est non pour l'une, l'autre ou les deux questions (n°3 et 4), alors il y a une relation de cause à effet entre une cyberattaque et l'événement redouté. Conserve cet événement redouté pour la suite de l'analyse de risque et passe à l'événement redouté suivant.

Etape 3

Toutes les autres variables de l'analyse de risque sont des constantes (30')

Presque toutes les méthodes d'analyse de risques cybersécurité parlent :

- de vraisemblance[3], qui découle de la motivation et de la compétence de l'attaquant, et du niveau d'exposition des fonctionnalités du système ;
- de niveau de contrôle, c'est à dire du niveau de mise en œuvre des mesures de protections, selon un référentiel ou une liste de bonnes pratiques.

Et globalement, le risque résiduel (le seul qui t'intéresse vraiment) dépendra de l'impact que tu viens de déterminer, augmenté par la vraisemblance et diminué par le niveau de contrôle.

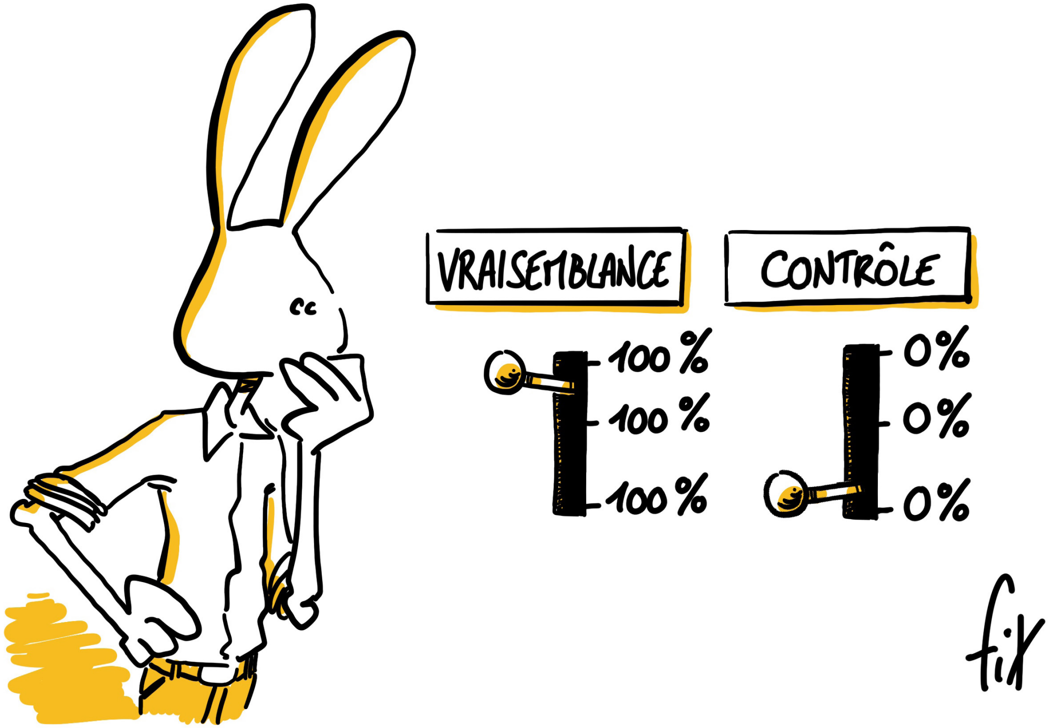
Crois-le ou non, ton analyse de risque est terminée. En effet, notre expérience et les cicatrices dont nous parlions plus haut nous permettent de connaitre la vraisemblance de l'attaque et le niveau de contrôle appliqué à tes systèmes de contrôles industriels, lorsque jamais aucun RSSI n'y a jeté un œil.

L'attaquant n'a pas besoin d'être particulièrement compétent ni motivé. À l'heure du *ransomware as a service*, ton entreprise peut être la cible fortuite d'une attaque générique qui ne la vise pas spécifiquement. Et nul besoin d'appartenir à un secteur d'activité d'importance vitale ou essentiel pour être victime collatérale d'une cyberattaque ciblée.

Ton système de contrôle industriel est exposé. Depuis l'invention de la clé USB, un réseau isolé, ça n'existe plus. Si tu en doutes, relis tout ce qui a été écrit sur Stuxnet. Il est également très probable que quelqu'un ait eu « l'excellente idée » de prévoir un accès à distance pour l'intégrateur qui maintient le système. Enfin, à l'heure de l'industrie 4.0, par où crois-tu que passent les données qui remontent des usines vers le datalake de l'entreprise ?

Rien n'est fait en matière de cybersécurité dans l'usine. Les mots de passe sont souvent faibles, voire inexistants. Personne n'applique les correctifs de sécurité. Les versions des systèmes d'exploitation ne sont plus souvent plus supportées. Il n'y a pas de sauvegarde régulière et encore moins de test de restauration. Le pare-feu, s'il existe, ne filtre pas, ou mal, et personne ne regarde ses journaux. Si tu en doutes, un audit de deux jours sur un ou deux sites judicieusement choisis (ou une discussion de 5 minutes avec les interlocuteurs avec qui tu as mené les deux précédentes étapes) complétera la démonstration.

[3] La vraisemblance est à l'attaque délibérée ce que la probabilité est à l'incident fortuit.



Conclusion

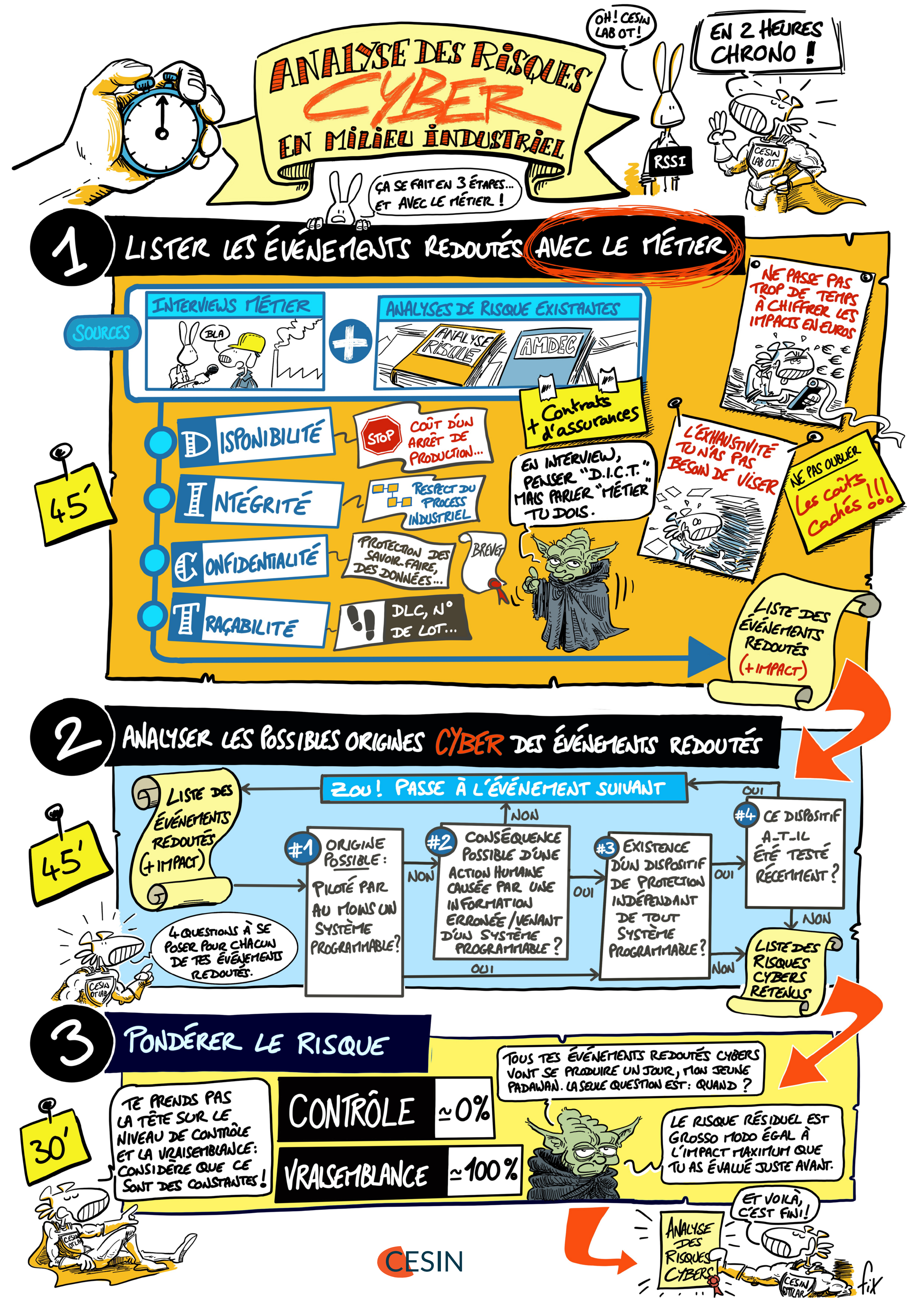
La conclusion de tout cela est assez simple : si tu es Lambert[4], le premier RSSI à t'intéresser à ce périmètre, la vraisemblance vaut 100% et le niveau de contrôle est proche de 0%. Le risque résiduel est donc, grossièrement, égal à l'impact maximum que tu as évalué juste avant. Autrement dit, tous les événements redoutés que tu as identifiés parce qu'ils peuvent être la conséquence d'une cyberattaque peuvent se produire.

La question est juste de savoir quand.

Tu as maintenant un risque résiduel probablement inacceptable, à moins que les événements redoutés soient négligeables. Cela devrait t'aider à obtenir le soutien et le financement de tes actions court terme et de ta feuille de route cybersécurité industrielle. Mais ça, nous en reparlerons dans une prochaine fiche !

Et si tu préfères toujours commencer un guide par la fin … voilà en résumé ce que tu as appris ..

[4] cf. l'excellent « Guide de survie du RSSI en environnement industriel » produit par le Lab Indus du CESIN


ANALYSE DES RISQUES CYBER EN MILIEU INDUSTRIEL
OH ! CESIN LAB OT !
EN 2 HEURES CHRONO !
RSSI
CESIN LAB OT
ÇA SE FAIT EN 3 ÉTAPES... ET AVEC LE MÉTIER !
1 LISTER LES ÉVÉNEMENTS REDOUTÉS AVEC LE MÉTIER
45'
SOURCES
INTERVIEWS MÉTIER
BLA
ANALYSES DE RISQUE EXISTANTES
ANALYSE RISQUE
AMDEC
+ Contrats d'assurances
DISPONIBILITÉ
STOP
COÛT D'UN ARRÊT DE PRODUCTION...
INTÉGRITÉ
RESPECT DU PROCESS INDUSTRIEL
CONFIDENTIALITÉ
PROTECTION DES SAVOIR-FAIRE, DES DONNÉES...
BREVET
TRAÇABILITÉ
DLC, N° DE LOT...
EN INTERVIEW, PENSER "D.I.C.T." MAIS PARLER "MÉTIER" TU DOIS.
NE PASSE PAS TROP DE TEMPS À CHIFFRER LES IMPACTS EN EUROS
L'EXHAUSTIVITÉ TU N'AS PAS BESOIN DE VISER
NE PAS OUBLIER Les coûts cachés !!! ooo
LISTE DES ÉVÉNEMENTS REDOUTÉS (+IMPACT)
2 ANALYSER LES POSSIBLES ORIGINES CYBER DES ÉVÉNEMENTS REDOUTÉS
45'
LISTE DES ÉVÉNEMENTS REDOUTÉS (+IMPACT)
ZOU ! PASSE À L'ÉVÉNEMENT SUIVANT
#1 ORIGINE POSSIBLE : PILOTÉ PAR AU MOINS UN SYSTÈME PROGRAMMABLE ?
NON
#2 CONSÉQUENCE POSSIBLE D'UNE ACTION HUMAINE CAUSÉE PAR UNE INFORMATION ERRONÉE / VENANT D'UN SYSTÈME PROGRAMMABLE ?
NON
OUI
OUI
#3 EXISTENCE D'UN DISPOSITIF DE PROTECTION INDÉPENDANT DE TOUT SYSTÈME PROGRAMMABLE ?
OUI
NON
#4 CE DISPOSITIF A-T-IL ÉTÉ TESTÉ RÉCEMMENT ?
OUI
NON
LISTE DES RISQUES CYBERS RETENUS
4 QUESTIONS À SE POSER POUR CHACUN DE TES ÉVÉNEMENTS REDOUTÉS.
CESIN OT LAB
3 PONDÉRER LE RISQUE
30'
TE PRENDS PAS LA TÊTE SUR LE NIVEAU DE CONTRÔLE ET LA VRAISEMBLANCE : CONSIDÈRE QUE CE SONT DES CONSTANTES !
CONTRÔLE ≃0%
VRAISEMBLANCE ≃100%
TOUS TES ÉVÉNEMENTS REDOUTÉS CYBERS VONT SE PRODUIRE UN JOUR, MON JEUNE PADAWAN. LA SEULE QUESTION EST : QUAND ?
LE RISQUE RÉSIDUEL EST GROSSO MODO ÉGAL À L'IMPACT MAXIMUM QUE TU AS ÉVALUÉ JUSTE AVANT.
ET VOILÀ, C'EST FINI !
ANALYSE DES RISQUES CYBERS
CESIN
fix

Ce guide a été commis par…

Anthony DUMAIS
VIVESCIA

Benoît GARNIER
MERSEN

Bruno LEFEBVRE
FRAMATOME

Emmanuel COUTURIER
GROUPE SAFRAN

Eric SINGER
SCHNEIDER ELECTRIC

Eric HERVÉ
ALSTEF GROUP

Eric KAWKA
ERAMET

Fabrice BRU
GROUPEMENT LES MOUSQUETAIRES

Frédéric MIRAULT
SUEZ

Hervé DEMÉE
SAVENCIA

Hervé BURY
FRAMATOME

Imane RADOUANI
LEGRAND

Jean-Eric LACOTTE
YARA

Loïs SAMAIN
EDF HYDRO

Nicolas de PESLOÜAN
GROUPEMENT LES MOUSQUETAIRES

Patrick BLANLUET
QUADIENT

Quentin RIVETTE
SNCF

Sabri KHEMISSA
IMERYS

Stéphane POTIER
ADVENS

CESIN

Note