Volet 1

Guide de survie du RSSI en environnement industriel

Do & Don't


SALUT, Ô HABITANTS DE LA PLANÈTE "INDUSTRIE". JE VIENS VOUS PARLER DE CYBERSÉCURITÉ.
RSSI
?
FiX

Sommaire

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.


LES BOTTES, LES CASQUES, LES COMBINAISONS... J'ADOOOOOORE VOS COSTUMES, LES GARS !
AMBIANCE TRÈS "INDUSTRIALO-CHIC" !
FiX

Préparer son rendez-vous

Tu as envie...

...de mettre ton costume et ta cravate, pour montrer que tu es quelqu'un de sérieux.

On a testé pour vous...

Tu seras le seul en costume et quand tu auras ajouté les bottes et le casque, tu auras le look d'un homme politique qui vient poser la première pierre dans un chantier boueux. Renseigne-toi !

Il vaut mieux...

Tu ne vas impressionner personne dans une usine avec un costume et une cravate.... tu peux même être ridicule. Demande s'il faut des EPI pour accéder au site et à être accompagné.

Attention : Parfois, pour des raisons culturelles, il faudra quand même être en costume.

Tu as envie...

...d'arriver en jean et polo dans l'usine, puisque qu'on t'a dit qu'il ne fallait pas y aller en costume et en plus il fait 35° dehors...

On a testé pour vous...

...et tu découvres que tu vas visiter une usine maintenue à une température de 4°C.

Il vaut mieux...

Renseigne-toi !
Tes usines ont peut-être des contraintes particulières de froid dont tu dois avoir connaissance.

Tu as envie...

...tu as prévu de lire uniquement le guide de la région avant ta visite....

On a testé pour vous...

Si tu arrives sans comprendre certains termes API, EPI, ...tu auras un peu de mal à suivre les échanges.

Il vaut mieux...

Apprends le vocabulaire minimum de survie (cf notre glossaire) avant d'entamer le guide de la région pour savoir où tu vas.

Tu as envie...

...tu choisis ton hôtel, les restaurants et tu n'as même pas l'adresse exacte de l'usine sur ton GPS... et tu envisages de leur faire ta présentation standard.

On a testé pour vous...

Si tu arrives avec une présentation standard cybersécurité, ton organigramme, ta stratégie classique et tes ressources, tu ne vas pas intéresser grand monde.

Il vaut mieux...

Prépare ta présentation... adapte la au contexte et aux informations clés de pilotage de l'usine. Tu peux obtenir ces informations auprès de ton département Audit, Contrôle Interne, Risque voire tes collègues en charge de l'informatique industrielle.

Tu as envie...

...de débarquer dans l'usine pour changer ton quotidien, comme si tu partais en vacances...et tu as juste un nom...

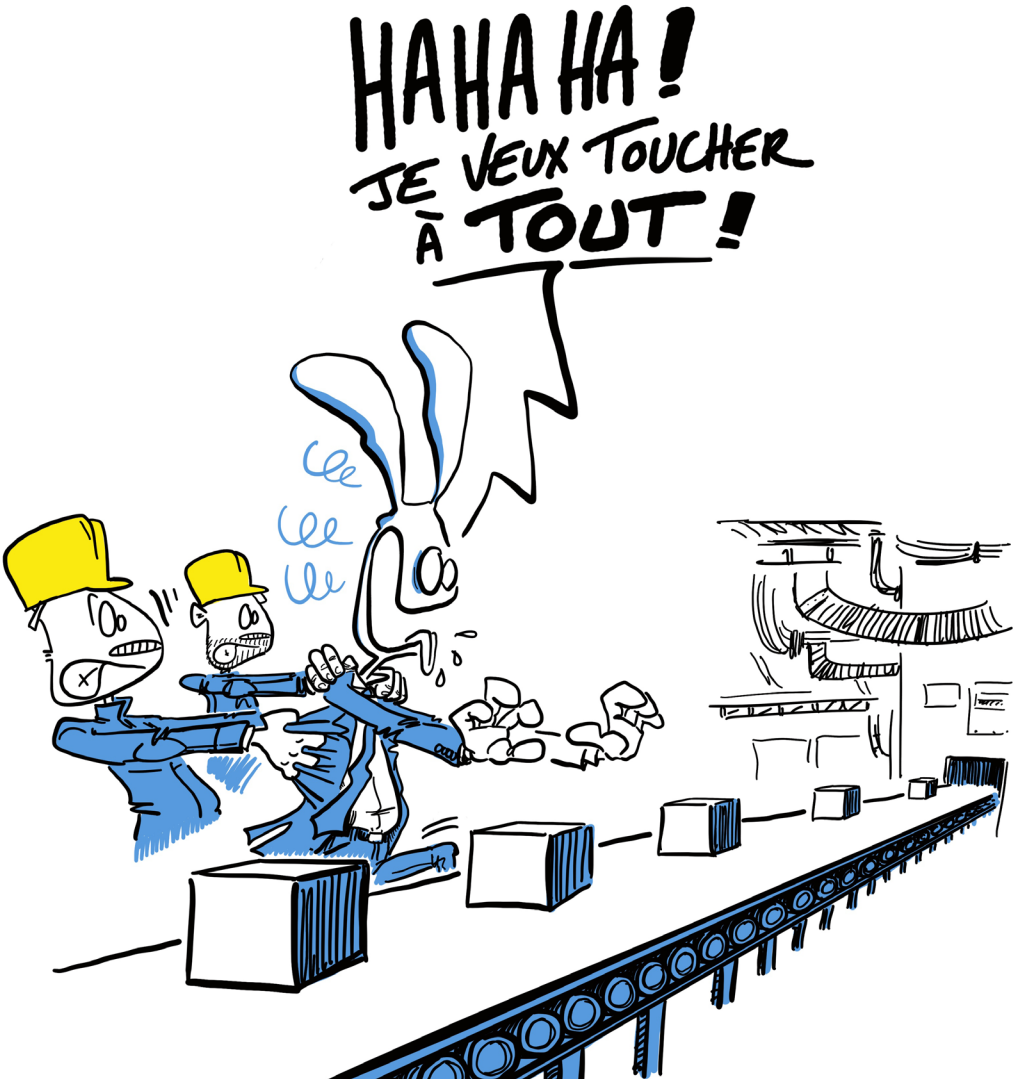
On a testé pour vous...

Si tu n'as pas identifié en amont les interlocuteurs tu vas avoir du mal à identifier et rencontrer les opérationnels compétents.

Il vaut mieux...

Apprends à connaître ton territoire (exemple : organigramme) et l'environnement culturel.


ALLÔ ? BONJOUR, JE DOIS VENIR VISITER VOTRE USINE CET ÉTÉ, SUR LES SUJETS DE SÉCURITÉ INFORMATIQUE...
... ET JE VOULAIS VÉRIFIER : EST-CE QUE VOUS AVEZ BIEN UNE PISCINE ET UN CLUB ENFANTS ?
F:K


HAHA HA !
JE VEUX TOUCHER À TOUT !

Le code de conduite

Tu as envie...

...de toucher à tout comme un enfant qui découvre un nouveau jouet... de prendre un échantillon sur la ligne.

On a testé pour vous....

Si tu ouvres une armoire par curiosité, tu peux activer une alarme... ou te faire jeter dehors parce qu'on va considérer que tu es dangereux..

Il vaut mieux...

Fais-toi accompagner !
Ne touche à rien. Éventuellement, passes une habilitation électrique.

Le code de conduite

Tu as envie...

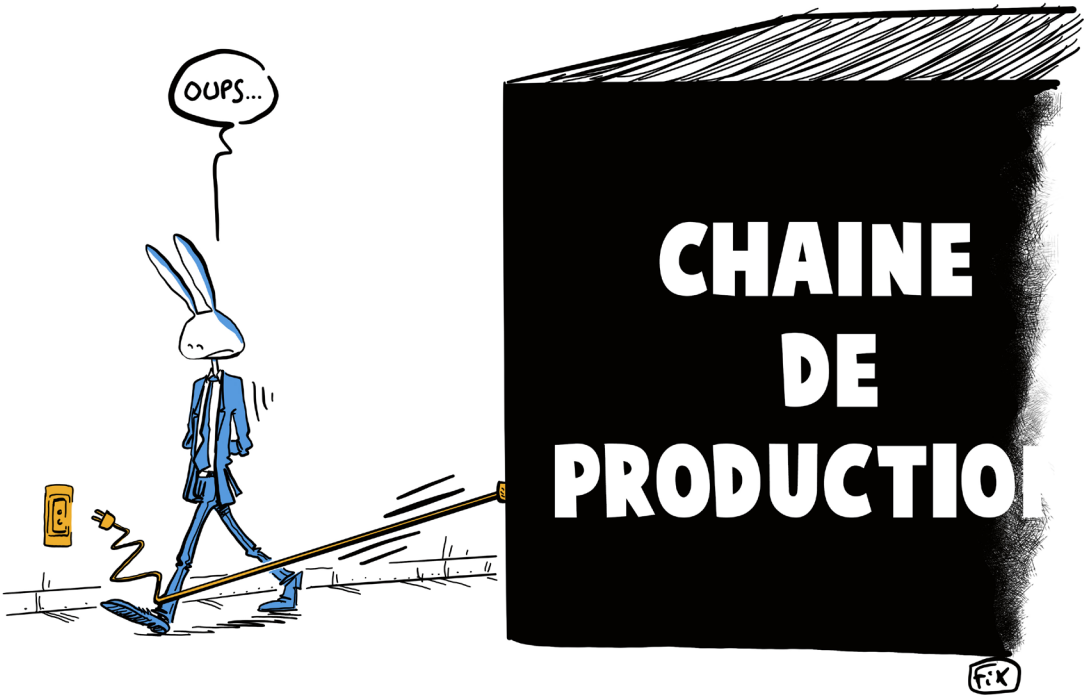
...de te balader à ta guise sans regarder où tu mets les pieds.

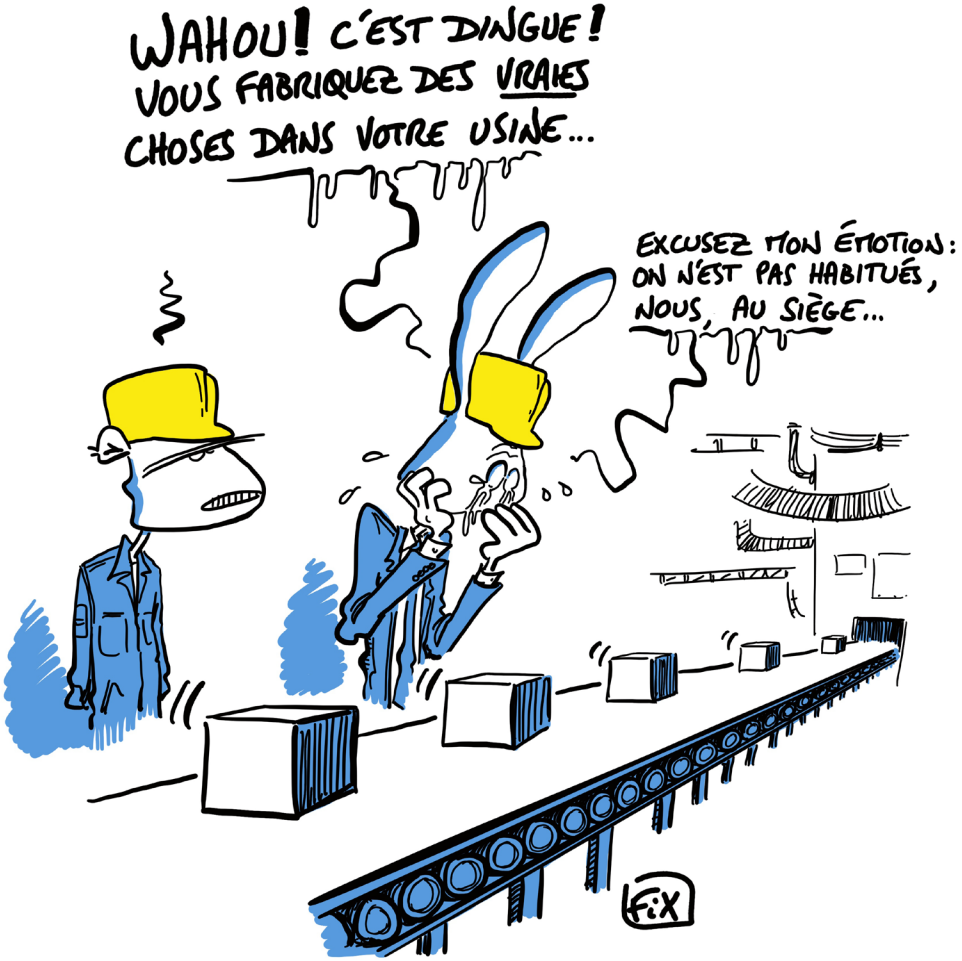
On a testé pour vous....

Tu peux te faire renverser ou blesser par un AGV. C'est le responsable HSE qui va être content de ta venue...

Il vaut mieux...

Fais-toi accompagner. Suis les lignes de circulation... et reste avec tes hôtes.


OUPS...
CHAINE
DE
PRODUCTIO
FIK


WAHOU ! C'EST DINGUE ! VOUS FABRIQUEZ DES VRAIES CHOSES DANS VOTRE USINE...
EXCUSEZ MON ÉTIOTION : ON N'EST PAS HABITUÉS, NOUS, AU SIÈGE...
FIX

Le code de conduite

Tu as envie...

...De voir de plus près le fonctionnement de cette machine de pointe qui débite des milliers de produits à la minute...

On a testé pour vous....

...et tu provoques : son arrêt, bloquant toute la production, les moqueries agacées du personnel de maintenance.

Il vaut mieux...

Attention à la signalétique ! Les risques encourus sur une chaîne de production sont la bête noire de la direction et, à la différence de la SSI, sont en général bien pris en compte et accompagnés de tout un tas de mesures de protection automatiques.

Tu as envie...

...d'éclater de rire, lorsque ton interlocuteur te présente son réseau avec des adresses IP publiques.

On a testé pour vous....

N'oublie pas que le réseau industriel peut avoir été créé avant la RFC 1918 qui introduit des plans d'adressage privés.

Il vaut mieux...

Lui montrer en temps réel le résultat d'un scan de sécurité visible d'internet (Shodan).

Tu as envie...

... de mettre en veille un écran devant lequel il n'y avait personne.

On a testé pour vous....

...l'opérateur revient et ne peut plus travailler.

Il vaut mieux...

Les règles SSI ne sont pas toutes applicables au monde industriel...

Le code de conduite

Tu as envie...

...de rentrer tôt.

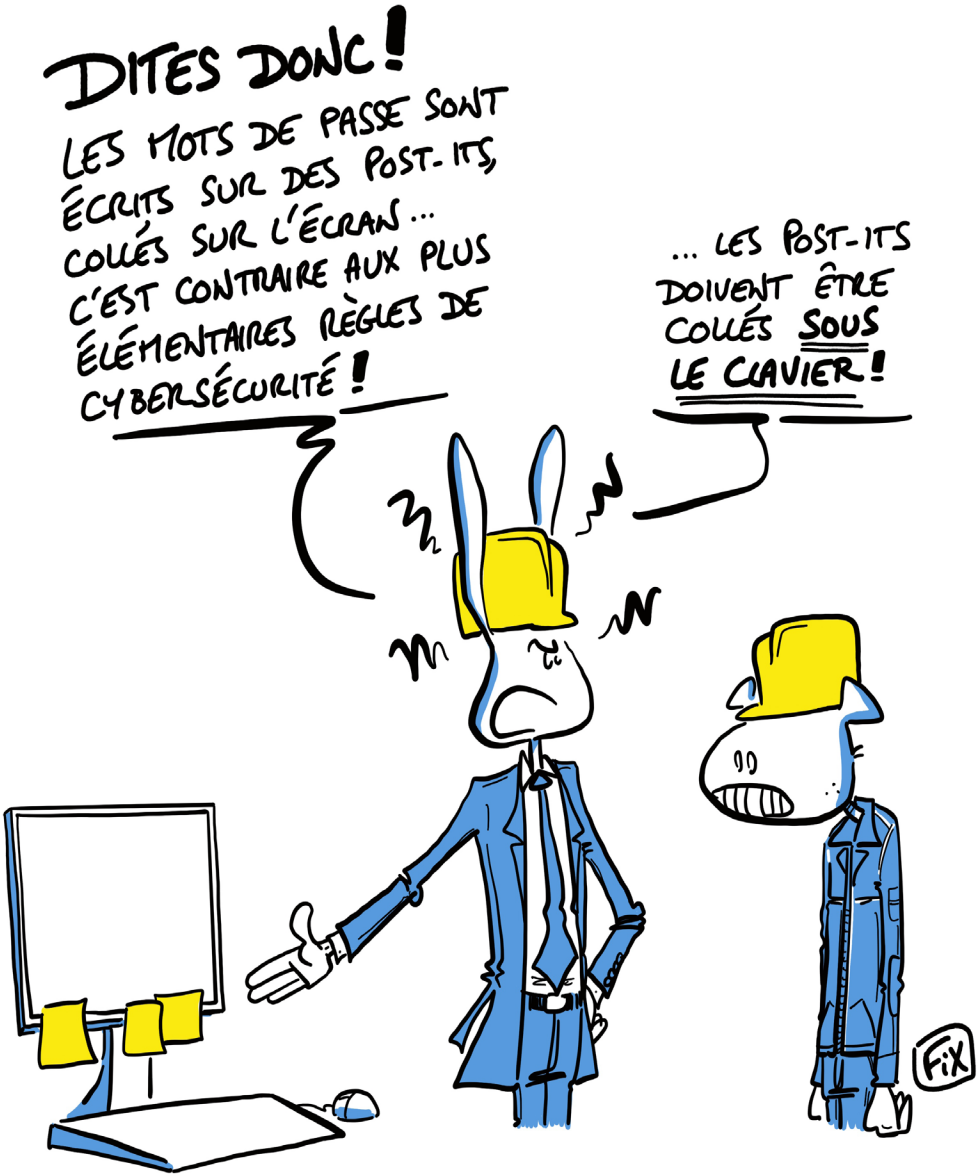
On a testé pour vous....

On se dit qu'on pourra faire un mail ou un compte-rendu la semaine prochaine.

Il vaut mieux...

Les automaticiens sont des spécialistes du process. Ils apprécieront un moment d'échange "à chaud" en fin de visite.

Cela te permettra d'apprendre que certains choix ont peut-être des raisons légitimes de ne pas être discutés dans l'immédiat (système validé, arbitrage budgétaire, réglementation spécifique).


DITES DONC !
LES MOTS DE PASSE SONT ÉCRITS SUR DES POST-ITS, COLLÉS SUR L'ÉCRAN... C'EST CONTRAIRE AUX PLUS ÉLÉMENTAIRES RÈGLES DE CYBERSÉCURITÉ !
... LES POST-ITS DOIVENT ÊTRE COLLÉS SOUS LE CLAVIER !
FIX

Le code de conduite

Tu as envie...

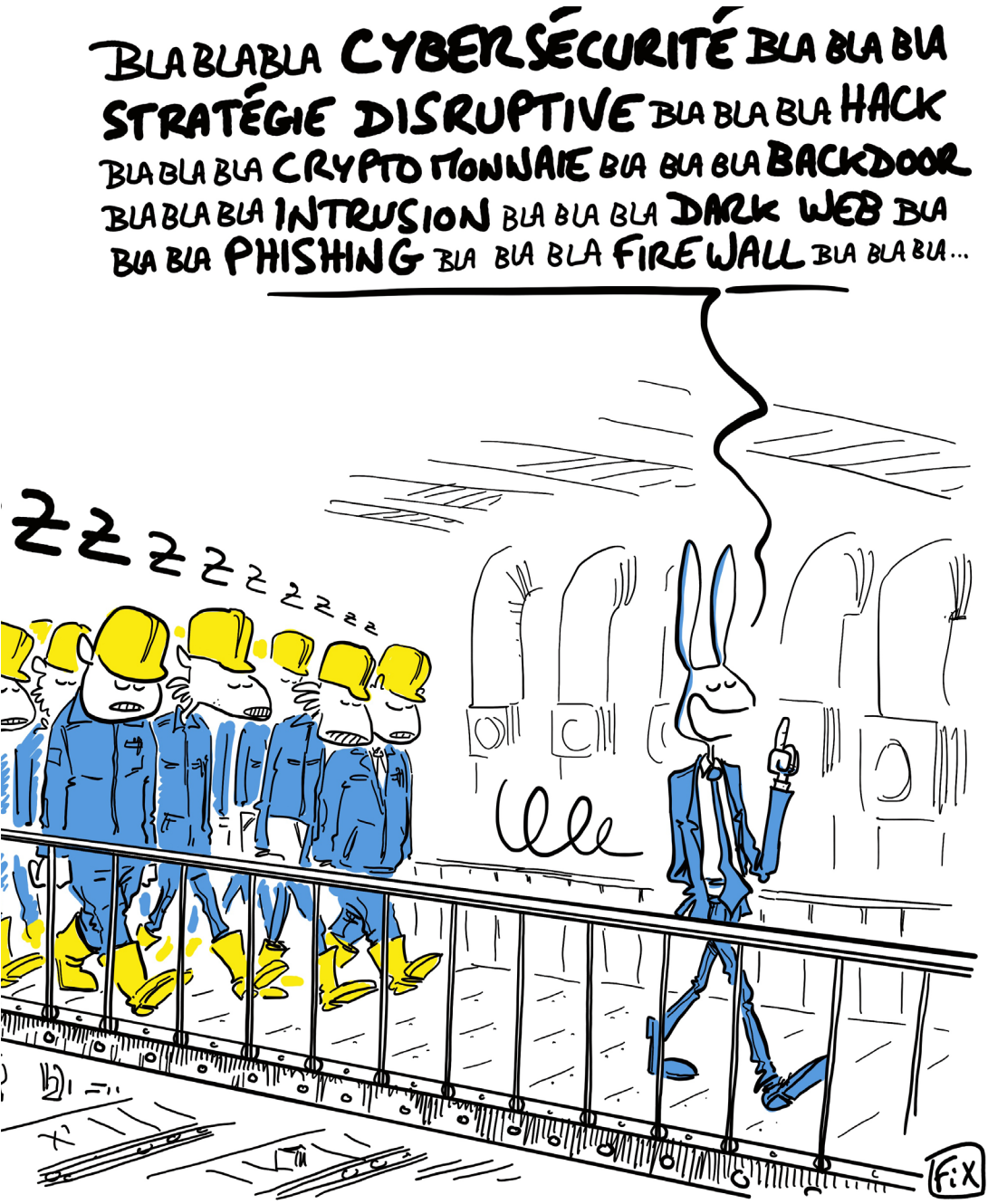
d'éclater de rire quand tu vois des mots de passe sur tous les écrans.

On a testé pour vous....

Dans une usine le contexte de travail n'est pas le même que dans un bureau classique (rotation de personnel, travail avec des gants, réactivité...).

Il vaut mieux...

La sécurité physique d'accès à la salle de contrôle peut être un contrôle compensatoire à privilégier pour diminuer le risque; ainsi elle devient un "espace de confiance".


BLA BLA BLA CYBERSÉCURITÉ BLA BLA BLA
STRATÉGIE DISRUPTIVE BLA BLA BLA HACK
BLA BLA BLA CRYPTOMONNAIE BLA BLA BLA BACKDOOR
BLA BLA BLA INTRUSION BLA BLA BLA DARK WEB BLA
BLA BLA PHISHING BLA BLA BLA FIREWALL BLA BLA BLA...
Zzzzzzzzz
FiX

Comprendre le contexte

Tu as envie...

...d'expliquer la cybersécurité à tes interlocuteurs.

On a testé pour vous....

Ils s'en moquent de la cybersécurité en général.. Tu dois leur démontrer qu'elle est une cause possible d'événement redouté et qu'à ce titre ils doivent s'en occuper. Ne les saoule pas avec des histoires de hackers !

Il vaut mieux...

Oriente ton discours sur leur métier, leurs risques, l'indisponibilité du procédé industriel etc. Surtout, laisse les parler !

Comprendre le contexte

Tu as envie...

... de proposer le déplacement de leurs serveurs dans ce superbe datacenter multi-redondé en région parisienne.

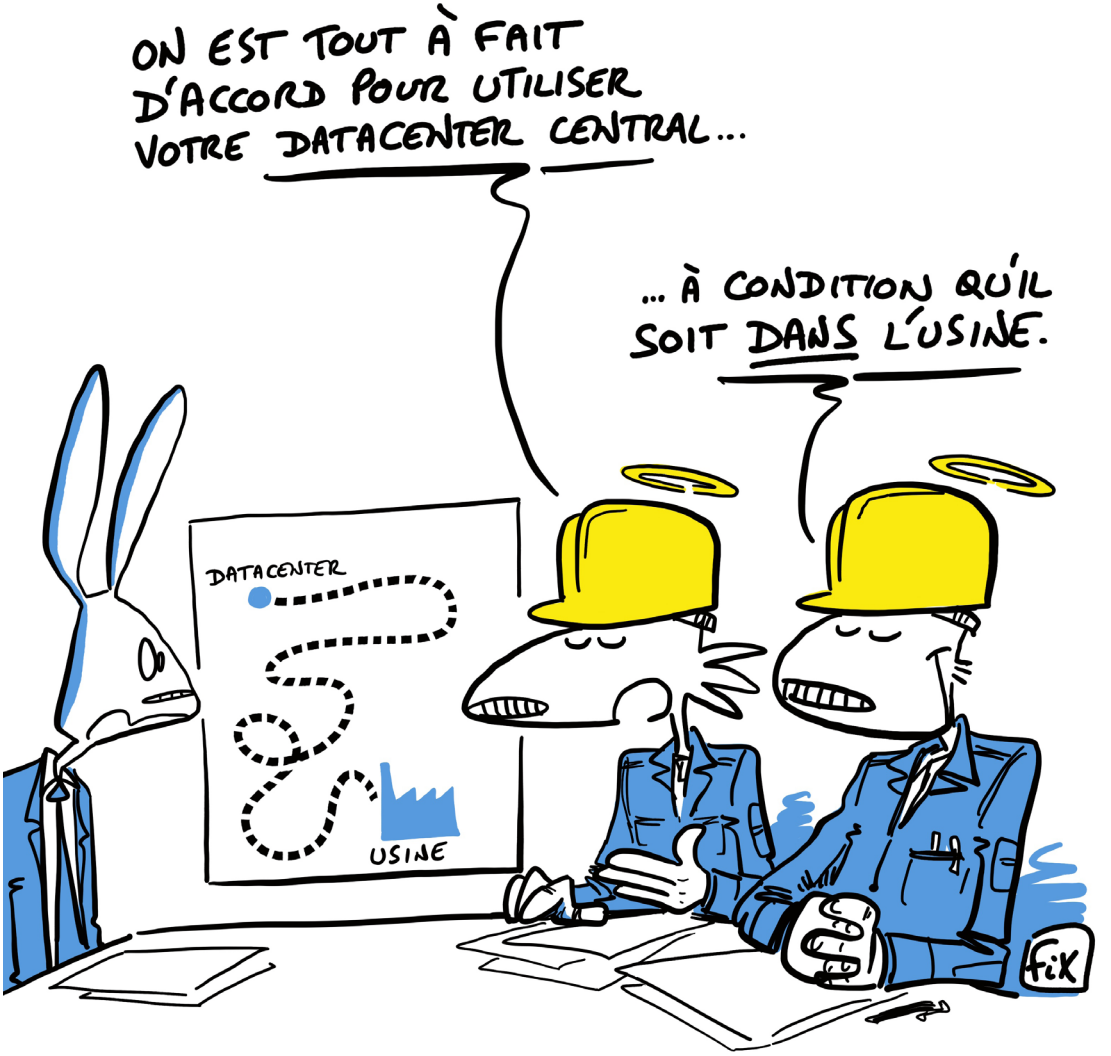
On a testé pour vous....

Tes interlocuteurs te répondent d'un air goguenard que leurs opérations se jouent à la milliseconde, et que le seul temps de transport des données vers ce datacenter explose les exigences de latence de leurs lignes.

L'usine doit fonctionner même quand le réseau vers le datacenter est en panne ! Tes interlocuteurs ont besoin de pouvoir intervenir rapidement en cohérence avec les horaires de production.

Il vaut mieux...

Les outils industriels nécessitent de respecter des temps de traitement très strictes ! La présence de serveurs de traitement à proximité des automates n'est pas qu'un choix dicté par la sensibilité des automaticiens.


ON EST TOUT À FAIT D'ACCORD POUR UTILISER VOTRE DATACENTER CENTRAL...
... À CONDITION QU'IL SOIT DANS L'USINE.
DATACENTER
USINE
FiK

Comprendre le contexte

Tu as envie...

...de migrer toutes ces vieilleries de Windows XP en Windows 10.

On a testé pour vous....

Qui a dit que l'application qu'ils utilisent fonctionne sur une autre version de Windows ? Ne sois pas surpris si ton voyage dans le monde industriel ressemble à Retour vers le futur.

Il vaut mieux...

Bien souvent, une simple modification demande une requalification complète de l'outil de production et des investissements qui dépassent largement ton salaire. Prends le temps de comprendre les impacts, travaille avec les équipes industrielles à définir un plan d'actions dans la durée et aide-les à obtenir le financement.

Une autre piste serait d'envisager des contrôles compensatoires.... Contrairement à l'IT où les cycles de vie sont entre 3 et 5 ans, ici on parle plutôt de 15 à 20 ans.

Comprendre le contexte

Tu as envie...

...d'installer un antivirus sur tous les postes de supervision.

On a testé pour vous....

Le jour où l'antivirus va arrêter la production sera le premier jour du reste de ta carrière.

Et de toute façon, l'éditeur de la solution, l'intégrateur de l'usine et le fabriquant du matériel ont tous dit qu'il ne fallait surtout pas installer d'antivirus.

Il vaut mieux...

Un antivirus, éventuellement, mais correctement configuré, avec des précautions, un moyen de le désactiver facilement, une liste blanche de process...

C'est un projet en soi, qui nécessite d'impliquer le fabricant de la solution, en espérant qu'il sera sensibilisé à la cybersécurité. Cela peut-être une bonne idée d'envisager des contrôles compensatoires...

Comprendre le contexte

Tu as envie...

... de proposer du WiFi pour éviter les échanges de clé USB.

On a testé pour vous...

En environnement industriel avec des perturbations électromagnétiques fortes, le Wifi peut-être très instable.

Il vaut mieux...

En environnement industriel, on fait appel à de vrais experts, car même un câblage cuivre classique peut être perturbé.

Comprendre le contexte

Tu as envie...

...d'une manière générale de vouloir considérer que l'informatique opérationnelle (OT) et l'informatique de gestion (IT) sont similaires.

On a testé pour vous...

Même si les technologies convergent et s'inter-connectent, les contraintes, besoins, priorités, risques, problèmes, solutions sont différents et spécifiques !
Le terme OT est très peu connu dans le monde industriel, c'est plutôt un terme utilisé dans le monde IT pour qualifier un autre monde

Il vaut mieux...

Apprends à connaître les spécificités du monde industriel (besoins de sécurité, cycle de vie, spécificités concernant les mises à jour, mots de passe etc...). Préfère utiliser par exemple "industriel" au terme "OT".


ET VOILÀ : JE VOUS AI INSTALLÉ UN JOLI PETIT FIREWALL AU MILIEU DE LA CHAÎNE DE PRODUCTION !
VOUS M'EN DIREZ DES NOUVELLES !
FIX

Comprendre le contexte

Tu as envie...

...de mettre un firewall au milieu de tout cela...

On a testé pour vous...

Sache que pour ton interlocuteur, un port est avant tout celui d'un switch et pas nécessairement un port TCP/IP.

Il vaut mieux...

Il faut isoler le réseau industriel et le réseau IT. Mettre un firewall au sein du réseau industriel peut comporter des défis: il faut une bonne connaissance du réseau (identifier des flux que personne ne connaît).

Cela peut être dangereux (le firewall peut bloquer un flux qui n'aura pas été identifié et qui sert par exemple à l'arrêt d'urgence).

Chaque fois qu'un message va arriver en retard sur un automate, quelqu'un va dire que c'est le firewall qui ralentit les communications.

Comprendre le contexte

Tu as envie...

...de faire tout cela en même temps.

On a testé pour vous...

Une erreur, tu auras une chance de t'en sortir.
Au delà, ils risquent de ne jamais te réinviter.

Il vaut mieux...

Sois attentif !
"On n'a pas deux fois l'occasion de faire une première bonne impression." (Coco Chanel)

"Il vaut mieux la fermer et passer pour un con, que l'ouvrir et ne laisser aucun doute à ce sujet." (Coluche).

Comprendre le contexte

Tu as envie...

...de demander si les ports USB sont protégés.

On a testé pour vous...

En fait, les stations d'automatisme sont souvent confinées dans des boîtiers (inox, plexiglas,...), et les ports USB ne sont pas accessibles.

Il vaut mieux...

Il vaut mieux parfois éviter de bidouiller les lecteurs USB sur ce type de matériel, le prestataire qui effectue maintenance en a peut-être besoin.

En revanche, on peut suggérer l'emploi d'une clé dédiée à cette machine et la scanner régulièrement à l'antivirus, si la clé est indispensable aux opérations.

Comprendre le contexte

Tu as envie...

... de croire que le monde industriel, tu connais parce que tu as l'expérience d'UN type d'industrie.

On a testé pour vous...

Et bien non, l'industrie pharmaceutique et l'industrie cosmétique ou agroalimentaire, n'auront pas les mêmes contraintes.

Il vaut mieux...

Mais rassure toi c'est pareil que dans l'IT...
Sois toujours humble !

Tu as envie...

...de demander pourquoi les baies sont en hauteur.

On a testé pour vous...

Ce n'est vraiment pas pratique. En plus, je n'ai pas l'autorisation d'utiliser un chariot élévateur.

Il vaut mieux...

Les chariots élévateurs sont de gros engins. Il n'est pas rare qu'il y ait des chocs, de la casse, des choses renversées - solides ou liquides. Il est plus sage de faire positionner les équipements réseaux fragiles en hauteur, à défaut de matériels durcis.

Tu as envie...

... placer tous les budgets SSI d'investissements dans les budgets de l'usine car tu sais que c'est un puits sans fond.

On a testé pour vous....

...c'est beau de rêver...

Il vaut mieux...

Parfois, le budget Cyber que tu as présenté contribue au P&L de l'usine. Les coûts de production sont augmentés. Ton Directeur d'Usine est challengé sur ces coûts. Tes actions doivent être priorisées et planifiées sur une échelle de temps adaptée.

Comprendre le contexte

Tu as envie...

...de renoncer à être RSSI industriel, parce que vraiment, c'est trop compliqué pour toi.

On a testé pour vous...

Nous aussi, les première fois, on a douté. Ces gens là parlent une langue que tu ne connais pas...

Il vaut mieux...

Mais en réalité, tu as une expertise nécessaire et complémentaire (par rapport aux automaticiens).... et une fois que vous aurez commencé à travailler ensemble tu vas acquérir de nouvelles compétences. Et puis, *in fine* ce dont on parle, ce sont simplement des "équipements" qui s'échangent des "données" :). Donc pour sûr tu devrais y arriver !


SNIF... C'EST VRAIMENT TRÈS TRÈS COMPLIQUÉ VOTRE MÉTIER...
HA HA ! T'INQUIÈTE PAS, NOUS C'EST PAREIL : ON N'Y COMPREND RIEN À TON MÉTIER !
FiX

Remerciements

Merci à toute l'équipe du Lab pour ces après-midi de travail, de rire et d'échanges qui ont permis d'aboutir à ces 3 premiers livrets.

- Nicolas de Pesloüan
- Eric Kawka
- Hervé Delmée
- Benoit Garnier
- Jonathan Boudet
- Patrick Blanluet
- Stephane Tournadre
- Caroline Roche
- Fabrice Bru

Merci à Fix pour avoir su croquer avec humour les travaux du Lab !

Ce guide a été commis par...

Eric Kawka
ERAMET
RSSI Industrie

Fabrice Bru
STIME
Directeur Sécurité des SI

Hervé Helmée
Savencia
RSSI Industrie

Jonathan Boudet
AgroMousquetaires
RSSI

Nicolas de Pesloüan
Veolia
Expert Cybersecurité Industrielle

Benoit Garnier
Mersen
Manager Qualité et Sécurité des Systèmes d'Information Groupe

Patrick Blanluet
Neopost
RSSI Groupe

Caroline Roche
Groupe Pernod Ricard
RSSI Groupe

Stephane Tournadre
Servier
RSSI Groupe

CESIN

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