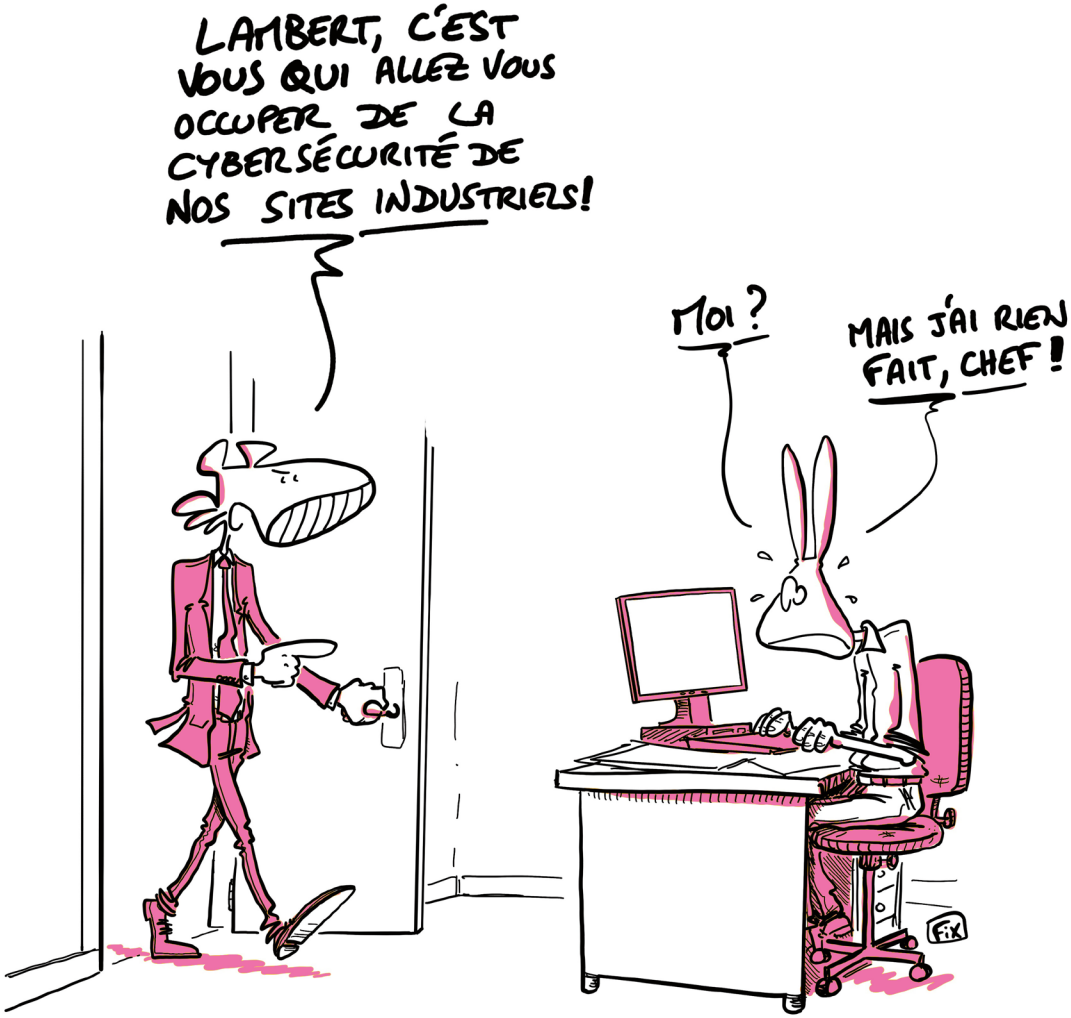
Volet 2

Guide de survie du RSSI en environnement industriel

Les 10 questions clés pour un premier contact (presque) réussi


LAMBERT, C'EST VOUS QUI ALLEZ VOUS OCCUPER DE LA CYBERSÉCURITÉ DE NOS SITES INDUSTRIELS!
MOI ?
MAIS J'AI RIEN FAIT, CHEF !
FIX

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.

Toi RSSI, tu as été désigné pour être en charge de la Cyber du monde industriel : bonne chance !

Dans cette partie, tu vas trouver les premières questions utiles pour t'aider à comprendre le contexte métier et évaluer les besoins en cybersécurité et peut-être espérer un deuxième rendez-vous.

Les 10 questions clés

01 Pouvez-vous me présenter l'activité métier de votre usine ?

> Raconte-moi ton usine ! (organisation, taille, interlocuteurs, processus)
> Visitons ton usine

02 Quels sont les évènements redoutés ?

…et pour l'aider dans sa réflexion : atteintes aux personnes, arrêt de la production, approvisionnement matière, conflit social, problème de transport.

- À l'échelle de l'usine ?
- À l'échelle de plusieurs usines ?
- Quels sont ceux qui se sont déjà produits ? Quand ?

03 Parmi les événements redoutés, identifions ceux qui pourraient être provoqués soit par une attaque informatique soit par un incident sur un système de contrôle industriel

- Cet événement redouté peut-il directement ou indirectement être causé par un ou plusieurs éléments gérés par un système de contrôle industriel ?

- Cet événement redouté peut-il être le résultat direct ou indirect d'une action humaine inappropriée causée par une information manquante ou erronée relative à un ou plusieurs éléments supervisés par un système de contrôle industriel (et si les outils industriels ne sont plus fiables) ?

04

Est-ce que vous avez des moyens de protection, automatiques et totalement non informatiques, qui permettent d'éviter les événements redoutés ?

Exemples :

- Soupape qui réagit mécaniquement à la pression ou la température
- Fusibles
- Sprinkler
- Trop plein

Attention : Les safety PLC ne sont pas des protections non Cyber

05 Quels peuvent être les impacts applicables aux évènements redoutés retenus ?

- Impact humain
  - Blessés, morts
  - Impact sanitaire (rappel produit)
  - Chômage partiel ou technique

- Impact opérationnel
  - Interruption de service
  - Destruction du procédé industriel, de l'outil de production

- Impact financier direct ou indirect
  - Pénalités légales et contractuelles
  - Frais liés à la fourniture d'un service alternatif
  - Frais de remédiation ou remise en état
  - Frais liés au fait que le produit n'est plus utilisable ou que sa qualité est altérée (ex : date limite de consommation, date limite de vente, qualité du produit dégradée

- Impact environnemental
- Impact juridique
- Impact d'image / réputationnel

06 A quelle fréquence avez-vous des pannes ?

07 **Avez-vous envisagé que ce qui apparaît sur vos écrans de supervision ne soit pas le reflet de ce qui se passe réellement sur votre chaîne de production ?**

- Quel est l'impact si les informations remontées ne sont pas exactes (qualité, conformité, sécurité des biens et des personnes) ?
- Si le système de conduite du procédé industriel (automates et superviseurs) est défaillant, le procédé va-t-il réagir de façon autonome pour revenir à un état stable et sûr (fail-safe) ?
- Si des phénomènes inexpliqués surviennent dans le procédé industriel, avez-vous envisagé une origine malveillante informatique ? Quelle serait votre réaction dans ce cas ?

08 Savez-vous combien de prestataires interviennent sur vos environnements industriels ?

- Qui ? Sur quel périmètre ?
- Le partage des responsabilités est-il bien établi ?
- Se connectent-ils à distance ? Comment ?

---

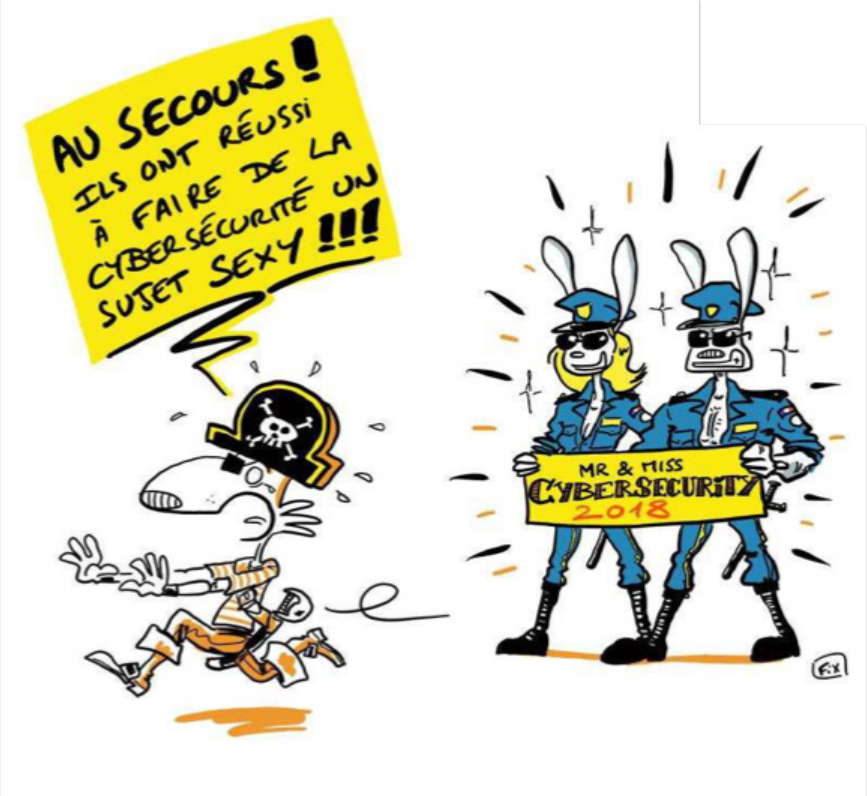
09 Quelles relations avez-vous avec l'IT ?

- Vous travaillez avec eux ? Ils vous aident ?
- Vous êtes interconnectés ?
- Vous leur envoyez des informations ?

10

Quand est-ce qu'on se revoit ?

Si tu décroches une nouvelle date,
tu as gagné ton pari !


AU SECOURS !
ILS ONT RÉUSSI À FAIRE DE LA CYBERSÉCURITÉ UN SUJET SEXY !!!
MR & MISS
CYBERSECURITY
2018

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