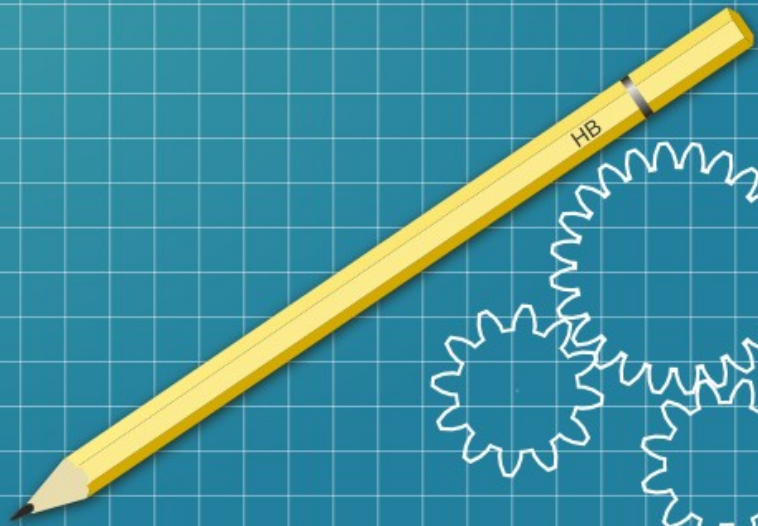
# Le guide de survie du RSSI intergalactique dans un monde de dingues



# INTRODUCTION

- La naissance du métier
- La pression quotidienne
- Les bonnes recettes de tonton Cédric pour ne pas terminer en chambre capitonnée

  (à prendre bien entendu au 2ème voire 3ème degré)

  Et un peu de sérieux à la fin

# Le CHU de NANTES...

7ème CHU de France, premier employeur de la région Pays de Loire

12000 agents, Budget global : > 1 Mds €

Etablissement support du GHT44, 3ème GHT de France

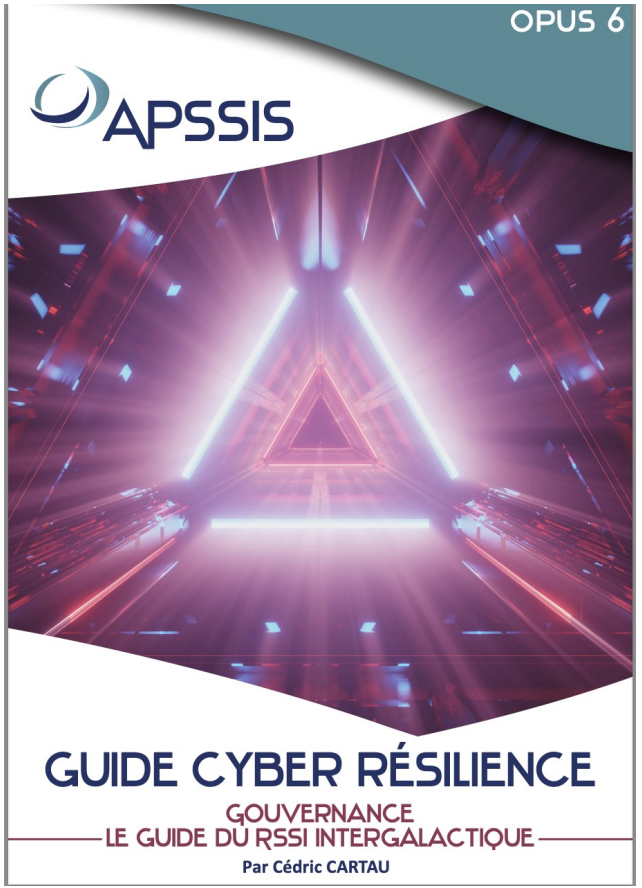
# Votre serviteur...

Cédric Cartau RSSI du CHU de NANTES du GHT44 A travaillé au CHU de REIMS blablabla CHU de RENNES blablabla Membre de l’APSSIS, ARCSI, CESIN, AFCDP blablabla Co-fondateur du groupe RSSI NANTAIS et ISO 27001 Pays de Loire blablablablablabla Chroniqueur dans DSIH Magazine Auteur de 6 ouvrages spécialisés Publication de 6 opus cyber résilience avec l’APSSIS blablabla Enseignant au CNAM, CNEH, EHESP, ESIEA, Université de Nantes, POLYTECH NANTES.

Ouf.

# En résumé :

# Jingle Pub

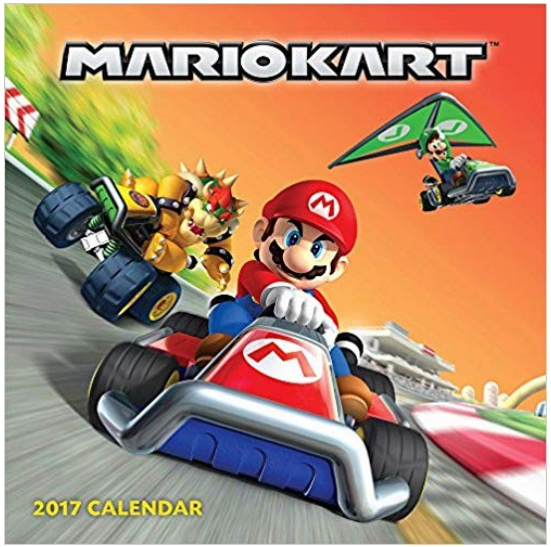



Avec Welliom, MIPIH, WALLIX

Et en guest star Philippe Loudenot et Marguerite Brac de la Perriere

# Petits retours historiques

Il y a eu les grandes découvertes de l’humanité


impots.gouv.fr

# Petits retours historiques

Puis vinrent les méchants et les mauvais

# Jingle Pub – il existe des sweat en couleur !

https://www.amazon.fr/Essentials-Performance-RCSWT763-Capuche-Cendrier/dp/B08THQHGDM/ref=sr_1_9?crid=37XLQCDCK9URZ&dib=eyJ2IjoiMSJ9.ybw17cauVITaawZLSM7PQKCheG6CEj-4rS8bhimhCJxwvtwMijKuCQwQ-w43gq7YWpuztSW69Uc9dA7a2d0A0FyIvRPIfzBvJCtVY2paD_iEu1We9r_emwkewujYZwBLT-DwrKDiyYb6tdn9NjrTP-SSgZQ-eNkIN10z58NuK_60oSHkeiC_2MH_5MSb_k5FEBBlDtdGjcibsI_uEZMVOyAgEG08LK62PK7Umrx0z8s1IVzMbmqLHz5YpeqWZxkJs8UGDSK8fvb0kjjjQkYqwm-xlqGiP1dmGOUMZTRlyZs.NXoL3z9lNw25rgOqbmhv4PqnE-oq0PCnLBASIv5cKws&dib_tag=se&keywords=sweat+a+capuche+homme&qid=1731190972&sprefix=sweat+a+%2Caps%2C142&sr=8-9

# Et quand on disait...

# Au mieux on avait ce type de réaction

# Mais les ransomewares arrivèrent

# Avant on voyait le RSSI comme cela

# Mais après...

# Ou aussi comme cela

# Mais en fait la réalité c’est plutôt ça

# Résumé de l’évolution Darwinienne


# Le concept du TBB

Faire de la cyber sans RH, TBB = DRH

Faire de la cyber sans flouze, TBB = DAF

Faire de la cyber sans appui SI, TBB = DSI

# Le concept du T3B et du T4B

Mais le DRH a aussi son TBB (qui est un TBBB)

Mais le DAF a aussi son TBB

Mais le DSI a aussi son TBB

Mais il y a pire...

# Le concept du TnB

...le TBBB a aussi son TBBBB

Et ainsi de suite…

Et la seule chose de certaine en ce bas monde...

# Le risque de classe chapi-chapo

Essayez juste une fois de stopper un projet de déploiement d'un gros progiciel (genre un ERP) en plein milieu…

...dans le meilleur des cas vous finirez votre hypothétique carrière au milieu de blouses blanches à sourire bêtement en jouant à chat et à vous extasier devant une rediffusion de chapi-chapo

CONCLUSION : ON VIT DANS UN MONDE DE JOBAR

# Et on risque terminer comme cela...

# Ou pire...

# Ou pire pire pire...

# Les stratégies pour garder son calme

Il y en a 3 :

- la stratégie technique
- la stratégie conseil
- la stratégie Détritus…

(promis on est sérieux après)

# La stratégie technique

Faire son analyse de risque EBIOBLABLABLA

Déployer son EDRRRRRRRRRRRRRRRRR

Acheter un SOOOOOOOOOOOOOOOOOC

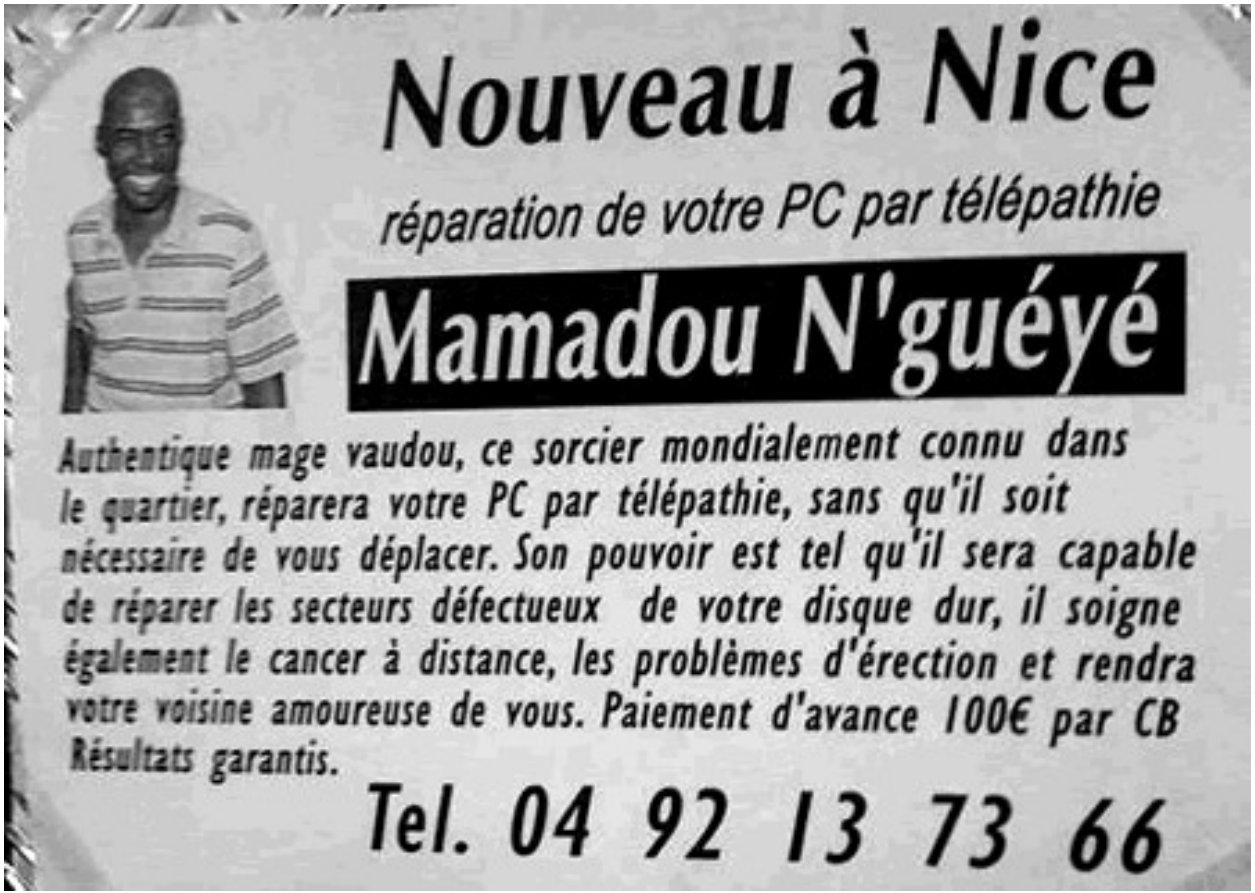
Faire du MFAAAAAAAAAAAAAAAAAAAA

...et attendre que ça pète

...et prétendre qu'on n'a pas pris les produits assez chers...que les utilisateurs sont des tanches...les consultants des buzes...les intégrateurs des truffes

# La stratégie technique en résumé

# La stratégie technique – version du pauvre



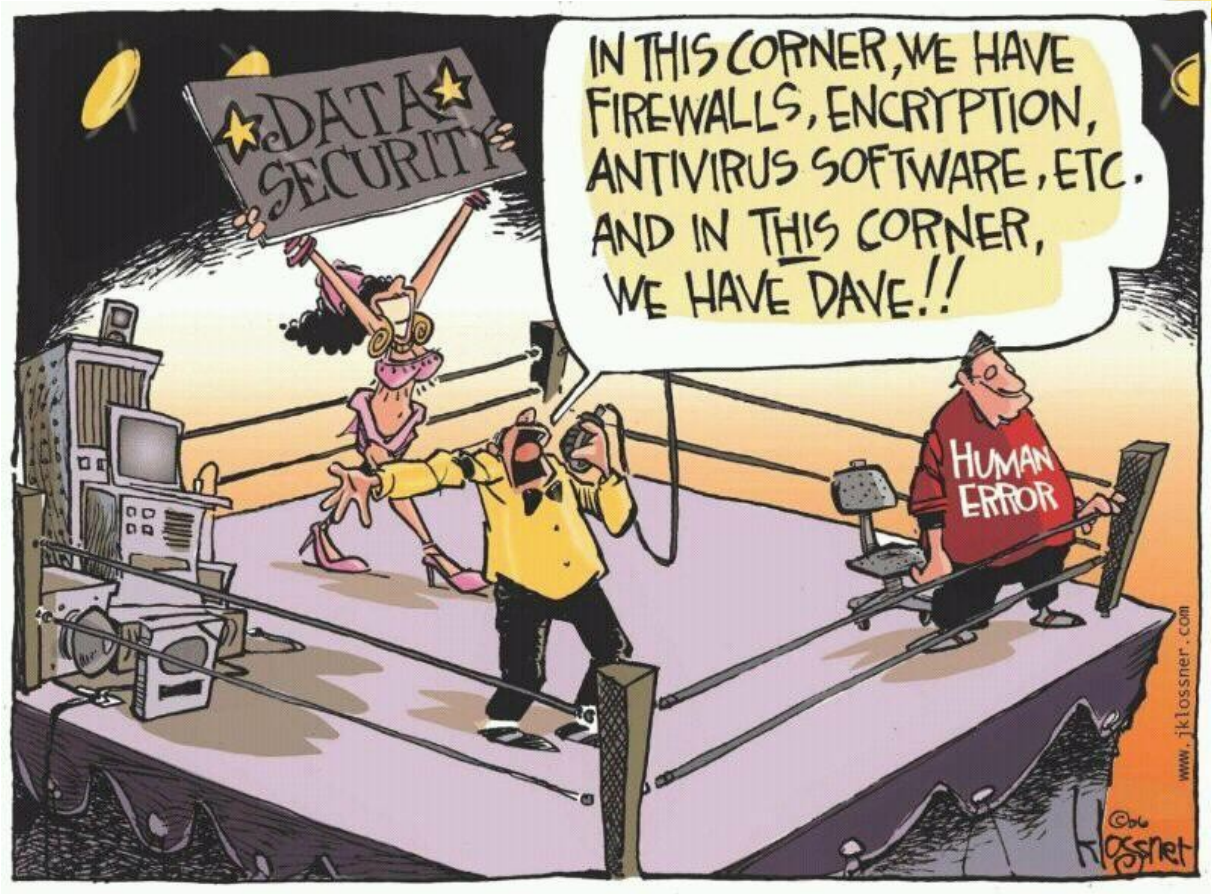
# La stratégie technique

D’autant qu’il y aura toujours un Dave pour vous pourrir votre EDR…

...asphyxier votre SOC

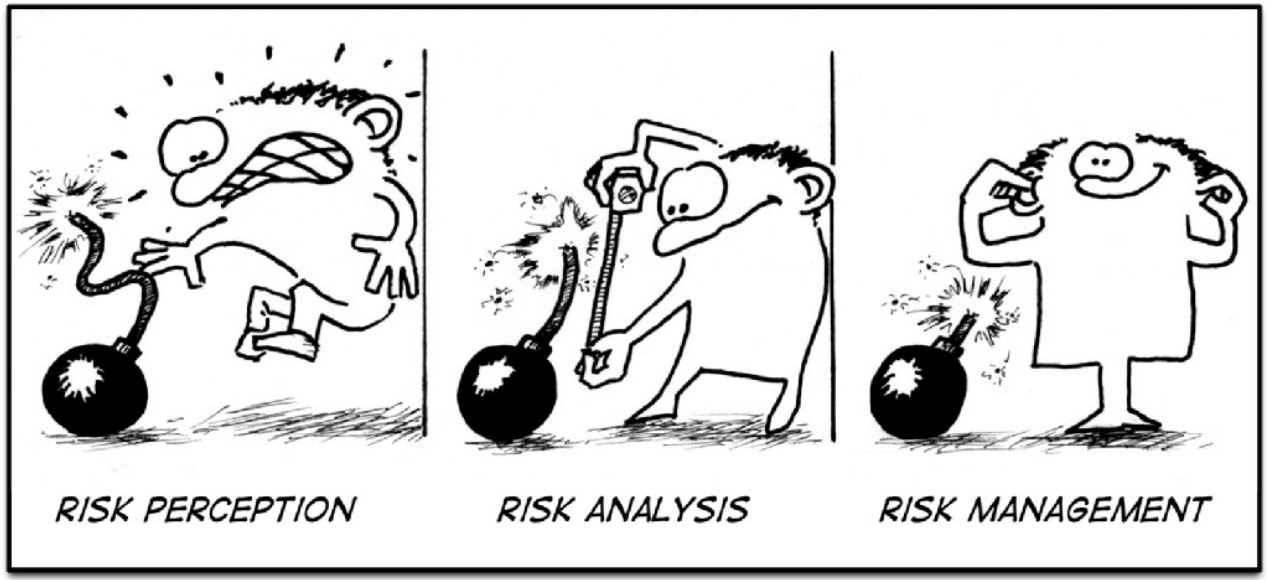
# La stratégie technique – Dave en action

...



# La stratégie conseil

Résumé en image :



# La stratégie conseil

L’idée consiste en gros à s’enterrer bien au fond des processus..

...dans un processus lui-même enterré

En résumé : prétendre que le RSSI n’est qu’en audit, conseil, alerte et qu’il n’est en rien propriétaire des risques car il n’est pas propriétaire des assets

Jingle teaser : tout pareil pour le DPO

# La stratégie conseil

Avantage 1 : la résilience du RSSI

(les boites de conseil pratiquent cela depuis des lustres en facturant des blindes et sans jamais être inquiétées)

Avantage 1 bis : pas besoin de s’y connaître

(les boites de conseil...)

Avantage 2 : l’opacité

(avant que qui que ce soit qui n’est pas Black Belt 27001 comprennent la notion de processus et de proprio d’asset vous serez à la retraite ou mort)

# La stratégie conseil

Inconvénient majeur : bouffer tout seul à la cantoche dos au mur pendant 172 trimestres

Inconvénient secondaire : ça va être vachement long avant que l'Organisation comprenne ce que vous lui racontez…

… et pendant ce temps là les incidents continent d'arriver

# La stratégie Detritus

Paradigme majeur : tant qu’à finir dingue, autant ne pas être le seul

Ou : dans un monde de dingue, c’est le plus dingue qui gagne

# La stratégie Detritus – quelques exemples 1/3

- faire une FEI de FEI (auto-référentiel) dans la GED (ne me remerciez pas les qualiticiens c’est kdo)
- **soumettre la DSI (80 % de mecs) à un test de phishing** promettant des jolies photos à oilpé
- faire une FEI sur l'absence de FEI (les qualiticiens je vous aime amour petites fleurs gros poutous)
- **lancer un scan sur les soft installés par les adminsys** sur leurs stations d'admin (ne soyez pas étonnés d’être surpris du résultat)
- **faire un test de phishing par semaine**, ceux qui se font avoir doivent venir chercher la clé de déblocage de leur MDP chez le DRH…
- et faire pareil avec les agents de la DRH

# La stratégie Detritus – quelques exemples 2/3

- stopper un serveur administratif au hasard 3h59 en pleine journée si le SLA est de 4h

- copier l'intégrale des films de Marvel sur son profil Windows afin de faire péter la sauvegarde...et expliquer au responsable prod qu'il gère mal son capacity planning

- **installer du minage de BTC** sur le serveur GRC et mesurer le temps que la DSI met à comprendre le problème

- **changer l'IP de son PC pour lui mettre celle du CTRL AD** (redoutable)

- **installer BOINC** (ex-SETI) sur le PC du DG, et attendre de voir combien de temps la hot line met à analyser ; et prétendre que le parc n'est pas géré ;

# La stratégie Detritus – quelques exemples 3/3

- installer un serveur DHCP rogue sur une prise RJ45 pour tester le déploiement du 802.1x (testé, redoutable)

- demander au consultant qui vous a pondu l'imbitable EBIOS...de faire une EBIOS sur son EBIOS

- arriver en audit au sein d'une MOA, avec l'auditeur qui audite votre méthode et le second auditeur qui audite l'audit du premier (très vache)

- poser une question RGPD à un avocat qui tienne en 20 pages, et lui demander une réponde qui tienne en une page (hyper vache)

# La stratégie Detritus

Avantage : toutes ces techniques sont faites pour éprouver l’Organisation (on rend service en fait, si si)

Inconvénient majeur : attendre d’être à 6 mois de la retraite pour les mettre en œuvre

Autre inconvénient : le RSSI ne peut même plus aller dej à la cantoche

# Petit point d’étape un tantinet désabusé

Durée de vie d’un RSSI à son poste : 3,7 ans

Multiplication des burn out

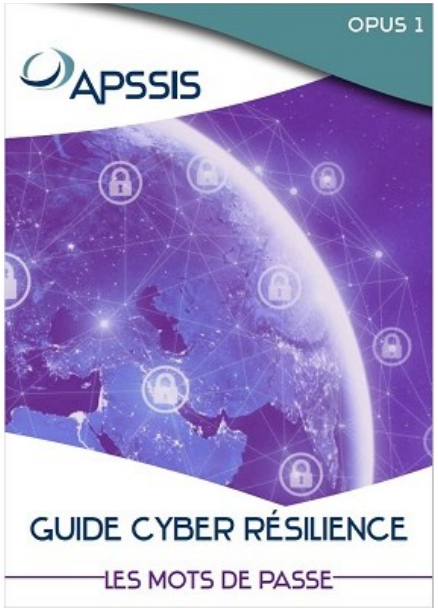
Postes multiplement exposés

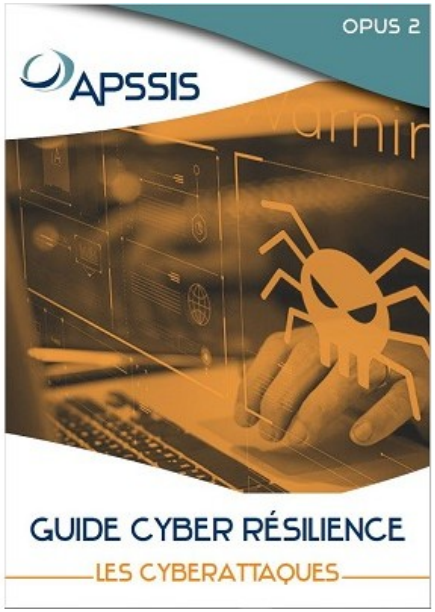
Seuls sont comptés les trains en retard

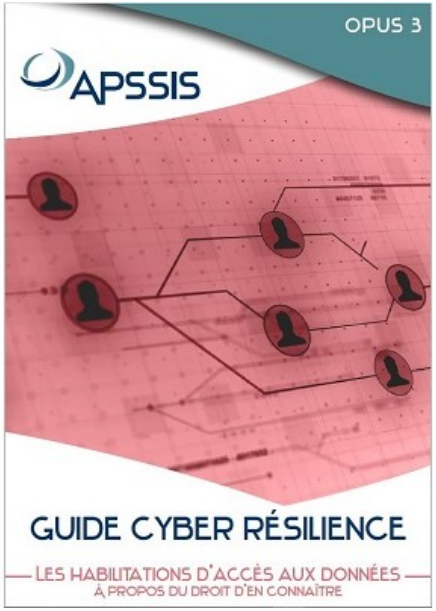
Même un DRH est plus populaire que le RSSI dans certaines boites (c’est dire...)

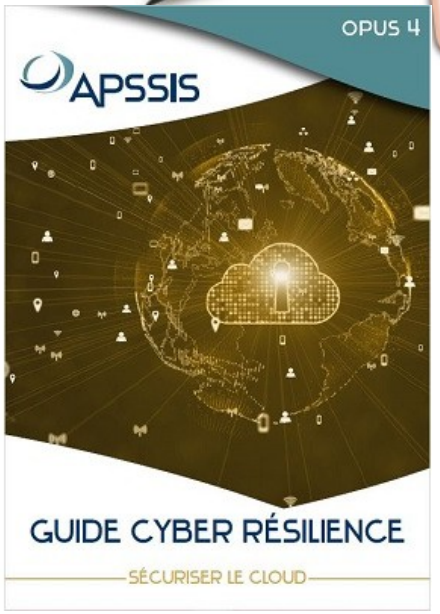
# Comment certains me voient

# Jingle pub – APSSIS forever



# Nécessité d’introspection...

# Soyons sérieux 2 mn

COMMENT EN EST-ON ARRIVES LA ?

(les fonctions support / transversales idem

Ceux sur qui on a tapé juste avant idem : DRH, DAF, DQ, etc.)

# Les axes de réflexion

Les frontières

L’entropie

Les moyens

...et surtout le temps

# Les axes de réflexion

L’Organisation malade de ses frontières : la supply chain de la supply chain

L’Organisation malade de son entropie: cf ISO, absence de « voiture balais »

L’Organisation malade de ses moyens : de la différence entre l’efficacité et l’efficience, ou la loi de Paréto

Et surtout…

...l’Organisation malade du temps : le paradigme du chat sur la commode

# Les pistes de solution

Les frontières : back to basic orga / techno, le zero trust, le zonage, etc.

L’entropie : LEAN, ITIL et 27001. De l’orga, rien que de l’orga

# Petite anecdote édifiante

## Du problème de l’entropie (j’aurais pu utiliser Chorus)

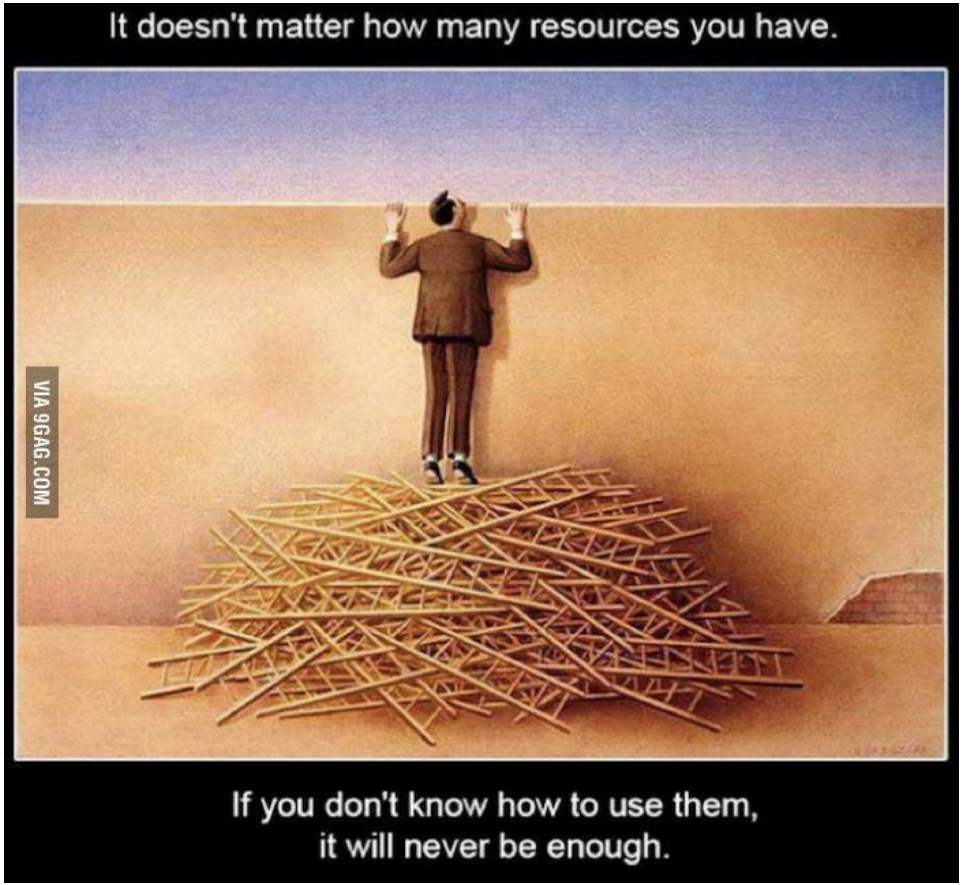
Formulaire(s)

- Formulaire 2042 : Déclaration de revenus - < 1 Ko
- Formulaire 2042-C : Déclaration de revenus complémentaire - < 1 Ko
- Formulaire 2042-IOM : Déclaration des investissements outre-mer - < 1 Ko
- Formulaire 2042-C-PRO : Déclaration de revenus complémentaire des professions non salariées - < 1 Ko
- Formulaire 2042-RICI : Déclaration des réductions et crédits d'impôt - < 1 Ko
- Formulaire 2042-TA : Demande de remboursement de la taxe additionnelle au droit de bail - < 1 Ko

# Les pistes de solution

Les moyens, la plus grande arnaque des sociétés modernes

# Petite anecdote



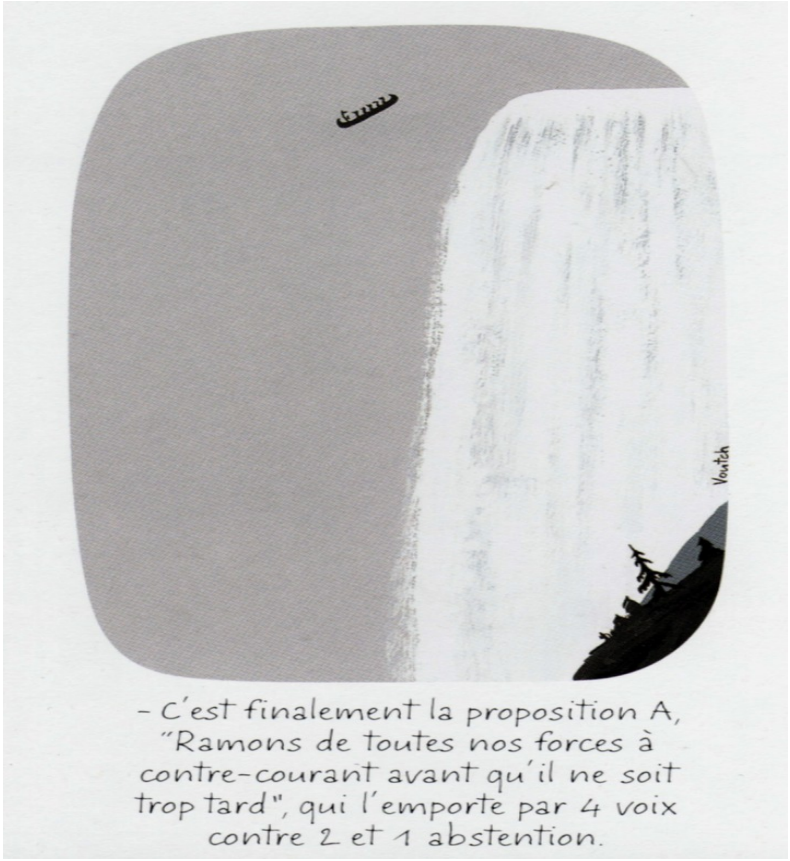
# Autre anecdote

Du problème des moyens :

# Les pistes de solution

Le temps, mais quelle est la véritable urgence chez moi (chez vous) ?

# Et le problème du temps



# Les éléments inquiétants

Accélération des ruptures de paradigmes cyber : Cloud, ransomeware, IA, poids réglementaire

Des évaluations Fi / RH de l’impact de ces ruptures ?

Une visibilité DG / Board de l’impact de ces ruptures ?

# Les éléments très très inquiétants

Les ruptures de paradigmes cyber à l’aune de la dichotomie Place / Tour

« La Place et la Tour », Niall Ferguson

Exemple : extrême agilité des black hat versus roadmap des éditeurs de logiciels mainstream

# Sans parler de l’explosion réglementaire

# Jingle pub – DSIH I Love you

DSiH Tribunes & Actus Webinaires Vidéos Magazines Etudes Annuaire

E-santé Sécurité Décryptage Intelligence artificielle Gestion administrative Territoires

## Dernier numéro du magazine.


### DSIH 43 : DSI, UN MÉTIER DE PASSION UN MÉTIER EN TENSION

01 oct. 2024 - 02:00, Rédaction

Les DSI sous pression, stoïques et motivés : Bienvenue dans le quotidien des DSI hospitaliers : des projets numériques à la chaîne, un cruel manque de moyens, la pression des cybermenaces... mais aussi un terrain d'innovation, et une thématique numérique qui devient stratégique. Les DSI ne connaissent pas l'ennui.

Choisissez votre version

# Mais faire aussi son auto-critique

Dysfonctionnement des processus de sélection : origine majoritairement technique des RSSI, quitter le faire pour se cantonner aux conseils, audit, faire son deuil

De la pyramide de Maslow : physiologique / sécurité / appartenance / estime / réalisation

# Mais faire aussi son auto-critique

Déclinaison du concept de résilience :

- résilience des organisation = PCA/PRA, capacité de réaction à une crise majeure

- résilience, vision darwinienne : celui qui a survécu (cf épidémie de peste et les Mayas)

- résilience version individuelle : optimisation du triptyque temps / complexité / ressources

# Mais faire aussi son auto-critique

La question qui pique :

« le stress et la surcharge de travail de l’agent doivent-ils être les variables d’ajustement de la non gestion de l’entropie, de l’efficience et de l’urgence des Organisations modernes »

Dit autrement : qui a un problème de ressources ? Le RSSI / CISO ou ses clients / financeurs internes ?

# La solution est peut-être...

Etre RSSI, c’est comme…

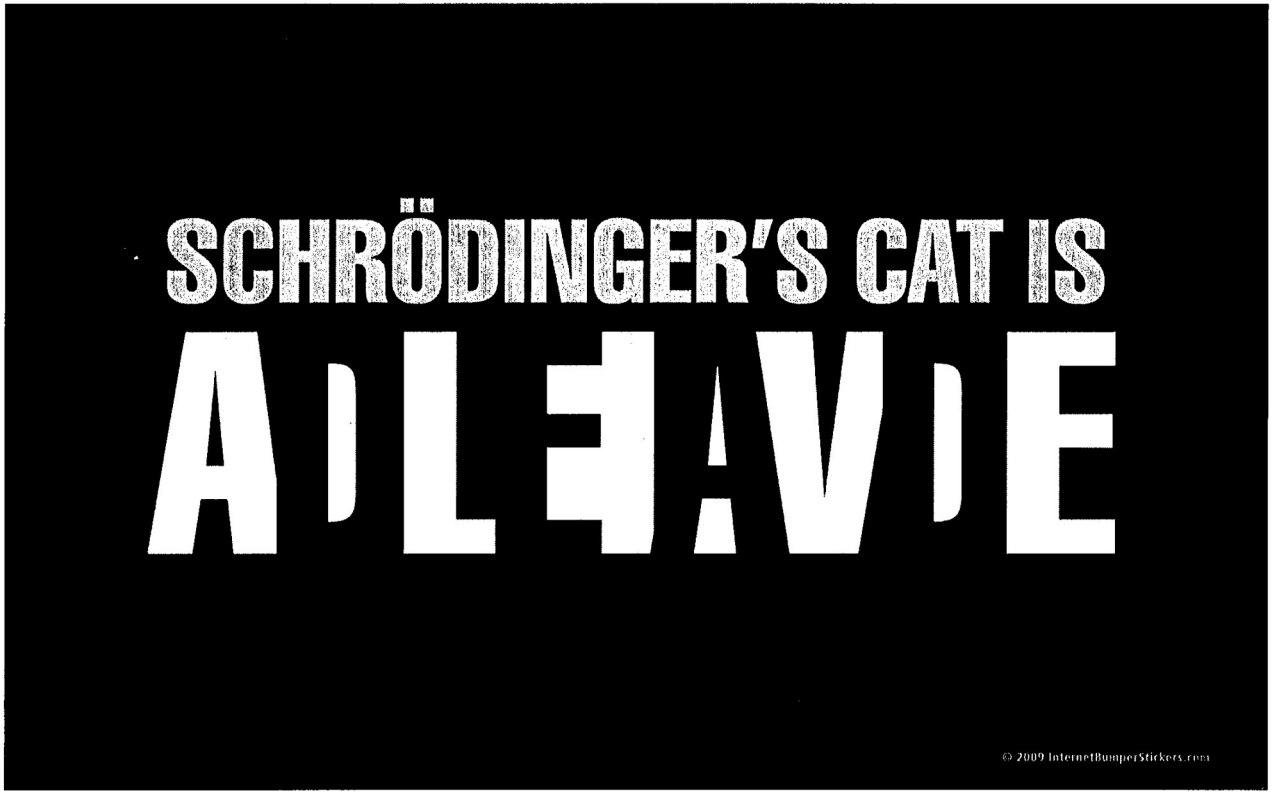
...marcher en équilibre sur la fine crête qui chemine entre la vallée du j’en foutisme et le gouffre de la sur-implication

# Au final il ne restera que

Nietsche : 8h de liberté par jour

Tonton Cédric : 2h de réflexion de fond par journée de travail

# Et une réalité bizarre



# Notes et liens

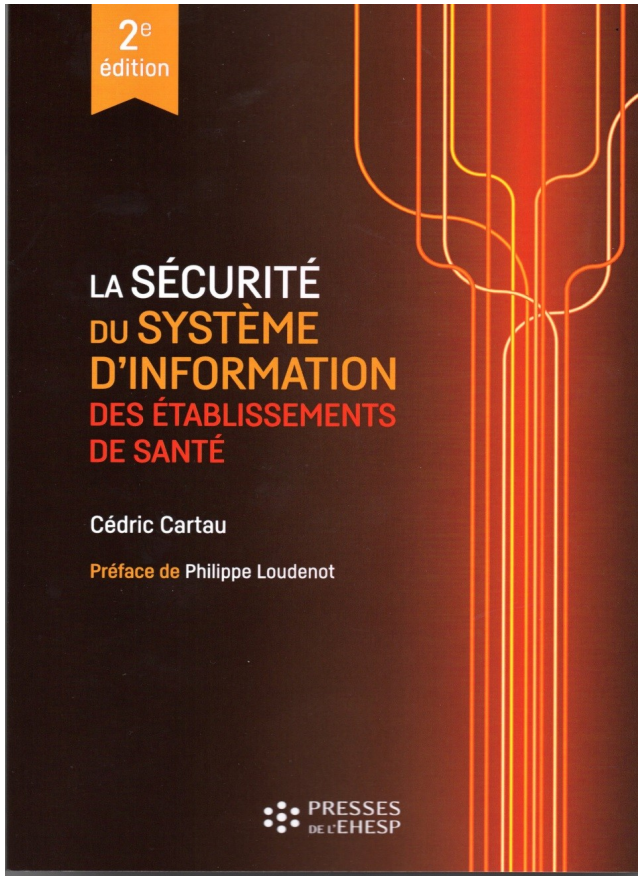
Suis-je une IA ?

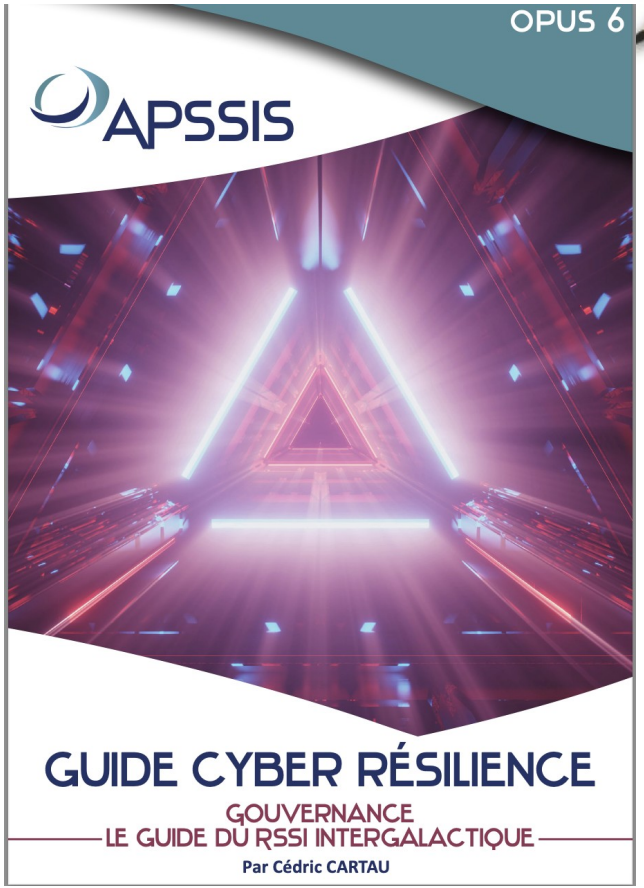
https://dsih.fr/articles/5295/suis-je-une-ia-ou-les-reflexions-metaphysiques-dun-rssi-sous-tension

Le site de l’APSSIS : www.apssis.com

Le site de DSIH : www.dsih.fr

# Ouvrage


2e édition
LA SÉCURITÉ DU SYSTÈME D'INFORMATION DES ÉTABLISSEMENTS DE SANTÉ
Cédric Cartau
Préface de Philippe Loudenot
PRESSES DE L'EHESP


OPUS 6
APSSIS
GUIDE CYBER RÉSILIENCE
GOUVERNANCE
LE GUIDE DU RSSI INTERGALACTIQUE
Par Cédric CARTAU