

Lettre des "Lundi de la cybersécurité" n° 75

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

v

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



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

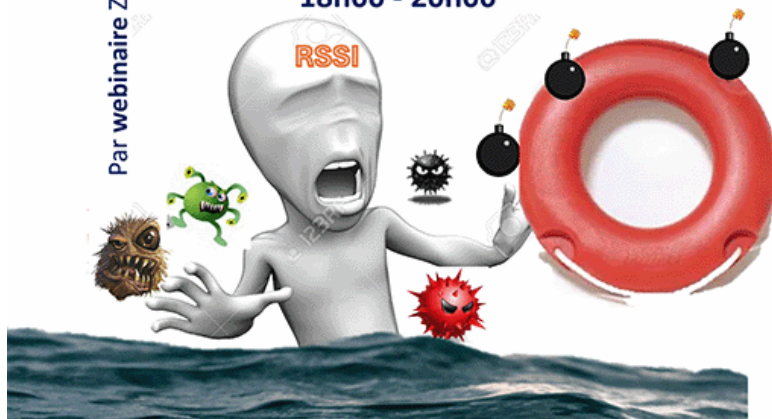
Organisateurs



Pr Ahmed Mehaoua
Université Paris Cité

Par webinaire Zoom

Lundi 18 novembre
18h00 - 20h00



Cédric CARTAU
RSSI & DPO du CHU de NANTES, RSSI du GHT44
Enseignant au CNAM
Vice-Président APSSIS



Béatrice Laurent



Gérard Peliks

Le métier de RSSI – Responsable Sécurité des Systèmes d'Information – et le métier de DPO comportent leur dose de stress, mais aussi de passion et des moments de bonheur. Quand une cyberattaque pénètre dans votre système, et ça peut (et ça va) vous arriver :

- Soit le RSSI a déployé les contre-mesures indispensables pour contrer cette agression et assurer la résilience de votre système et de vos informations. Il est alors le sauveur que tous ses camarades admirent et remercient.
- Soit l'attaque fait de gros dégâts, jusqu'à paralyser l'entreprise. Le RSSI est désigné comme coupable de cette tragédie, même si bien sûr, ce n'est pas lui l'attaquant.

Bon, on comprend que dans le cyberspace, ces métiers connaissent leur part d'angoisse mais aussi leur satisfaction du travail bien fait. Le « risque zéro » ne pouvant exister, le lot quotidien du RSSI, est la peur, mais la peur peut être bonne conseillère, s'il garde son sang-froid.

Vous voulez des chiffres récents ? En voici :

<https://www.solutions-numeriques.com/56-des-professionnels-de-la-cybersecurite-en-france-sont-victimes-depuisement-professionnel/>

Je donne la plume à l'intervenant Cédric CARTAU

Le moins que l'on puisse dire, c'est que si la cyber était pépère dans les années 90 et au début de la décennie 2000 - d'ailleurs y avait-il de la cyber au-delà des barbus du chiffrement à courbe elliptique de niveau 5 ?

Les années 2010 furent synonymes de gueule de bois matinée d'attaques russo-coréo-irano-americano-mafiosiennes.

Les historiens de l'IT s'écharperont dans des décennies pour savoir si l'an 0 a été *STUXNET*, *I LOVE YOU* ou les tentatives de phishing à base de photos « de gens ».



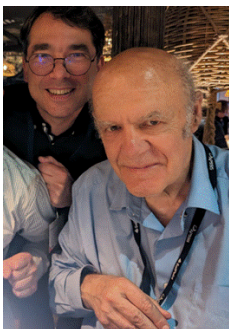
Toujours est-il que du passé il n'y a plus, et que les journées pépères ont cédé la place au stress.

Dans ce contexte, le plan de carrière classique du RSSI est assez standard : adminsys, responsable infra, RSSI, Directeur cyber, et pensionnaire de l'aile ouest 3ème étage chambre 315 avec repas à heures fixes, nourri blanchi camisolé.

Comment garder son calme dans un monde de dingue ? Plusieurs stratégies pour éviter de finir à rire bêtement en jouant à chat devant les feux de l'amour et parler à longueur de temps à son ami imaginaire.

Tant qu'à terminer dingue, autant y amener du monde...

Je reprends la plume



Qui est Cédric CARTAU ?



l'intervenant, Cédric Cartau, est le RSSI du CHU de NANTES depuis 2009.
Il a travaillé au CHU de REIMS et au CHU de RENNES

Membre de l'APSSIS, ARCSI, CESIN, AFCDP, il est co-fondateur du groupe RSSI NANTAIS et ISO 27001 Pays de la Loire.

Il est chroniqueur dans DSIH Magazine et auteur de 6 ouvrages spécialisés.
Il a publié dans 6 opus cyber résilience avec l'APSSIS
Pour l'open 6, voyez en :

<https://www.arcsi.fr/doc/APSSIS-Guide-Cyber-resilience-RSSI-Intergalactique.pdf>

Cédric est enseignant au CNAM, au CNEH, à l'EHESP (École des hautes études en santé publique), à l'ESIEA, à l'Université de Nantes et à POLYTECH NANTES.

Pour en savoir plus sur notre intervenant :

<https://dsih.fr/articles/5621/a-qui-appartient-le-dossier-medical-du-patient-1>

<https://dsih.fr/articles/5332/quelques-news-dejantees-de-la-planete-cyber>

<https://dsih.fr/articles/5017/debut-dannee-cyber-lambiance-en-soute-nest-pas-jouasse>

<https://dsih.fr/articles/5653/a-qui-appartient-le-firewall-de-lentreprise-une-approche-service-dun-sujet-faussement-simple>

et écoutez notre ARCSliste Cédric qui s'exprime aux 15^e Rencontres de l'ARCSI en :

<https://www.dailymotion.com/video/x8ruw71>



Demande d'inscription pour le « Lundi de la cybersécurité » du mois de novembre 2024

Lundi 18 novembre, à partir de 18 h 00, par visio-conférence Zoom.



Nos « Lundi de la cybersécurité » sont gratuits et veulent vous offrir une fête technologique. Demandez votre inscription, par courriel, nous vous enverrons, un peu avant le jour de l'événement, un hyperlien vers la visioconférence.

Les demandes d'inscriptions sont à adresser par mail à :

beatricelaurent.CDE@gmail.com

Les prénoms, noms et adresses mails des inscrits seront connus des organisateurs et communiqués aux intervenants. Si vous voulez être ajoutés à ma liste de distribution de mes lettres des « *Lundi de la cybersécurité* » mensuels, demandez-le-moi par mail (gerard.peliks@noos.fr).

La salle d'attente Zoom sera ouverte aux alentours de 17 h 00. L'évènement commencera à 18 h 00. Prévenez-nous, dès que possible si vous êtes inscrits mais avez un empêchement qui ne vous permet pas d'assister à ce webinaire.

Quelques minutes avec une organisation :



Suivant la tradition de nos « Lundi de la cybersécurité », entre l'exposé de l'intervenant et la session questions / réponses, nous donnons, autour de 19 h 15, pour une quinzaine de minutes la parole à une organisation ou à une personne qui opère dans l'écosystème du numérique et dans la sécurité de l'information.

Pour ce Lundi de novembre, nous donnons la parole à l'ANSSI, à **Laure Hélène-Duhesme**, Coordinatrice sectorielle santé, Bureau santé et affaires sociales, Division coordination sectorielle, sous-direction stratégie Agence Nationale de la Sécurité des **S**ystèmes d'Information.

Le coin des « Lundi de la cybersécurité » précédents.

Vous trouverez tous les détails, slides, parfois aussi les enregistrements et des comptes rendus, écrits par Clarisse Véron, aujourd'hui élève du master2 « Cybersécurité et e-Santé » de l'université Paris Cité sur le web de l'ARCSI en https://www.arcsi.fr/evt_passes.php.

Mais attention, il n'est pas garanti qu'il y aura tous ces documents pour chacun de nos lundis. Donc il est conseillé d'être connectés pour y assister par Zoom (donc de demander votre inscription).

Le coin-coin de l'IA Générative

Allons-nous obtenir une « hallucination » ou une réponse qui décrit une situation bien réelle ?

Question posée à Gemini (IA Générative de Google) :

Un RSSI peut-il survivre dans un monde de dingues ?

Voici une partie de la réponse reçue :

La question de la survie d'un RSSI (Responsable de la Sécurité des Systèmes d'Information) dans le paysage numérique actuel, en constante évolution et de plus en plus complexe, est tout à fait pertinente.

Les défis auxquels font face Multiplication des menaces :

- Multiplication des menaces : Les cyberattaques se sophistiquent, se multiplient et deviennent de plus en plus ciblées. Les ransomwares, les attaques par phishing, les intrusions dans les systèmes d'information sont devenues monnaie courante.
- Complexité des systèmes d'information : Les entreprises utilisent un nombre croissant de technologies, de logiciels et de dispositifs connectés, ce qui rend la gestion de la sécurité de plus en plus complexe.
- Pénurie de talents : Il y a une pénurie mondiale de professionnels de la cybersécurité qualifiés, ce qui rend difficile de recruter et de retenir les meilleurs talents.
- Pression réglementaire : Les réglementations en matière de protection des données se multiplient et se durcissent, ce qui impose de nouvelles contraintes aux entreprises et à leurs RSSI.
- Transformations digitales : La transformation digitale accélérée des entreprises entraîne de nouveaux risques et de nouvelles vulnérabilités.

Néanmoins, les RSSI peuvent non seulement survivre mais aussi prospérer dans ce contexte en :

- Adoptant une approche proactive : Plutôt que de réagir aux incidents, les RSSI doivent anticiper les menaces et mettre en place des mesures de prévention solides.
- Investissant dans la formation : Il est essentiel de former les employés à la sécurité informatique pour qu'ils deviennent le premier rempart contre les cyberattaques.
- Utilisant les technologies émergentes : L'intelligence artificielle, la blockchain et d'autres technologies peuvent aider à améliorer la sécurité des systèmes d'information.
- Collaborant avec les autres services de l'entreprise : La cybersécurité ne doit pas être un silo, mais doit être intégrée dans l'ensemble de l'entreprise.
- Communiquant efficacement : Les RSSI doivent être capables de communiquer clairement les risques et les enjeux de la sécurité informatique à la direction et aux employés.

En conclusion, le métier de RSSI est certes exigeant, mais il est aussi passionnant et porteur d'avenir. Les RSSI qui sauront s'adapter aux évolutions du paysage numérique et adopter une approche stratégique de la sécurité pourront non seulement survivre mais aussi jouer un rôle clé dans la protection des entreprises.

Je reprends la plume.

Bon là, ça me semble être une bonne réponse de Gemini.

Cédric CARTAU nous en dira plus le 18 novembre 18h et répondra aussi à nos questions.

Une évidence qui m'est apparue depuis que je termine ces lettres des "Lundi de la Cybersécurité" par une interrogation via une IA Générative : Pour obtenir une réponse édifiante, et pas qu'une hallucination, il faut

formuler le bon prompt et il est ensuite indispensable de garder une hauteur de vue pour interpréter la réponse en s'appuyant sur sa compétence en cybersécurité et sa connaissance des métiers de son organisation.

Un métier d'avenir : **EPIR** – Editeur de **P**rompts et **I**nterpréteur des **R**ésultats. A faire valoriser par votre COMEX !

Gérard