Votre pentest est **idiot** !

@jpgaulier

cyberzen

Sans eux, pas de talk !

OSSIR

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

NO LIMIT SECU

* Legal, ne riez pas.

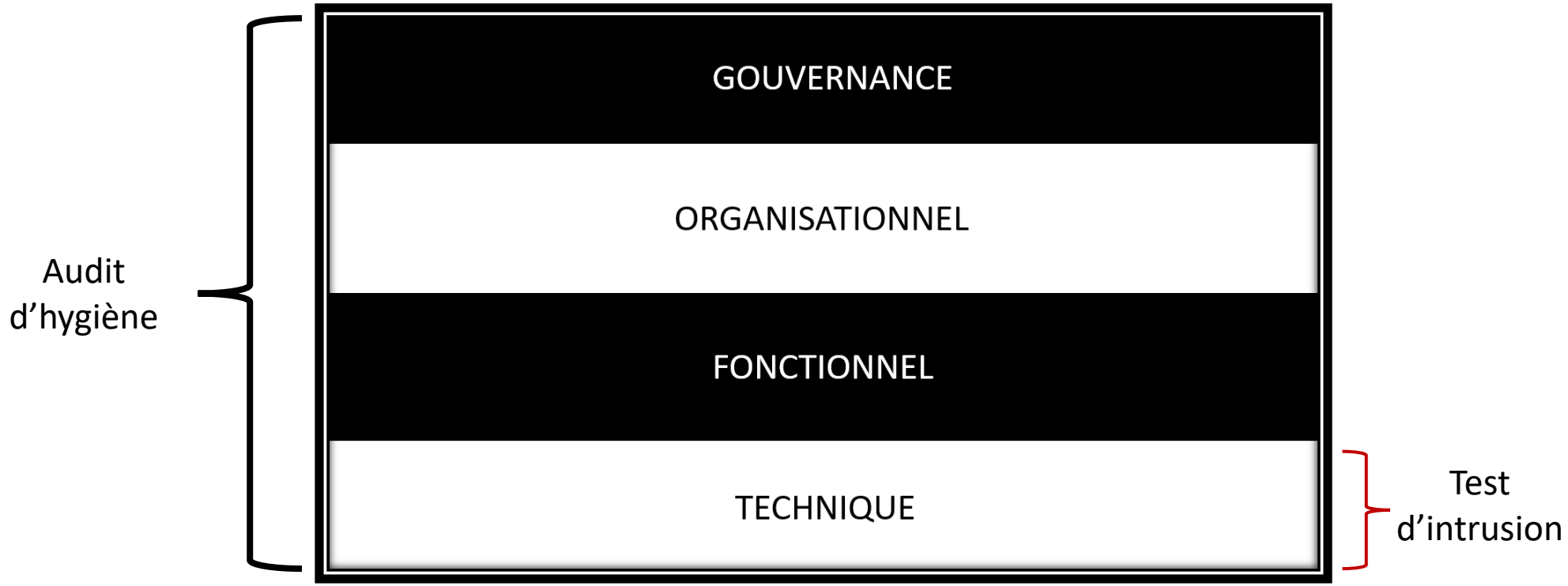
Et nos chers clients !

cyberzen

C’est simple comme un coup de fil…

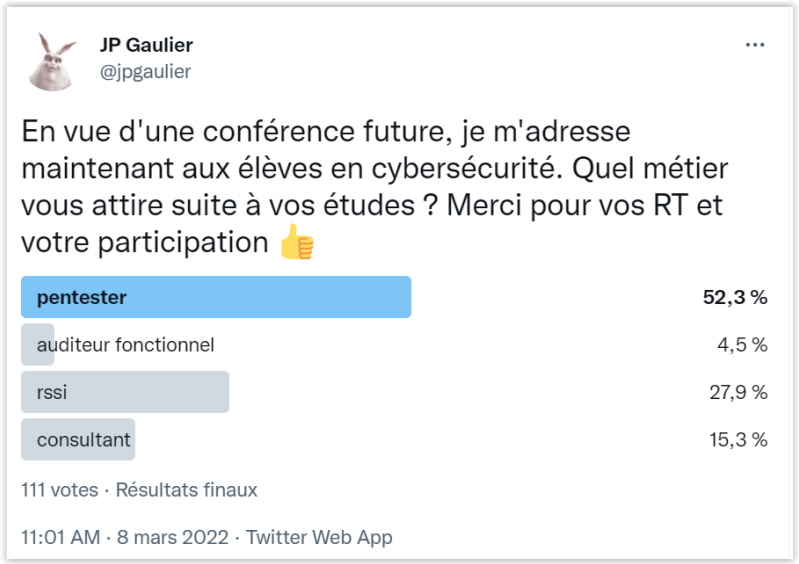
« Bonjour, on est la *clinique machin*, on a vu que vous faisiez des audits, on est intéressé vu que c’est l’ANSSI ***qui va tout payer***
- Aucun problème, nous faisons des audits organisatio…
- Ah non, moi je veux un pentest, sinon **c’est pas remboursé** ! »

Portée



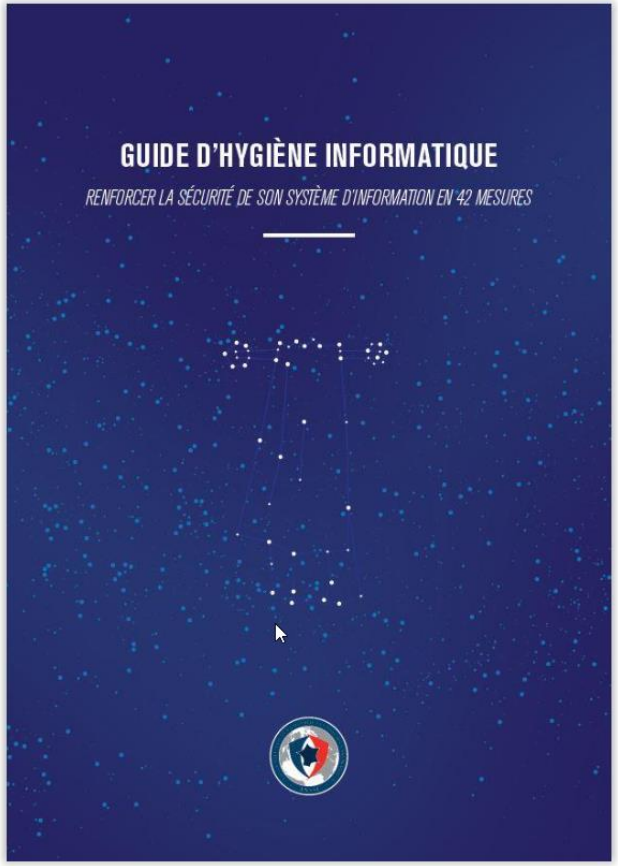
cyberzen

Quand je serai grand !



cyberzen

Base de dialogue



200k€ < CA < 100M€

=

42 audits

5 < employés < 400

cyberzen

100% des anecdotes racontées
durant ce talk sont factuelles.

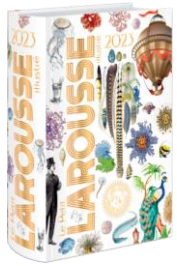
Tous les cas présentés permettent un accès
à un STAD ou une élévation de privilège.

Ces propos n’engagent que moi.

Aucun chat n’a été maltraité.

cyberzen

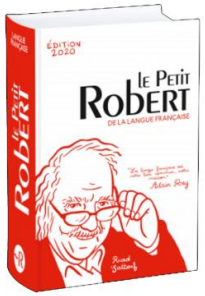
Vers une définition. tion. tion.



« Ensemble des principes, des pratiques individuelles ou collectives visant à la conservation de la santé, au fonctionnement normal de l'organisme »

CNRTL

« Ensemble des mesures, des procédés et des techniques mis en œuvre pour préserver et pour améliorer la santé. »



« Ensemble des principes et des pratiques tendant à préserver, à améliorer la santé »

« Règles et pratiques nécessaires au maintien de la santé et de la propreté »

cyberzen

linterGute

Comprenons-nous bien.

	0	Rien. Le vide.	*Un arbre qui tombe ne fait-il du bruit que s'il y a quelqu'un pour l'entendre tomber ?*
	1	Preuve de concept	Promis, on a un projet en cours. Il est commencé, j'ai mis un titre.
	2	Les techs ont bossé	Ouais, même que là, j'ai implem la RFC 1149, lol!
	3	C'est documenté	Ah, tiens, ils ont une ingénieur qualité.
	4	Des indicateurs !	Une supervision ! Une supervision !
	5	Iso 27001	Amélioration continue, vers l'infini et au-delà !
	N/A	Non-applicable	On l'a refilé à un prestataire (sans contrat)

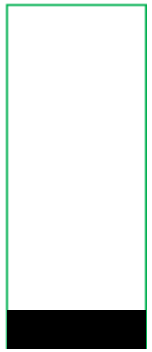
cyberzen

Thèmes (park)

	standard	renforcé
SENSIBILISER ET FORMER	1.14	1.35
CONNAITRE LE SYSTÈME D'INFORMATION	1.66	1.28
AUTHENTIFIER ET CONTRÔLER LES ACCÈS	1.46	1.07
SÉCURISER LES POSTES	1.41	1.24
SÉCURISER LE RÉSEAU	2.69 💪	2.35
SÉCURISER L'ADMINISTRATION	0.89	2.28 WTF?!
GÉRER LE NOMADISME	1.20	0.87
MAINTENIR À JOUR LE SYSTÈME D'INFORMATION	1.28	N/A
SUPERVISER, AUDITER, RÉAGIR	1.43	0.80
POUR ALLER PLUS LOIN	N/A	2.96
Global	**1.62**	**1.53**

cyberzen

Les équipes informatiques opérationnelles sont-elles formées en cybersécurité, au moment de leur prise de poste, puis de manière annuelle ?



Moyenne : 0.58 Ecart type : 1.07

Slide sponsorisée par

HS2
Hervé Schauer Sécurité

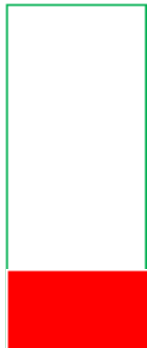
cyberzen

📅 Date : 2021

- Serveur *mariadb* en écoute sur le port 3306.
- Compte root utilisé pour administrer la base.
- Mot de passe était complexe d’une longueur de 8 caractères.
- Pas d’anti-rejeu.
- Serveur de production non supervisé.

cyberzen

Sensibilisez-vous vos utilisateurs aux risques cyber et à la valeur de vos données et de votre système d'information ?



Moyenne : 1.19 Ecart type : 1.27

cyberzen

📅 Date : 2022

Client 1

- « Chez nous, tout le monde passe la sensibilisation de l'ANSSI »
- 11 collaborateurs
- 1 certificat (*ndlr : on félicite le courageux*)

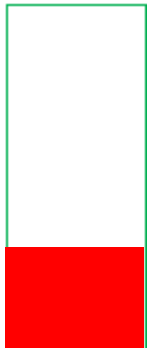
Client 2

« Oui, j'ai cliqué sur le lien dans le mail et j'ai cru que c'était une vraie mire Office365, alors j'ai mis mon login et mon mot de passe. C'est pas grave, hein ? »

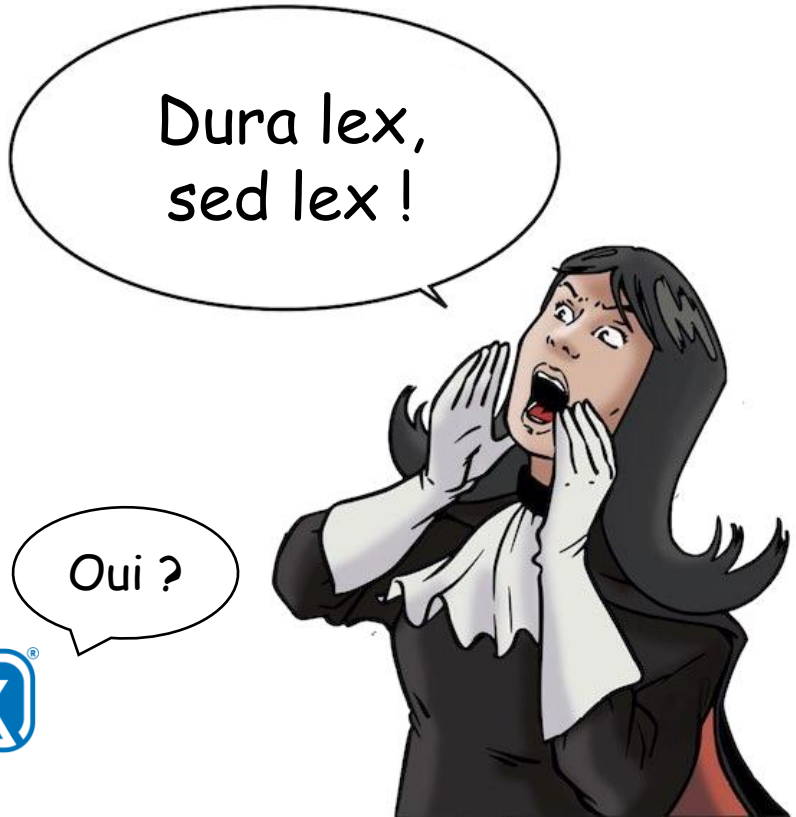
« Ah, et on s'est rendu compte que le pirate a envoyé un nouveau rib à nos clients… »

cyberzen

Avez-vous une charte de bon usage informatique et est-elle obligatoirement signée par vos collaborateurs ?



Moyenne : 1.35 Ecart type : 1.53



cyberzen

durex

EXAMPLE

📅 Date : régulièrement

« Dans la charte, il est inscrit que vous devez respecter la Politique de Sécurité du Système d'Information. Avez-vous signé cette charte ?

- Oui, bien sûr !

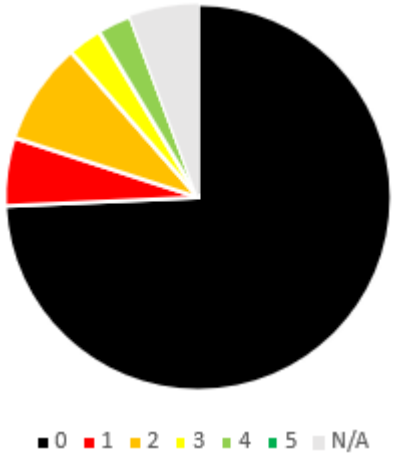
- Donc vous avez lu la PSSI afin de pouvoir la respecter ?

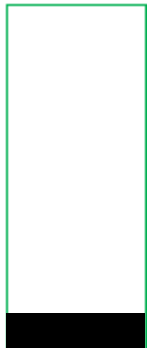
- Euuuuh…

- Et donc vous savez que si vous ne chiffrez pas un document confidentiel comme indiqué dans la PSSI, vous enfreignez la charte est commettez une faute vis-à-vis de votre contrat de travail…

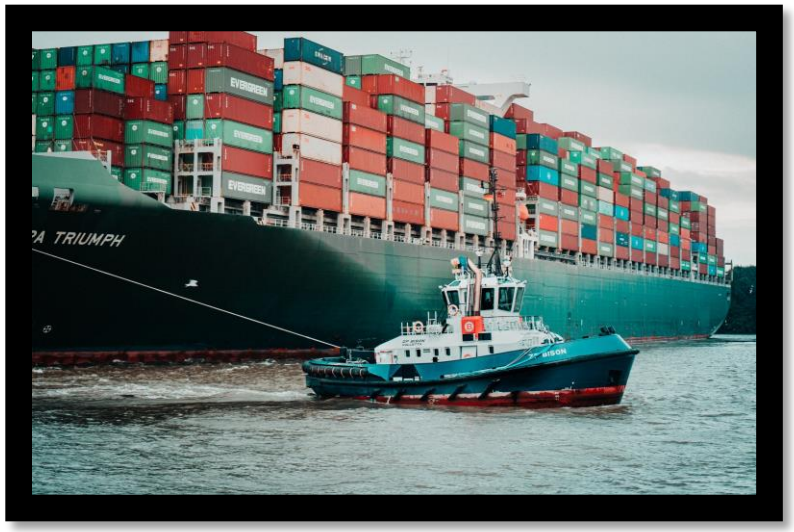
cyberzen

Vos contrats d'infogérance incorporent-ils des clauses de SSI ? Demandez-vous systématiquement la fourniture d'un PAS ?





Moyenne : 0.45 Ecart type : 0.99



cyberzen

EXAMPLE

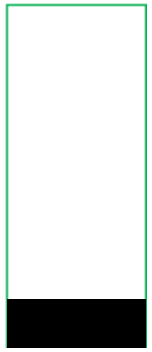
🗓️ Date : 2022

« Toute l’informatique est déléguée à un bureauticien.

- (le bureauticien) Non, mais nous, on est super fort en cyber, hein !
- Ok, donc vous avez des clauses dans le contrat ?
- Oui, bien sûr ! On a une **assurance cyber** !!!

cyberzen

Existe-t-il une mesure technique obligeant l'authentification des postes sur le réseau ?



Moyenne : 0.66 Ecart type : 0.92

cyberzen

EXAMPLE

🗓️ Date : 2022

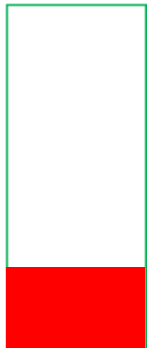
« On est bien d’accord, je ne peux pas me connecter chez vous avec mon laptop ?

- Ah oui, ça c’est sûr !
- Ok, mais si je m’interface sur le lien de votre imprimante ?
- Mais vous n’avez pas le droit !!! »

Bonus : *Bien sûr, le personnel de ménage a la clé et vient le soir ou le week-end.*

cyberzen

Les accès aux données sensibles de l'entreprise sont-ils revus de manière régulière ?



Moyenne : 1.08 Ecart type : 1.13

cyberzen

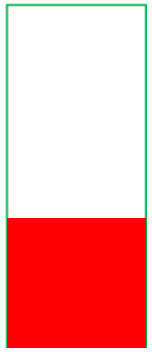
EXAMPLE

📅 Date : 2022

« On a un employé qui s'occupait de tout le réseau qu'on a licencié il y a un mois mais on pense qu'il a gardé des accès et potentiellement il a pris beaucoup de nos informations et que potentiellement il continue parce qu'on ne sait pas trop. »

cyberzen

Il y a-t-il une politique de mots de passe* en place ?



Moyenne : 1.76 Ecart type : 1.16

NOMBRE DE CARACTÈRES	UNIQUEMENT DES CHIFFRES	LETTRES MINUSCULES	LETTRES MINUSCULES ET MAJUSCULES	LETTRES MINUSCULES ET MAJUSCULES + CHIFFRES	LETTRES MINUSCULES ET MAJUSCULES + CHIFFRES + CARACTÈRES SPECIAUX
4	IMMÉDIATEMENT	IMMÉDIATEMENT	IMMÉDIATEMENT	IMMÉDIATEMENT	IMMÉDIATEMENT
6	IMMÉDIATEMENT	IMMÉDIATE	ENT	1 sec	5 sec
8	IMMÉDIATEMENT	5		1 heure	9 heures
10	IMMÉDIATEMENT	58		7 mois	5 ans
12	45 sec	3 sem		2000 ans	34 000 ans
14	41 min	51 ans	800 000 ans	9 millions d'années	200 millions d'années

*source : SCSP Community (Seasoned Cyber Security Professionnals)

cyberzen

🗓️ Date : permanent

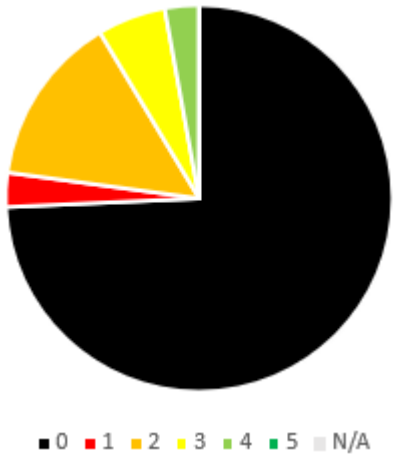
« Evidemment qu’on a une politique de mots de passe ! C’est 8 caractères, mais attention !

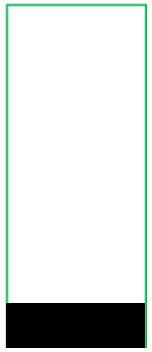
Il faut des majuscules, des minuscules, un caractère spécial et un chiffre, on n’a pas le droit

d’utiliser les 10 derniers mots de passe et il faut les changer tous les trois mois !

cyberzen

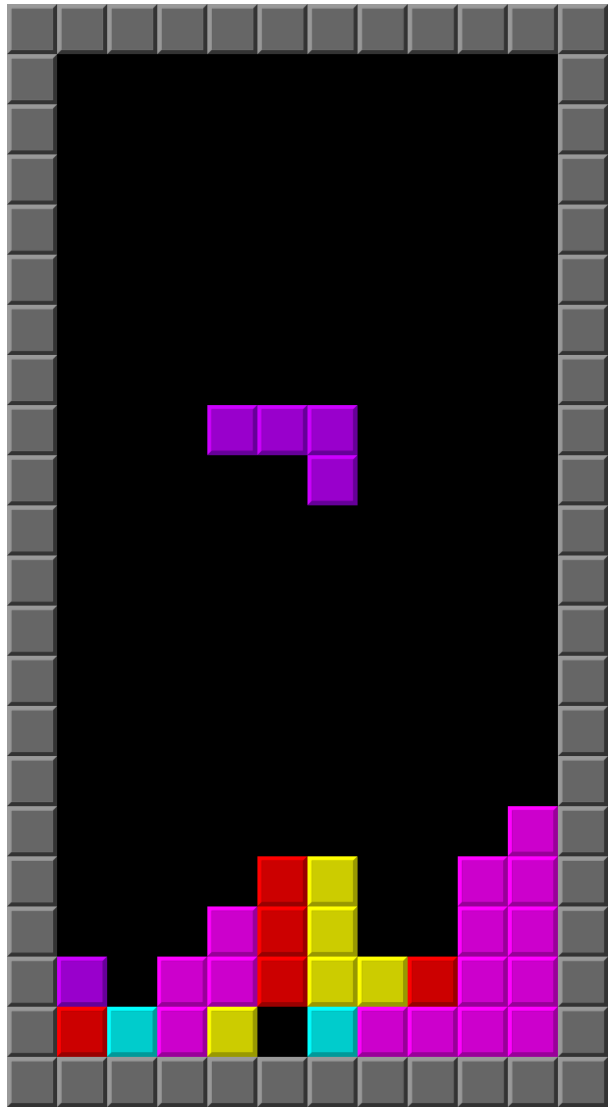
Avez-vous une gestion de la sécurité des ports USB ?





Moyenne : 0.60

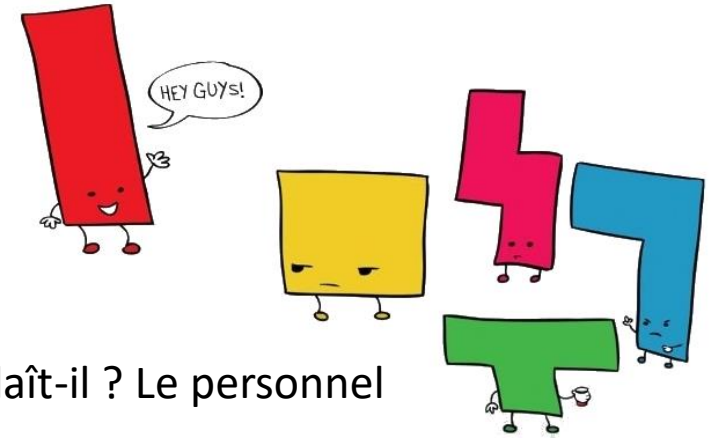
Ecart type : 1.10



cyberzen

EXAMPLE

Date : 2022



Client 1

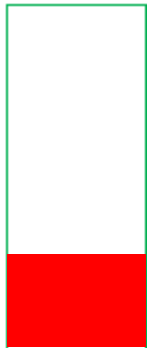
« Oui, nos projets sont secrets, nous faisons très attention. Vous ? Quoi ? Plaît-il ? Le personnel de ménage a-t-il la clé pour venir le week-end ? Nos ordinateurs restent sur place ? Oui, bien sûr, pourquoi ? »

Client 2

« Monsieur machin, c'est le DGA ? Oui ? Ah non, parce qu'il vient juste de brancher la clé de la red team… »

cyberzen

Utilisez-vous un outil de gestion centralisée des politiques de sécurité pour les postes utilisateurs ?



Moyenne : 1.24 Ecart type : 1.27

cyberzen

EXAMPLE

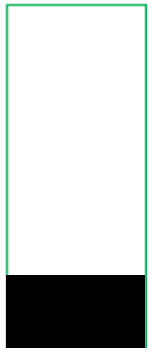
📅 Date : 2022

« Je passe sur tous les ordinateurs une fois par mois pour m’assurer que les mises à jour sont bien là et sur le NAS une fois par semaine. »

« Les imprimantes ? Non, jamais »

cyberzen

Les utilisateurs sont-ils administrateurs de leur poste ?



Moyenne : 0.97 Ecart type : 1.00

cyberzen

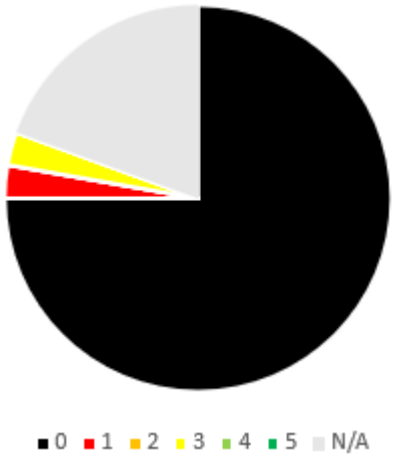
EXAMPLE

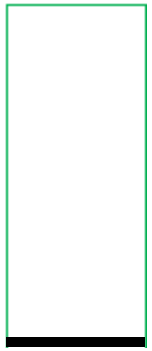
📅 Date : 2020

« Oui, ils sont administrateurs de leur poste, parce que sinon, pour nous c'est plus contraignant et on doit passer plus de temps à faire le travail alors que là, il peuvent installer tous les logiciels directement. »

cyberzen

Avez-vous une politique de gestion de flotte mobile ?





Moyenne : 0.14 Ecart type : 0.57

cyberzen

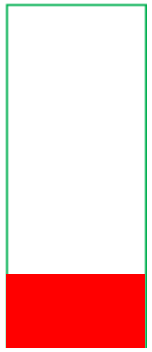
EXAMPLE

🗓️ Date : permanent

« Nous avons effectivement des téléphones pour nos collaborateurs. En fait, il s’avère que ce sont leurs téléphones, mais ils sont bien sûr d’accord pour l’utiliser dans le cadre du travail. C’est pratique et ça nous coûte moins cher. »

cyberzen

Comment gérez-vous l'obsolecence du parc ?



Moyenne : 1.00 Ecart type : 0.93

cyberzen

EXAMPLE

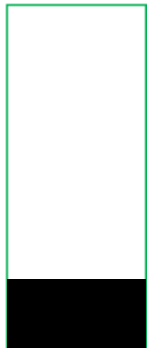
📅 Date : 2016

« Le maintien des mises à jour pour Microsoft Windows XP coûtera **1 000 000 €** la première année puis **5 000 000 €** l'année suivante »

Oui Non

cyberzen

Les journaux sont-ils centralisés sur les éléments essentiel de votre SI ?



Moyenne : 0.91 Ecart type : 1.08

cyberzen

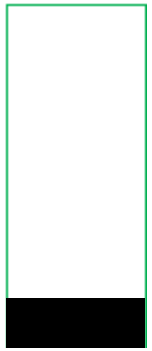
EXAMPLE

🗓️ Date : permanent

« Le SOC n’a rien vu »

cyberzen

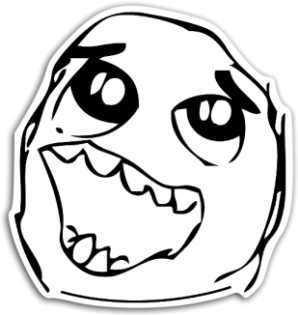
Avez-vous un plan de test des sauvegardes ?



Moyenne : 0.67 Ecart type : 1.00

EXAMPLE

🗓️ Date : 2021

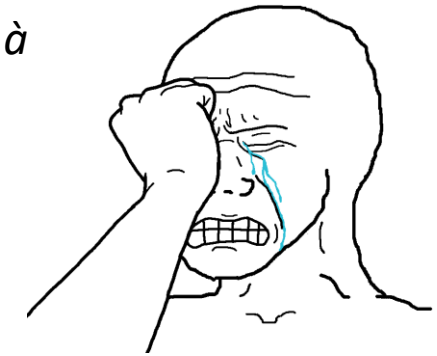


« Nous, on est dans la tech, on est super fort !

- Du coup, on fait un audit, vous aurez une bonne note ?

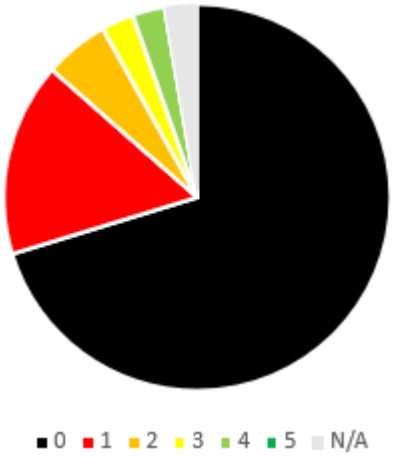
- Mais oui, bien sûûûûr ! »

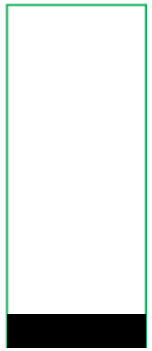
« Ah, votre sauvegarde est sur le même NAS que là où sont vos données à sauvegarder?! »



cyberzen

Avez-vous mené une analyse de risque ?





Moyenne : 0.47 Ecart type : 0.93

cyberzen

🗓️ Date : permanent

« Vous avez un plan d’audit annuel ?

- Bien sûr ! On fait des pentests !
- C’est très bien ! C’est dans le but de circonscrire quels risques ?
- Euhhhhhhhhhhh »

cyberzen

Conclusion (enfin)

- ✓C’est **beau** toutes ces statistiques !
- ✓Le niveau de sécurité standard est défini par les options activées par défaut dans les systèmes d’exploitation (chiffrement, antivirus, pare-feu, logs…). Vive le monopole.
- ✓Le niveau moyen du **bureauticien** est en-dessous.
- ✓Un DSI externalisé est un bureauticien.
- ✓Si les mesures d’hygiènes sont en place, le niveau moyen du pentesteur va **devoir** s’améliorer.
- ✓Je suis plus sympa après avoir bu un coup.

MERCI POUR CE MOMENT