
Cycle Sécurité
Quelles leçons tirer de la crise sanitaire
et de la professionnalisation
des cyber attaques ?
CLUB UTILISATEURS
DE SOLUTIONS ORACLE

# Cycle Sécurité
# Quelles leçons tirer de la crise sanitaire et de la professionnalisation des cyber attaques ?
# 9 MARS 2021

**Session pilotée par :**

Jean-Jacques CAMPS, *Directeur Global E&C Solutions, Sécurité Informatique*
**AIR LIQUIDE**

***Pilote du Cycle Sécurité et Président Honoraire de l'AUFO***

# Cycle Sécurité
# Quelles leçons tirer de la crise sanitaire et de la professionnalisation des cyber attaques ?
# 9 MARS 2021

Une session animée par
Jean-Jacques CAMPS, pilote du Cycle Sécurité

- Etat de l'art
  - ✓ Les grandes tendances | Prise de conscience
  - ✓ "Kit d'hygiène" | Bonnes pratiques

- Quelles leçons (provisoires!) tirer de la crise Covid-19 ?
  - ✓ La vision des experts membres du CESIN au travers des baromètres hebdo et du baromètre annuel
  - ✓ Les tendances et leçons tirées

- Echanges avec les intervenants et entre utilisateurs

mazars

*David LUPONIS, Associé au sein de la practice de conseil et d'audit Cybersécurité*

CESIN

*Alain BOUILLE, Fondateur et Délégué Général*

# Etat de l’art

*David LUPONIS,*

*Associé au sein de la practice de conseil et d’audit Cybersécurité*

mazars

# De la sécurité informatique à la cybersécurité

Responsable Sécurité

Responsable Sécurité des Systèmes d'Information

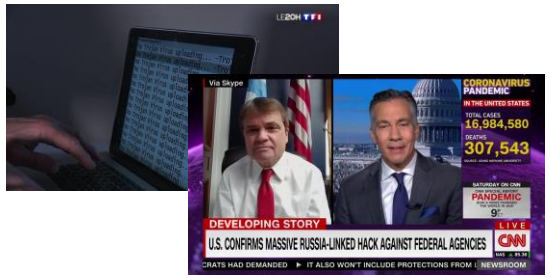
**Directeur Cybersécurité**

***Évolution de la menace***

2000

2010

2020




*Focus des attaques sur les infrastructures*

ORACLE DATABASE

*Attaques applicatives*

ORACLE E-BUSINESS SUITE

*Attaques combinées focus utilisateurs*

# La cybersécurité, nouveaux challenges des décideurs et des régulateurs

Fonds monétaire international

ANSSI

ACPR BANQUE DE FRANCE

SWIFT


https://reports.weforum.org/global-risks-report-2021/

# La cybersécurité, une actualité toujours brûlante

solarwinds

*Éditeur US de solutions IT dont l'outil de monitoring ORION*

solarwinds

*1ere alerte et 1er communiqué de presse*

FIREEYE

08/12/2020

solarwinds

*Information globale sur l'étendue de l'attaque et alerte du département de la Sécurité intérieure **

13/12/2020

FIREEYE

*Editeur de solution cyber et consulting/red-teaming, impacté par l'attaque qui a été le 1er à alerter*

> *18.000 clients utilisent la solution ORION dont des agences gouvernementales US (NSA/Pentagone/etc.), mais aussi Microsoft, VMWare, Crédit Suisse, etc.*

1. Principes de l'attaque

- Similaire à l'attaque qui avait touché Saint-Gobain en juin 2017
- Insertion dans le cycle de développement/produit de l'éditeur de la solution ORION d'un malware (bien entendu sans que l'éditeur s'en aperçoive)
- Attendre patiemment que la solution et le malware soient publiés/téléchargés chez des clients dans la cadre d'une mise à jour logicielle

2. Impacts

- Toutes les sociétés utilisant l'outil ORION (ou quasi) sont impactées car elles utilisaient un produit à jour intégrant le malware
- Chronologie complexe – le malware et ses effets sont peut-être installés depuis un certain temps sur les SI permettant l'espionnage, la récupération de données, etc.
- Fireeye indique dans son rapport que la faille existe depuis le printemps 2020 d'où le déploiement en masse de l'attaque et les craintes associées

- https://cyber.dhs.gov/ed/21-01/
- https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html

# Les tendances Cyber 1/2

## Assurances cyber

Evaluation et transfert des risques vers des assurances

+ Couverture financière et assistance en cas d'attaques

− Coûts financiers de la police d'assurances

Délimitation de l'assurance (vs disponibilité)

## Training

Rendre les collaborateurs acteur de la protection de l'entreprise

+ Couts limités

Apport assez direct

− Trouver l'angle le plus approprié pour la formation des collaborateurs

## Évaluation réglementaire (Swift, LPM/NIS, etc.)

Se conformer aux différents règlements cyber

+ Nécessaire pour qualifier des SI

− Coûts importants

Chronophage

# Les tendances Cyber 2/2

## Socles techniques

Mesures techniques pour protéger ses biens (SOC, EDR, zéro-trust, patch management, etc.)

+ Réduction de l'exposition aux risques

− Coûts d'investissement et de maintenance

Multiplicité des équipements

## Ransonware

Cauchemar des DSI et RSSI

− Verrouillage des données

Impossibilité de passer des opérations

Coûts de restauration/reconstruction

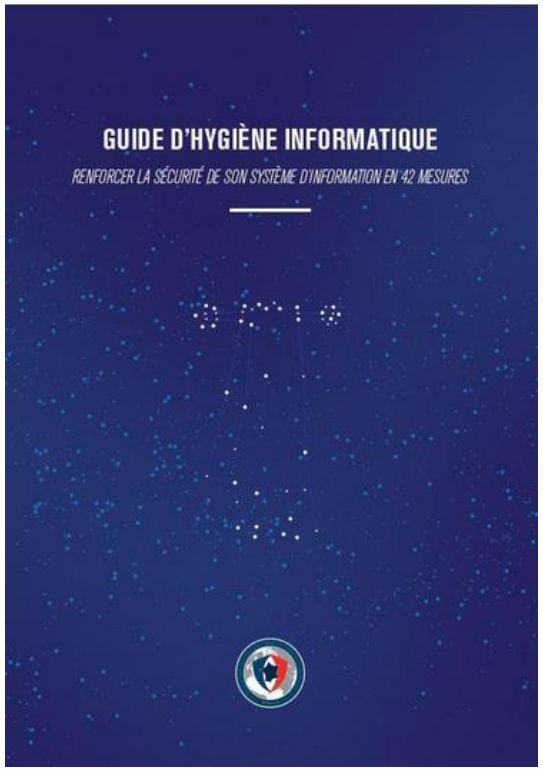
## Résilience cyber

Renforcer la continuité et la cybersécurité du SI

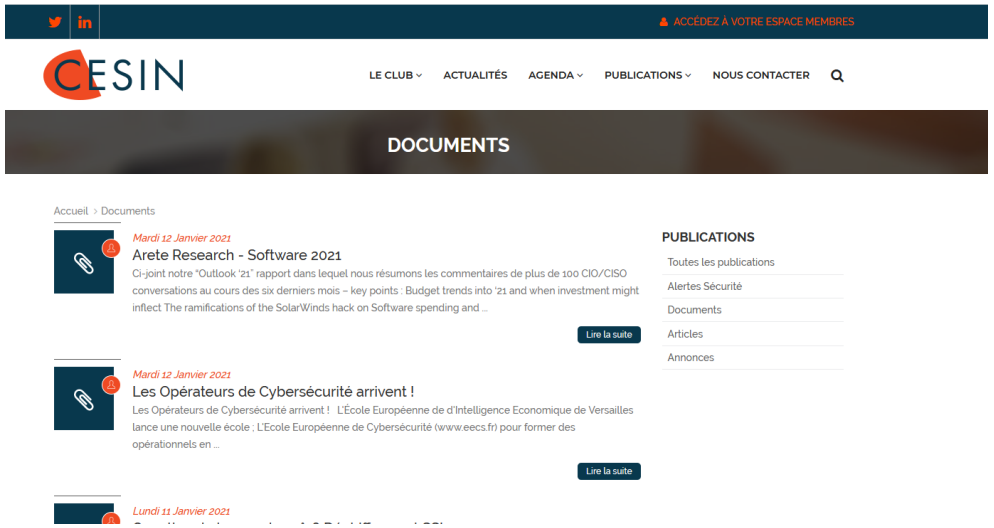
+ Dispositif de Place

− Chronophage

# Les bonnes pratiques




https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/




https://www.cesin.fr/fonds-documentaires.html

- **Évaluer** régulièrement les risques
- Mettre en place des **plans d'actions** pour remédier les risques cyber
  - Quick win
  - Travaux de fond
- **Organiser** la cybersécurité
- **Appliquer et renforcer les socles techniques**
- **Former** les utilisateurs
- Définir des **indicateurs** de cybersécurité

# Vos contacts

**Mazars**

# Suivez-nous

**LinkedIn :**
www.linkedin.com/company/Mazars

**Twitter :**
www.twitter.com/MazarsFrance

Mazars est un groupe international et intégré spécialisé dans l'audit, la fiscalité et le conseil ainsi que dans les services comptables et juridiques*. Présents dans plus de 90 pays et territoires, nous nous appuyons sur l'expertise de nos 40 400 professionnels – 24 400 au sein de notre partnership intégré et 16 000 au sein de « Mazars North America Alliance » – pour accompagner les entreprises de toutes tailles à chaque étape de leur développement.

*dans les pays dans lesquels les lois en vigueur l'autorisent

mazars

# Club des Experts de la Sécurité de l'Information et du Numérique

## Quelles leçons (provisoires!) tirer de la crise Covid-19 ?

*Alain BOUILLE, Fondateur et Délégué Général*

CESIN

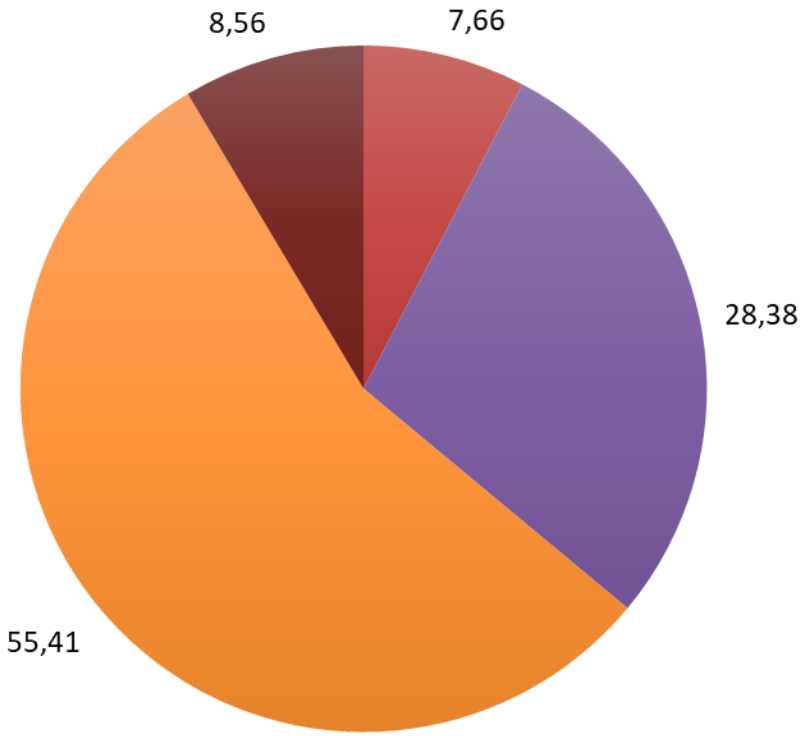
# Sommaire

1. Que disaient nos membres avant la crise ?
2. Qu'ont-ils dit pendant la crise ?
3. Trois types d'entreprises
4. Conclusions et recommandations

# Que disaient nos membres avant la crise ?

# Question de la semaine 15

21 janvier 2020



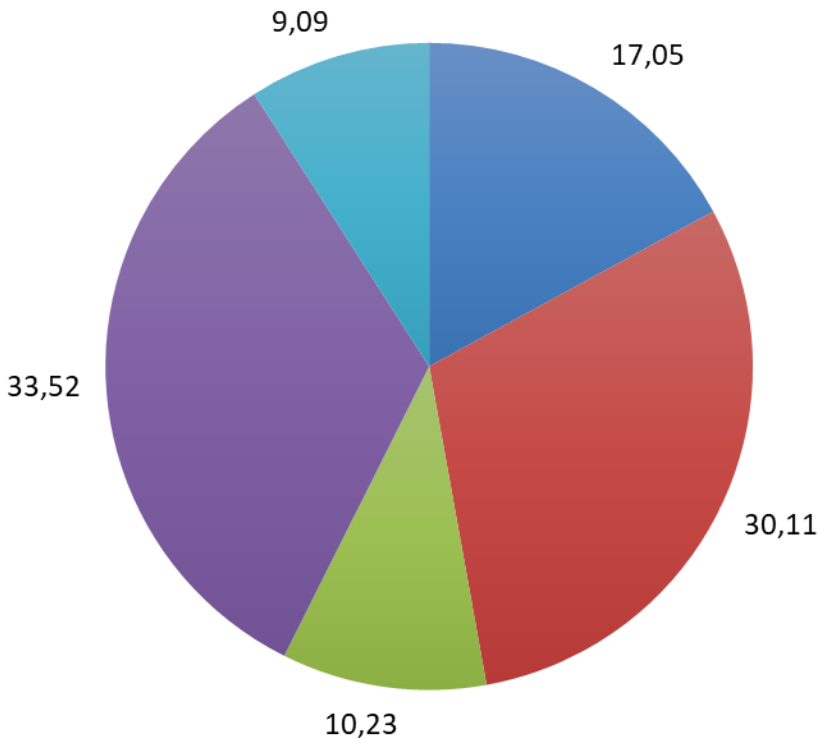

*222 répondants*

**Vulnérabilités et patching** : Avez-vous une bonne maîtrise de ce processus en termes de veille, couverture produit, réactivité, vitesse de déploiement (avec différents types de vitesse et de pilotes selon l'urgence/la gravité), exhaustivité, validation, relations avec les métiers et la production, traçabilité, vue consolidée, contrôle ?

- Non, le processus est mal maîtrisé
- Plutôt non, ce processus n'est pas vraiment sous contrôle, il manque un certain nombre de critères
- Plutôt oui, le processus est assez bien maîtrisé même s'il est perfectible
- Oui, le processus est bien maîtrisé dans ses différents axes

# Question de la semaine 17

4 février 2020



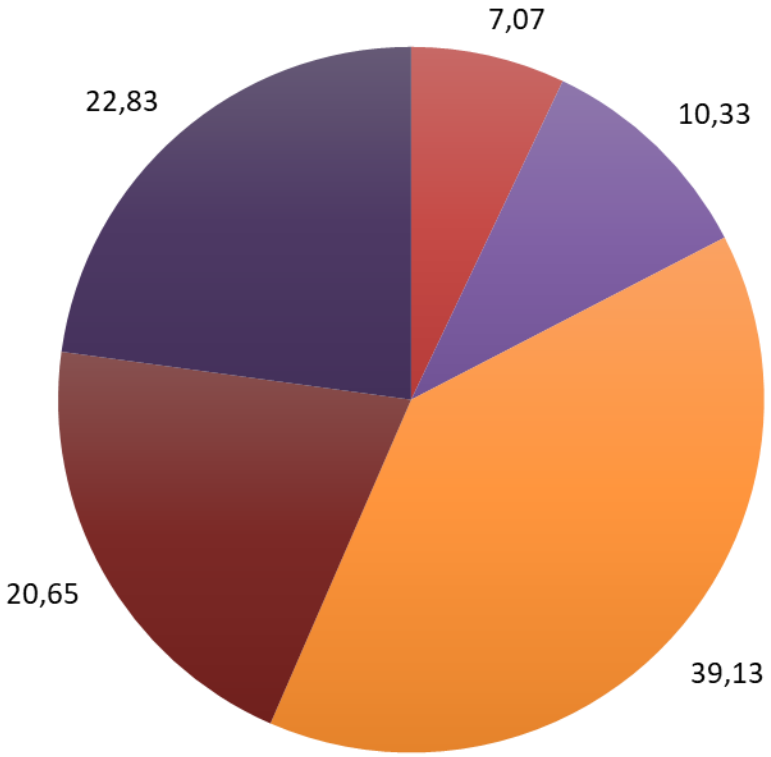

*176 répondants*

**Fuite de données** : Une part croissante de nos données est désormais confiée à des fournisseurs de solutions Cloud. Lorsque ces fournisseurs, grands ou petits, subissent des fuites de données, tout un processus doit être déroulé. **Quelle est votre maturité dans ce processus ?**

- Ce processus n'a pas été particulièrement étudié, aucune procédure spécifique n'est en place
- Seul le volet contractuel amont est réellement intégré dans ce processus
- Seuls des dispositifs de réaction technique à ce type d'incident sont en place.
- Ce processus est en train d'être mis en place dans ses différentes dimensions, le sujet est en cours.
- L'ensemble du processus est maîtrisé, depuis la relation contractuelle jusqu'à la prise en compte des incidents, sous tous ses aspects.

# Question de la semaine 19

18 février 2020



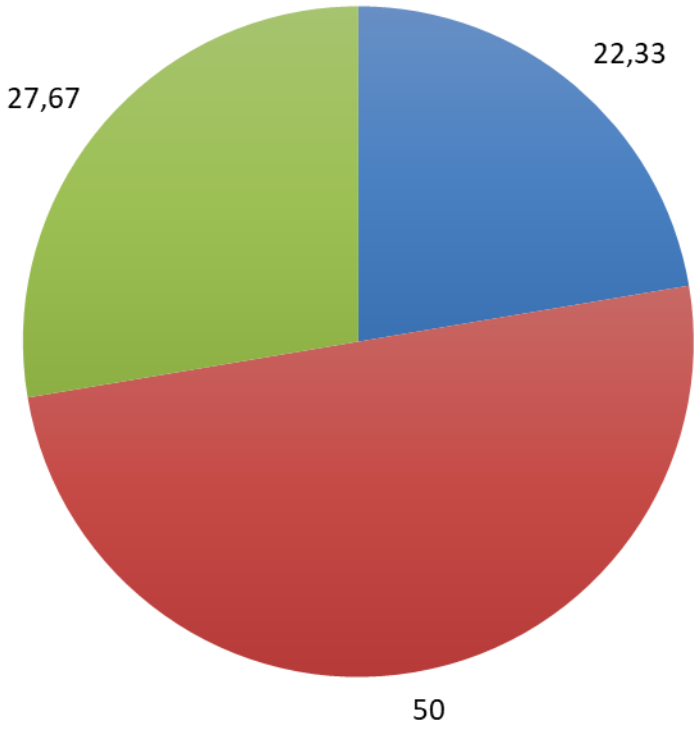

*184 répondants*

**Stress** : Nos métiers sont soumis à une pression permanente et très intense. Un sondage publié dernièrement fait état d'une charge mentale mal supportée dans nos communautés. **Et vous, comment le vivez-vous ?**

- Je me sens à la fois très stressé(e) et surmené(e) et je le vis assez mal.
- Je me sens très stressé(e) et je vis assez mal cette pression mentale.
- Je ressens clairement une pression mentale et un surmenage mais j'arrive à les gérer relativement bien.
- Mon métier entraîne une pression mentale et un surmenage mais je le vis bien, je trouve même que c'est assez galvanisant.
- Je considère que mon métier est exigeant mais ne comporte pas de spécificité sur le plan mental ou physique. Il y a une pression comme pour tous les postes de management et ça se gère bien.

# Question de la semaine 20

25 février 2020




*206 répondants*

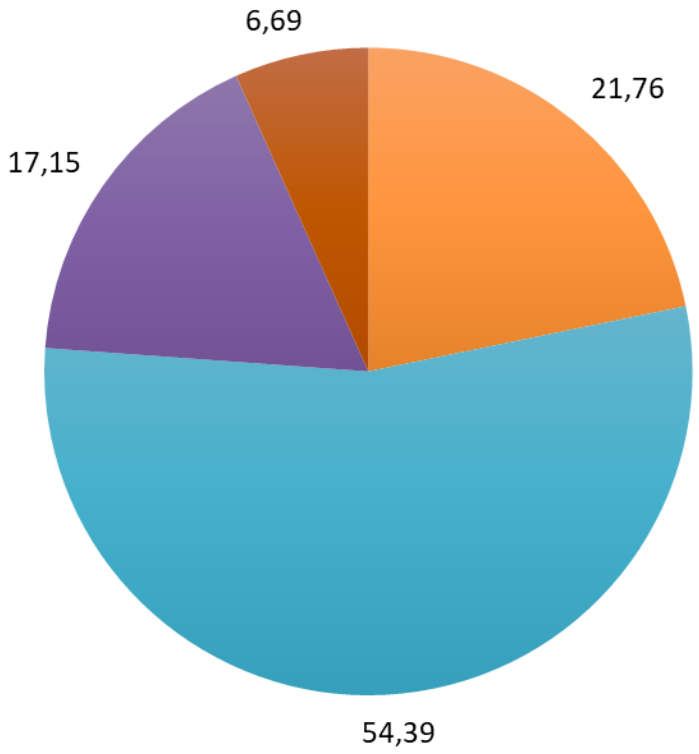
Avez-vous identifié ces données que l'on nomme parfois les « joyaux de la couronne » et qu'il faut protéger tout particulièrement ?

- Oui, cet inventaire est fait, formalisé et maintenu
- Oui, nous avons fait un inventaire a minima mais le travail est encore partiel
- Non, nous n'avons pas une liste précise de nos joyaux de la couronne

# Que disent nos membres pendant la crise ?

# Question de la semaine 21

3 mars 2020



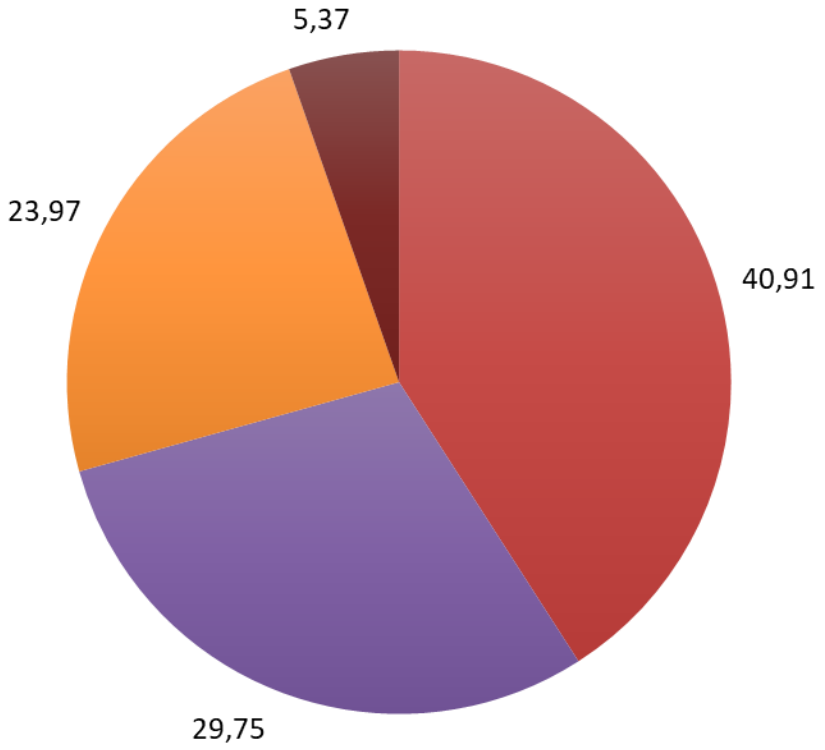

*239 répondants*

Nous sommes au démarrage de l'épidémie de coronavirus sur notre territoire. Quel est pour vous le principal impact de cette crise sur votre activité sécurité, du fait de ce contexte?

- Il y a très peu ou pas d'impact.
- L'impact est principalement dû à l'augmentation du télétravail qui devrait arriver et ce qu'il requiert en termes de disponibilité et de sécurité des moyens de connexion à distance.
- Il y a d'importantes actions en cours sur le plan de continuité d'activité.
- L'impact majeur est économique et concerne la réduction des dépenses sur les projets sécurité en cours et un frein sur les projets à venir.

# Question de la semaine 22

10 mars 2020



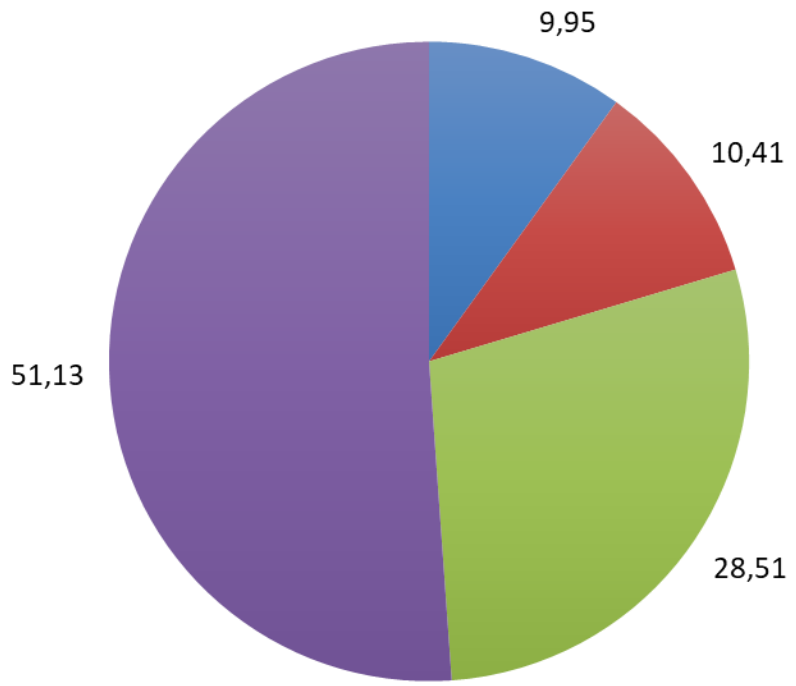

*242 répondants*

## Le Coronavirus met-il à l'épreuve la sécurité du travail à distance ?

- Seulement une partie des salariés est équipée pour travailler à distance et vous n'avez rien changé à date.
- Tous les salariés peuvent travailler à distance avec un niveau de sécurité adapté et cette situation ne change rien au dispositif habituel.
- Seulement une partie des salariés est équipée pour travailler à distance et vous avez dû adapter la sécurisation de votre dispositif, en réduisant les exigences de sécurité, pour permettre sa généralisation.
- Vous avez réduit certaines exigences de sécurité (cas 2), mais vous avez renforcé les mécanismes de supervision et de détection.

# Question de la semaine 24

31 mars 2020



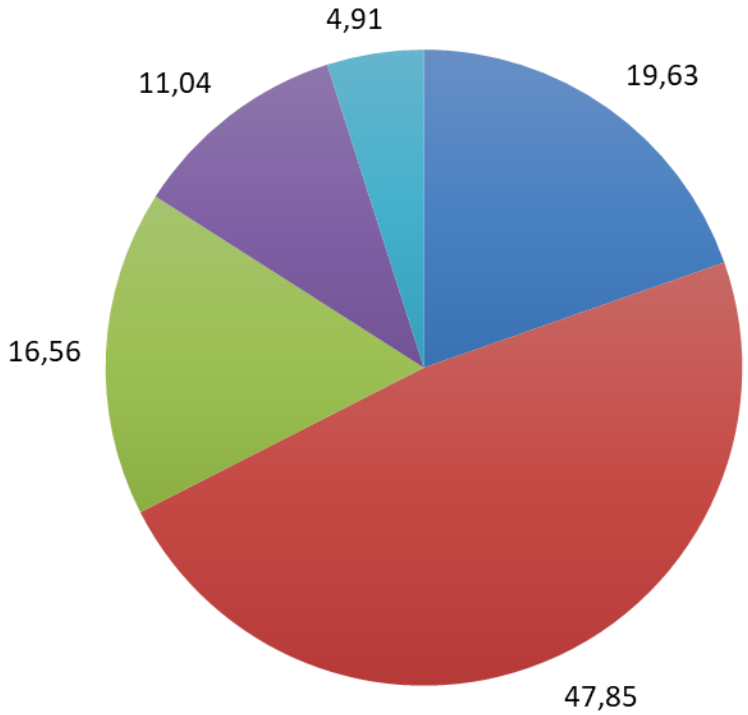

*221 répondants*

**Chiffrement** : Qu'en est-il de votre parc de postes de travail en mobilité ?

- Ils ne sont pas chiffrés
- Une petite partie de ce parc est chiffrée, pour les personnes à risque (VIP, administrateur)
- L'essentiel du parc mobile est chiffré
- L'intégralité du parc mobile est chiffrée

# Question de la semaine 30

19 mai 2020

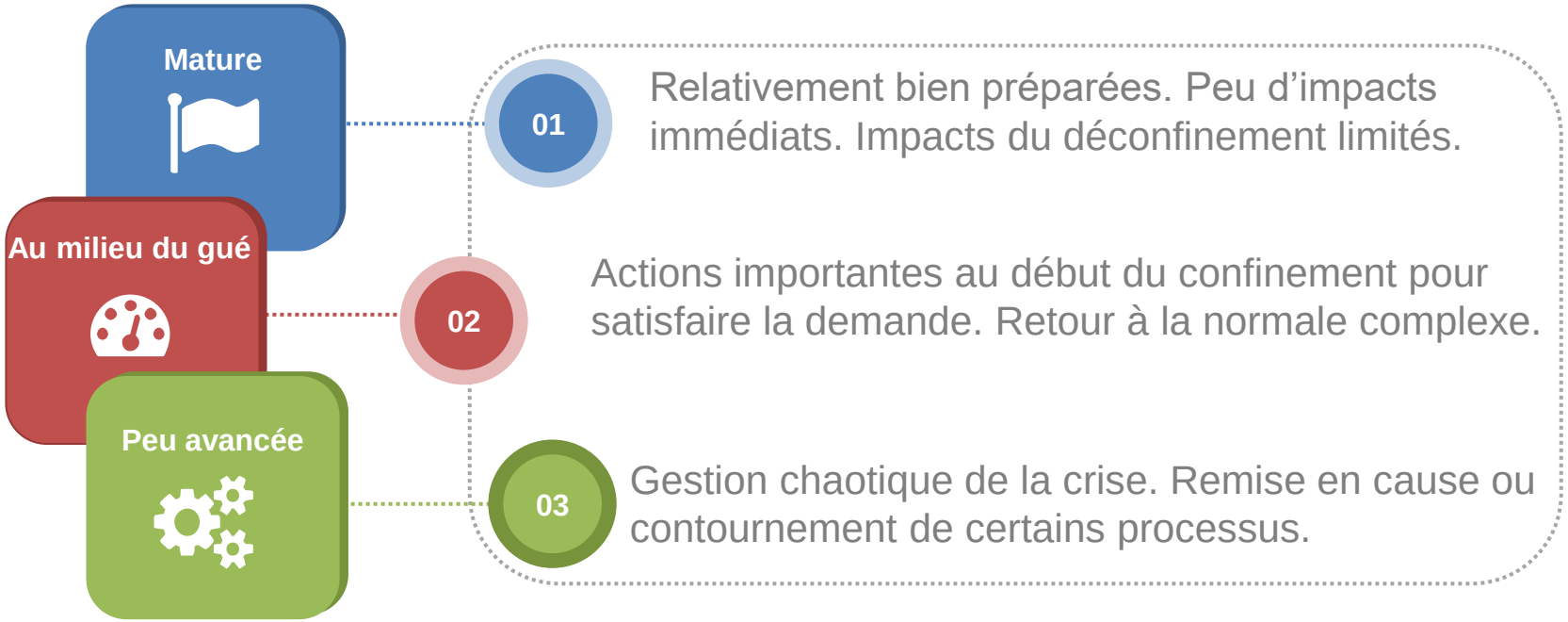



*163 répondants*

## Budget Cybersécurité post-crise : qu'en est-il au sein de votre entreprise ?

- Le budget Cybersécurité devrait être augmenté. La crise sanitaire a montré d'une part que les cyber risques n'ont jamais été aussi importants et que d'autre part des sujets liés aux nouveaux modes de travail devaient être démarrés ou renforcés
- Le budget Cybersécurité ne devrait pas être impacté
- Le budget cybersécurité devrait être réduit. Cette réduction devrait être inférieure à 20%
- Le budget cybersécurité devrait être réduit. Cette réduction devrait se situer entre 20% et 50%
- Le budget cybersécurité devrait être drastiquement réduit de plus de 50%

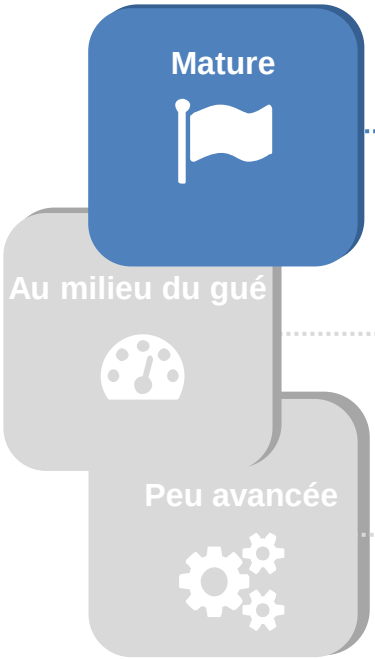
# Trois types d’entreprises pendant cette crise




On parle ici de « maturité » en terme de transformation numérique et d’évolution vers le cloud

CESIN

# L’entreprise Mature




01

✓ Familière du télétravail, outils de collaboration déployés, applications métier dans le cloud, accès VPN en nombre suffisants, etc.

02

✓ En conséquence, la sécurité des terminaux est déjà assurée, où que soient les postes : gestion des patchs, Mobile Device Management ou Unified Endpoint Management, Endpoint Detection & Response, MultiFactor Authentication, etc.

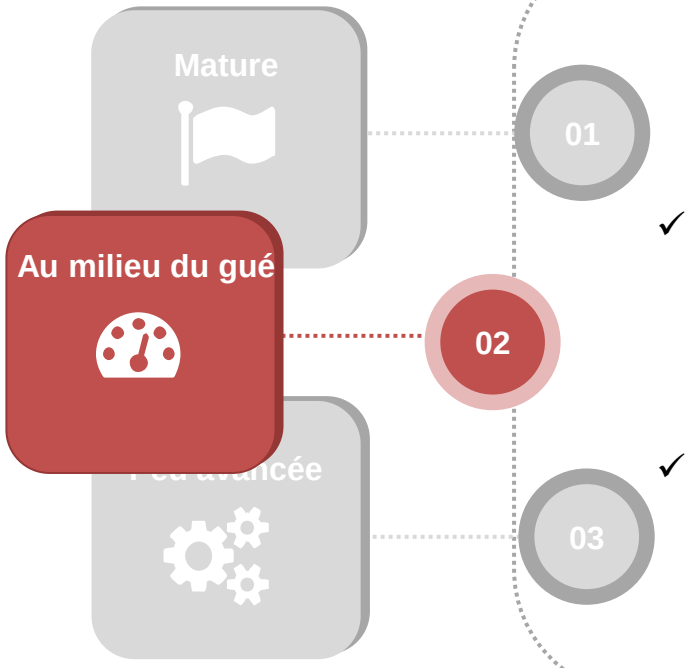
03

✓ **Impact de la crise**: La crise a nécessité juste quelques ajustements d’échelle et a été une bonne opportunité pour accélérer certains projets de cybersécurité.

**Quels risques résiduels ?**
L’utilisateur final confronté à des attaques de (spear-) phishing ou tous types de malwares. Il faut aussi garder un minimum de « joignabilité » des postes pour la sécurité des quelques % d’usages legacy.

CESIN

# L’entreprise « Au milieu du gué »




- ✓ Ces structures sont dans “l’entre-deux” : le télétravail n’est pas nécessairement généralisé, bien qu’en cours de développement. Les outils collaboratifs ne sont pas tous déployés, il reste un stockage centralisé sur filers et encore beaucoup d’applications métiers on premises.
- ✓ La crise a entraîné l’accélération de la transformation numérique. Fourniture rapide en ordinateurs portables supplémentaires, appareils mobiles, accès à distance… Avec un niveau de sécurité pas toujours approprié sur ces terminaux.
- ✓ **Impact de la crise**: Nouveau parc d’ordinateurs portables, augmentation des licences VPN, extension de l’usage des outils de collaboration, développement des processus et acquisition de solutions de cybersécurité pour l’entreprise. Les utilisateurs ont dû recourir à des services cloud plus vite que prévu.

**Quels risques résiduels ?**
Les nouveaux ordinateurs portables seront-ils conformes aux politiques de sécurité au moment du retour en entreprise ? Comment faire le tri et sécuriser les données à cheval entre le stockage cloud et le stockage traditionnel ? Comment former rapidement les utilisateurs à sécuriser leurs nouvelles pratiques ?

CESIN

# L’entreprise peu avancée


01

- ✓ Pas d’outils de collaboration en place. Bien que possible par rapport à l’activité de l’entreprise, le télétravail n’est pas dans la culture et rien n’est en place pour le déployer. Pas ou peu d’usage du Cloud

02

- ✓ **Impact de la crise**: déménagement de postes fixes à la maison, utilisation de postes privés, voire de stockages privés, déploiement accéléré du télétravail et des VPN

03

- ✓ Les utilisateurs ont du transférer leurs données d’un hébergement sur site vers un cloud. Ils ont dû apprendre très vite à gérer l’accès à leurs nouveaux espaces partagés.

**Quels sont les risques résiduels ?**
Utilisateurs non préparés aux nouveaux usages. Dispersion/exposition massive des données d’entreprise.
Comment assurer le retour à la normale ? Reconstituer les données et sécuriser les partages. Comment réorienter le programme cyber à l’avenir ?

CESIN

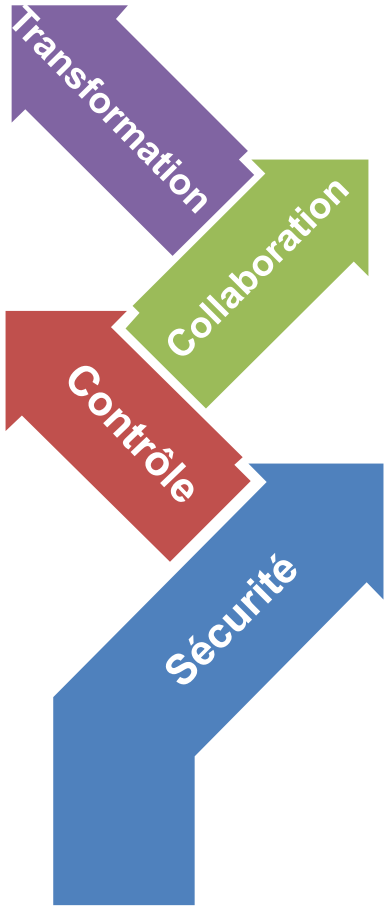
# Conclusions

## FORTE MODIFICATION DE L'ORGANISATION

- Le télétravail peut devenir une nouvelle norme de travail (économie d'espace et du coût des locaux) : le curseur a bougé
- La mobilité avant tout
- L'indépendance au lieu de connexion
- Attention aux accès des comptes à privilèges

## COMMENT CONTROLER SES DONNEES DANS CETTE NOUVELLE CONFIGURATION ?

- Contrôler la création et le partage de nouvelles données dans un contexte de travail à distance sur un environnement cloud :
  gérer la délégation / responsabiliser les utilisateurs




## LES SOLUTIONS COLLABORATIVES CLOUD VONT DEVENIR LA NORME

- Comment s'assurer de la protection des données ?
- Avec quel niveau d'authentification ?
- Avec quelle vision consolidée sur son patrimoine ?

## LA CYBERSECURITE POUR TOUS

- Il faut garder le contrôle sur la sécurité du terminal mobile connecté au cloud : gestion des patchs, détection des menaces, etc.
- Il faut fournir aux utilisateurs une vue consolidée sur leurs applications et leurs partages de données

CESIN

# Conséquences

Du point de vue de la sécurité, le curseur a indéniablement bougé et de façon pérenne. Que peut-on prédire ?

- Le PC fixe est mort
- Le VPN traditionnel va disparaitre
- Le MFA n'est plus une option
- Le principe du zero trust est plus que jamais d'actualité
- La mise à jour des postes devra être repensée
- Adieu aux répertoires bureautiques !
- Le SOC est incontournable

# Recommandations

## Facteur technologique

- Si ça n'est pas déjà engagé, préparez votre entreprise à une approche Zéro Trust Architecture (ZTA). Renforcer l'authentification
- Protégez vos utilisateurs : Advanced Malware Analysis, Browser Isolation, CASB …
- Installez une solution d'authentification des emails (DMARC), pour détecter les cas d'usurpation d'identité de l'expéditeur et pour protéger votre marque de l'usurpation
- Renforcer les capacités de supervision des données et de leur partage et donc exposition
- Renforcer la surveillance et la détection par les SOC sur les environnements cloud.
- Surveiller particulièrement les connexions des utilisateurs à privilèges.
- Veiller à la conformité du parc : finir de chiffrer tous les terminaux. Rendre le patching direct et plus automatique (marche forcée). Généraliser les EDR.

## Facteur humain

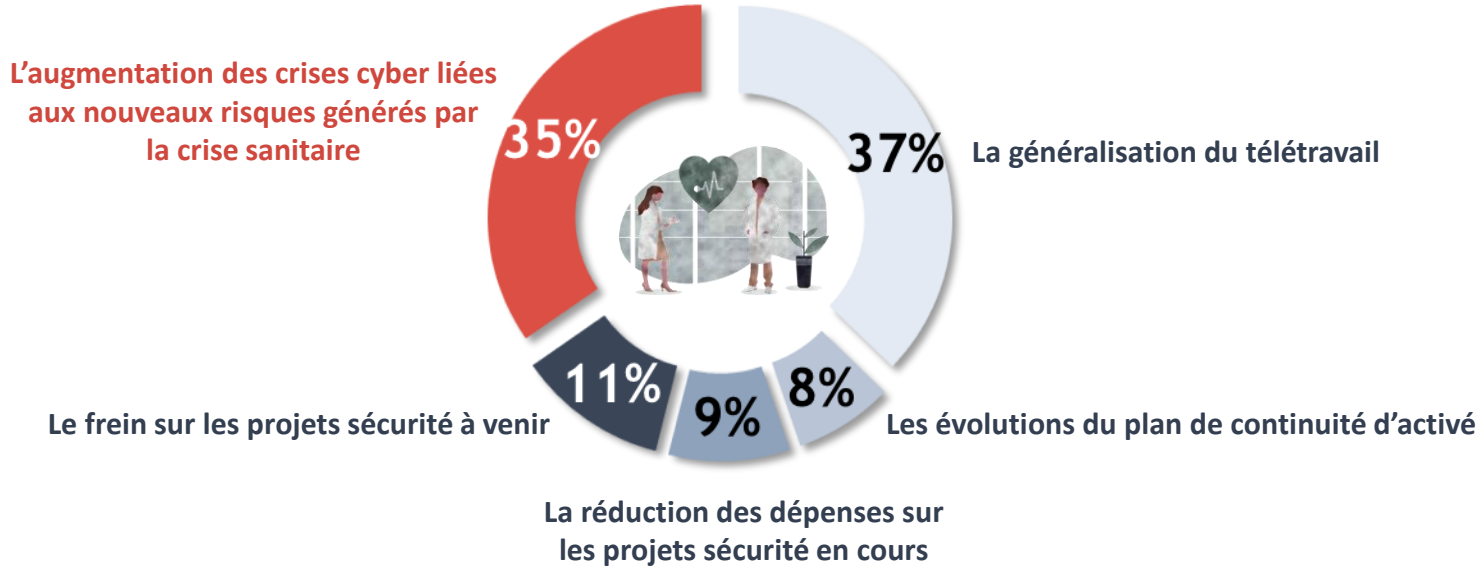
- Aider les utilisateurs à identifier les données sensibles et les protéger.
- Former l'utilisateur à son nouveau rôle « délégué » pour la protection des données.
- Restituer à l'utilisateur une vue sur ses données. L'aider à maîtriser ses partages (où sont les données ? avec qui est-ce que je les partage ? avec quels droits ? qui y a accédé ?).
- Développer des nouvelles chartes de travail à distance. Renforcer les règles de séparation pro/perso.
- Mais ne pas compter uniquement sur la vigilance de l'utilisateur. Si le clic de trop déclenche une crise, c'est que l'environnement était vulnérable.

CESIN

# Quelques éléments du Baromètre CESIN 2020 relatifs à la crise sanitaire (janvier 2021)

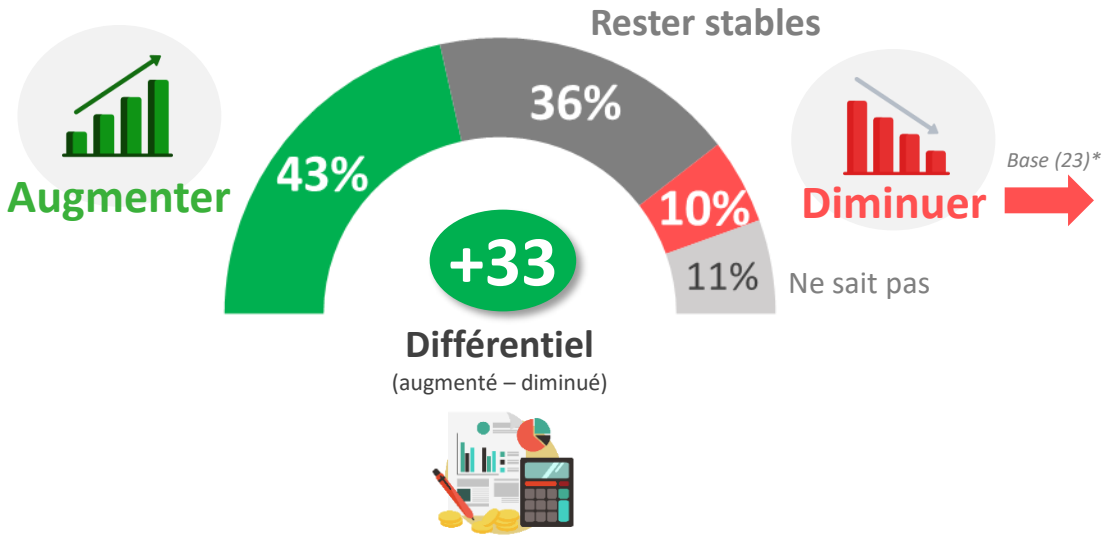
# Le télétravail et l'augmentation des crises cyber sont les changements les plus impactants pour les entreprises pendant la crise sanitaire

Q1. Avec la crise sanitaire en cours, quel phénomène impacte le plus l'activité de cybersécurité de votre entreprise ?
*Base : ensemble (228)*



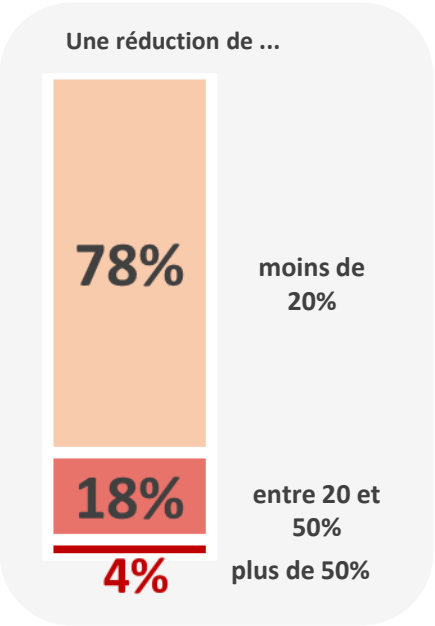
# Poussant 2 entreprises sur 5 à augmenter les budgets cybersécurité pour 2021

Q2. En 2021, les budgets cybersécurité de votre entreprise vont-ils… ?
*Base : ensemble (228)*




*Base (23)**

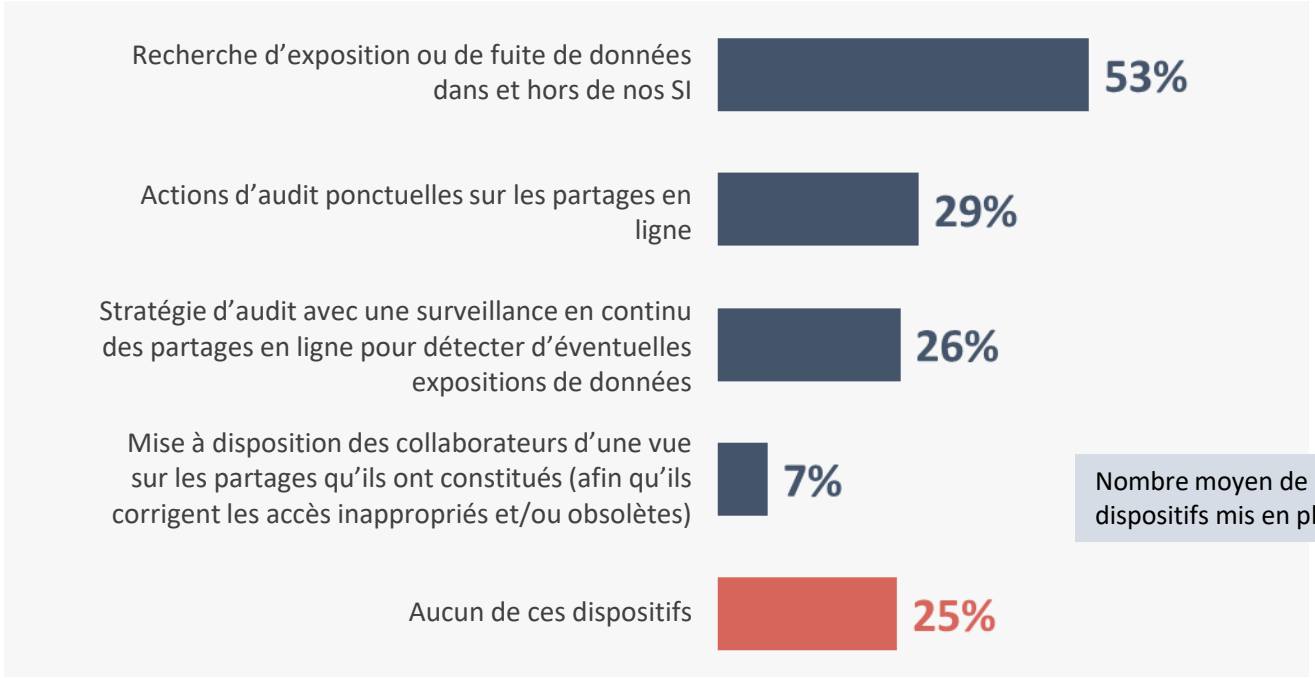
Q2bis. De combien devraient diminuer les budgets cybersécurité en 2021 ?



# 1 entreprise sur 2 a mis en place une recherche dans et hors des SI pour se prémunir de l'exposition ou de fuites de données

Q3. Votre entreprise a-t-elle mis en place les dispositifs suivants pour détecter l'exposition des données en ligne et/ou les fuites de données avérées ?

*Base : ensemble (228)*



# Cycle Sécurité
# Quelles leçons tirer de la crise sanitaire et de la professionnalisation des cyber attaques ?
# 9 MARS 2021

Une session animée par
Jean-Jacques CAMPS, pilote du Cycle Sécurité


CLUB UTILISATEURS
DE SOLUTIONS ORACLE

# Les prochains webinars

| | |
|---|---|
| Cycle Tech \| J.D. Edwards<br>Move to Oracle Cloud Infrastructure | 9 mars \| 11:00 |
| Automatisation \| RPA | 11 mars \| 9:00 |
| J.D. Edwards \| Blue Green Deployment | 16 mars \| 10:00 |
| Migrating & Managing Customizations for Oracle E-Business Suite 12.2 | 16 mars \| 14:30 |
| Communauté HCM | 18 mars \| 17:00 |
| Cycle IA \| Saison 2 - Session 1 : Deep Learning | 25 mars \| 11:00 |
| Déploiement core model J.D. Edwards<br>Retour d'expérience CEVA, gagnant du Trophée Industrialisation | 30 mars \| 11:00 |



Pour s'inscrire : https://clubutilisateursoracle.org/evenements/

# Les Replays pour nos adhérents

- Gestion du risque et ségrégation des tâches dans J.D. Edwards — 12 janvier
- Communauté Finance Cloud
  Tour d'horizon des fonctionnalités 2020 ERP Cloud — 15 janvier
- Communauté Eloqua
  Lancement | Retour d'expérience ALD Automotive — 2 février
- De l'importance de la conduite du changement lors des migrations Cloud
  Les apports de la conduite du changement lors des migrations Cloud — 5 février
- J.D. Edwards | Cycle fonctionnel – Les achats — 11 février
- Communauté NetSuite — 11 février
  Focus sur les principales fonctionnalités de la dernière release & prospective sur la prochaine

https://clubutilisateursoracle.org/evenements/

# Pour nous rejoindre
# Pour nous suivre

@clubutilisateursoracle

@ClubUtilisateursOracle

@ClubAUFO

https://clubutilisateursoracle.org/

Délégation Générale des Clubs Utilisateurs Oracle

delegation@clubutilisateursoracle.org

Patricia Azzaro | Sabine Grosdidier | Laurine Guillaume

CLUB UTILISATEURS
DE SOLUTIONS ORACLE