CCI PARIS ILE-DE-FRANCE

›lesdigiteurs

Mouvement des Entreprises de France
MEDEF Ile-de-France

Webinaire - Cybersécurité : Comment limiter les risques pour les PME face au COVID-19 ?

JEUDI 15 OCTOBRE 2020 DE 10H A 11H

Comment limiter les risques pour les PME face au Covid-19?

Animé par **Maxime Garreta**, Coordinateur DAS Numérique CCI Paris IDF

>lesdigiteurs | l'offre digitale de la CCI PARIS ILE-DE-FRANCE

Pierre-Arnaud Moreau
Chef de projet CCI Paris IDF

CCI PARIS ILE-DE-FRANCE

Aymeric Harmand
Vice-President, Développement de produits et Innovation

mastercard

Gilles Souris
Conseiller Numérique CCI 93

CCI PARIS ILE-DE-FRANCE

Jimmy Odouha
Chef de produits Devices et Security services

orange

01.

Cybersécurité en entreprise: constat, cyber résilience et acculturation des dirigeants

Pérenniser l'entreprise face au risque cyber

De la cybersécurité à la cyberrésilience

CHAMBRE DE COMMERCE ET D'INDUSTRIE
1er ACCÉLÉRATEUR DES ENTREPRISES

CCI PARIS ILE-DE-FRANCE

LES CYBERATTAQUES EN 3 CHIFFRES

60% des PME qui subissent une cyberattaque déposent le bilan

1 cyberattaque a lieu toutes les **39** secondes dans le monde

99% des cyberattaques profitent de failles humaines

Les répercussions financières peuvent courir sur des mois, voire des années

LA CYBERSÉCURITÉ, C'EST BIEN

Préservation des systèmes d'information

LA CYBERRÉSILIENCE, C'EST MIEUX

Pérennité des ressources et de l'activité de l'entreprise

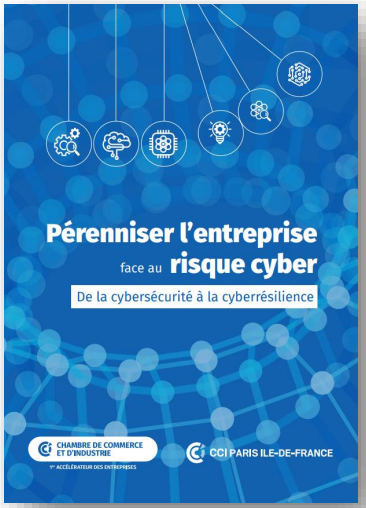
MEILLEURE EST LA PRÉPARATION, MOINDRE EST LE CHOC

Configuration et mises à jour sont les premiers **cybergestes barrières**

Formation et **acculturation** des collaborateurs peuvent **endiguer** une cyberattaque

Agilité et **réactivité** de l'organisation permettent le **rebond**

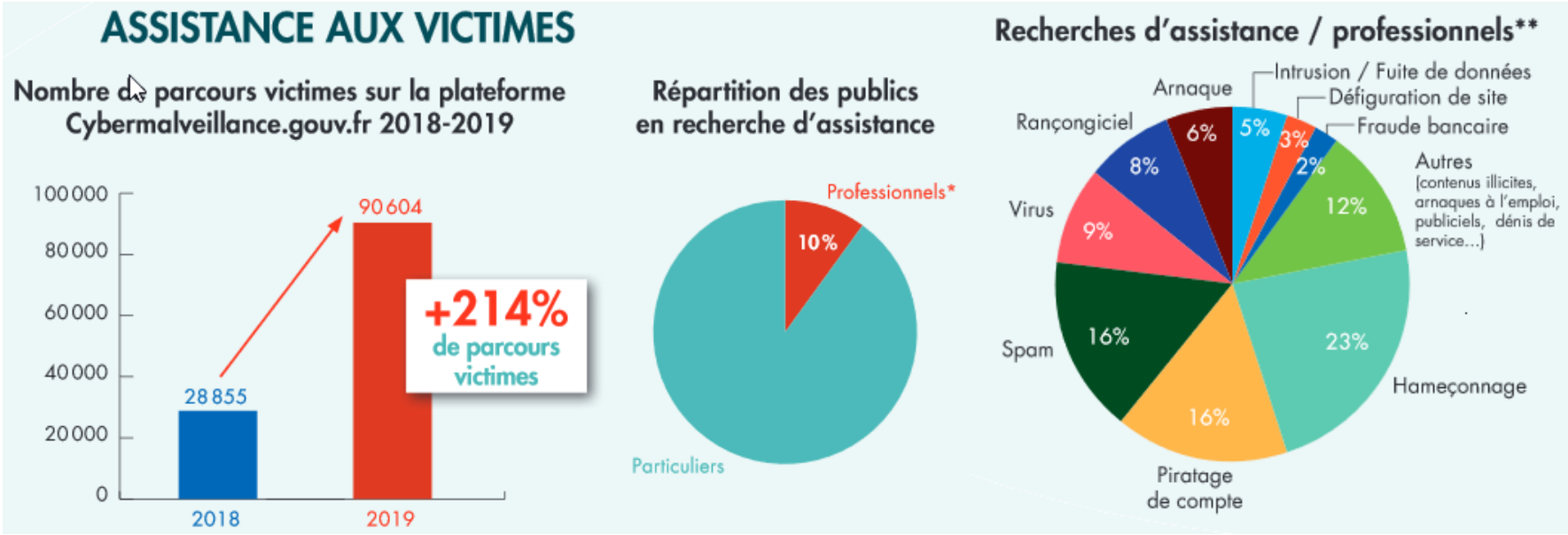
SENSIBILISATION DES DIRIGEANTS, FORMATION ET ACCULTURATION DES COLLABORATEURS



02.

Cybermalveillance: évolution du panorama et retours d'expérience

Infographie ANSSI 2019*



400 % d'augmentation entre mars et juin 2020 ...

*** Infographie liée au rapport d'activité de l'ANSSI pour l'année 2019***

En 2019 spam et hameçonnage = 49 % des signalements

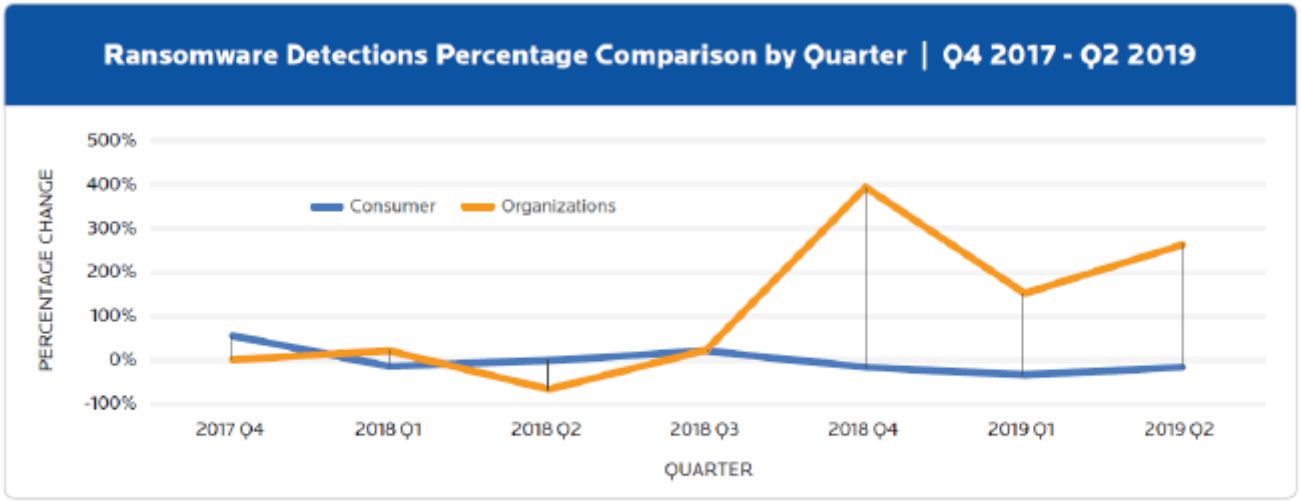


Fig. 3.2 : Comparatif de l'évolution du nombre d'attaques par rançongiciels impactant les particuliers et les entreprises. Source : MalwareBytes

Source : « ÉTAT DE LA MENACE RANÇONGICIEL » - https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-001/

Première source de faille(s) :
Nos comportements

Premier rempart de sécurité :
Nos comportements

Suivi d'échanges de mails...

Exemple d'attaque ciblée

Résumé d'un cas réel :

- Introduction du pirate dans le système de messagerie du client ou du fournisseur.
- Collecte d'informations.
- Élément déclencheur.
- Envoi d'un mail « frauduleux » adressé au bon moment ou bon endroit à la bonne personne.

Bilan : 50 000€ de pertes nettes, conflit entre ce client et son fournisseur (impact difficile à évaluer sur la durée), complexité d'un recours en justice car client et fournisseur résident dans des pays différents.

03.

Mastercard & la cybersécurité: analyse des points de vulnérabilité des PME

Mastercard et la cyber sécurité

Notre Approche

PREVENT

Sécuriser les actifs de nos partenaires en utilisant les technologies les plus récentes

IDENTIFY

Eliminer les mots de passe et créer des Identités Digitales

DETECT

Détecter les comportements frauduleux et les attaques

EXPERIENCE

Concevoir des experiences et des parcours client sûrs

Des acquisitions récentes

Brighterion mastercard

NU Data Security mastercard

riskrecon mastercard

Press Releases

Mastercard announces its first European Cyber Resilience Centre

Mastercard's European Cyber Resilience Centre will bring together partners and industry bodies to lead the way to enterprise resiliency

Waterloo, Belgium – 17 February, 2020 – Mastercard today announced it is developing its first European Cyber Resilience Centre, a state-of-the-art cyber and security centre in Europe that will drive collaboration between both public and private sectors, as well as regulatory bodies to further support enterprise resilience in the region.

Located in Waterloo, Belgium at Mastercard's European Headquarters, the centre is the first of its kind that the company has invested in outside of North America. The new centre highlights Mastercard's ongoing commitment to addressing threats faced by the European payments ecosystem, including financial institutions and fintechs. The facility will serve as a single cybersecurity hub for the region, bringing together a diverse pool of talent from across Mastercard's global community.

Protéger les TPE / PME avec RiskRecon

Les TPE / PME sont ciblées par les hackers

Les **risques** encourus

- Interruption (temporaire) des activités
- Détérioration de la confiance des clients
- Acquittement d'amendes

3 **faiblesses** récurrentes

- Correctifs logiciels
- Sécurité e-mails
- Encryption web

riskrecon
mastercard

Pour souscrire: www.riskrecon.com

RiskRecon évalue en continue vos vulnérabilités et vous fournit les solutions pour y remédier

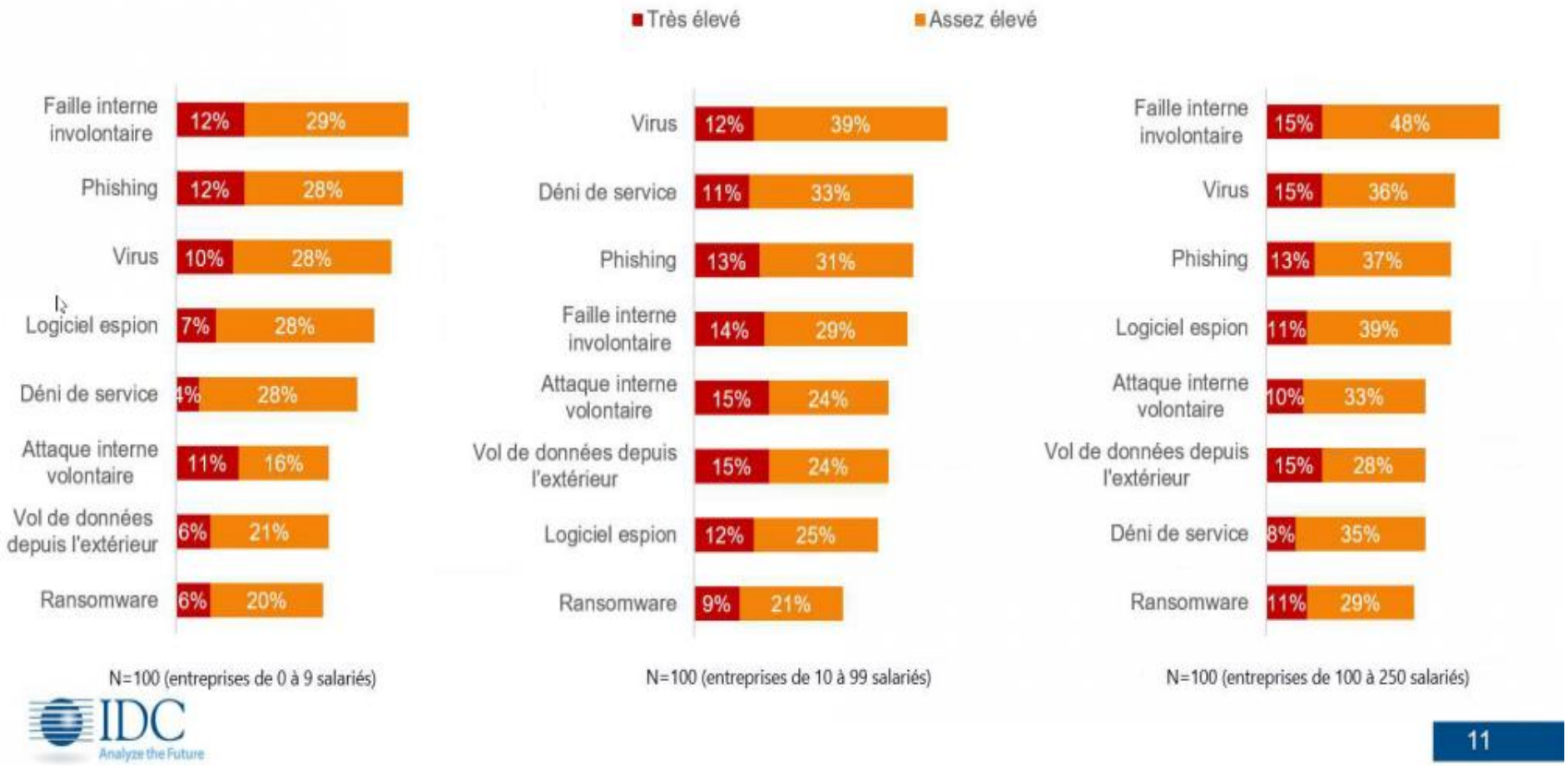
04.

Les données sont la recherche de votre business: protégez-les!

Quelle est votre perception du risque d'exposition aux menaces (étude IDC) ?

Selon vous, quel est le risque que votre entreprise soit exposée aux menaces informatiques suivantes ?

Etude IDC – Enquête sur la Cyber-sécurité – 13 octobre 2020



11

Les bonnes pratiques / les bons réflexes

1. Sensibilisez vos salariés (> maillon fort).

2. Force du mot de passe (mdp). 1 mdp / compte. Changement à fréquence régulière.

3. Hygiène numérique : ne cliquez pas sur les liens « douteux » (hameçonnage).

4. Protégez vos ordinateurs, tablettes et smartphones. Mettre à jour vos antivirus, systèmes d'exploitation et applications.

5. En télétravail : Clé WiFi robuste et WiFi invités. Accès distants à l'Intranet de l'entreprise via VPN.

6. En déplacement : filtre de confidentialité. Ne pas se connecter à n'importe quel hotspot WiFi.

7. Sauvegardez / archivez régulièrement vos données (localement, serveur, cloud).

8. Mettre en place des droits d'accès aux dossiers sauvegardés.

9. Disposez d'un référent pour les questions relatives à la cyber-sécurité (prise en charge des sujets)

Les outils pour se protéger

1. Sauvegarde
   Assurer la poursuite de l'activité en cas de problème

2. Archivage
   Disposer de la trace de vos données dans le temps

3. Antivirus
   Se protéger des virus, pages malveillantes, applications malicieuses…

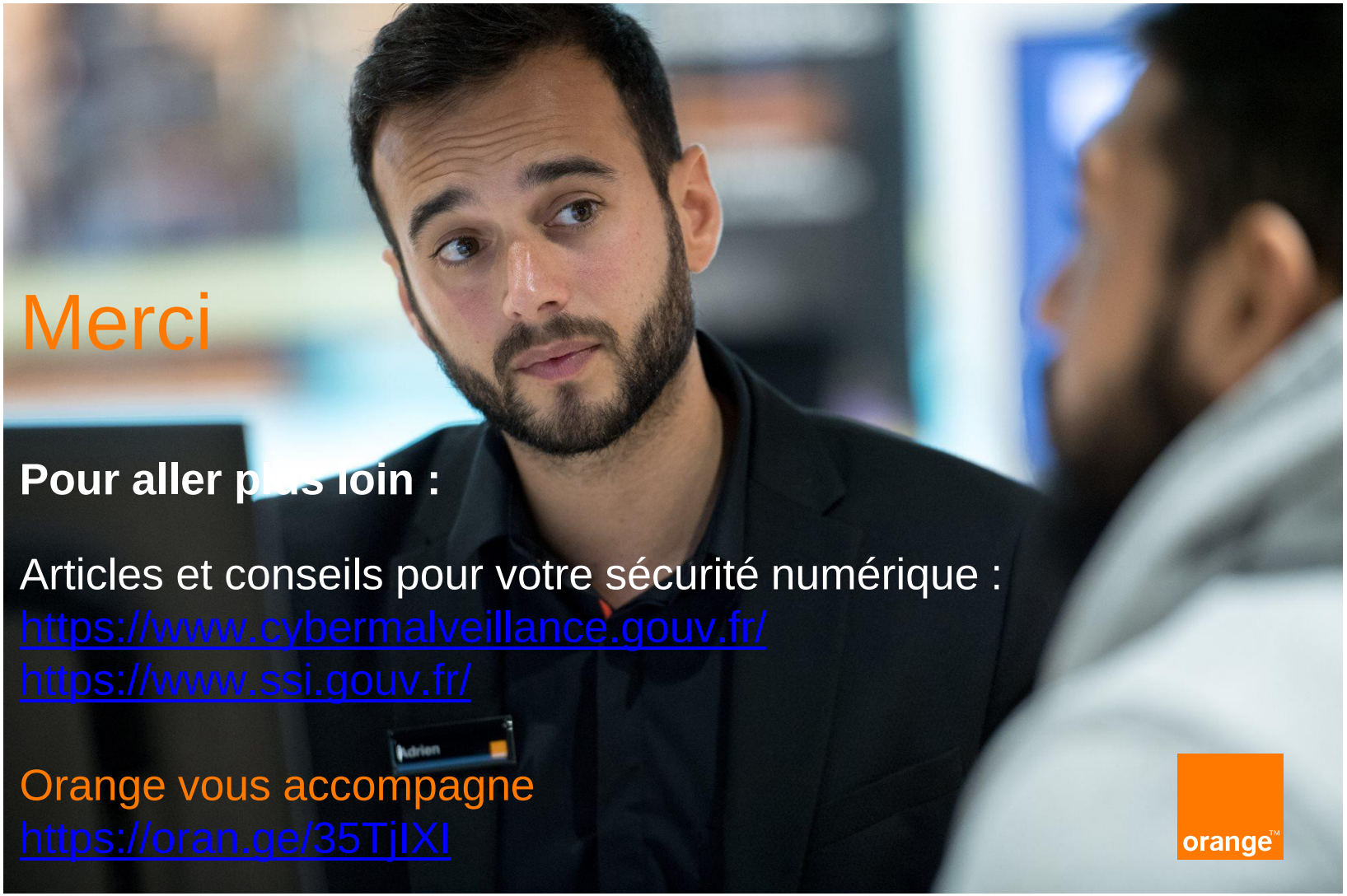
4. Pare-feu
   Se protéger des intrusions

5. Device Management
   Piloter à distance la politique de sécurité de vos équipements

6. Audit de sécurité
   Identifier les faiblesses de mon IT (tous équipements compris)

7. Prestation de conseil
   Me conseiller, me former, m'accompagner à l'amélioration de ma protection

8. Cyber-assurance
   Se prémunir contre la perte d'exploitation liée à la menace cyber



Merci

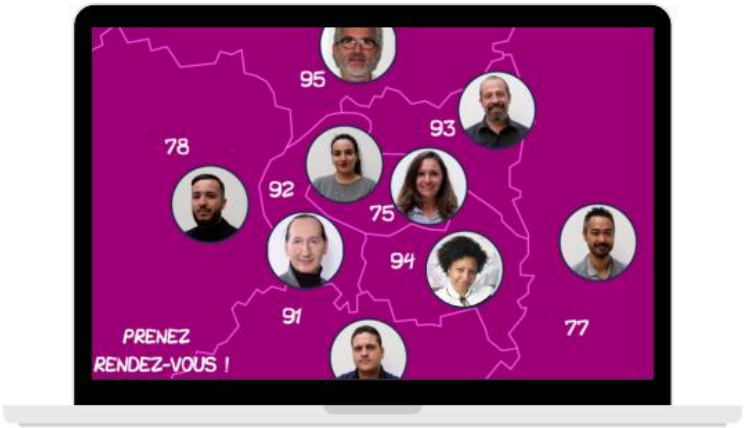
Pour aller plus loin :

Articles et conseils pour votre sécurité numérique :
https://www.cybermalveillance.gouv.fr/
https://www.ssi.gouv.fr/

Orange vous accompagne
https://oran.ge/35TjIXI

L’OFFRE DIGITALE DE LA CCI PARIS ILE-DE-FRANCE

10 Conseillers Numériques en IDF pour fournir des solutions concrètes aux besoins numériques de nos clients TPE/PME



- **S’INFORMER >** webinars, ateliers, business coffee
- **SE FAIRE ACCOMPAGNER >** diagnostic, coaching
- **SE FORMER >** programme de formation
- **PARTICIPER >** évènements numériques régionaux (Hackathon, Digiteurs Day)

CCI PARIS ILE-DE-FRANCE

Mouvement des Entreprises de France
MEDEF Ile-de-France

lesdigiteurs

Merci à tous pour votre participation
Questions/Réponses