certilience
EXPERTS EN SÉCURITÉ INFORMATIQUE

Apprendre aux utilisateurs à Ne Pas se faire pirater

CertiAware

Sommaire

- Statistiques sur les attaques
- Différents vecteurs d'attaque ciblant les utilisateurs
- Programme de sensibilisation Certiaware
- Démonstration de notre plateforme de E-learning
  - Vue niveau utilisateur
  - Vue niveau reporting
- Questions / Réponses

Statistiques sur les attaques

Qui est concerné

80 %

des entreprises sont victimes d'au moins une attaque par an (*)

Hameçonnage (phishing et spear phishing)

73 % des entreprises sont touchées

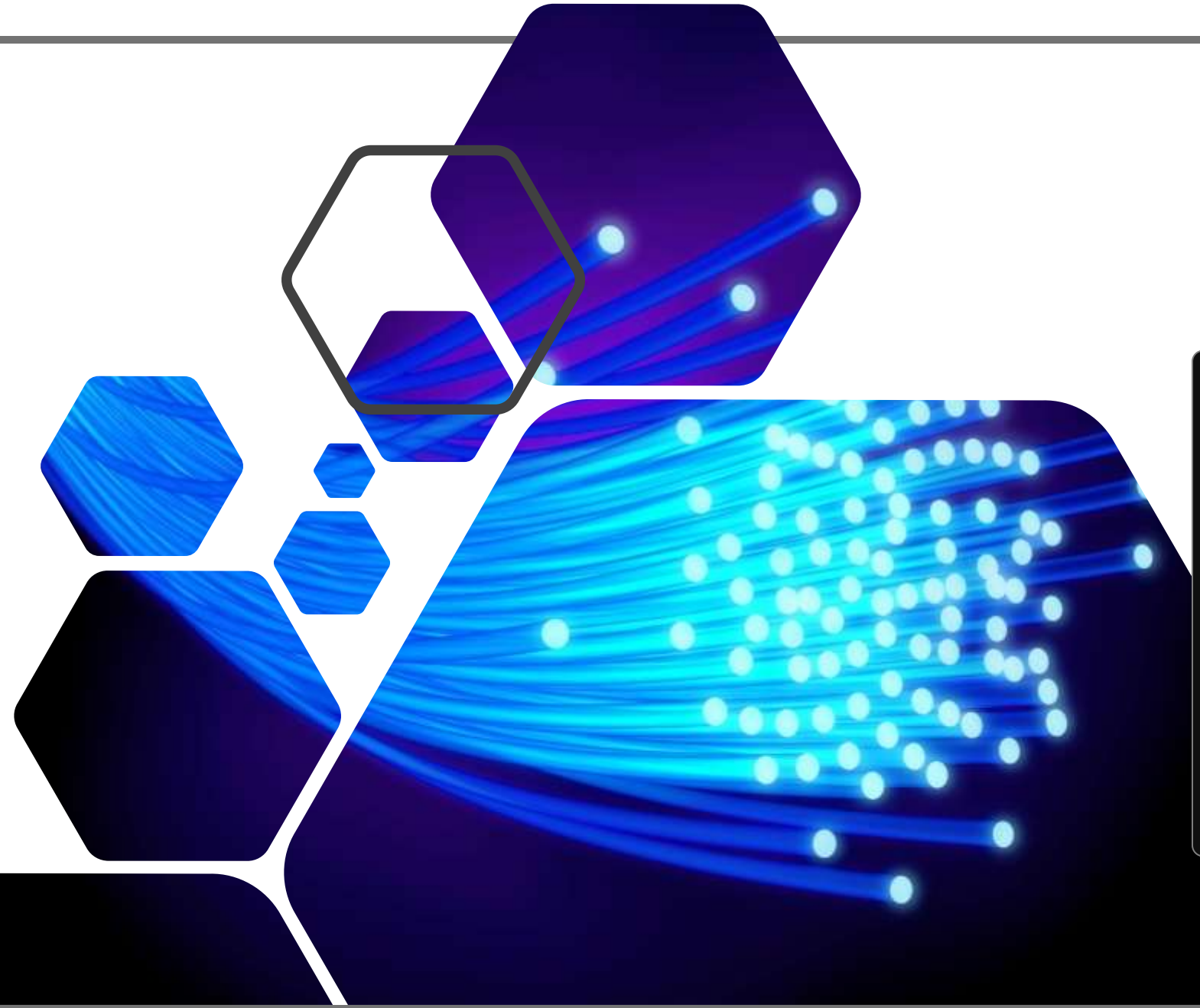
Ingénierie sociale et fraude au président (social engineering)

50 % des entreprises sont touchées

Logiciels malveillants (ransomware et malwares)

44 % des entreprises sont touchées

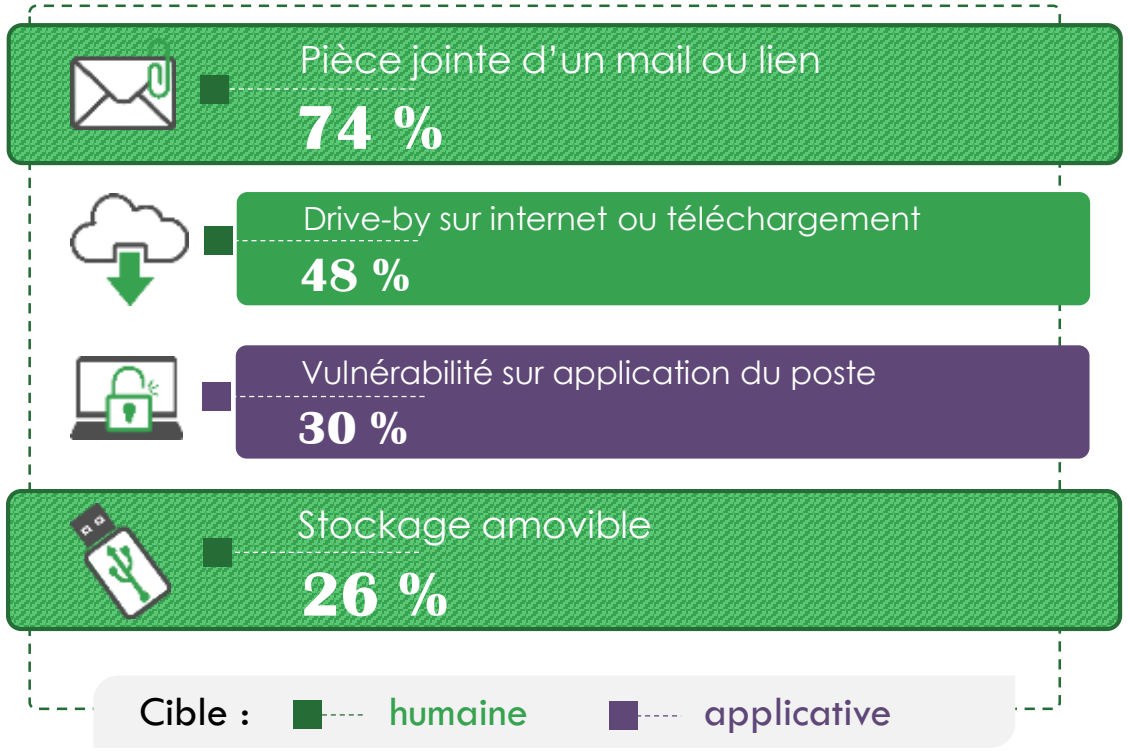
(*) « Baromètre de la cybersécurité des entreprises », Cesin - Opinion Way, janvier 2019



Vecteurs d'attaque ciblant les utilisateurs

L'utilisateur, maillon faible de la sécurité....

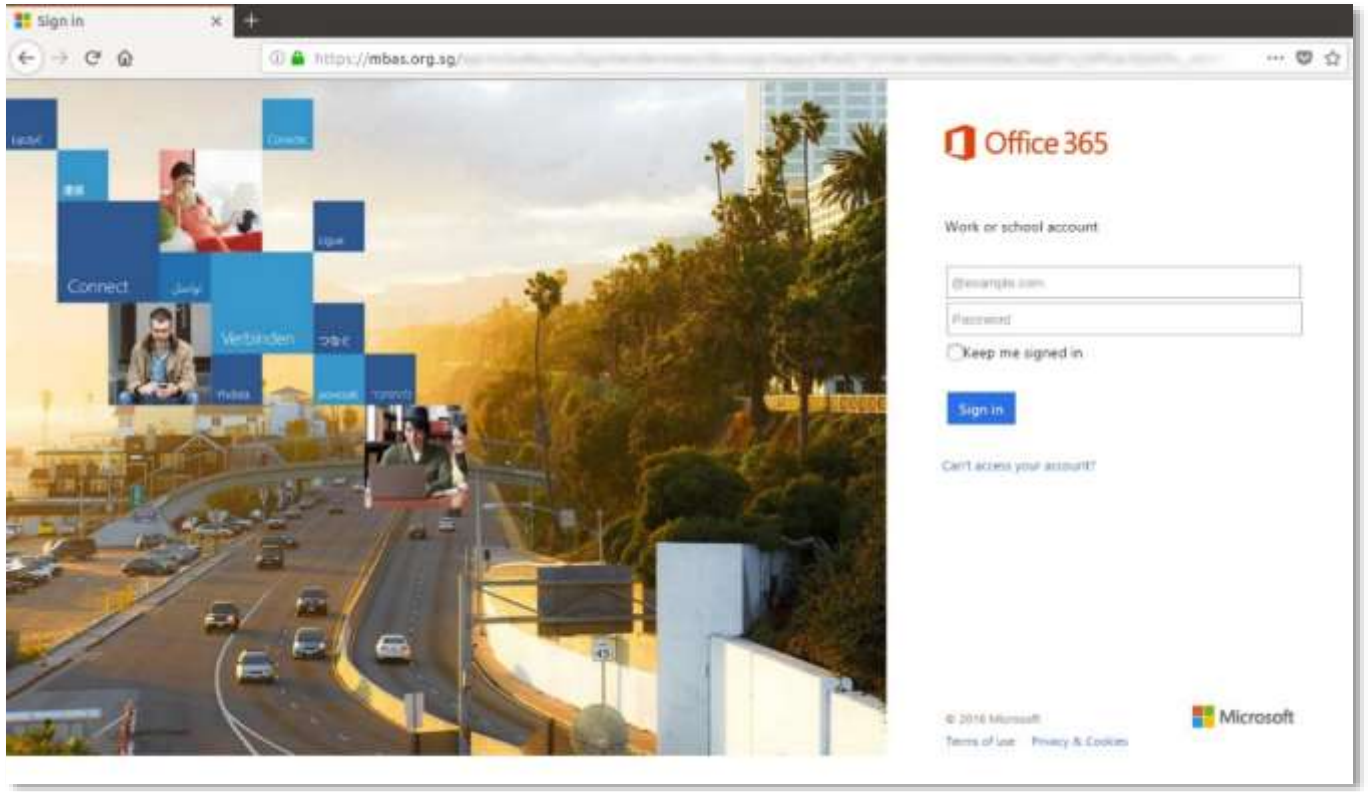
Vecteurs d'attaques les plus utilisés (**):



(**) enquête SANS Institute 2017 sur 263 entreprises

Exemple 1 : Usurpation de Microsoft Office365

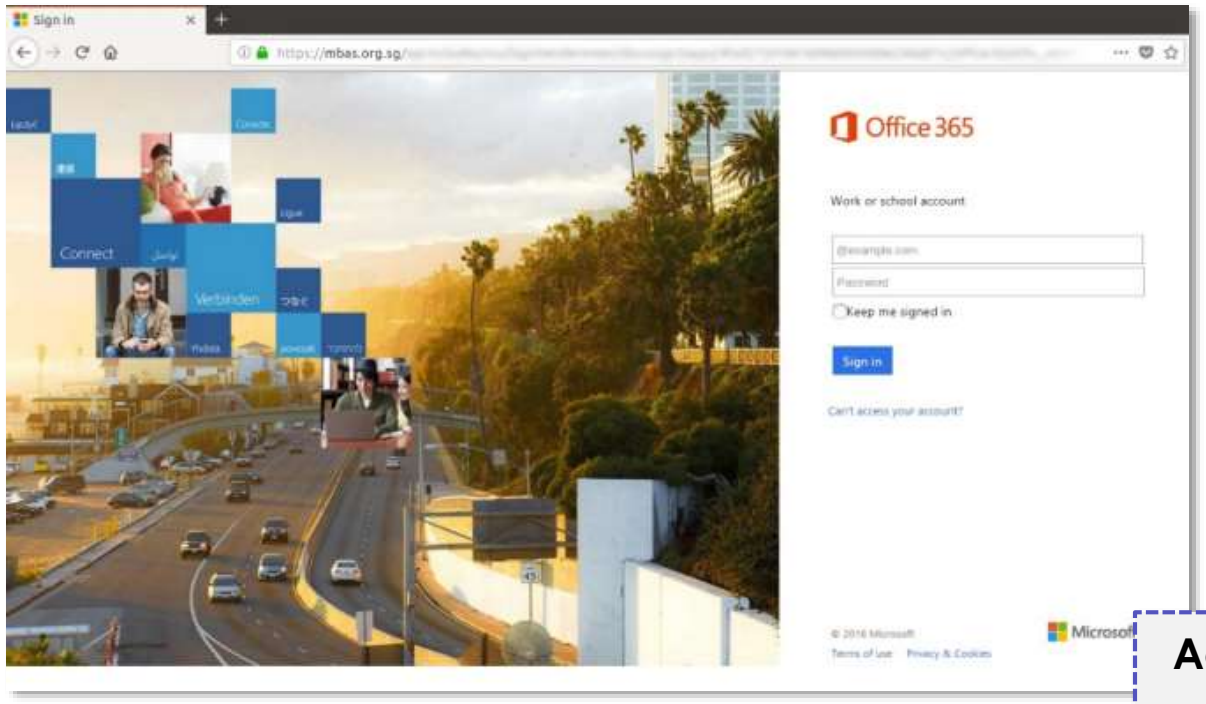
Exemple 1 : Usurpation de Microsoft Office365



UTILISATEUR

HACKER

Exemple 1 : Usurpation de Microsoft Office365



UTILISATEUR

Récupération des identifiants

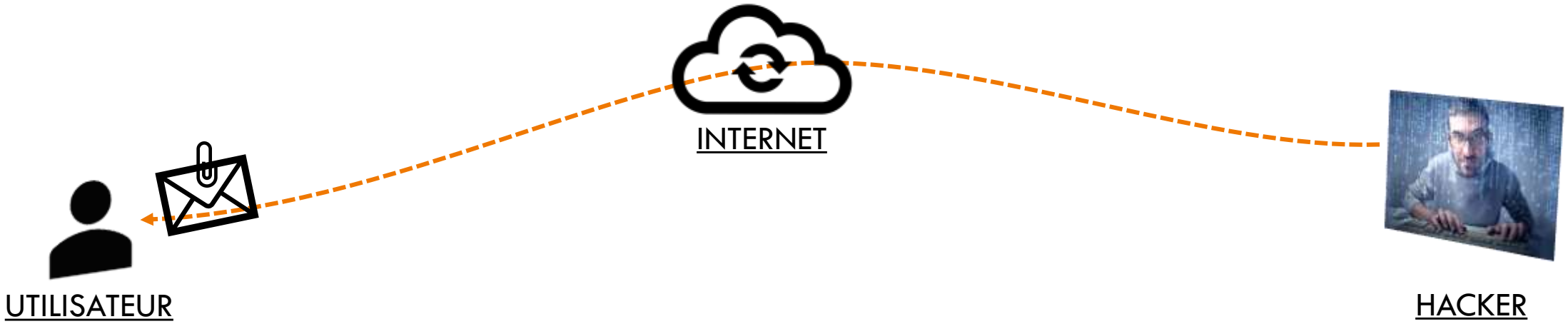
HACKER

Actions potentielles :

- Accès à la boite mail
- Utilisation de la boite mail pour du phishing interne
- Accès à tous les services de la suite Office365 :
  - Sharepoint
  - Onedrive
  - Skype/Teams
  - …

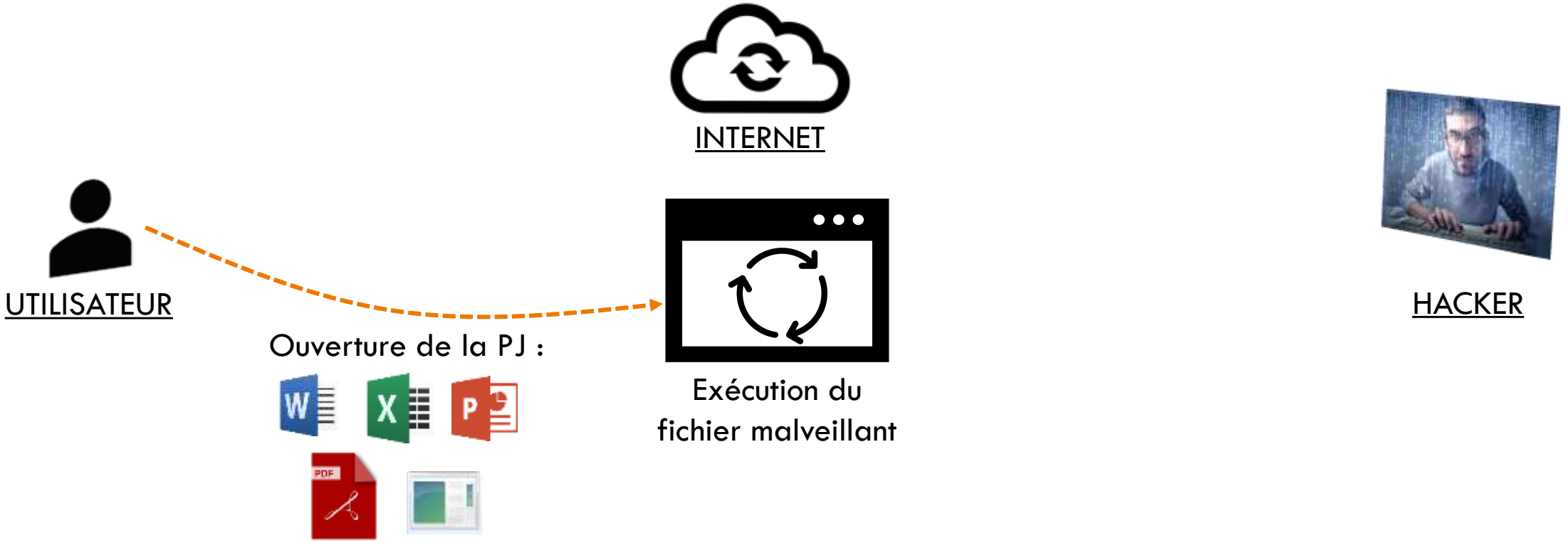
Exemple 2 : Réception d'un mail avec pièce jointe malveillante

Un lien dans le mail pourrait également permettre au hacker de télécharger un fichier malveillant



Exemple 2 : Réception d'un mail avec pièce jointe malveillante

Un lien dans le mail pourrait également permettre au hacker de télécharger un fichier malveillant



Exemple 2 : Réception d'un mail avec pièce jointe malveillante

Un lien dans le mail pourrait également permettre au hacker de télécharger un fichier malveillant

INTERNET

HACKER

UTILISATEUR

Ouverture de la PJ :

Exécution du fichier malveillant

Actions potentielles :

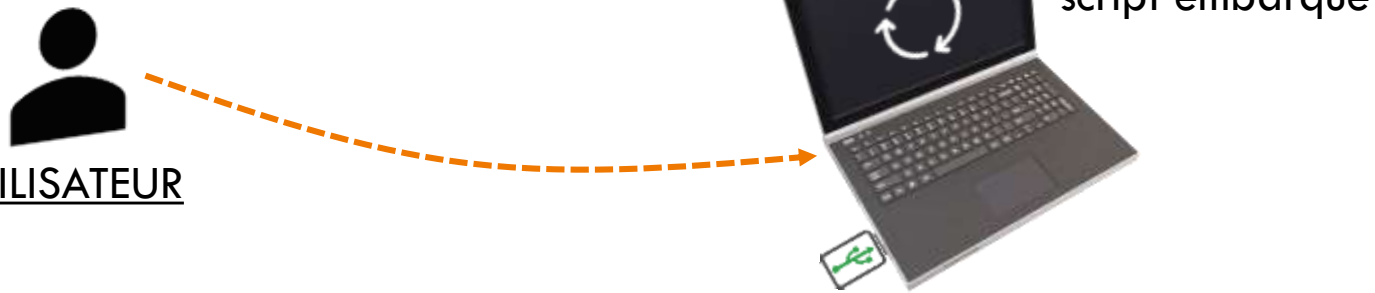
- Prise de contrôle du poste
- Chiffrement du poste et demande de rançon
- Infiltration sur votre réseau
- …

Exemple 3 : Connexion d'une clé USB trouvée

UTILISATEUR

HACKER

Exemple 3 : Connexion d'une clé USB trouvée



UTILISATEUR

Exécution du script embarqué

HACKER

Exemple 3 : Connexion d'une clé USB trouvée

UTILISATEUR

HACKER

Actions potentielles :

- Récupération d'informations du poste
- Prise de contrôle du poste
- Chiffrement du poste et demande de rançon
- Infiltration sur votre réseau
- …

L'utilisateur est aussi la meilleure protection de l'entreprise

Pour se protéger des cyberattaques,
il faut apprendre à les (re)connaitre !

Avoir une bonne hygiène informatique, c'est :
apprendre les bons réflexes, changer son regard sur l'informatique

certilience
EXPERTS EN SÉCURITÉ INFORMATIQUE

CertiAware

La sensibilisation des utilisateurs

Programme de sensibilisation Certiaware

Tests utilisateurs

- Phishing
- Clés USB

Formations sur site

- Stand
- Conférence

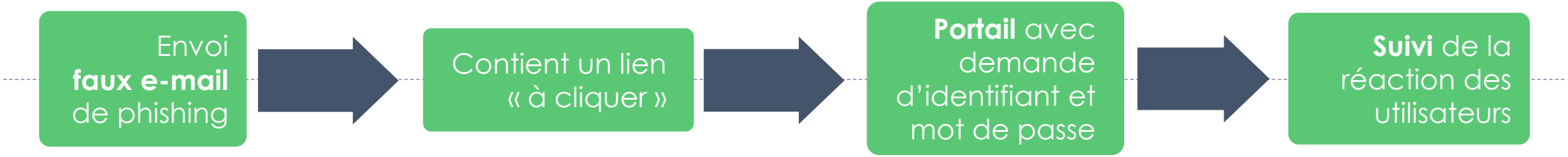
Formations en ligne

- Modules à lire / sonorisés
- Modules multi-lingues

Tests utilisateurs

- Phishing
- Clés USB

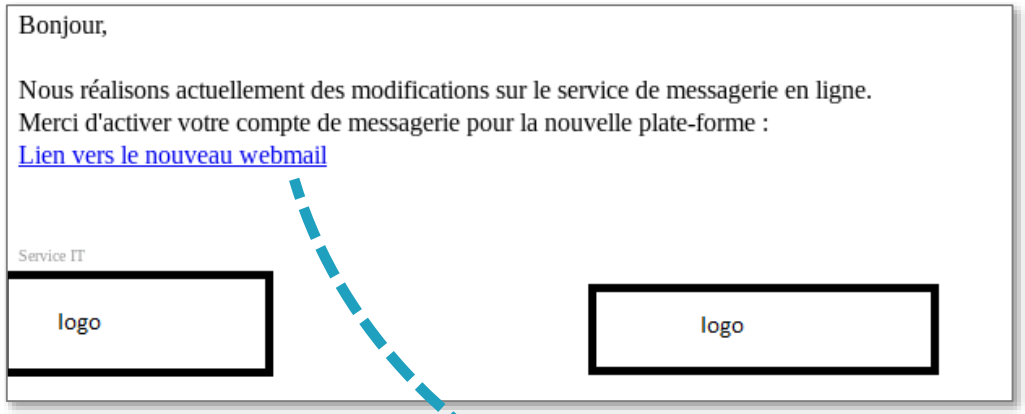
Fonctionnement des campagnes de phishing



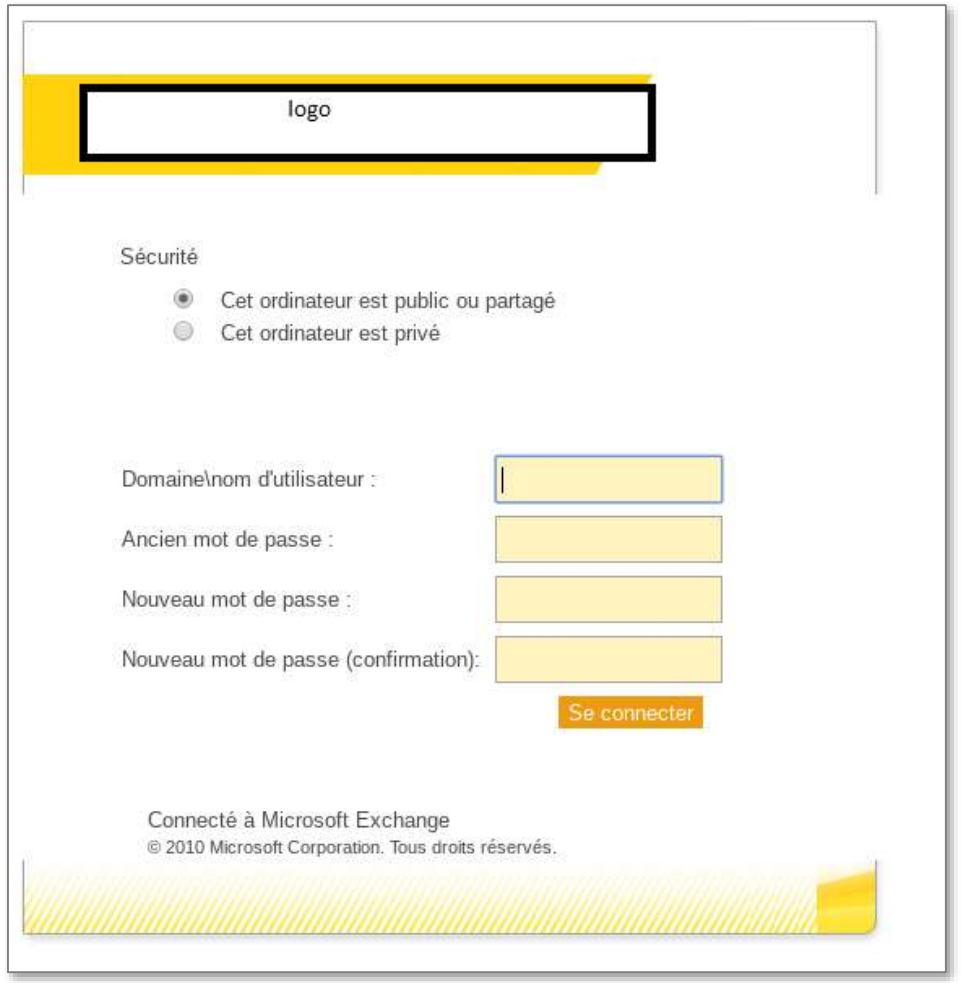
- Accès au choix de thème de phishing et suivi des campagnes sur le portail ***reporting.certilience.fr***
- Mail d'accroche personnalisable,
  portails de login standards ou personnalisables en fonction du thème

Exemple de campagnes de phishing

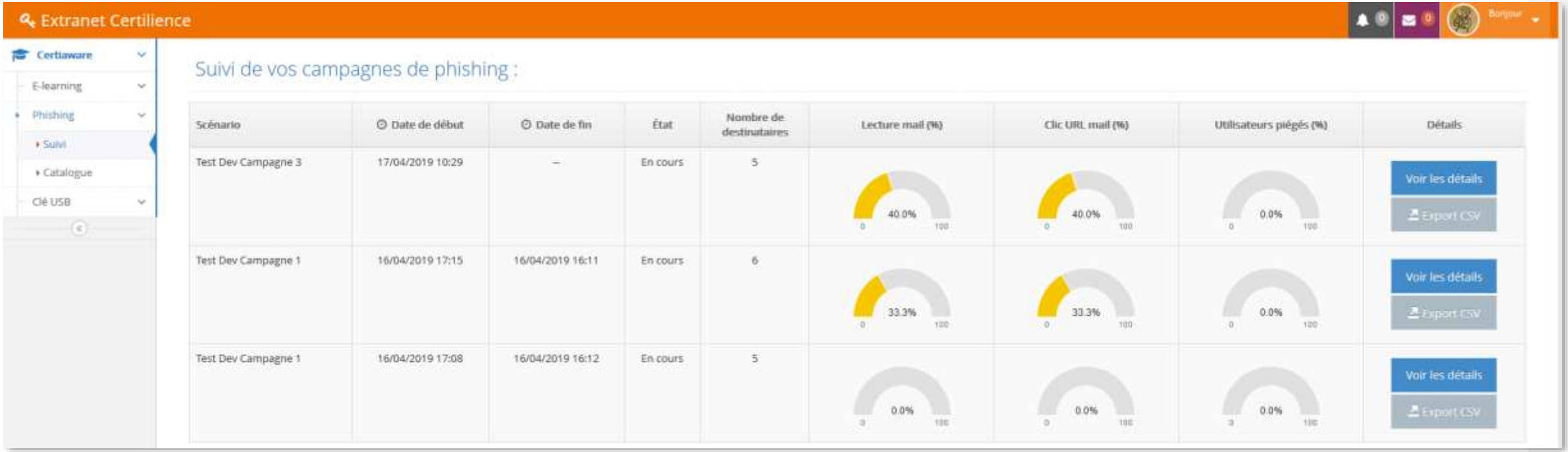
→ mail envoyé :



→ portail correspondant :

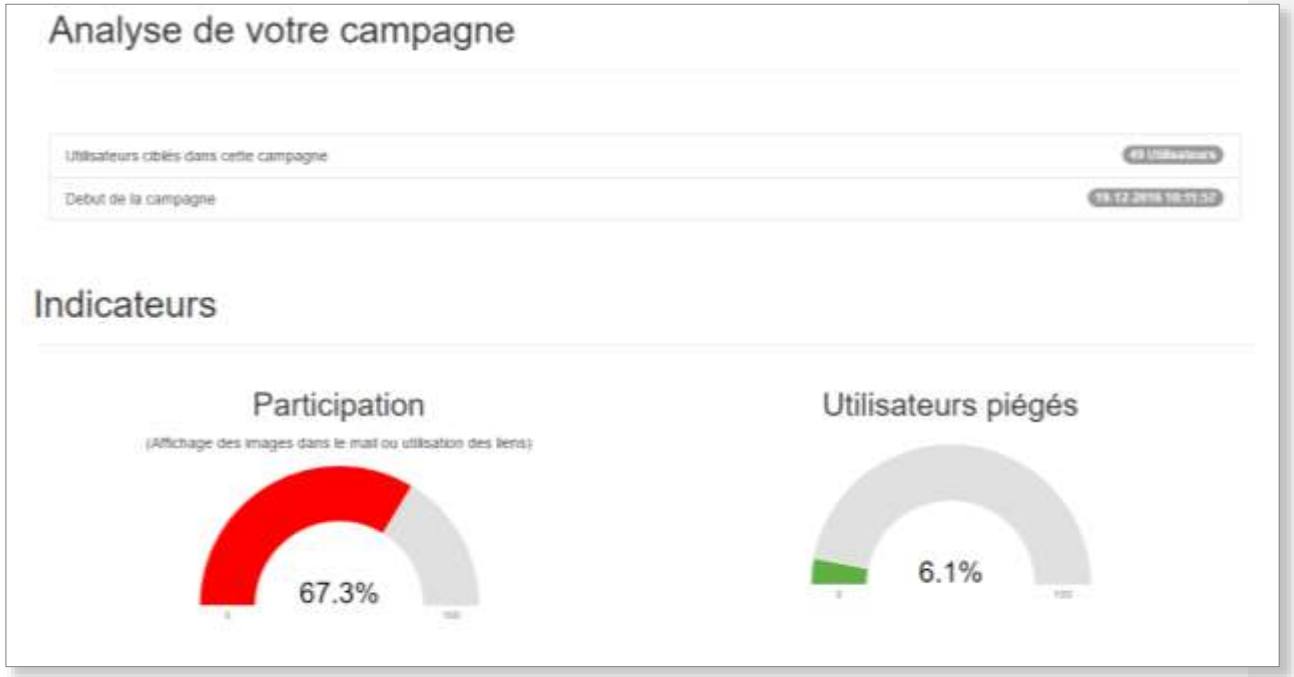


Suivi des campagnes de phishing



Résultats

- Suivi du comportement des collaborateurs grâce à différents indicateurs :
  - Utilisateurs dans la campagne
  - Utilisateurs piégés
  - Temps avant ouverture du premier mail
  - Temps avant « infection du poste » / récupération de l'identifiant + mot de passe
  - Historique des ouvertures des emails
  - Les systèmes utilisés
  - Les appareils mobiles utilisés
  - Les navigateurs et clients de messageries utilisés
  - Origine des visiteurs (IP)
  - Etc.



Ouverture du mail

Ouverture des emails (Affichage de l'image ou utilisation du lien) :	33 Utilisateurs
Version des clients de messageries utilisés	12 différentes
Client de messagerie mobile	7 (21.212121212121 %)
Système Android	1
Système Apple	6
Temps d'ouverture du premier mail (Affichage de l'image ou utilisation du lien)	16 Secondes
Système Linux (Hors Android)	-
Réseaux IP utilisés	8 différents

Ouverture du site

Ouverture du site	3 Utilisateurs
Version des clients utilisés	2 différentes
Ouverture du site depuis un mobile	(0 %)
Système Android	-
Système Apple	-
Système Linux (Hors Android)	-
Temps d'infection du patient 0	21.433333333333 Minutes
Réseaux IP utilisés	1 différents

Résultats

- Suivi du comportement des collaborateurs grâce à différents indicateurs

Détails

Contact	Groupe	Affichage de l'image	Client de messagerie	Utilisation du lien	Validation du formulaire	Navigateur	Date dernier clic sur le lien du mail	Date dernier affichage mail	Date d'envoi du formulaire
[redacted]	[redacted]	✉						16/12/2019 13:20:03	
[redacted]	[redacted]	✉						16/12/2019 09:04:51	
[redacted]	[redacted]	✉						16/12/2019 16:05:21	
[redacted]	[redacted]	✉		✔			16/12/2019 10:49:43	16/12/2019 10:49:13	
[redacted]	[redacted]	✉		✔			16/12/2019 08:50:36	16/12/2019 09:41:40	
[redacted]	[redacted]	✉						16/12/2019 10:58:48	
[redacted]	[redacted]	✉						16/12/2019 15:12:42	
[redacted]	[redacted]			✔	✔		16/12/2019 11:54:16		16/12/2019 11:54:44

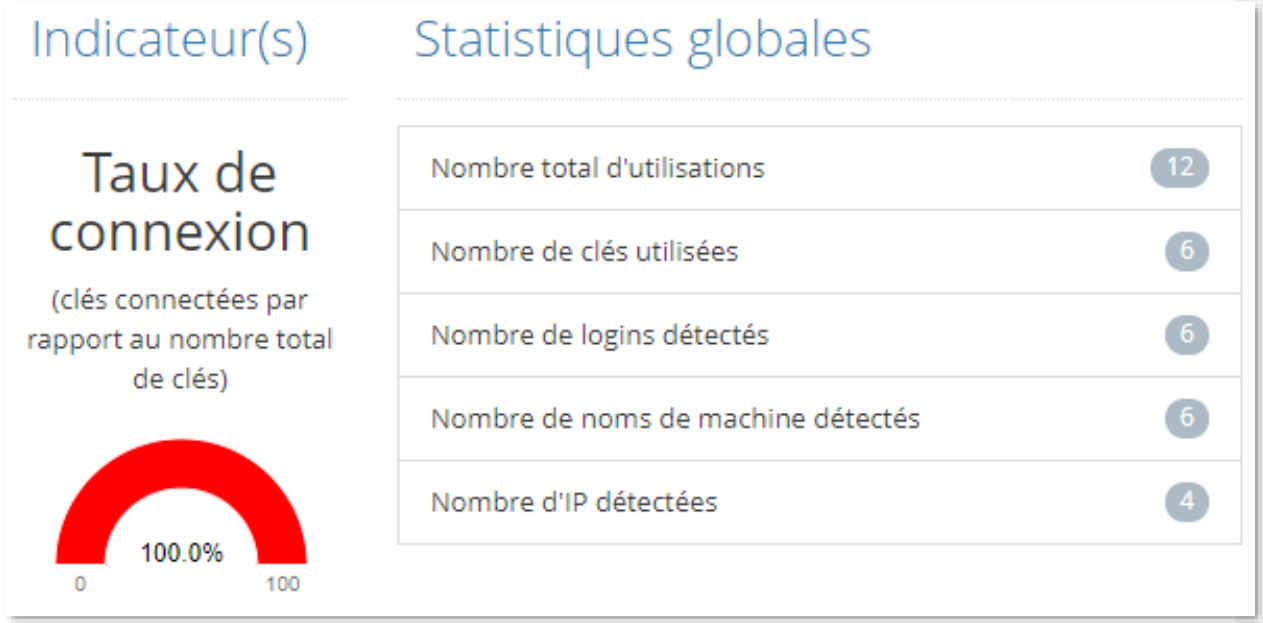
Fonctionnement des campagnes de clés USB

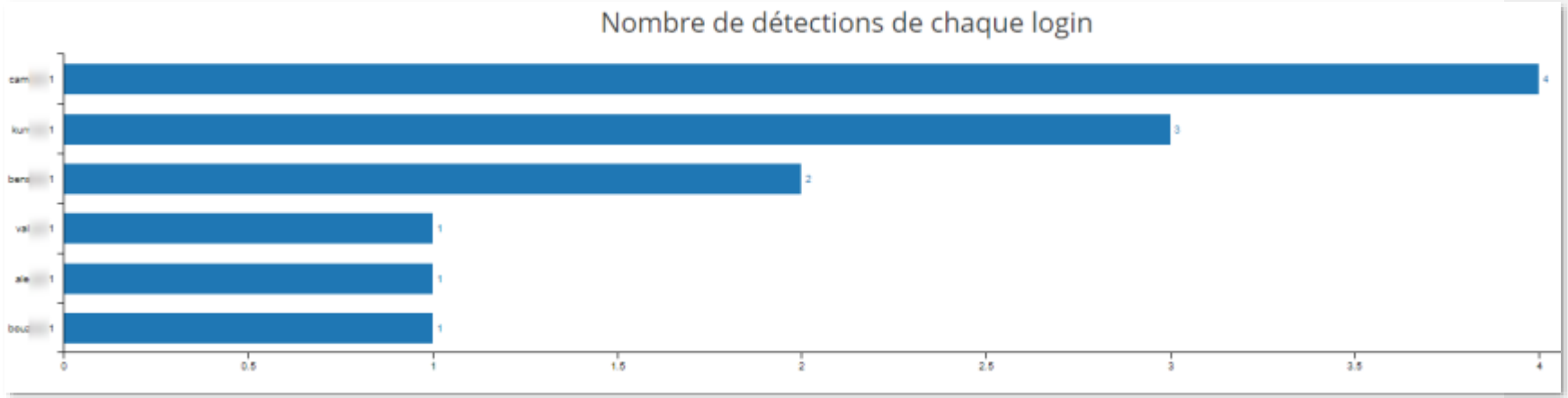
- 2 types de clés pour des pièges différents :
  - → Le piège s'exécute à la connexion de la clé
  - → Le piège s'exécute au clic de l'utilisateur
- Possibilité de personnalisation

Suivi des campagnes de clés USB

Résultats

- Suivi du comportement des collaborateurs grâce à différents indicateurs :
  - Nombre de clés de la campagne
  - Nombre d'utilisateurs
  - Nombre de clés utilisées
  - Taux de connexion
  - Nombre de logins / noms de machine / IP détectées
  - Détails des détections
  - Historique des détections des clés
  - Etc.





Résultats

- Suivi du comportement des collaborateurs grâce à différents indicateurs :
  - Nombre de clés de la campagne
  - Nombre d'utilisateurs
  - Nombre de clés utilisées
  - Taux de connexion
  - Nombre de logins / noms de machine / IP détectées
  - Détails des détections
  - Historique des détections des clés
  - Etc.

Détails des détections (par ordre chronologique)

Date	Clé (identifiant)	Login	Machine (nom)
11/09/2019 14:26:33	5	ca[illegible]1	S2[illegible]2
06/10/2019 18:03:43	1	ca[illegible]1	S2[illegible]2
06/10/2019 18:03:43	1	ca[illegible]1	S2[illegible]2
06/10/2019 18:03:43	1	ca[illegible]1	S2[illegible]2
14/10/2019 17:38:38	9	va[illegible]l	S6[illegible]2
29/10/2019 09:06:52	3	al[illegible]l	S5[illegible]2
22/11/2019 13:18:24	12	bo[illegible]1	S2[illegible]2
28/11/2019 10:15:57	12	be[illegible]1	S[illegible]2
28/11/2019 10:15:57	12	be[illegible]1	S[illegible]2
09/12/2019 11:06:03	21	ku[illegible]1	SE[illegible]2
09/12/2019 11:06:03	21	ku[illegible]1	SE[illegible]2
09/12/2019 11:06:03	21	ku[illegible]1	SE[illegible]2

La formation sur site

- Stand / Evènement interne
- Conférence

Fonctionnement des stands

- Un expert Certilience intervient et propose un atelier
  - Démonstrations / Explications
  - Bonnes pratiques
  - Questions / Réponses
- Durée : 2h
- Possibilité d'animation simultanée de plusieurs stands (format « salon »)

Les stands - catalogue

LA FORMATION

Nom du stand	contenu
Les mots de passe	.... Démonstration d'un vol de mot de passe Les risques et les conséquences Les bonnes pratiques
Les applications malveillantes	.... Téléchargement d'une appli mobile malveillante Les risques et les conséquences Les bonnes pratiques
Les clés USB	.... Connexion d'une clé « trouvée » Les risques et les conséquences Les bonnes pratiques
Les cyber-Risques	.... L'ingénierie sociale Le phishing Les réseaux sociaux Le WiFi

Fonctionnement d'une conférence

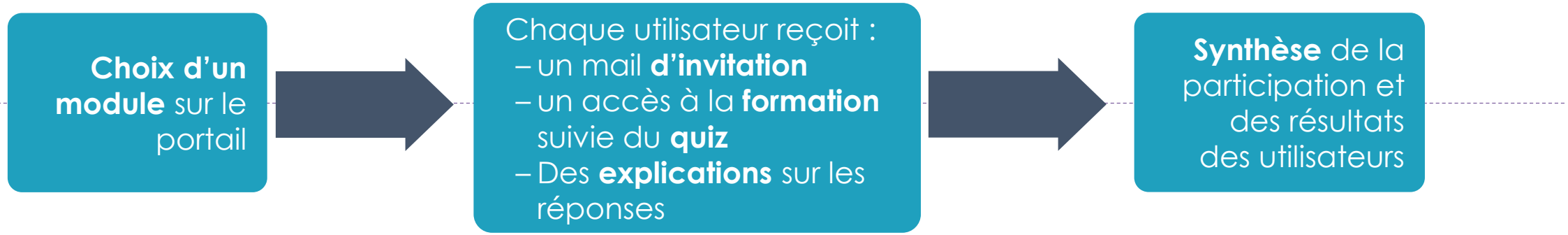
- Un expert Certilience intervient sur tous les thèmes liés à la cybersécurité

- 1 modèle de conférence standard :
  - durée entre 1h45 et 2h
  - « Comment puis-je participer à l'amélioration du niveau de sécurité de mon entreprise ? »

La formation en ligne :

- Plateforme Certiaware

Fonctionnement e-learning



- 1 module = 1 formation + 1 quiz
- Accès au catalogue de modules de formation sur le portail ***reporting.certilience.fr*** :
  - Modules sonorisés / modules à lire
  - Différentes langues disponibles sur les modules standards « à lire » : français - anglais - allemand - italien
  - Possibilité d'autres langues

Démonstration

Niveau utilisateur

lun. 02/12/2019 18:43

S

sensibilisation@certilience.fr

Sensibilisation 2019 : les réseaux sociaux

À Adrien BRUN

Bonjour,

La sécurité de l'information est une préoccupation constante à Certilience.
Je vous propose donc aujourd'hui de suivre un module interactif sur les risques des réseaux sociaux.

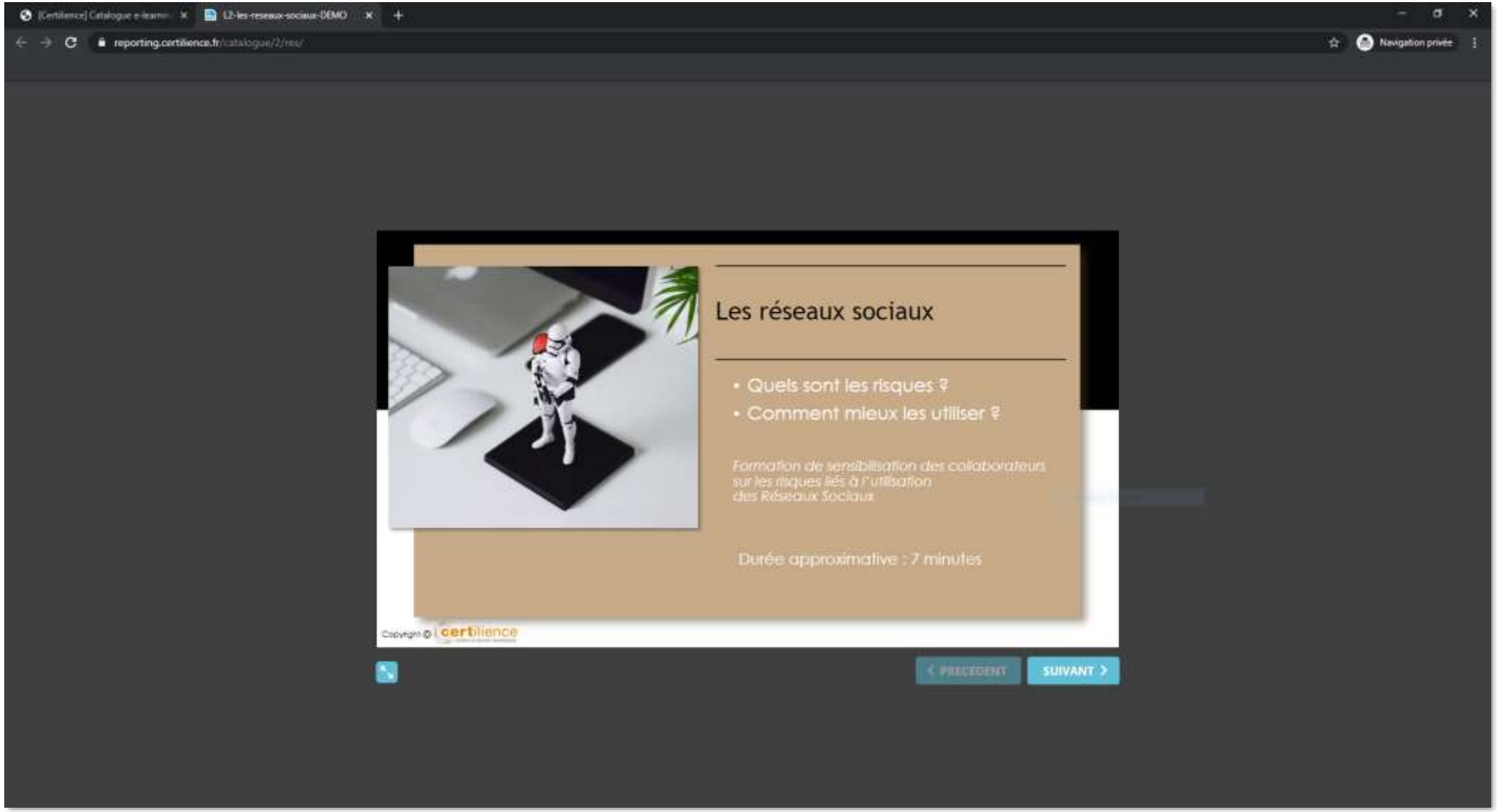
En quelques minutes, vous aurez l'opportunité de réactualiser vos connaissances sur le sujet pour adopter les bonnes pratiques, à la maison ou au travail !

Vous avez jusqu'au 12/12/2019 pour participer.

Pour commencer, cliquez ici.

Ce mail est généré par la plateforme de sensibilisation Certiaware.

Nicolas PERRIER


reporting.certilience.fr/catalogue/2/res/
Navigation privée
Les réseaux sociaux
• Quels sont les risques ?
• Comment mieux les utiliser ?
Formation de sensibilisation des collaborateurs sur les risques liés à l'utilisation des Réseaux Sociaux
Durée approximative : 7 minutes
Copyright © certilience
PRECEDENT
SUIVANT

Qu'est-ce-que les réseaux sociaux ? Á quoi peuvent-ils servir ?

Les réseaux sociaux ont différentes utilités et utilisations :

- Ils permettent aux personnes de **se connecter** entre elles, dans un **cadre professionnel** aussi bien que **personnel**.
- Ils peuvent servir à la **gestion des carrières professionnelles** (coaching professionnel, visibilité sur Internet), à **la distribution** et **la visibilité médiatique**, mais aussi à **favoriser les contacts personnels**, à **partager des informations**, des photos, etc.
- Enfin, ils peuvent être utilisés par une entreprise **pour réaliser de la publicité** ou **partager du contenu**.

< PRECEDENT SUIVANT >

Les risques

Mal utilisés, les réseaux sociaux peuvent :

- → Nuire à la **réputation** et à **l'image** de l'entreprise.
- → Entraîner des **fuites d'information** ou le **vol de données**
- → Permettre **l'usurpation de votre identité**
- → Servir à **la propagation d'un virus** à cause de vulnérabilités présentes sur les sites Web, ou de contenus partagés à travers ceux-ci
- → Provoquer une **perte de productivité**
- → Servir de cible aux **campagnes de phishing**

Voici quelques exemples d'utilisation des réseaux sociaux qui ont mis en difficulté des personnes ou des entreprises :

- Licencié pour avoir posté un message : *https://www.capital.fr/votre-carriere/reseaux-sociaux-l-exces-de-franchise-peut-vous-couter-tres-cher-1095946*
- Le cours de la bourse d'une entreprise chute pour un tweet : *https://www.presse-citron.net/comment-flinguer-le-cours-de-bourse-dune-entreprise-avec-seulement-11-followers-sur-twitter/*

< PRECEDENT SUIVANT >

Conseils
- les données personnelles

Ne pas afficher publiquement d'informations personnelles telles que votre **âge**, votre **numéro de téléphone**, votre **adresse postale** ou votre **adresse mail**.

Attention aux **questions secrètes** utilisées en cas d'oubli du mot de passe :

→ Ne pas mettre d'information sur son profil pouvant permettre à des personnes malveillantes de récupérer un mot de passe via la question secrète.

Par exemple :
publier une photo de son chien sur Facebook avec en commentaire s
messagerie en ligne la question secrète du type : « *quel est le nom de*

Les bons réflexes

Les bons réflexes à retenir :

- **Régler les options de sécurité** du réseau social utilisé afin de réduire la visibilité
- **Ne pas faire confiance** aux personnes inconnues
- Ne pas diffuser **d'informations personnelles**
- Ne pas diffuser **d'informations sur votre entreprise ou ses clients**

PRECEDENT SUIVANT

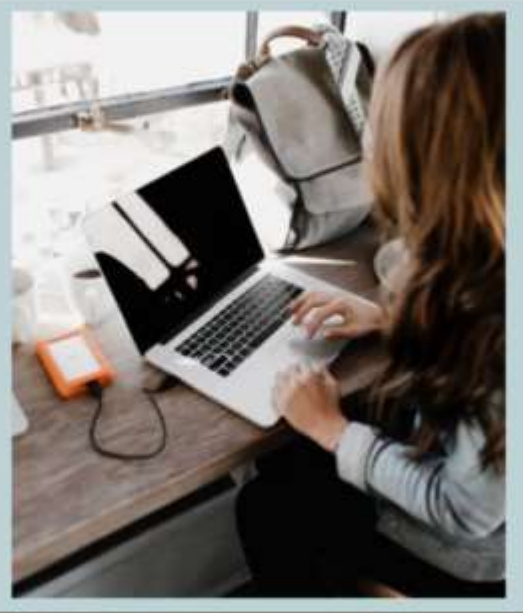
Évaluation de vos connaissances

La formation est désormais terminée, vous allez maintenant pouvoir passer un test.

Ce quiz a pour objectif de valider vos connaissances et votre compréhension des risques et menaces liés à votre utilisation de l'outil informatique.

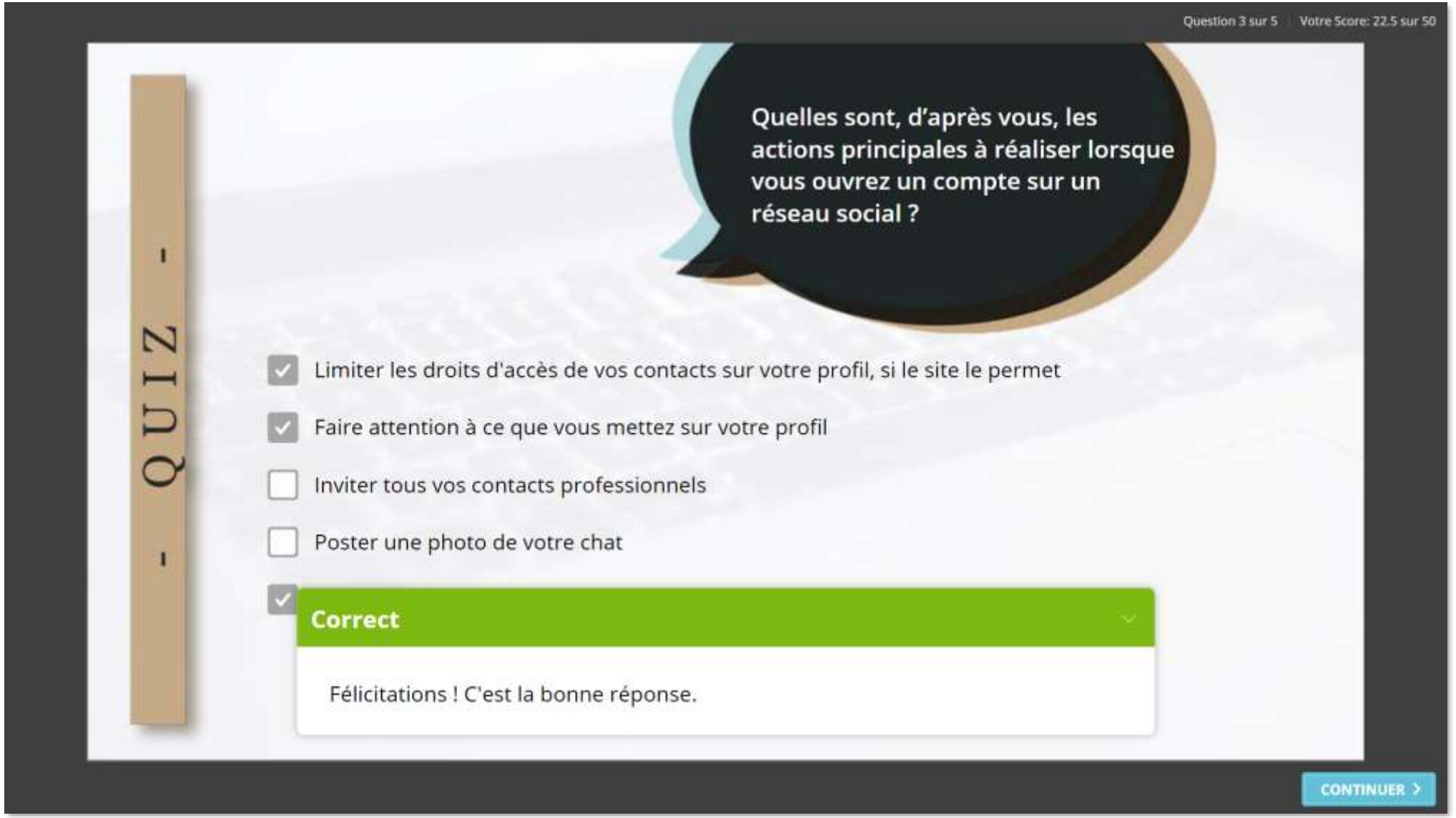
A l'issue, votre évaluation vous sera délivrée.

Pour chacune des questions, il y aura une ou plusieurs bonnes réponses possibles.

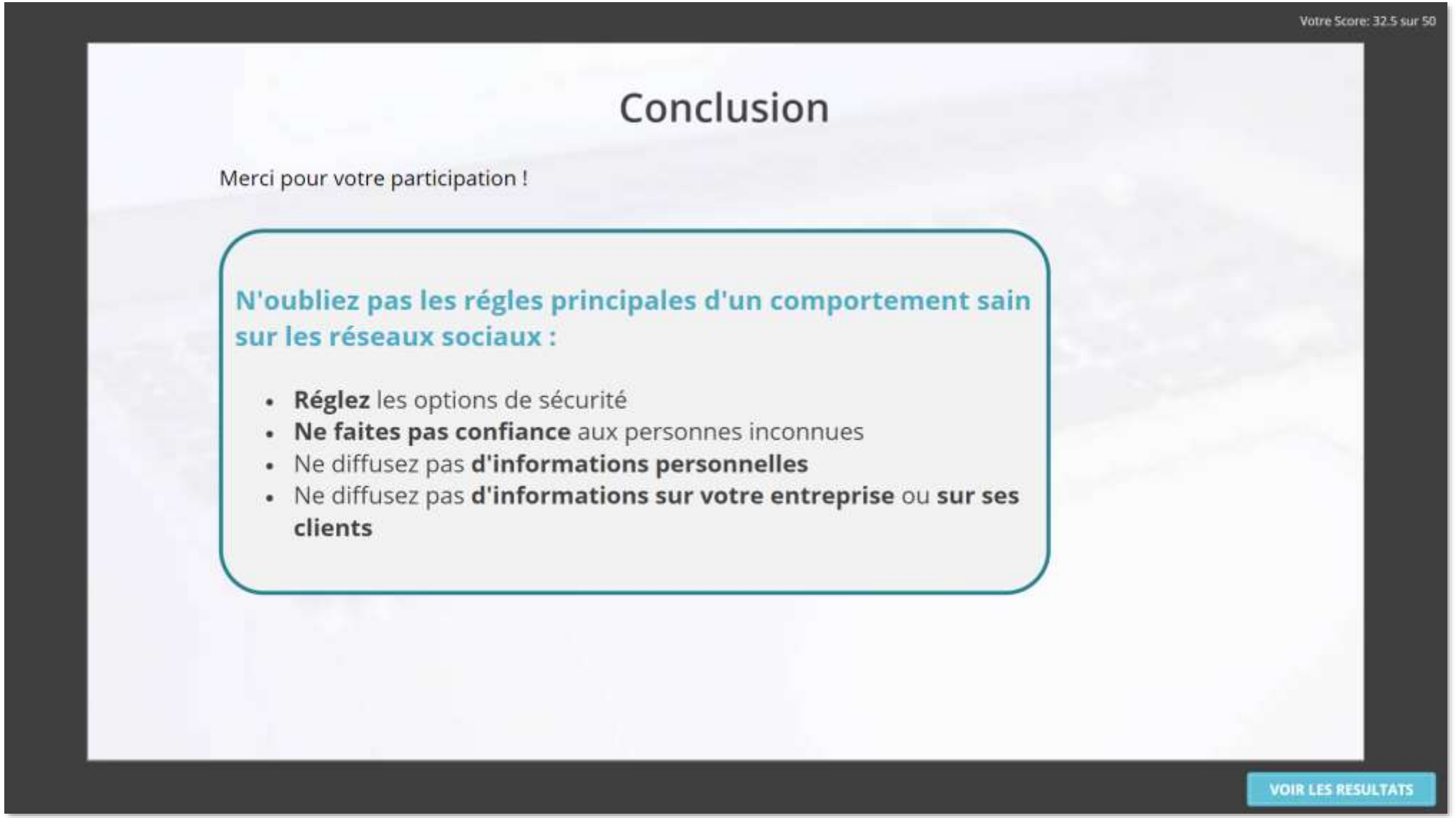


< PRECEDENT SUIVANT >


Question 1 sur 5
Votre Score: 0 sur 50
- QUIZ -
Quels sont les principaux risques liés aux réseaux sociaux pour les entreprises ?
Nuire à la réputation de la société
La non productivité
La fuite d'informations
Découvrir une photo gênante d'un de vos collègues
ENVOI


Question 3 sur 5 | Votre Score: 22.5 sur 50
- QUIZ -
Quelles sont, d'après vous, les actions principales à réaliser lorsque vous ouvrez un compte sur un réseau social ?
Limiter les droits d'accès de vos contacts sur votre profil, si le site le permet
Faire attention à ce que vous mettez sur votre profil
Inviter tous vos contacts professionnels
Poster une photo de votre chat
Correct
Félicitations ! C'est la bonne réponse.
CONTINUER >


Question 1 sur 5
Votre Score: 2.5 sur 50
- QUIZ -
Quels sont les principaux risques liés aux réseaux sociaux pour les entreprises ?
Nuire à la réputation de la société
La non productivité
La fuite d'informations
Partiellement Correct
Les réseaux sociaux sont un lieu public : il convient de ne pas y déposer d'informations liées à l'entreprise, tant pour son image que pour éviter les fuites d'informations. Attention au temps consacré à leur utilisation !
CONTINUER >


Votre Score: 32.5 sur 50
Conclusion
Merci pour votre participation !
N'oubliez pas les régles principales d'un comportement sain sur les réseaux sociaux :
Réglez les options de sécurité
Ne faites pas confiance aux personnes inconnues
Ne diffusez pas d'informations personnelles
Ne diffusez pas d'informations sur votre entreprise ou sur ses clients
VOIR LES RESULTATS

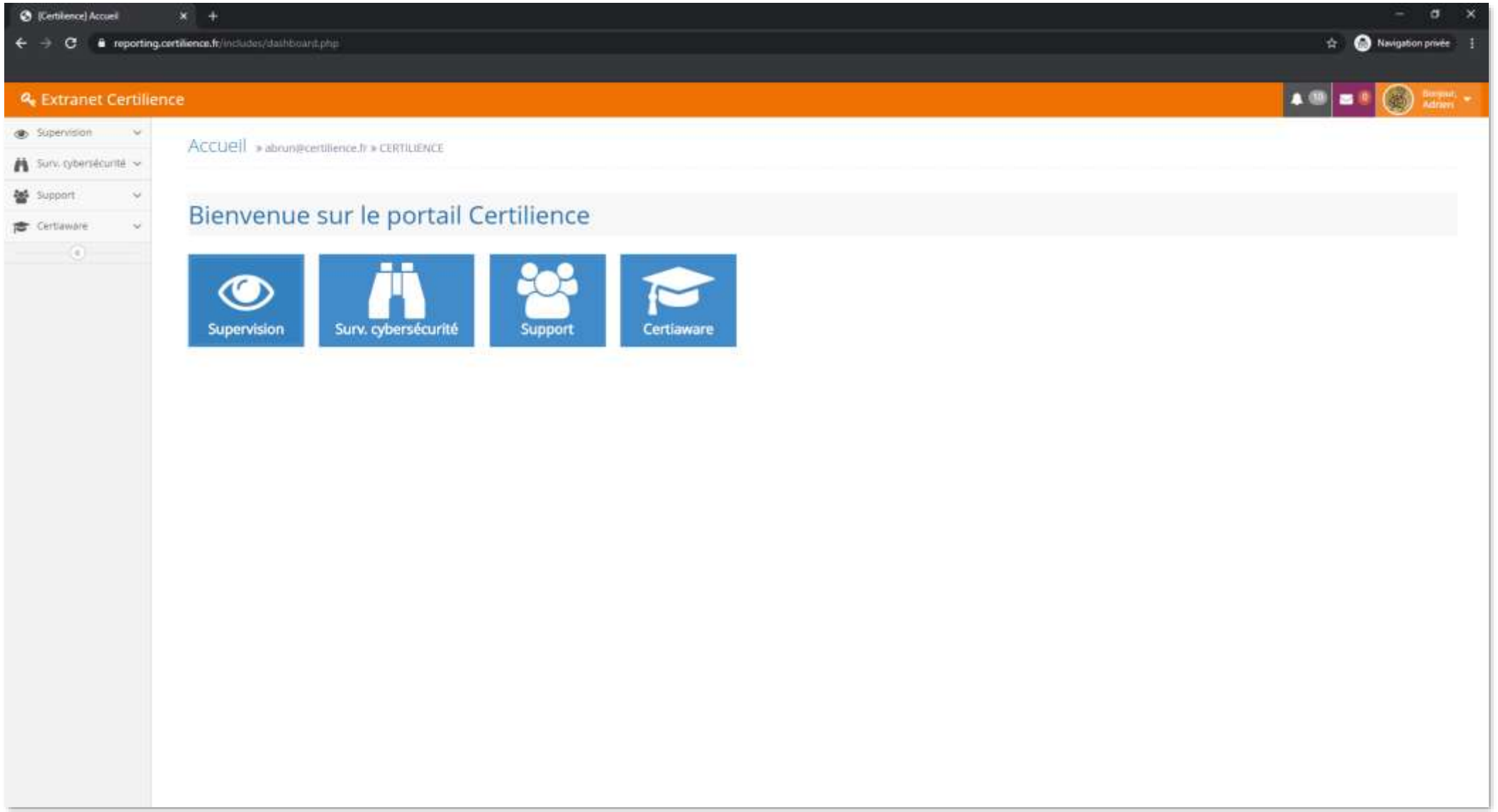

Question 1 sur 5 | Votre Score: 32.5 sur 50
- QUIZ -
Quels sont les principaux risques liés aux réseaux sociaux pour les entreprises ?
Nuire à la réputation de la société
La non productivité
La fuite d'informations
Partiellement Correct
Les réseaux sociaux sont un lieu public : il convient de ne pas y déposer d'informations liées à l'entreprise, tant pour son image que pour éviter les fuites d'informations. Attention au temps consacré à leur utilisation !
FeRMER LA FENETRE
< PRECEDENT
SUIVANT >


Désolé, vous n'avez pas réussi le quiz.
Votre Score: 65% 32.5 points
Score minimum requis: 80% 40 points
REVOIR LE QUIZ
REFAIRE LE QUIZ
PRECEDENT
QUITTER LE QUIZ

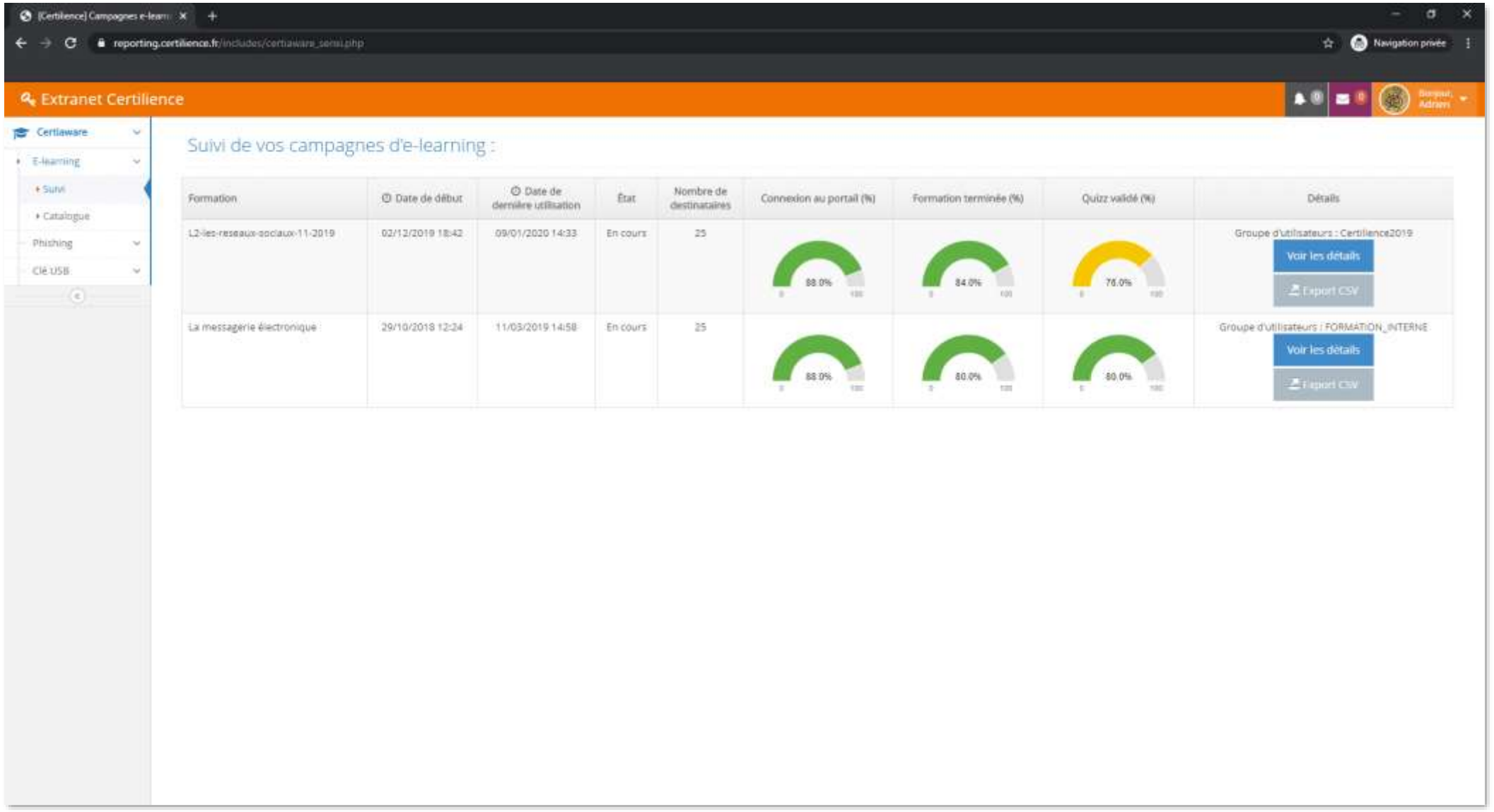
Démonstration

Niveau reporting

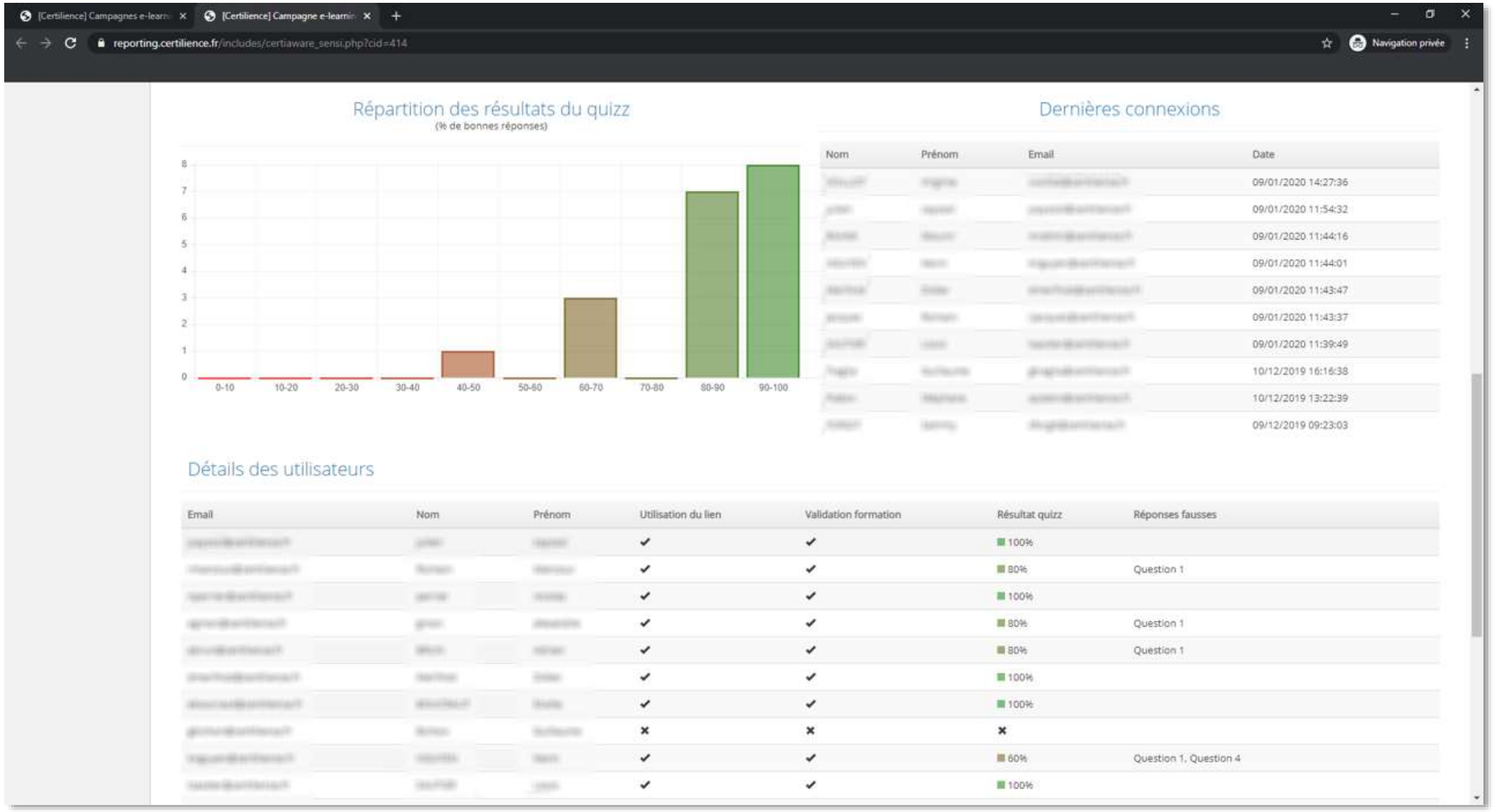
Reporting.certilience.fr



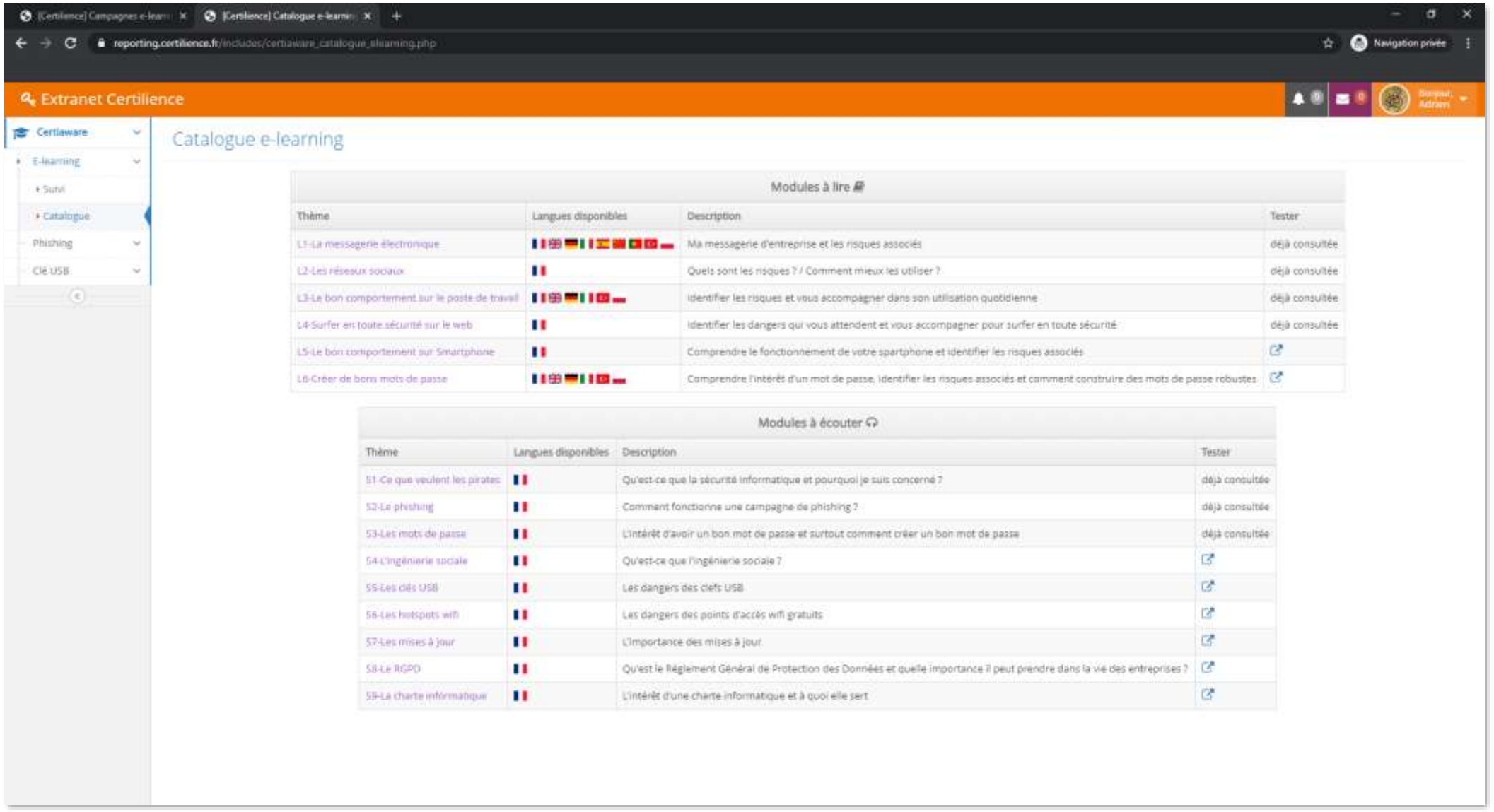
Le E-learning



Le E-learning



Le catalogue des formations E-learning



Références

Industrie Pharmaceutique

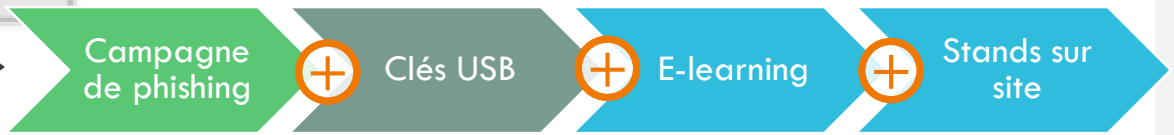
12700 utilisateurs - français / anglais / espagnol →

Communauté d'agglomération

1000 utilisateurs →

Acteur de référence dans le recyclage

50 utilisateurs →



Secteur bancaire

70 000 utilisateurs →

En termes de tarification

- Prérequis (pour Phishing/Clés USB ou E-learning) :
  - Abonnement au portail pour 1 an ou 3 ans
- Pour le phishing - standard
  - 150 crédits pour l'adaptation du scénario :
    - Choix du mail de phishing à envoyer
    - Création du faux portail sur lequel les collaborateurs seront « incités » à aller renseigner des informations sensibles
    - Validation de la bonne réception du mail avant envoi à tous les collaborateurs
  - 1 crédit par envoi
- Pour les clés USB – standard
  - Prix par lot de clés et dépend du scénario
- Pour le e-learning - standard :
  - 1 crédit par utilisateur par sujet
- Pour les formations sur site - standard :
  - Prix par session de 2H
- Personnalisation (sous forme de banques d'heures ou forfaits) :
  - Plusieurs langues pour le phishing ou le e-learning
  - Adaptation du contenu à votre contexte

Merci de votre attention

Vos contacts Certilience :

Adrien Brun	06 89 12 96 68	abrun@certilience.fr
Romain Marcoux	06 27 99 79 78	rmarcoux@certilience.fr
Elodie Boucraut	06 89 92 37 96	eboucraut@certilience.fr
Julien Cayssol	06 03 36 05 25	jcayssol@certilience.fr

www.certilience.fr

Retrouvez tous nos webinars sur notre chaîne

YouTube