Forum des Compétences

Document
C0 - Public
C1 - Interne
C2 - Restreint
C3 - Confidentiel
C4 - Secret

Forum des compétences

Efficacité de la sensibilisation Cyber : rêve ou réalité ?

Livrable final du Groupe de Travail

Travaux menés avec

ERIUM

SOMMAIRE

INTRODUCTION SUR LE GROUPE DE TRAVAIL *(2022)*

« Efficacité de la sensibilisation Cyber : rêve ou réalité ? »

Mai	Novembre	Décembre	13 Décembre
START	**FIN DES GT**	**LIVRABLE**	**COLLOQUE – Campus Cyber**

6 mois de travail et un constat général :
Capter et maintenir l'attention pour une bonne hygiène Cyber de tous au quotidien est un exercice difficile

L'ENJEU

Imposer les bons réflexes Cyber dans le quotidien numérique

LA DIFFICULTÉ

Nous vivons la transformation du **capitalisme numérique** des systèmes globaux qui imposent progressivement leurs propres codes sociaux et usages (et rendent désuet les actions de "sensibilisation")

Alors, quelles réponses ?

6 MOIS D'INTERACTIONS EN 2022

1

16 mai
REX sur des actions entreprises par les participants

Vue globale / Quelles solutions / efficacité / coûts ...

2

13 juin
Qui adresser et pourquoi ?

Qui sont les personae et comment les adresser ?

3

11 juillet
Les actions par persona

Ce qui fonctionne ou pas pour chaque persona

4

29 août
Les contenus par persona

Les boosters d'efficacité par cible

5

19 septembre
Quels indicateurs ?

Les kpi de pilotage (déploiement) et d'efficacité (engagement)

6

17 octobre
Quel pilotage global de la culture cyber ?

Les leviers de démultiplication et l'apprentissage en réseau

7

17 octobre
Budget

Coûts, leviers et ROI

8

17 novembre
Synthèse & consolidation des ateliers

9

13 décembre
Colloque 2022 du Forum des Compétences

PARTICIPANTS

Xavier MIGAUD – AG2R La Mondiale

Laure Anne BESANCENOT – AG2R La Mondiale

Thomas MATUSZAK – AG2R La Mondiale

Lia SCHIFFMANN – Allianz

Alexandra COHADON – Banque de France

Laurent CHAILLEY – Banque de France

Alexandre CHOPIN – BNP Paribas

Isabelle DIDELOT – BNP Paribas

Olivier THOMAS – BNP Paribas – Bivwak

Franck BICHET – BNP Paribas – Cardif

Xavier BOIDARD – CA Assurances

Vianney DERMY – CA Assurances

Frank VAN CAENEGEM – CNP Assurances

Estelle BOYER-TCHIGIQUE – CNP Assurances

Roland CORNEAU – COVEA

Marek KUREK – Euro-Information

Laurence HERROU – IEDOM-IEOM

Marc DEVALLIER – La Banque Postale

Christophe HISTA – La Banque Postale

Hulya SONMEZ – Swisslife

Florent SKRABACZ – Erium

Emilien MARIMPOUY – Erium

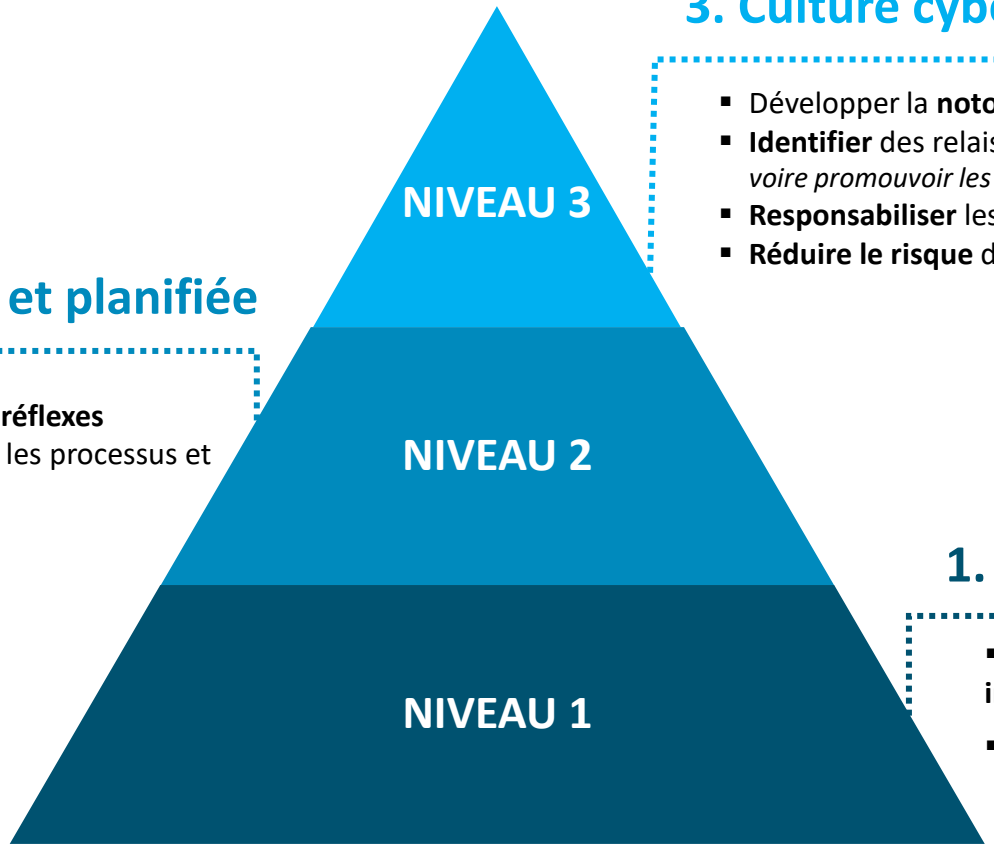
POURQUOI SENSIBILISER LES UTILISATEURS ?

3. Culture cyber développée et durable

- Développer la **notoriété cyber** de l'organisation
- **Identifier** des relais & **ambassadeurs** hors des populations IT
  voire promouvoir les postes cyber en interne
- **Responsabiliser** les utilisateurs sur leurs rôles cyber pour l'organisation
- **Réduire le risque** d'incidents cyber

2. Sensibilisation régulière et planifiée

- Atteindre un niveau de **culture cyber** en développant et maintenant les **bons réflexes**
- Assurer la **conduite du changement** sur les processus et outils de **cybersécurité**



1. Conformité élémentaire

- Faire **prendre conscience** du risque cyber – **informer** les utilisateurs - **démystifier** la cyber
- **ÊTRE CONFORME À LA RÉGLEMENTATION**

OBJECTIFS PAR NIVEAU DE MATURITÉ

Ces objectifs globaux se déclinent par profil d'utilisateurs avec des attentes supérieures pour les populations les plus exposées.

QUI SONT LES PRINCIPALES CIBLES OU PERSONAE ?

INTRO

En marketing, un **persona** est un **portrait fictif d'une typologie d'utilisateurs**.

Chaque persona a des **comportements**, des **enjeux** et une **exposition cyber** communs.

Persona 1

- Exposition Cyber
- Comportements
- Enjeux

Action 1	Action 4
Action 2	Action 5
Action 3	Action 6

Persona 2

- Exposition Cyber
- Comportements
- Enjeux

Action 1	Action 4
Action 2	Action 5
Action 3	Action 6

Maturité ++ ›

En adoptant un ciblage « marketing » des utilisateurs, les actions d'acculturation sont plus adaptées aux contraintes métiers et plus à même de mobiliser

LES PERSONAE IDENTIFIÉS (INTERNES)

TOUS LES UTILISATEURS

“Je passe de plus en plus de temps devant un PC ou un Smartphone. Au bureau ou à la maison. Je subis ou j’adore, ça dépend“

- **Mots-clés**
  #12BonnesPratiques #Réflexes #Signalement
- **Rôle**
  Tous les métiers
- **Enjeu**
  Obtenir un engagement optimal sur des actions *de masse*

VIP

“Je représente l’entreprise, ses obligations et valeurs. Ma responsabilité peut être engagée. Je peux être ciblé par une attaque. Comment bien mobiliser mes managers ?“

- **Mots-clés**
  #RSE #Conformité #Régulateur
- **Rôle**
  Conseil d’Administration / C-Level / Cadres dirigeants / Assistants
- **Enjeu**
  Obtenir un sponsoring sur le programme d’acculturation

LES PERSONAE IDENTIFIÉS (INTERNES)

UTILISATEURS D'ACTIVITÉS À RISQUES

"J'ai des privilèges étendus. J'interagis avec des données et/ou des environnements stratégiques. J'intéresse les attaquants."

- **Mots-clés**
  #Privilèges #Risques #Responsabilités #RGPD
- **Rôle**
  Resp. Financiers / Gestionnaires de données personnelles sensibles - confidentielles / Administrateurs fonctionnels métiers
- **Enjeu**
  Leur faire prendre en compte qu'ils sont à risques

ACTEURS IT

"Les systèmes informatiques sont mon quotidien. Je les développe, les améliore ou les supporte dans la limite du raisonnable"

- **Mots-clés**
  #Privilèges #Admin #Dev #Incidents
- **Rôle**
  Utilisateurs IT à privilèges / Filière Cyber / Filière IT
- **Enjeu**
  Mobiliser des utilisateurs qui peuvent *être persuadés de tout connaître*

LES PERSONAE IDENTIFIÉS (EXTERNES)

PRESTATAIRES

“Je passe mon temps dans cette entreprise. En même temps ce n’est pas elle qui me paie, et je peux changer du jour au lendemain. SA cyber c’est quand même SON problème …

- **Mots-clés**
  #Entre prestas… #Obligations #Contrat #Contrôle
- **Rôle**
  potentiellement équivalent aux rôles internes
- **Enjeu**
  Prendre en compte le turnover

CLIENTS

“Mon banquier ou mon assureur me parlent de Cyber en permanence. Franchement, au bout d’un moment …

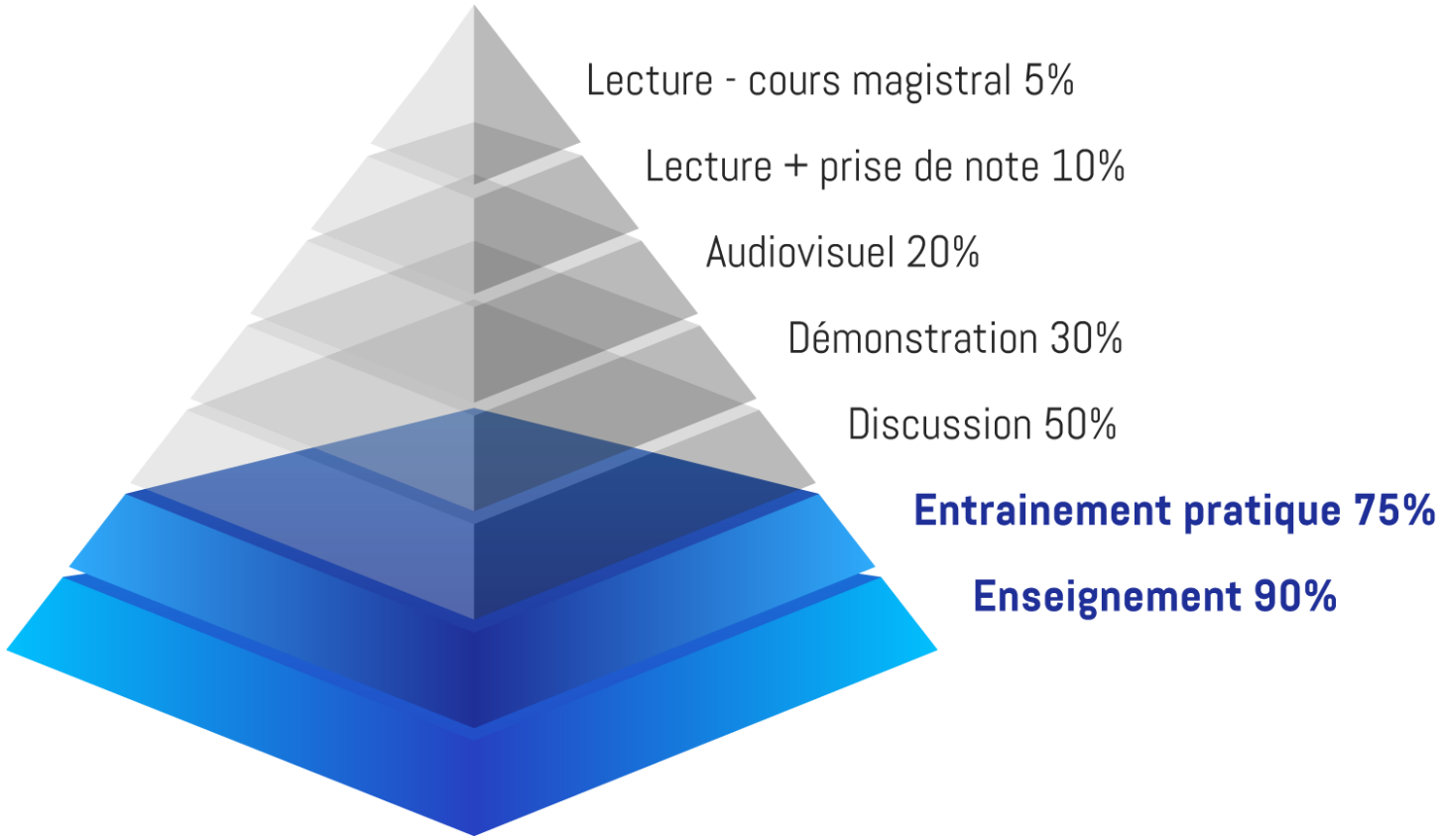
- **Mots-clés**
  #Droit #Danger #Facilité #Simplicité #Hackers…
- **Rôle**
  Particulier / Entreprise
- **Enjeu**
  Prendre en compte des niveaux de culture numérique hétérogènes

LES MODES D'ENGAGEMENT

Notre clé de lecture

La learning pyramid

D'écouter à faire agir, il y a de nombreux gradiants en termes d'efficacité



PANORAMA DES ACTIONS PAR PERSONA

TOUS LES UTILISATEURS

Rôle
Tous les métiers

Objectif
Développer et maintenir les réflexes relatifs aux bonnes pratiques usuelles.

Enjeu
Obtenir un engagement optimal sur des actions de masse.

Campagnes de **phishing de masse**
(Cofence PhishMe, Sensiwave, ProofPoint,….)

Pour les grandes organisations, il est préférable de faire des campagnes « ciblées » par pays / zone (prise en compte des différences culturelles et de maturité)

Entrainement – 75%

E-learning sur les bonnes pratiques

- Intégration aux LMS notamment pour les formats obligatoires
- Personnalisation plus complexe dans les grandes organisations
- Formats courts (<15 min), récurrents et multimédia
- Mesure de la compréhension par des QCM

Audiovisuel – 20%

Evénements : CyberMois et autres marronniers

- Il est complexe d'organiser des ateliers ludiques pour tous – le format distanciel (ou mixte) le facilite
- Beaucoup d'événements sont déjà prévus au mois d'octobre => certains organisent le CyberMois en avril

Démonstration – 30%

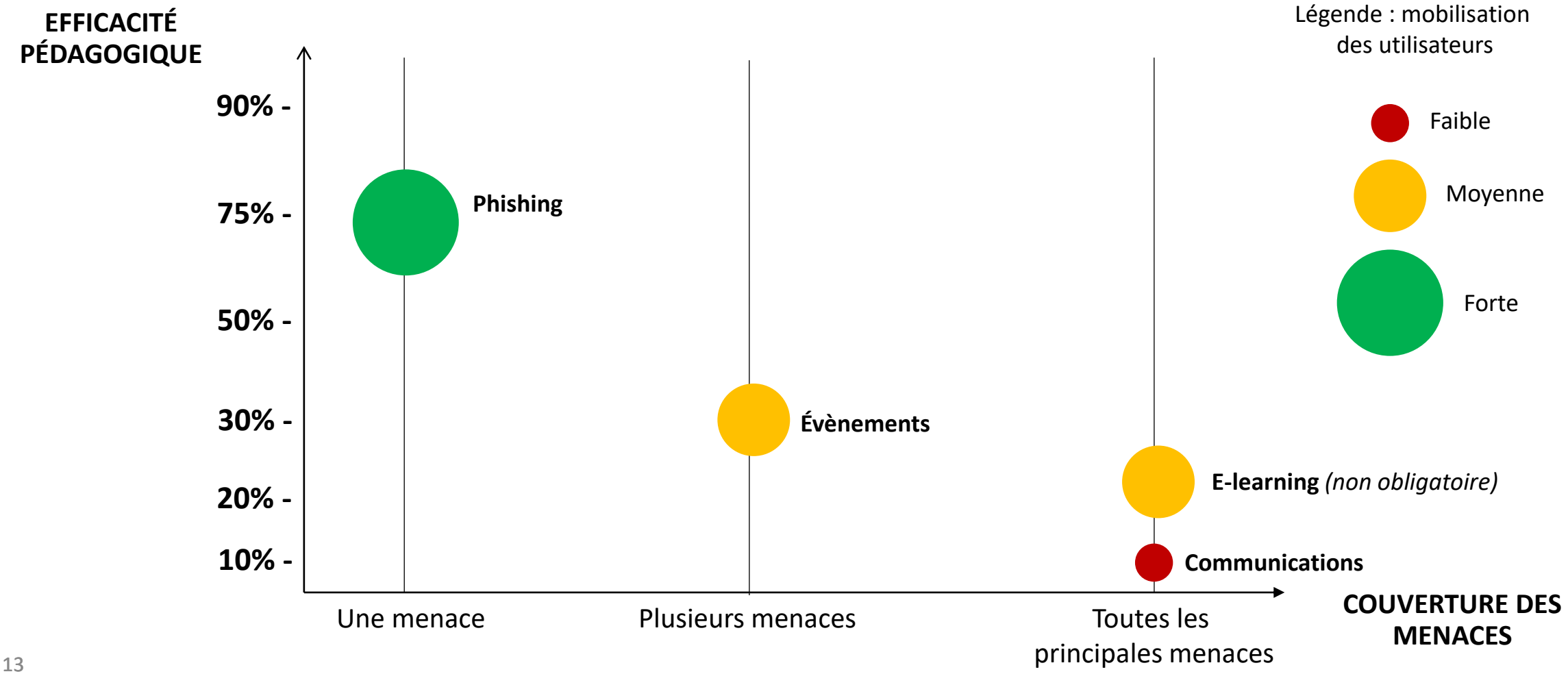
Communications

Lockscreens sur les terminaux (très visible mais difficilement mesurable), intranet, newsletters et revues de presse, posters, flyers, Charte à signer…

Lecture – 5 à 10%

EFFICACITÉ & COUVERTURE DES ACTIONS

TOUS LES UTILISATEURS



FACTEURS CLÉS DE SUCCÈS POUR TOUS LES UTILISATEURS

FORMAT

Court **Concret**

(exemple : un passeport cyber intégré au livret d'accueil)

Humoristique

Multimédia

Récurrent

Des mises en situation pratiques

exercices de classification des documents, mises en situation réelle *(exemple : collecte d'informations sur les réseaux sociaux pour déduire des identifiants)*

Ludique

compétition positive entre Directions avec publication & reporting des résultats et participations

APPRENTISSAGE

Des bonnes pratiques utiles à la fois dans la **vie professionnelle** et **personnelle**

Des actions **adaptées** au niveau de **maturité** de l'utilisateur :

exemple d'un outil d'auto-évaluation sur les bonnes pratiques qui adapte les contenus proposés à l'utilisateur

PANORAMA DES ACTIONS PAR PERSONA

VIP

Rôle
Conseil d'Administration / C-Level / Cadres dirigeants / Assistants

Objectif
Savoir détecter et réagir face aux attaques ciblant les Dirigeants / Connaître les spécificités d'une crise cyber

Enjeu
Obtenir un sponsoring sur le programme d'acculturation

Campagnes de **phishing ciblé**

Certaines organisations challengent les Directeurs entre eux

Entrainement – 75%

Interventions & Coaching pour les CODIR / COMEX

- La participation d'**intervenants externes** est préférable pour cette cible (pas de jugement RSSI)
- Le coaching peut être fait après une analyse OSINT sur le dirigeant concerné (exemple d'utilisation d'ANOZR WAY)
- Des événements réguliers avec les CODIR créent de la proximité avec la filière cyber

Discussion – 50%

Exercices de gestion de crise cyber

Les exercice de gestion de crise n'ont pas été approfondis dans ce groupe de travail

Entrainement – 75%

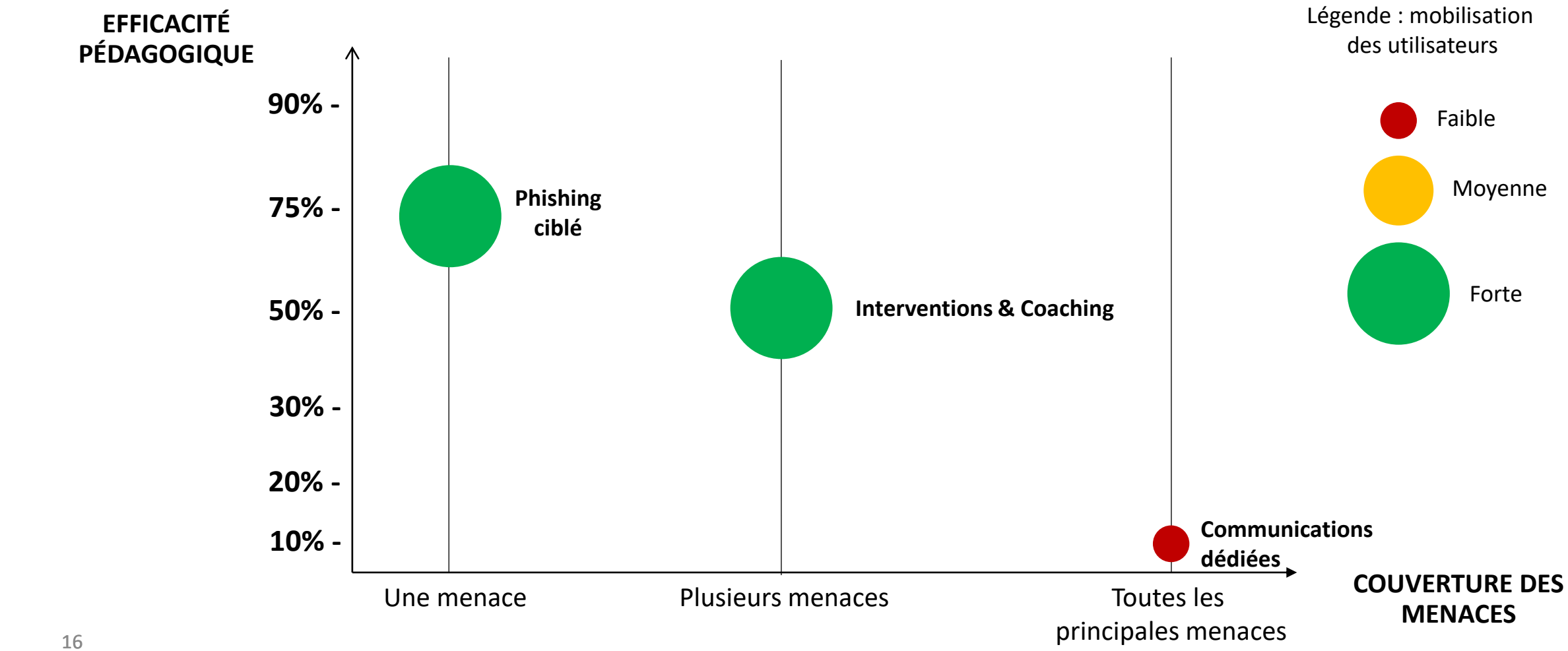
Communications

- **Newsletters** : utilisation de newsletters existantes ou dédiées
- **Lettre du RSSI** vers le COMEX et N-1 : actualités et informations & actions à faire décliner
- Mise en place d'un **canal de communication** (app) entre RSSI et Top Management (bonnes pratiques, actus cyber, questions / réponses)

Lecture – 5 à 10%

EFFICACITÉ & COUVERTURE DES ACTIONS

VIP



PANORAMA DES ACTIONS PAR PERSONA

UTILISATEURS D'ACTIVITÉS À RISQUES

Rôle

Resp. Financiers / Gestionnaires de données personnelles sensibles - confidentielles / Administrateurs fonctionnels métiers

Objectif

Connaître les risques cyber les ciblant spécifiquement et renforcer les réflexes associés

Enjeu

Leur faire prendre en compte qu'ils sont à risques

Campagnes de **phishing ciblé**

Des actions qui peuvent réalisées avec les acteurs anti fraude

ProofPoint met en avant le concept de ***Very-Attacked People*** (utilisateurs les plus ciblés) qui ne sont pas forcément les VIP

Entrainement – 75%

Interventions en plénière de Directions traitant des données sensibles

Les supports doivent être contextualisés par rapport aux activités quotidiennes des utilisateurs

Discussion – 50%

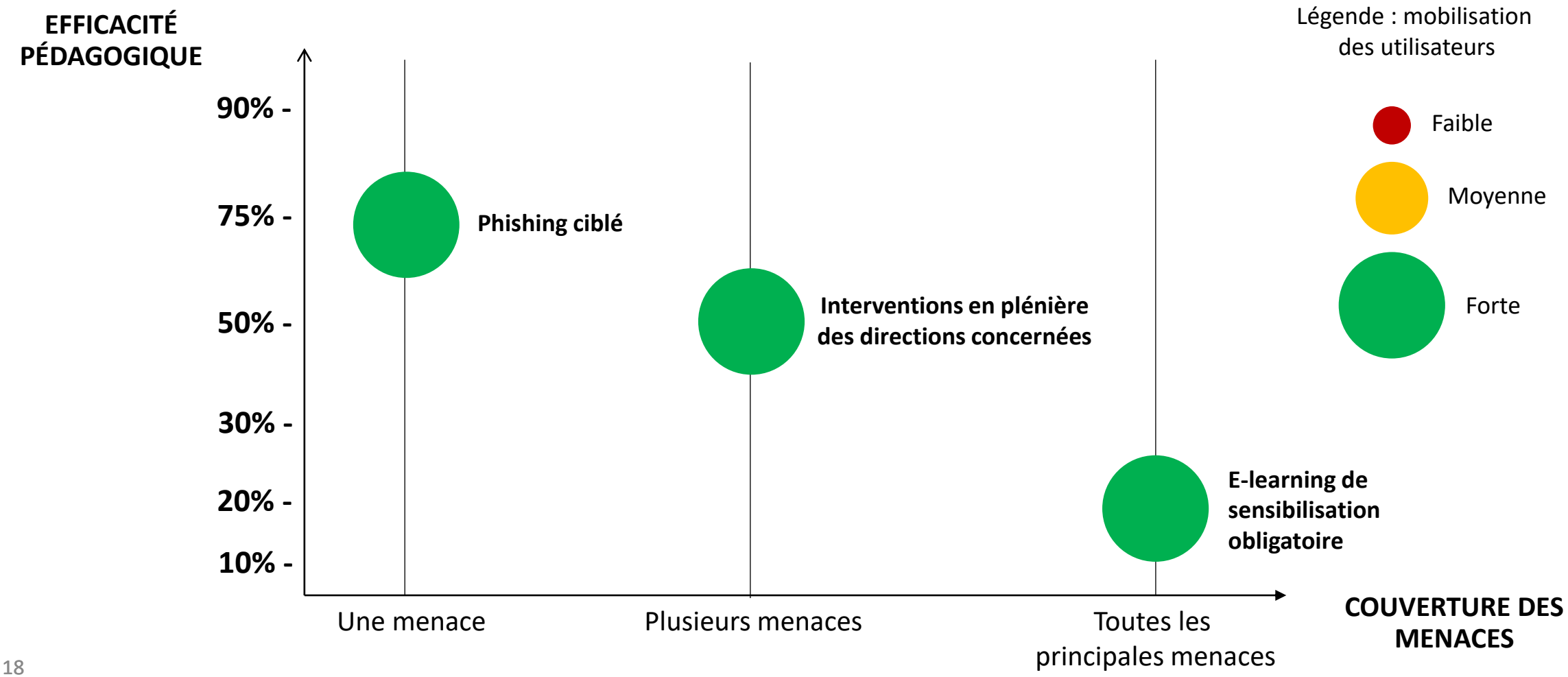
E-Learning de sensibilisation

Pour cette cible, les sessions sont souvent obligatoires à l'arrivée et sont à renouveler

Audiovisuel – 20%

EFFICACITÉ & COUVERTURE DES ACTIONS

UTILISATEURS D'ACTIVITÉS À RISQUES



PANORAMA DES ACTIONS PAR PERSONA

ACTEURS IT

Rôle

Utilisateurs IT à privilèges / Filière Cyber / Filière IT

Objectif

Les attentes sont supérieures pour ces utilisateurs pour lesquels les actions de formation sont importantes. La sensibilisation de ces cibles doit permettre le maintien des compétences clés.

Enjeu

Mobiliser des utilisateurs qui peuvent être persuadés de tout connaître.

Exercices de gestion de crise IT

Les exercice de gestion de crise n'ont pas été approfondis dans ce groupe de travail

Entrainement – 75%

Parcours d'onboarding ciblé sur les cyber golden rules IT

Sensibilisation e-learning pouvant être obligatoire et conditionner les accès au SI

Audiovisuel – 20%

Espaces de veille et de partage par thématique

- Exemples : groupe Yammer par thématique
- Sessions présentiels avec tips pour les développeurs

Discussion – 50%

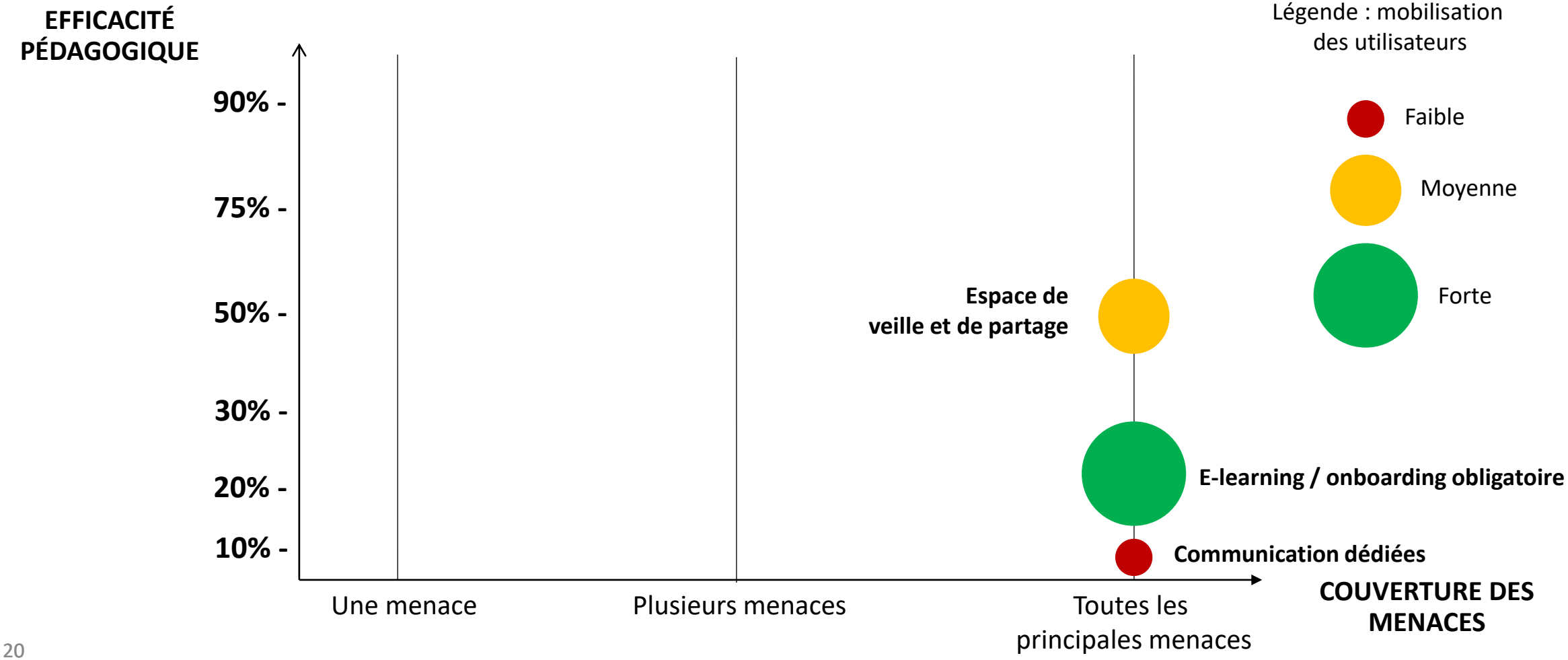
Communications

Supports de communication dédiés

Lecture – 5% à 10%

EFFICACITÉ & COUVERTURE DES ACTIONS

ACTEURS IT



PANORAMA DES ACTIONS PAR PERSONA

PRESTATAIRES

Les prestataires doivent être sensibilisés à la cybersécurité par leur employeur.
Les **actions déployées pour cette cible viennent renforcer et contextualiser** cette base.
Un niveau de maturité pourrait être exigé avant le début des missions.

Prestataires **ponctuels n'ayant pas d'accès au SI**
accès à des données internes (exemple : projets au forfait)

Objectif
Faire appliquer les règles de protection des données

Action
Communication / Signature des règles de manipulation des informations

Lecture – 5%

Prestataires **disposant d'un poste de travail interne**
(exemples : projets en régie)

Objectif
Faire appliquer les bonnes pratiques comme tous les utilisateurs du SI

Actions
Actions de sensibilisation identiques aux internes

5% à 75%

Fournisseurs disposant d'accès à privilèges

Objectif
Rappeler les réflexes et mesures de cybersécurité contractualisées

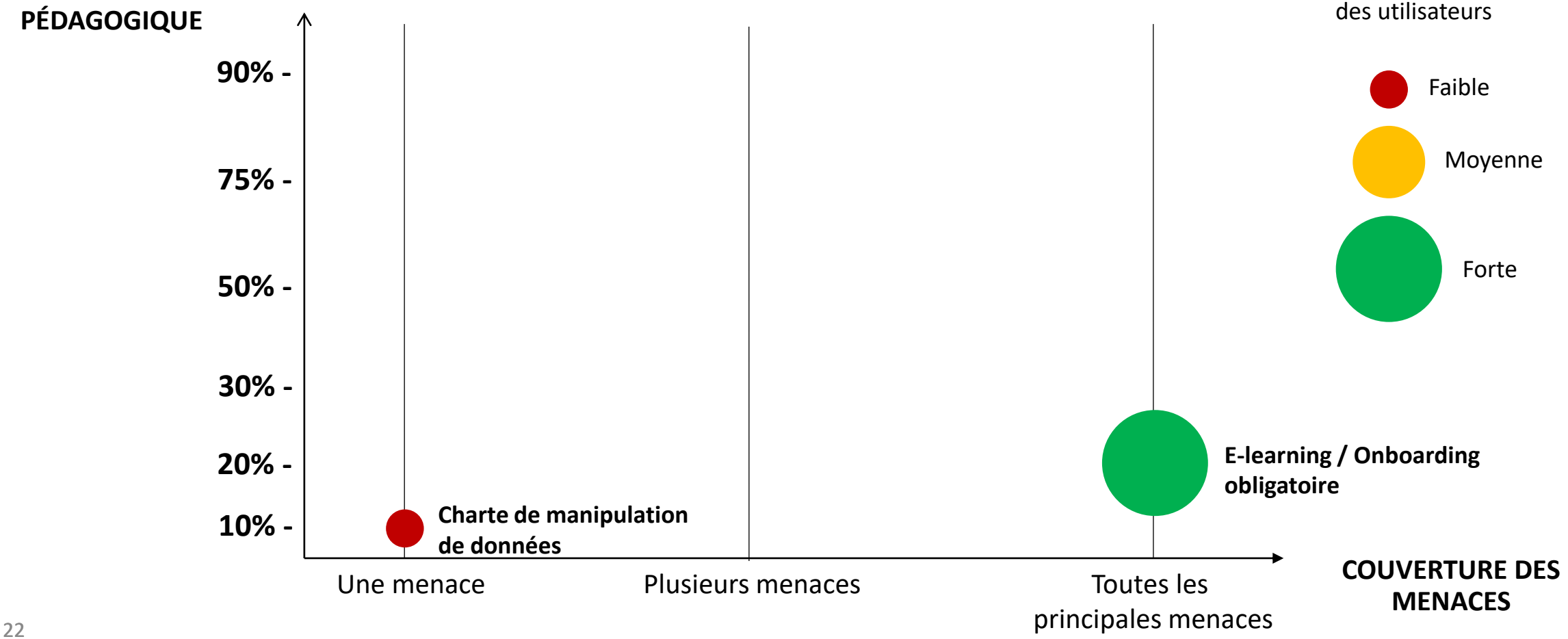
Actions
Onboarding ciblé rappelant les mesures cyber. Rappel tous les 6 mois

Audiovisuel – 20%

A NOTER : Arrêté du 25.02.2021 relatif au contrôle interne des entreprises soumises au contrôle de l'ACPR *: Les entreprises assujetties mettent également en œuvre un programme de sensibilisation et de formations régulières, soit au moins une fois par an, à la sécurité du système d'information* ***au bénéfice de tous les personnels et des prestataires externes****, et en particulier de leurs dirigeants effectifs*

EFFICACITÉ & COUVERTURE DES ACTIONS

PRESTATAIRES



PANORAMA DES ACTIONS PAR PERSONA

CLIENTS

Rôle
Particulier / Entreprise

Objectifs
Connaître les bonnes pratiques cyber lors de la souscription et de l'usage d'un service
Faciliter la remontée d'alerte en cas d'événement suspect

Enjeu
Prendre en compte des niveaux de culture numérique hétérogènes

Communications

- Rappel des bons réflexes : sur le site web, dans des lettres / emailing, suite à l'authentification à un service…
- Mise en avant de contenus (ex : cybermalveillance)

Lecture – 5%

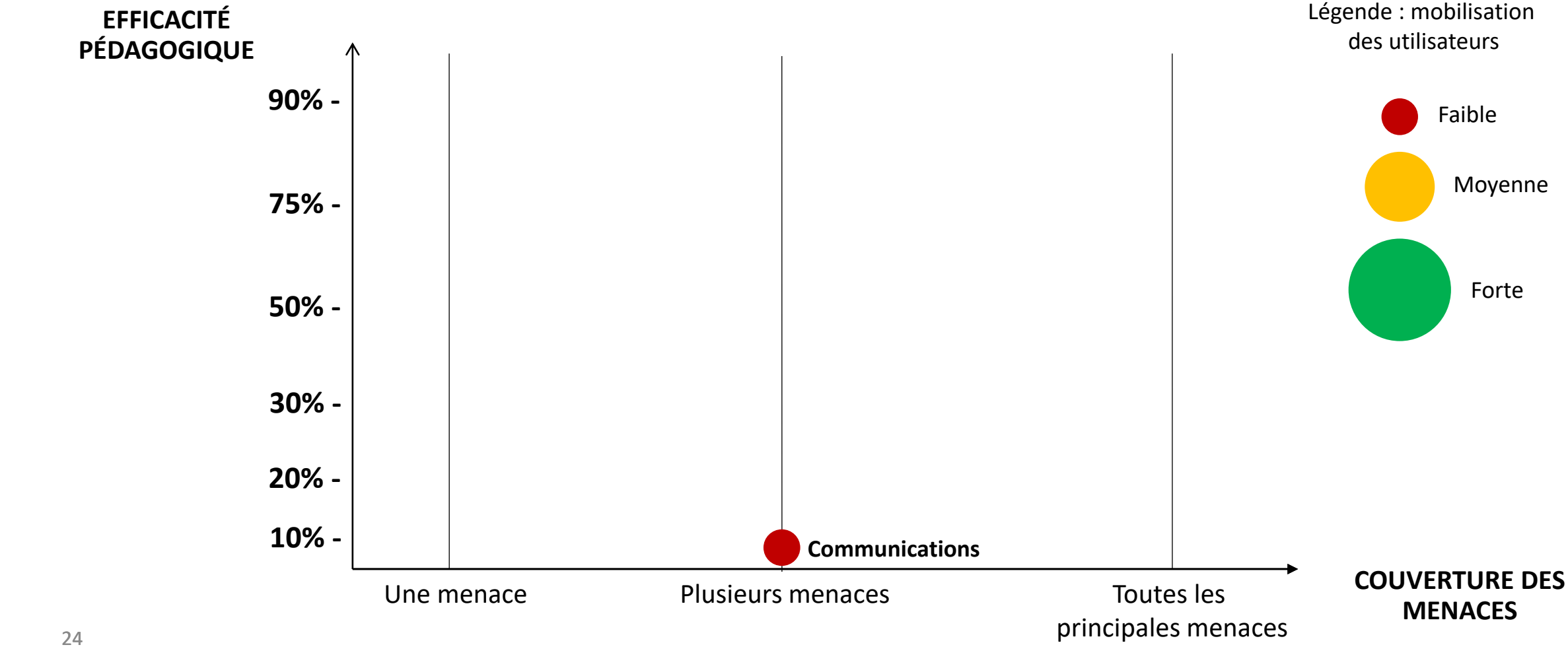
Messages pour imposer un niveau de cybersécurité

- Exemple : message pour imposer un navigateur à jour

Lecture – 5%

EFFICACITÉ & COUVERTURE DES ACTIONS

CLIENTS



QUELS ACTEURS POUR LE PILOTAGE ET L'ANIMATION DES ACTIONS

LE SPONSOR

QUI

- Très souvent le sponsor est le Directeur Cybersécurité
- Peu de sponsors COMEX sauf pour certaines actions obligatoires
- Certains Directeurs de filiales / sites

QUOI

Sponsoring du plan d'acculturation auprès de la Direction Générale et de toute l'organisation

LA FILIERE CYBER

QUI

RSSI locaux (dans les métiers / sites / pays…), référents cyber, RSSI métiers…

QUOI

- Déploiement de kits d'acculturation (pour des événements, ateliers, interventions, communications…)
- Accès admin fonctionnel aux solutions de sensibilisation (campagnes de phishing locales, accès LMS pour piloter la réalisation des e-learning localement…)

COMMENT

Des comités récurrents avec la filière : suivi des indicateurs & des actions à déployer

Des **Cyber Awards** peuvent récompenser les RSSI Locaux qui se sont investis sur les actions de sensibilisation

DES AMBASSADEURS HORS CYBER

Très peu répandu

Dans les organisations n'ayant pas de filière cyber couvrant tout le périmètre, des points de contacts ou des « clubs utilisateurs » sont identifiés

QUOI

- Participation de la formation, de la communication et de contacts métiers pour **optimiser l'impact des messages**
- Rediffuser les communications
- Témoigner sur les actions

Les messages ont plus d'efficacité lorsqu'ils sont mis en avant par des non IT

ACTIONS OBLIGATOIRES VS FACULTATIVES

EN MOYENNE

les actions **facultatives** obtiennent
10 à **40%** de participation

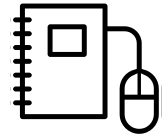
les actions **obligatoires** obtiennent
plus de 75% de participation

Les utilisateurs du SI doivent avoir une culture cybersécurité minimum
Pour les nouveaux arrivants, des actions obligatoires sont souvent déployées :

validation du code de conduite comprenant des golden rules cyber

charte à **signer** conditionnant la récupération des accès

sensibilisation e-learning



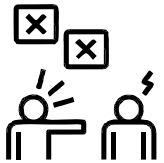
Pour maintenir les réflexes dans la durée, certaines organisations rendent obligatoires la réalisation d'un e-learning à une fréquence définie (annuelle, tous les 3 ans) ou après plusieurs échecs lors de campagnes de phishing voire suite à un incident

RÉCOMPENSES VS ‘ACCOMPAGNEMENT RENFORCÉ’

Quelles actions pour les **utilisateurs les plus vulnérables** ?

Quelles actions pour les **utilisateurs les plus impliqués** ?

Accompagnement gradué en fonction de l’impact des ***négligences et de leur répétition***



En cas de **non respect des règles** de manipulation des données aboutissant à une fuite de données confidentielles.

Entretien managérial pouvant aboutir à une sanction disciplinaire

En cas de **manque de vigilance** sur un phishing ou Internet.

Accompagnement renforcé avec une sensibilisation obligatoire

Des **goodies** *(faibles montants)* pendant le CyberMois notamment

Une **mise en avant des « *meilleurs* »** sur les **actions ludiques** *(avec points, classements, trophées…)*

Dans certaines organisations, les utilisateurs peuvent perdre temporairement : leur accès à Internet, la capacité à envoyer et recevoir des mails vers l’extérieur

MESURER LES ACTIONS DE SENSIBILISATION : POURQUOI ET POUR QUI ?

POURQUOI ?	POUR QUI ?
• **S'assurer de la conformité**	• Auditeurs externes / Régulateurs • RSSI / Formation

• **Suivre l'efficacité des actions de sensibilisation** :
  • sur le développement de la maturité des utilisateurs
  • sur la réduction des risques cyber
  • sur la réduction du nombre d'incidents ayant pour origine la négligence d'un utilisateur
	• DSI / Risques / RSSI

• **Se benchmarker** en interne et par rapport au secteur	• DG / DSI / RSSI
• **Mettre en avant les résultats** des actions de cybersécurité en interne	• Toute l'entreprise
• Faire évoluer le plan de sensibilisation	• RSSI / Formation

MESURER LES ACTIONS DE SENSIBILISATION : QUOI ?

QUANTITATIFS

Réalisation des actions
Taux de participation, taux de réalisation, taux de consultation des communications…

Résultats quantitatifs des actions
Taux de clic, taux et temps de signalement sur les campagnes de phishing

Impacts au quotidien
Evolution du taux de clic sur les vrais phishing *(ProofPoint)*

Taux d'utilisation des solutions de sécurité (ex : AIP, solutions de protection des données..) : ***peu répandu***
nombre de sollicitations du support / SOC sur des événements cybersécurité : ***peu répandu***
nombre de sollicitations de la filière cybersécurité : ***peu répandu***
nombre et évolution des incidents ayant pour origine une négligence : ***très peu répandu***

QUALITATIFS

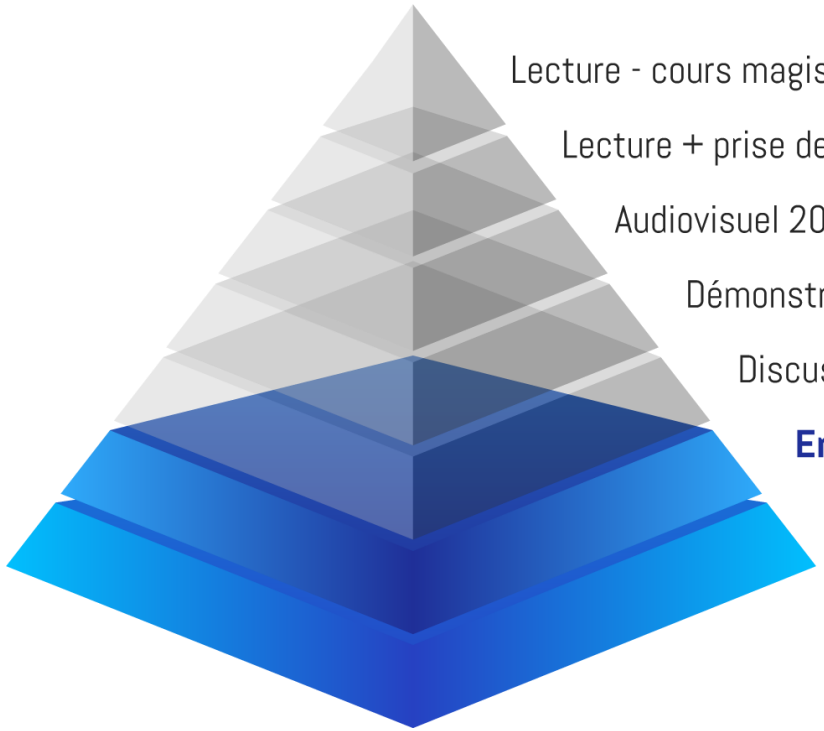
Connaissance et compréhension des concepts

Satisfaction des utilisateurs
Format et/ou apprentissage appréciés par les utilisateurs

Intérêt pour la cybersécurité
Taux de participation volontaire à un événement de cybersécurité
Identification d'interlocuteurs clés devenant des relais de la filière cyber

Les plans d'acculturation sont désormais challengés sur leur efficacité *(ex : diminution du taux de clic en production)*

SYNTHÈSE



Dominant aujourd'hui

Communications multimédia, E-learning de sensibilisation, Espaces de partage & veille, Evénements, Interventions, Coaching Dirigeants…

Campagnes de **phishing**

Appui sur la filière cyber
Peu de relais / ambassadeurs hors cyber

SYNTHÈSE : DES ACTIONS POUR QUELLE EFFICACITÉ ?

ADVOCATE

PERSONNE ?

ACT

KNOW

VIP

Utilisateurs d'activités à risques

Utilisateurs IT

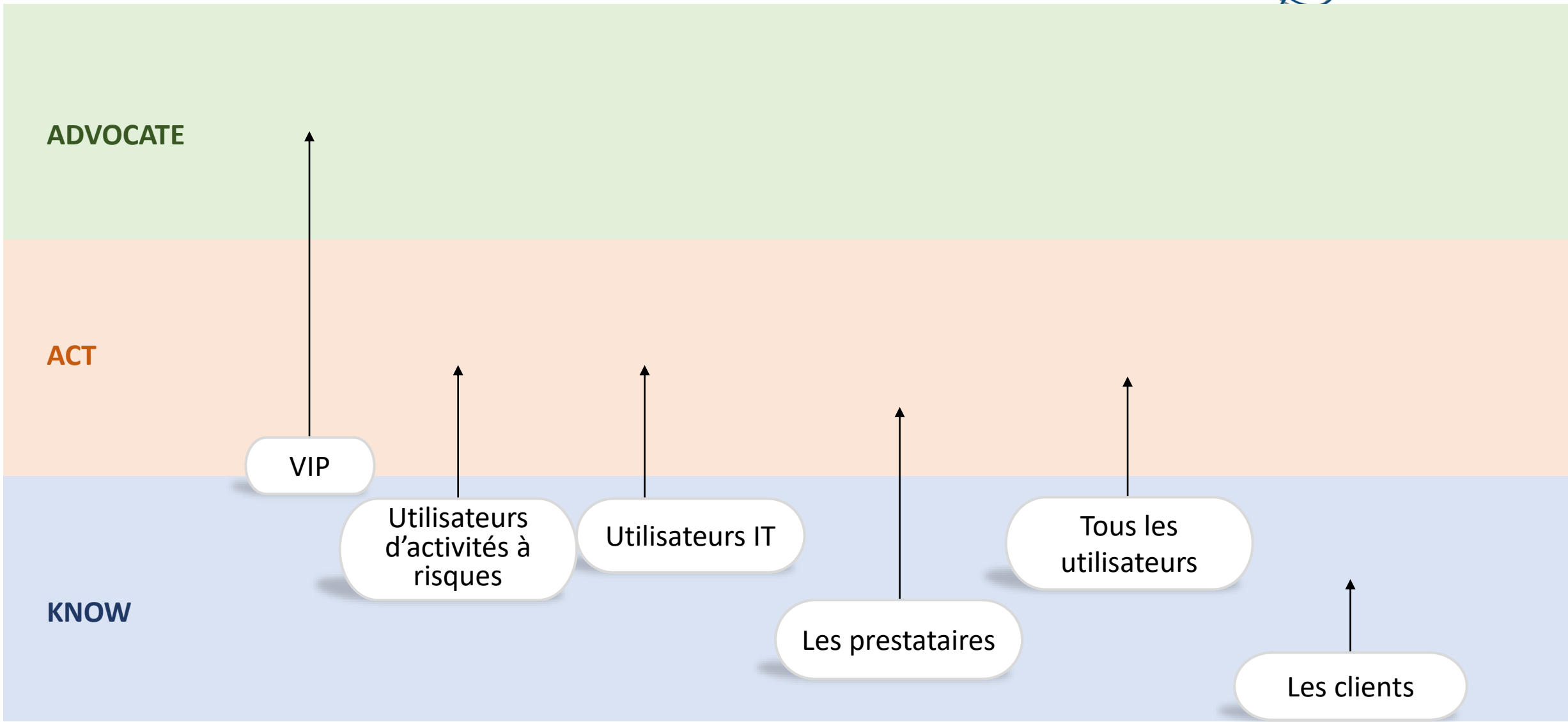
Tous les utilisateurs

Les prestataires

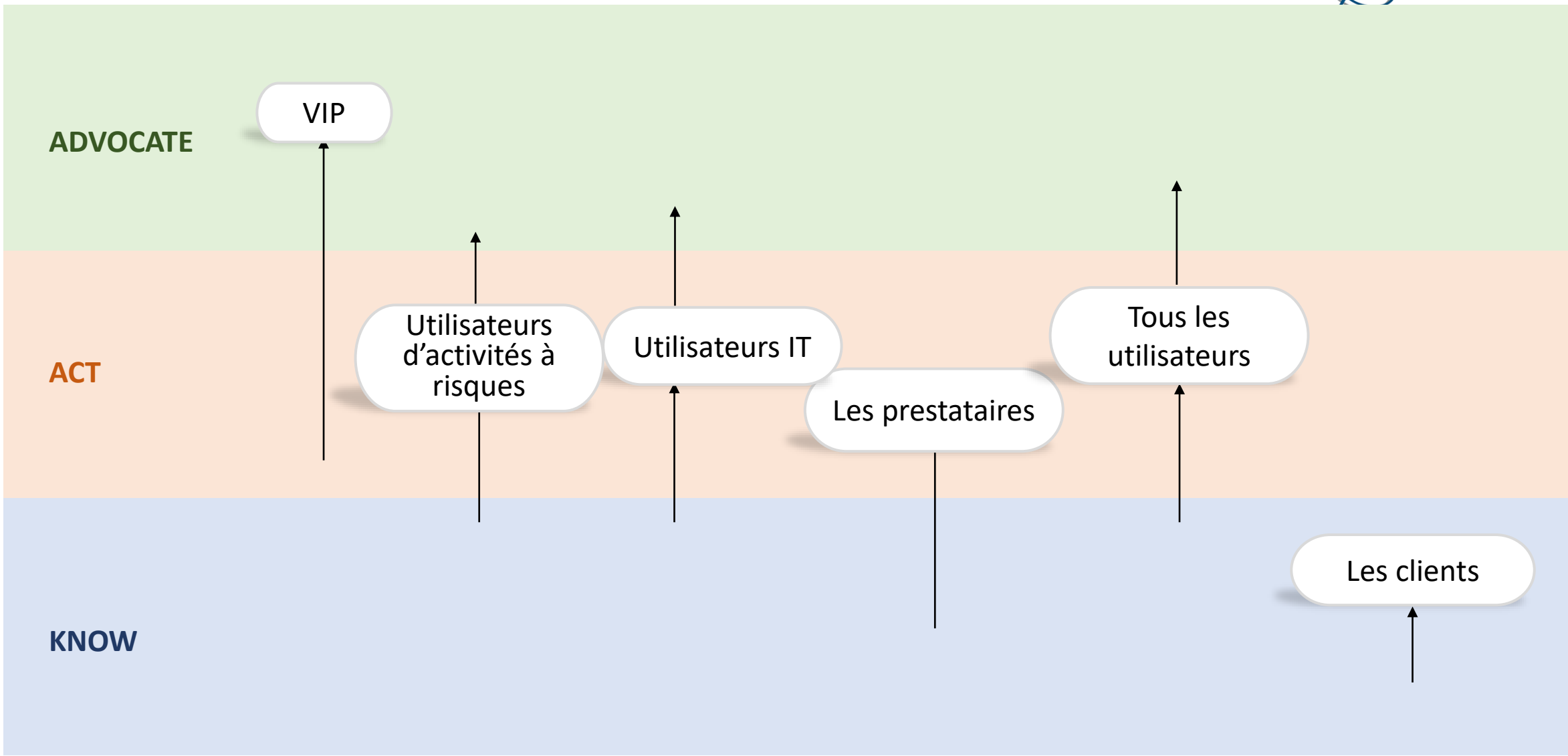
Les clients

SOME ⟷ MANY

AMBITION : VERS UNE ÉNERGIE MIEUX RÉPARTIE ?



AMBITION : VERS UNE ÉNERGIE MIEUX RÉPARTIE ?



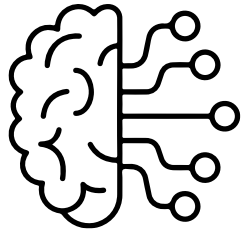
BILAN

- Beaucoup d'actions diverses mais un **engagement** des utilisateurs **difficile tant que ce n'est pas obligatoire**
- Des campagnes de **phishing** dans tous les plans d'acculturation : **concret / en condition réelle / mesurable**
- Des **investissements** (env. 2% du budget cyber) qui restent **très inférieurs** par rapport aux *solutions techniques*

Comment changer la donne ?

[hors GT]

Regagner l'attention des utilisateurs avec **des actions permanentes, variées, concrètes, mesurables et tournées vers l'entraînement**



Rééquilibre de **l'humain** vs la **technologie** ??

AMBITION : UNE CULTURE CYBER POSITIVE ?

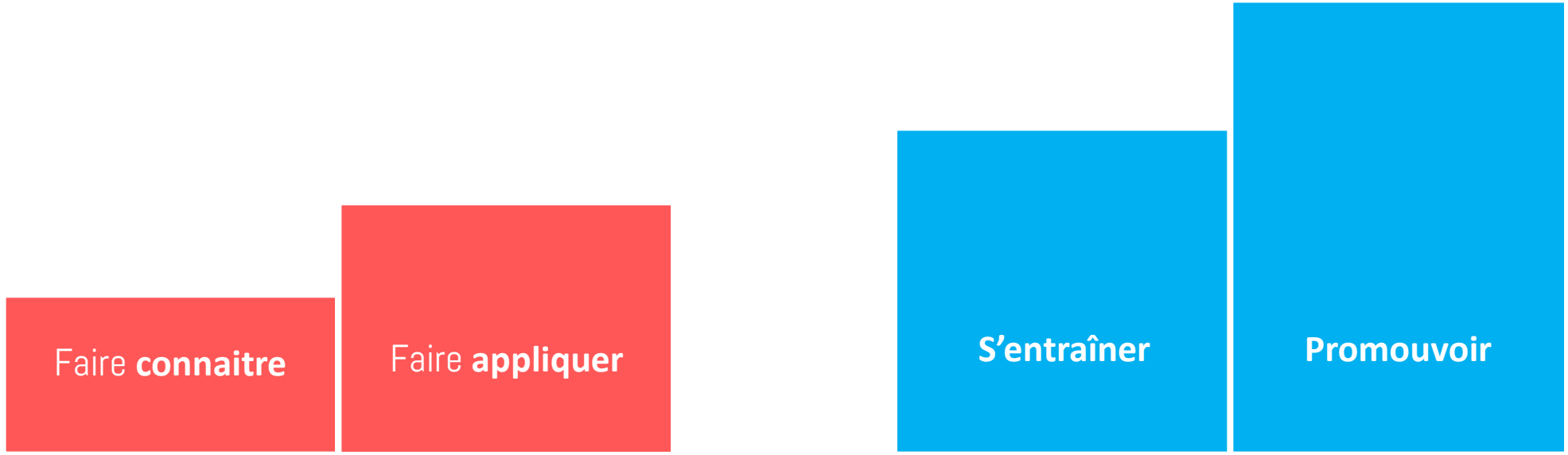
Demain ?

ÊTRE CONFORME **80%**

Focus : **participation**

20% **ENCOURAGER**

Focus : **efficacité** et **notoriété**



REGAGNEZ L'ENGAGEMENT DE VOS COLLABORATEURS

Identifier clairement les **personae** clés

+

Construire la stratégie l'acculturation Cyber autour des personae et d'un **modèle d'engagement**

+

Privilégier la **reconnaissance** et la valorisation

+

Passer d'un modèle de sujets à un modèles d'**acteurs** avec des **ambassadeurs**

+

Repenser la place des solutions par **niveau de disruptivité** et par pertinence d'adressage des personae

=

De la sensibilisation à l'acculturation Cyber

Forum des Compétences

avec

ERIUM