

Sensiwave ETI

Une démarche de
sensibilisation cybersécurité
conçue pour les ETI



PARTIE 1

ETI, un contexte particulier

En termes de cybersécurité, une ETI, vit une réalité particulière :

- ✓ Temps RSSI compté, des effectifs moindres que dans les grandes entreprises
- ✓ Peu ou pas de ressources dédiées à la sensibilisation
- ✓ Equipe RSSI en général sans compétences en pédagogie
- ✓ Une pression réglementaire qui monte (NIS2)

Le vrai problème des ETI n'est pas de sensibiliser.

C'est de réussir à le faire... malgré leurs contraintes.

- ✓ L'ETI sait qu'elle est une cible (souvent plus vulnérable)
- ✓ Elle n'a pas les moyens d'un CAC40
- ✓ Elle doit obtenir des résultats probants avec un vrai impact sur les comportements de ses collaborateurs



IMPACT NIS2

- Pas de contenus ou de thématiques particulières
- Stipule que la sensibilisation des utilisateurs est obligatoire
- Les thématiques de base (protection de l'information, mot de passe, phishing, ingénierie sociale, codes malveillants, mobilité, etc) auxquelles viennent s'ajouter au fur et à mesure des sujets plus avancés (*clickfix*, signalement des événements, *shadow IT*, *quishing*, *deep fakes*, etc.).

› Le devoir de diligence

- En revanche NIS2 apporte des exigences nouvelles sur ce qu'il convient de faire et sur la façon d'en évaluer le niveau et les résultats obtenus.
- NIS2 introduit ce qu'on pourrait appeler un devoir de diligence. Le devoir de diligence repose sur une logique simple : une entité ne peut pas se contenter de faire le minimum, histoire de cocher une case. Elle doit faire ce qu'un acteur raisonnable et prudent ferait dans la même situation.

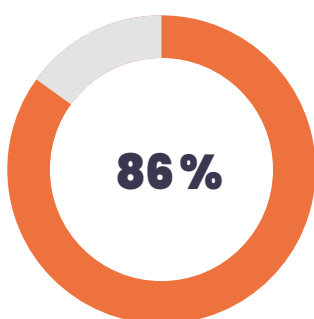
› Le RGPD comme précédent

La CNIL et ses homologues européens ont déjà sanctionné des organisations non pas parce qu'elles n'avaient rien fait, mais parce que ce qu'elles avaient fait était insuffisant au regard des risques et des pratiques courantes. NIS2 suivra la même logique.

› Nécessité d'une approche d'amélioration continue pour la sensibilisation avec une mesure de résultats

- Le niveau de satisfaction au regard des supports proposés
- Le niveau de montée en compétence qui indique de combien l'apprenant estime avoir progressé sur les sujets traités
- La note d'impact individuelle et collective, qui permet à chacun de donner une évaluation de la prise en comptes des bonnes pratiques, pour lui et autour de lui. A ce titre la différence d'appréciation entre ces deux mesures est assez révélatrice.

LES CHIFFRES-CLÉS



Satisfaction
des apprenants



+51 %
de progression
individuelle moyenne



7,5/10
Note d'impact



PARTIE 2

Limites des approches classiques en ETI

➤ Les retours observables dans une ETI :

- La participation est souvent **insuffisante** (priorités métier > cyber)
- Les contenus, souvent trop long, conduisent à une **mauvaise complétion** (manque de temps)
- Sans réactivation, la rétention est quasi **inexistante**
- L'application dépend davantage du **manager** que du RSSI



PARTIE 3

La "sensibilisation frugale"

C'est là que vous pouvez vraiment marquer les esprits.

➤ Principe : faire moins, mais mieux structuré

4 règles :



1. Un seul objectif prioritaire à la fois
2. 1 campagne = 1 comportement concret
3. Des formats ultra courts (contrainte ETI = temps)
4. Une activation managériale minimale mais ciblée

➤ La performance ne vient pas du volume, mais du focus

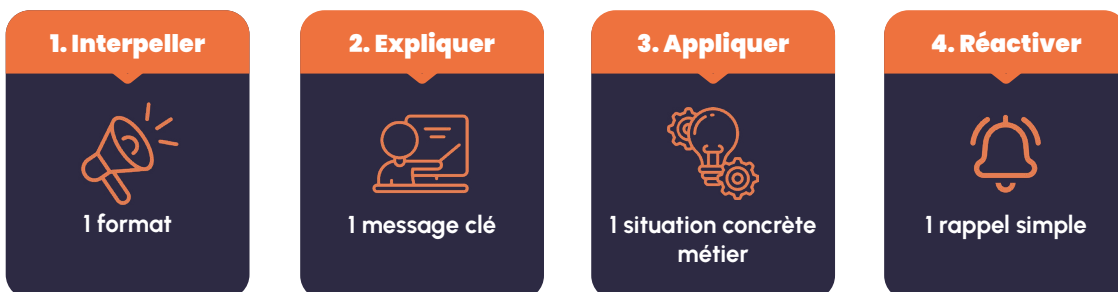
LES 4 PILIERS PÉDAGOGIQUES ADAPTÉS À LA RÉALITÉ ETI

Conscio Technologies a défini une démarche pédagogique propre à ses opérations de sensibilisation.

Elle s'appuie sur les 4 piliers :

Interpeller ➤ Expliquer ➤ Appliquer ➤ Réactiver

Pour une ETI, nous resserrons cette démarche pour une sensibilisation frugale :



➤ Résultat : une exécution simple et efficace



PARTIE 4

Comment faire avec moins

› Le modèle “1h30 par an”

- 6 à 7 campagnes maximum en privilégiant une approche multi-formats,
- 3 à 5 phishing tests
- 1 évaluation à froid, étude d'impact

› Le rôle du RSSI

Dans une ETI, le RSSI :

- n'a pas de team awareness
- n'a pas le temps d'animer

**Le RSSI n'exécute pas la sensibilisation.
Il orchestre un système qui fonctionne sans lui.**

- automatisation programmée des campagnes
- génération statistiques et rapports (RSSI, Direction, management)

› Levier essentiel : le management

- 1 message du dirigeant / an
- 1 relais managérial / campagne
- Indicateurs partagés simples :
 - Taux de participation
 - Taux de clics sur les phishings
 - Taux de signalements
 - Taux de montée en compétences
 - Note d'impact

**La culture cyber
se diffuse
par capillarité.**



PARTIE 5

En complément

Pour beaucoup d'ETI, notamment dans le secteur industriel, tous les collaborateurs n'ont pas de PC dédié. C'est pourquoi nous proposons des outils qui viennent compléter le dispositif :

- Des **affiches sectorielles et génériques** à placer dans les espaces clés
- Un **atelier animé** par équipe en présentiel autour du Cyber Mystère
- Les **cyber flashes**

PARTIE 6

Conclusion

Vous avez en charge la cybersécurité d'une ETI, avec la démarche de sensibilisation frugale pensée par Conscio Technologies, bénéficiez de la **pédagogie**, de la **culture du résultat** et de la **performance** de Sensiwave adaptées à vos contraintes.

Votre succès est le nôtre !



La sensibilisation c'est bien,
les résultats **C'EST MIEUX !**



www.conscio-technologies.com