bluesecure

GUIDE DE LECTURE

Comprendre votre Smart Report™

Ce que mesure chaque indicateur, comment le lire et quand agir, page par page.

PAGE 2
Les repères communs
Période, variations, barèmes sur 10, tendances.

PAGE 3
Général
La vue d'ensemble : risque, phishing, formation, exposition et groupes.

PAGE 4
Learning
L'avancement des formations par groupe et par module.

PAGE 5
Phishing
Les résultats des simulations d'hameçonnage et des campagnes.

PAGE 6
Datawatch et analyses
L'exposition des adresses, les blocs Analyse et Recommandations.

PAGE 7
Les bons réflexes de lecture
Pièges d'interprétation et questions fréquentes.

À qui s'adresse ce guide ? À toute personne destinataire d'un Smart Report™ : direction, managers, RH, DSI ou RSSI. Les exemples présentés sont fictifs ; votre rapport peut afficher plus ou moins de sections selon le paramétrage choisi par votre administrateur.

AVANT DE COMMENCER

Les repères communs à toutes les pages

Quatre conventions reviennent dans chaque section du rapport. Une fois ces repères en tête, chaque page se lit en quelques secondes.

1 · La période et la fréquence

Général Mensuel · 1 oct. 2026 – 31 oct. 2026

Sous chaque titre de section figure la **période couverte**. Tous les chiffres de la page portent sur cette période, et chaque variation la compare à la **période précédente de même durée** (le mois précédent pour un rapport mensuel, la semaine précédente pour un rapport hebdomadaire).

2 · Les variations

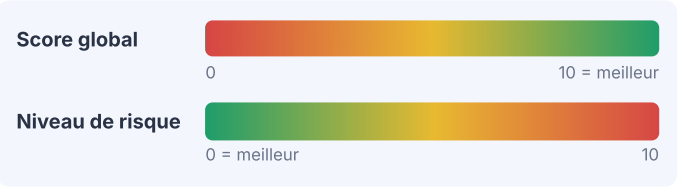
+ 12 % rouge = évolution défavorable

+ 20 % vert = évolution favorable

– = stable ou pas de comparaison possible

Le petit chiffre à droite de chaque indicateur indique l'écart avec la période précédente. **La couleur dit si c'est une bonne nouvelle**, pas le signe : une hausse du taux de phishing apparaît en rouge, une hausse du taux de formation en vert.

3 · Les deux barèmes sur 10



Les deux notes se lisent **en sens inverse** : on cherche un **score global élevé** et un **niveau de risque bas**. Le **score global** combine la progression des formations et le niveau de risque. Le **niveau de risque** traduit le comportement face aux simulations : un clic compte, une saisie d'informations ou l'envoi d'un formulaire compte davantage.

4 · Les tendances des groupes

Mauvais | Aucun changement | Nouveau

Mauvais : la situation du groupe s'est dégradée par rapport à la période précédente. **Aucun changement** : situation stable. **Nouveau** : groupe qui apparaît pour la première fois dans le rapport, sans historique pour comparer. Une tendance porte sur l'évolution, pas sur le niveau : un groupe bien noté peut afficher « Mauvais » s'il a reculé.

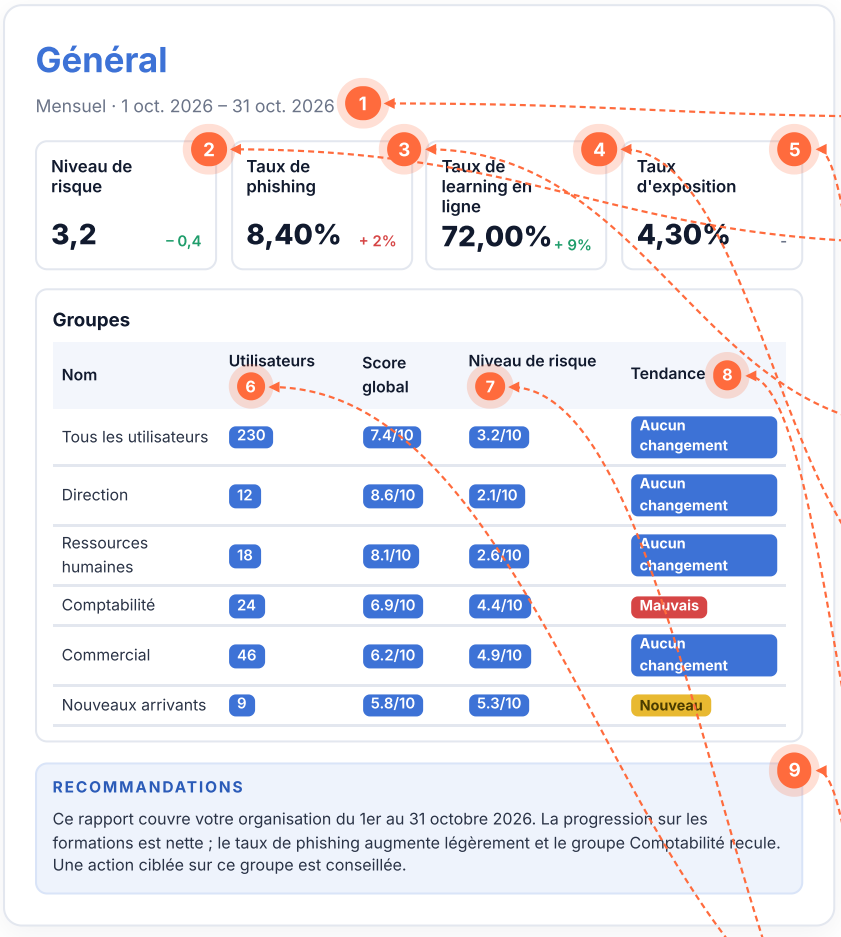
Le principe à garder en tête

- → Le rapport s'arrête au **groupe** (service, entité, site) : aucun résultat individuel n'y figure.
- → Sur un petit groupe, **une seule personne fait varier fortement** les pourcentages.
- → Une **tendance sur plusieurs rapports** dit plus qu'un chiffre isolé.
- → Les blocs **Analyse** et **Recommandations** sont rédigés automatiquement à partir des chiffres.

SECTION 1

Général : la vue d'ensemble

La première page résume la situation de votre organisation en quatre chiffres, puis la détaille groupe par groupe. C'est la page à lire en priorité.



1 Période couverte
Fréquence et dates ; comparaison avec la période précédente.

2 Niveau de risque
Note de 0 à 10 issue des simulations : un clic compte, une saisie ou un formulaire envoyé compte davantage.
Plus c'est bas, mieux c'est

3 Taux de phishing
Part des simulations envoyées ayant abouti à une compromission (page 5).
Plus c'est bas, mieux c'est

4 Taux de learning en ligne
Part des utilisateurs en formation ayant terminé leurs formations (page 4).
Plus c'est haut, mieux c'est

5 Taux d'exposition
Part des utilisateurs dont l'adresse figure dans une fuite. Exposition subie, pas un comportement.
Plus c'est bas, mieux c'est

8 Tendance
Évolution du groupe depuis la période précédente.

6 Utilisateurs
Taille du groupe. À 0, les notes ne sont pas exploitables.

7 Score global et niveau de risque
Score global : plus haut = mieux. Risque : plus bas = mieux.

9 Recommandations
Synthèse automatique : une piste, pas un diagnostic.

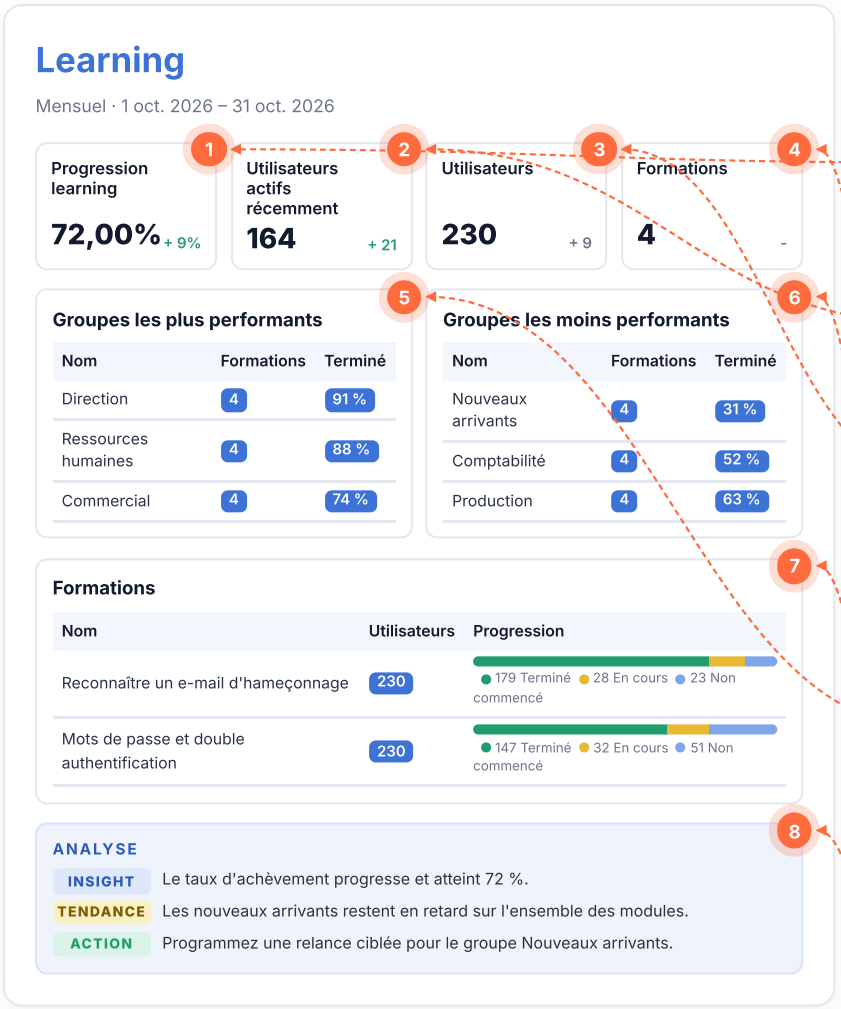
Comment l'exploiter

- Commencez par les **4 chiffres du haut** et leur couleur de variation.
- Comparez un groupe à la ligne **« Tous les utilisateurs »**, qui sert de moyenne.
- Dans le tableau, repérez les groupes en **« Mauvais »** et ceux au **risque le plus haut**.
- Un groupe **« Nouveau »** se juge sur ses prochains rapports, pas sur le premier.

SECTION 2

Learning : l'avancement des formations

Cette page montre si les formations assignées sont suivies et terminées, par qui et sur quels modules.



1 Progression learning
Part des utilisateurs en formation ayant terminé leurs formations, sur la période.
Plus c'est haut, mieux c'est

2 Utilisateurs actifs récemment
Utilisateurs actifs au cours des 92 derniers jours, quelle que soit la période du rapport.

3 Utilisateurs
Personnes couvertes par le rapport ; la variation reflète arrivées et départs.

4 Formations
Nombre de formations proposées au périmètre du rapport.

5 Groupes les plus performants
Les 3 groupes au taux d'achèvement le plus élevé.

6 Groupes les moins performants
Les 3 groupes les plus en retard : là où une relance aura le plus d'effet.

7 Formations
Par module : inscrits, puis la barre Terminé / En cours / Non commencé.

8 Analyse
Généré automatiquement : un constat, une évolution, une piste d'action.

Comment l'exploiter

- → Une forte part de **« Non commencé »** appelle une relance ou une communication interne.
- → Un fort taux d'achèvement avec **peu d'actifs** signale souvent un petit nombre de formations assignées.
- → Beaucoup d'**« En cours »** : rappelez la date limite plutôt que le contenu.
- → Les **nouveaux arrivants** apparaissent naturellement en bas du classement les premières semaines.

SECTION 3

Phishing : les simulations d'hameçonnage

Cette page restitue les réactions des collaborateurs aux faux e-mails envoyés lors des campagnes de simulation : qui clique, qui va plus loin, qui signale.



1 Envoi
E-mails de simulation envoyés sur la période. **Campagnes** : campagnes actives sur la période.

2 Taux de phishing
Utilisateurs phishés ÷ simulations envoyées, sur la période.
Plus c'est bas, mieux c'est

3 Taux de signalement
Utilisateurs ayant signalé ÷ utilisateurs ciblés. C'est le réflexe attendu.
Plus c'est haut, mieux c'est

4 Que s'est-il passé ?
Jour par jour, **envois**, **clics** et **phishés**. Les pics suivent les lancements.

5 Appareils
Répartition des interactions : ordinateur, mobile, tablette, inconnu.

6 Groupes les plus / moins exposés
Groupes qui réagissent le plus, et le moins, aux simulations.

7 Détail par campagne
Clics : lien ouvert. **Phishé** : au moins une action retenue comme compromission (par défaut : informations, mot de passe ou formulaire envoyés). **Signalé** : déclaré suspect.

8 Statut
active : campagne en cours. *draft* : brouillon, pas encore envoyé.

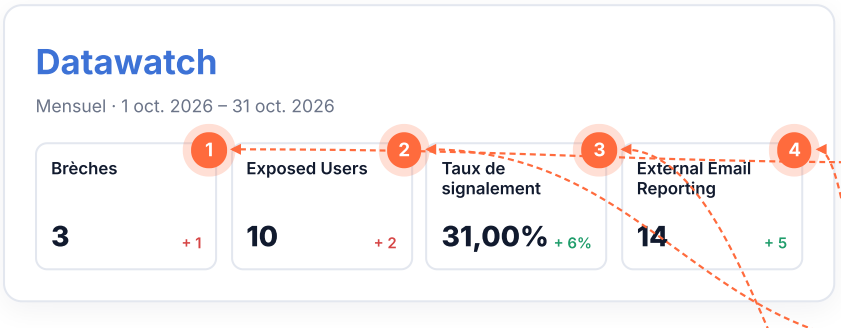
Comment l'exploiter

- Regardez **phishing et signalement ensemble** : idéalement le premier baisse et le second monte.
- Comparez des campagnes **de même difficulté** : un scénario plus crédible fait mécaniquement monter le taux.
- L'écart **Clics → Phishé** mesure la profondeur : un clic seul est moins préoccupant qu'une saisie.
- Ce qui compte comme « phishé » se **règle pour chaque campagne** : avant de comparer deux campagnes, demandez à votre administrateur.

SECTION 4

Datawatch : l'exposition des adresses

Datawatch (DataWatch™) surveille le web et le dark web pour repérer les adresses professionnelles de votre organisation présentes dans des fuites de données. Il mesure une **exposition subie**, jamais un comportement.



1 Brèches
Fuites de données détectées contenant au moins une adresse de votre organisation.
Plus c'est bas, mieux c'est

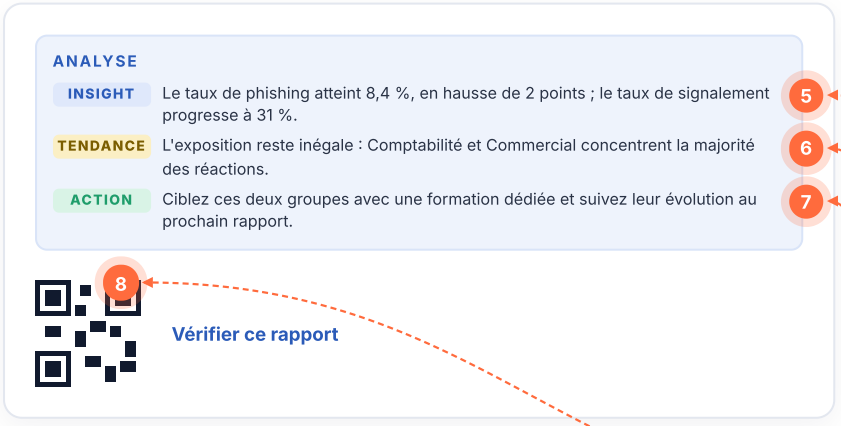
2 Exposed Users (utilisateurs exposés)
Nombre de collaborateurs dont l'adresse figure dans ces fuites.
Plus c'est bas, mieux c'est

3 Taux de signalement
Part des e-mails suspects signalés par les collaborateurs.
Plus c'est haut, mieux c'est

4 External Email Reporting
Incidents remontés par les collaborateurs : e-mail ou SMS suspect, URL suspecte, compte compromis, incident de sécurité.
Plus c'est haut, mieux c'est

Les blocs rédigés automatiquement

Chaque section peut se terminer par un encadré de texte rédigé automatiquement à partir des chiffres de la page.



5 Insight
Le constat principal de la période, chiffres à l'appui.

6 Tendance
Ce qui évolue, ou ce qui se concentre sur certains groupes.

7 Action
Une piste concrète. À arbitrer avec votre administrateur BlueSecure : c'est une suggestion, pas une consigne.

8 QR code de vérification
En dernière page : il permet de vérifier que le rapport est authentique et n'a pas été modifié.

POUR CONCLURE

Les bons réflexes de lecture

Cinq habitudes pour tirer du rapport des décisions fiables plutôt que des conclusions hâtives.

1. **Suivre la trajectoire, pas la photo.** Un chiffre isolé dit peu de chose. Comparez trois rapports successifs avant de conclure qu'un groupe progresse ou recule.

2. **Rapporter chaque pourcentage à la taille du groupe.** Dans un groupe de 4 personnes, une seule réaction fait passer le taux de phishing de 0 à 25 %. Dans un groupe de 200, il faut 50 personnes.

3. **Lire les indicateurs par paires.** Phishing avec signalement, achèvement avec utilisateurs actifs, exposition avec comportement : c'est leur combinaison qui raconte la situation.

4. **Distinguer exposition et comportement.** Une adresse retrouvée dans une fuite n'est pas une faute du collaborateur : cela signifie seulement qu'il risque de recevoir davantage de tentatives d'hameçonnage.

5. **Transformer le constat en action ciblée.** Relance de formation, campagne adaptée, message d'équipe : une action par groupe concerné, puis vérification au rapport suivant.

Questions fréquentes

Pourquoi des groupes affichent-ils 0 utilisateur ?

Ce sont des groupes créés dans la plateforme mais encore vides. Leurs notes ne reflètent aucune activité réelle : ignorez-les et signalez-les à votre administrateur pour qu'il les retire du rapport.

Puis-je voir les résultats d'une personne ?

Non. Le rapport s'arrête au groupe. C'est un choix de conception : il est diffusé par e-mail et ne doit permettre aucun classement individuel.

Que faire après avoir lu le rapport ?

Repérez un ou deux groupes à accompagner, partagez le constat avec les managers concernés et convenez avec votre administrateur d'une action : relance de formation, campagne ciblée, message d'équipe.

Taux de phishing ou niveau de risque : quelle différence ?

Le taux de phishing mesure le résultat des campagnes. Le niveau de risque est propre à chaque utilisateur et tient compte de la profondeur de ses actions : il est ensuite moyenné par groupe.

Mon rapport n'a pas toutes ces sections. Est-ce normal ?

Oui. L'administrateur choisit les sections, les groupes, les destinataires et la fréquence du rapport. Chacun ne reçoit que ce qui le concerne.

Une question sur votre rapport ? Adressez-vous à l'administrateur BlueSecure de votre organisation : il peut ajuster les groupes, les sections et la fréquence d'envoi, et relayer vos questions à votre chargée de compte BlueSecure.