bluesecure

NEWSLETTER

Nouveautés septembre 2026

Vos actualités BlueSecure en 3 minutes.

01
Learning
Les nouveaux modules disponibles.

02
Plateforme
Les nouvelles fonctionnalités.

03
Phishing
Les nouveaux scénarios.

01 — LEARNING

Les nouveaux learnings disponibles

4 MIN

Donnée personnelle & RGPD

Un micro-learning pour comprendre ce qu'est une donnée personnelle, ce que le RGPD encadre et pourquoi cela concerne toutes les organisations. La formation présente les 3 réflexes essentiels avant de manipuler une donnée : vérifier son droit d'utilisation, s'assurer de sa nécessité et veiller à sa protection.

Suivre le learning

4 MIN

Supply Chain Attack

Un micro-learning pour comprendre les attaques de la chaîne d'approvisionnement : leur fonctionnement, pourquoi elles peuvent contourner les défenses classiques et comment elles exploitent la confiance envers les fournisseurs. La formation présente notamment le cas SolarWinds et vous apprend les 4 réflexes essentiels pour limiter les risques au quotidien.

Suivre le learning

02 — PLATEFORME

Les nouvelles fonctionnalités

Ces évolutions sont déjà disponibles dans votre espace d'administration.

01 Rapports automatiques

Un nouveau module vous permet de créer et de planifier vos rapports PDF sans intervention manuelle.

- Envoi périodique par e-mail ou envoi immédiat.
- Choix des destinataires, des populations et des indicateurs.
- Prévisualisation avant envoi.
- Synthèses et recommandations assistées par IA.

02 Trois nouveaux rôles d'administration

Learning Manager, Phishing Manager et Studio Editor : vous déléguez la gestion d'un périmètre précis sans ouvrir l'accès à toute la plateforme.

03 Suivi des quiz par apprenant

Dans les campagnes learning, vous consultez désormais les réponses de chaque apprenant, ainsi que ses tentatives précédentes. Également, il n'est plus possible de repasser un quiz deux fois, sauf si vous l'autorisez en tant qu'administrateur.

04 Groupes automatiques par score de quiz

Un nouveau filtre classe les utilisateurs d'un groupe automatique selon leur résultat à un quiz. Vous pouvez ainsi lancer une campagne d'auto-évaluation, puis répartir vos populations par niveau et adapter les parcours.

05 Scénarios de phishing traduits automatiquement

Par campagne, chaque scénario est envoyé dans la langue de l'utilisateur. Une seule campagne suffit pour couvrir des équipes multilingues.

06 Nouvelles colonnes utilisateurs

Division, Sous-Division et Direction s'ajoutent aux attributs utilisateurs, pour refléter les organigrammes complexes et cibler ou filtrer vos campagnes à ce niveau.

Découvrir les nouveautés

03 — PHISHING

Les nouveaux scénarios disponibles

Douze scénarios s'ajoutent à la bibliothèque, prêts à être intégrés à vos campagnes.

BAMBOOHR
Expiration congés

AMAZON
Connexion suspecte

AGICAP
Invitation à rejoindre

ARMADO
Demande de mission

DEEZER
Tentatives de connexion

TOMORRO
Signature nécessaire

AIRTABLE
Nouveau commentaire

CALENDLY
Rapport de sécurité

INSTAGRAM
Politique de confidentialité

LINKEDIN
Merci de votre inscription

KEEPER
Récupérer mon compte

GITHUB
Confirmer votre adresse mail

Tester les scénarios

CAS D'ATTAQUE

SFR : un outil interne, deux millions de lignes exposées

Le 20 août 2026, SFR a confirmé une fuite de données touchant ses abonnés fibre. L'incident, détecté le 2 juillet par ses équipes de sécurité, visait un outil interne de gestion et d'analyse des raccordements fibre. Les données temporairement accessibles comprennent des adresses postales, des adresses e-mail et des numéros de téléphone. Les mots de passe et les données bancaires ne sont pas concernés.

L'opérateur a désactivé le compte utilisé pour accéder à l'outil, bloqué les adresses IP à l'origine de l'accès, notifié la CNIL et déposé plainte. Une revendication publiée mi-juillet sur un forum cybercriminel évoque un portail interne nommé NOVA et une extraction de plus de 2,1 millions de lignes, volume que SFR ne reprend pas dans sa notification.

À RETENIR

- Un message inattendu ? Prenez le temps de vérifier avant de cliquer ou de répondre.
- Une demande urgente ou inhabituelle ? Méfiez-vous, surtout si elle vous pousse à agir rapidement.
- Un lien dans un e-mail ? Passez directement par le site ou l'application officielle plutôt que de cliquer.
- Un expéditeur connu ne garantit pas un message légitime. Son compte peut avoir été compromis.
- Une pièce jointe inattendue ? Ne l'ouvrez pas sans vérifier son origine.
- Un doute ? Signalez le message à votre équipe informatique. Mieux vaut signaler un faux positif que laisser passer une attaque.

SOURCES : LE FIGARO, FRENCH BREACHES — AOÛT 2026

La cybersécurité ne peut plus se limiter à des outils techniques : elle repose aussi sur des gestes simples du quotidien et une culture de la vigilance partagée.

Restez informé(e), restez protégé(e).

Un problème technique ?

Veuillez contacter notre support. Pour toute demande fonctionnelle, je vous invite à contacter votre **Customer Success Manager**, qui vous assistera dans l'utilisation de notre solution.

bluesecure LINKEDIN X

@BlueSecure2026, La Défense, PARIS, FRANCE

Se désabonner Gérer les préférences