



1

3 nouveaux micro-learning :
Qu'est-ce que la cybersécurité,
Comprendre l'OSINT, Sécuriser sa
boîte e-mail.

2

Événements à ne pas manquer :
Hactiv'Summit, IT &
Cybersecurity One to One
Meetings, Cas d'OR de la
Cybersécurité

3

Nouvelles fonctionnalités sur la
plateforme :
Nouvel Éditeur IA et Groupes
dynamiques

Nouveaux micro-learning :

Découvrez nos nouveaux micro-learnings, chacun dédié à une thématique clé : **les bases de la cybersécurité** pour comprendre les principes essentiels de sécurité des SI, **l'OSINT** afin d'identifier les risques liés aux informations publiques et mieux protéger ses données en ligne, **la sécurisation de la messagerie** pour renforcer sa première ligne de défense contre le phishing et les tentatives d'usurpation ; trois modules complémentaires.

Tester les nouveautés

Venez nous rencontrer

Nous serons présents lors de plusieurs événements clés de la cybersécurité en mars 2026 :

- **Hactiv'Summit** – 12 & 13 mars à Chantilly
- **IT & Cybersecurity One to One Meetings** – 17 au 19 mars à Cannes
- **Cas d'OR de la Cybersécurité** – 17 mars à Paris

Ces rendez-vous incontournables sont l'occasion idéale pour échanger sur les enjeux actuels de la cybersécurité, partager notre expertise et rencontrer les acteurs

majeurs du secteur.

Voir la vidéo

Découvrez nos nouvelles fonctionnalités sur la plateforme

Nouvel Éditeur IA

Notre éditeur intelligent transforme la création de campagnes en un jeu d'enfant :

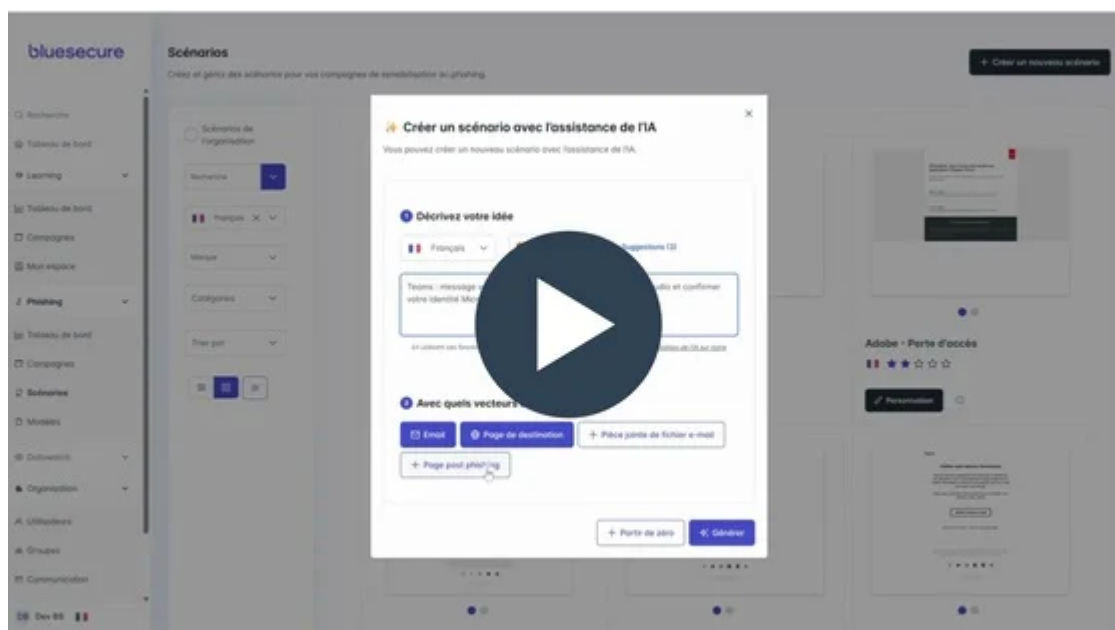
- **Générez vos contenus automatiquement** : scénarios et modèles pour e-mails, pages de connexion, fichiers, pages pédagogiques post-phishing et contenus de SMS.
- **Optimisation IA pour vos envois** : suggestions pour l'adresse e-mail de l'expéditeur, l'objet, le nom de l'expéditeur et la marque, afin de maximiser l'impact de vos messages.
- **Page post-phishing automatique** : bénéficiez d'un template par défaut pour vos pages de redirection, simplifiant la configuration de vos scénarios et affichant les caractéristiques du scénario envoyé : e-mail expéditeur et lien affiché au survol.

Groupes dynamiques maintenant disponibles

Gérez vos audiences plus facilement avec les groupes dynamiques. Cette fonctionnalité permet de **regrouper automatiquement vos utilisateurs** dans des groupes en fonction de **critères spécifiques paramétrables**, comme par exemple : les utilisateurs hameçonnés sur les 30 derniers jours et les utilisateurs ayant un score de risque élevé du fait de leur hameçonnage récurrent...

Ces groupes sont **mis à jour en temps réel** en fonction des critères choisis. Ils peuvent être utilisés pour **recibler les utilisateurs** avec de nouvelles campagnes de simulation de phishing ou les inviter à suivre une sensibilisation en e-learning.

Découvrir les fonctionnalités



[En savoir plus](#)

Un problème technique ?

Veuillez contacter notre support. Pour toutes demandes fonctionnelles, n'hésitez pas à contacter votre **Customer Success Manager** qui vous **assistera** dans l'utilisation de notre solution.



Cliquez [ici](#) pour consulter les newsletters précédentes. Pour rester informé sur l'actualité cyber et sur les nouveautés BlueSecure, suivez-nous sur les réseaux sociaux.

Cas d'attaque : fuite de données bancaires sur Ficoba — plus d'un million de Français concernés

La base Ficoba, qui recense les comptes bancaires des particuliers et entreprises en France, a été la cible d'une fuite massive de données. Cet incident a exposé les informations bancaires d'un nombre important de français, suscitant des inquiétudes

sur les risques de fraude et d'usurpation d'identité.

À l'origine de l'incident : des données sensibles concernant plus d'un million de comptes ont été compromises, incluant noms, adresses et détails bancaires. La faille exacte n'a pas été rendue publique, mais cet événement met en évidence que même des bases administratives critiques peuvent devenir des cibles privilégiées pour des cybercriminels.

Les points clés à retenir :

- Plus d'un million de comptes bancaires français exposés
- Données sensibles compromises : identités, adresses et informations financières
- Risque accru de fraude bancaire et usurpation d'identité

Rappel des bonnes pratiques :

- Vérifier régulièrement vos comptes bancaires et signaler toute opération suspecte
- Ne jamais partager vos informations bancaires par email ou téléphone
- Activer les alertes SMS ou notifications sur vos comptes
- Être vigilant face aux tentatives de phishing ciblées suite à la fuite

Cette fuite rappelle que la protection des données financières reste un enjeu majeur. La vigilance est indispensable pour se prémunir contre les risques de fraude.

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).

Une question ? N'hésitez pas à contacter votre service informatique.

