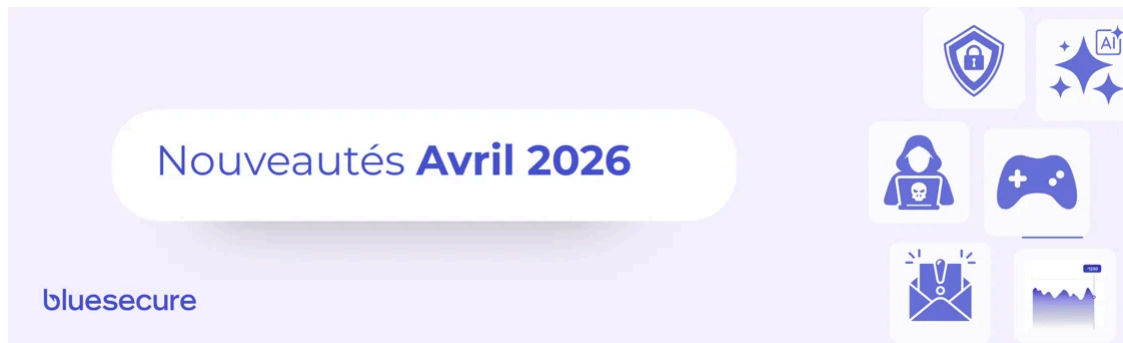




- 1**
Nouvelles Fonctionnalités :
Chatbot intégré à Teams & amélioration de l'interface
- 2**
Événements:
Notre présence sur les grands rendez-vous cybersécurité
- 3**
Campagne de phishing:
Nouveaux scénarios

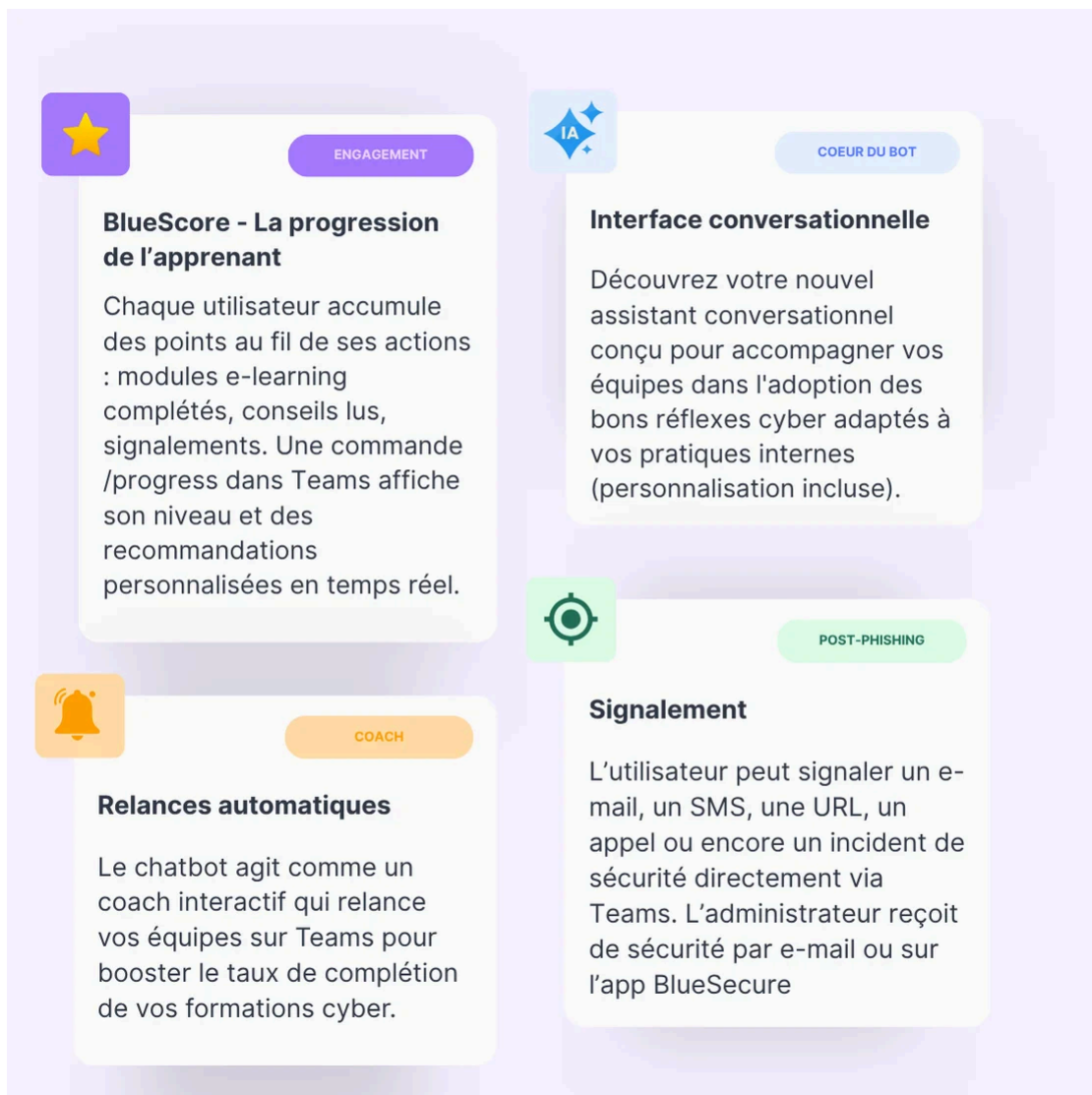
Notre Chatbot disponible sur Teams



L'Assistant AI Bluesecure

Bienvenue ! Je suis L'Assistant AI Bluesecure !

15:17



Vous souhaitez devenir client bêta test ? Rapprochez-vous de votre CSM

En savoir plus

Nouveaux scénarios de phishing :

- UpDéjeuner - Réinitialisation Mot De Passe
- Calendly - Invitation
- Salesforce - Compte Suspendu
- Expensya - Invitation à rejoindre
- Workday - Nouvelle connexion
- Okta - Compte suspendu
- Notion - Nouveau commentaire
- Alan - Compte suspendu
- Stripe - Mise à jour du compte Bancaire
- Pennylane - Connexion suspecte
- Airbnb - Modification de mot de passe

Créer ma campagne





Événements clés

Nous avons participé à plusieurs événements majeurs de l'écosystème cybersécurité et digital, dont le **Forum InCyber Europe**, **'Hacktiv' Summit** et les **One to One Meetings IT & Cybersecurity**, des rendez-vous riches en échanges autour des enjeux et innovations du secteur. Nous avons également eu l'honneur d'être distingués aux **Cas d'Or** avec un lauréat dans la catégorie « Sensibilisation à la cybersécurité » pour notre dispositif CyberGames. Une belle reconnaissance qui valorise notre engagement à rendre la cybersécurité plus accessible, pédagogique et engageante.

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 médicales chez Cegedim Santé — 15 millions de Français concernés

La société **Cegedim Santé**, spécialisée dans les logiciels et services pour le secteur médical, a été la cible d'une **cyberattaque majeure**. Cet incident a exposé les données personnelles et médicales de **15 millions de Français**, suscitant de fortes inquiétudes sur la protection des informations sensibles et les risques de fraude ou d'usurpation d'identité.

À l'origine de l'incident : des données comprenant **noms, adresses, numéros de sécurité sociale et informations médicales** ont été compromises. La méthode exacte utilisée par les cybercriminels n'a pas été rendue publique, mais l'attaque souligne que même les acteurs du secteur de la santé peuvent devenir des cibles privilégiées pour des hackers.

Les points clés à retenir :

- 15 millions de Français touchés par la fuite de données
- Informations sensibles compromises : identités, coordonnées, numéros de sécurité sociale et données médicales
- Risque accru de fraude, usurpation d'identité et exploitation des données médicales

Rappel des bonnes pratiques :

- Méfiez-vous des e-mails suspects : Vérifiez toujours l'adresse de l'expéditeur et soyez prudent(e) avec les liens et pièces jointes.
- Utilisez des mots de passe complexes: Privilégiez des phrases longues ou des générateurs de mots de passe et activez l'authentification à deux facteurs.
- Mettez vos logiciels à jour régulièrement : Les mises à jour corrigent des failles de sécurité exploitées par les cybercriminels.
- Vérifiez régulièrement vos comptes et dossiers : si vous constatez une activité inhabituelle (changement de données, accès que vous ne reconnaissez pas), signalez-le immédiatement.
- Soyez vigilant face à l'ingénierie sociale : Les hackers jouent sur vos émotions (urgence, peur, curiosité) pour vous inciter à divulguer des informations sensibles.

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.

