

Décembre 2025

Retour sur l'année 2025 avec bluesecure



2025 a été marqué par de **grands changements** et de **belles réussites** pour Bluesecure.

Retour sur l'année 2025

500K

Utilisateurs
sensibilisés



+20%

Taux
d'engagement
des utilisateurs



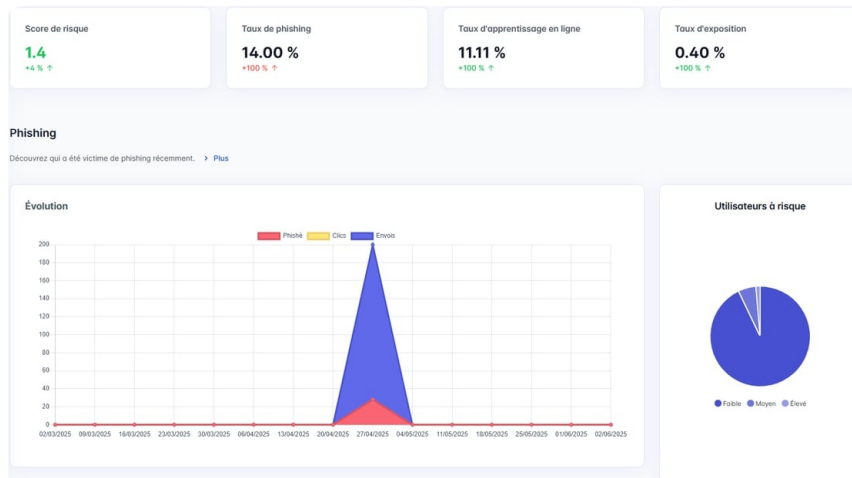
+70

Contenus
engageants



Une expérience utilisateur totalement repensée

Cette année, nous avons **redessiné Bluesecure de A à Z** pour rendre votre navigation plus fluide et intuitive. La nouvelle interface modernisée vous permet de suivre vos résultats plus facilement, d'accéder à vos parcours personnalisés et de profiter de tableaux de bord interactifs pour un suivi précis des scores et performances.



Mon espace

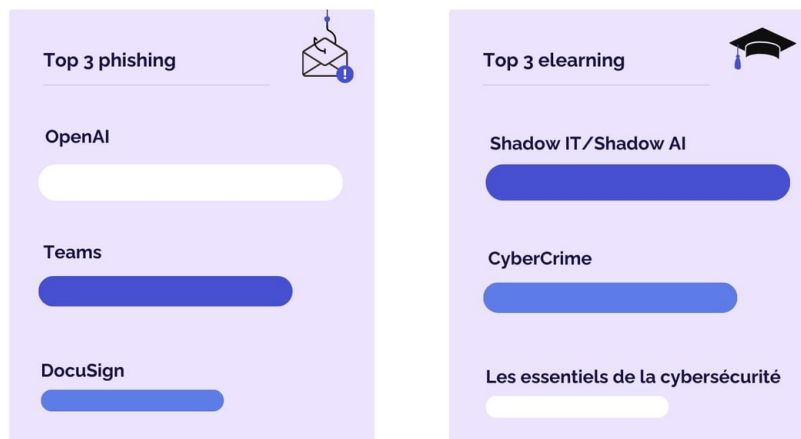
Événements marquants

- **FIC** : échanges passionnants et démonstration de nos **3 environnements VR**, déployables lors d'ateliers de sensibilisation en présentiel
- **Assises de Monaco** : découverte de **BlackOut**, notre futur jeu de simulation de gestion de crise cyber et rencontres inspirantes
- **Hacktiv Summit** : présentation de notre jeu de société plateau **CyberCrime**, pour une expérience ludique et engageante
- **Je Sensibilise** : participation à la table ronde "Mois de la cyber : on y va ou pas ?", pour partager nos perspectives et mettre en avant les différents ateliers possibles à mettre en place
- **Cybernight** : nous remportons le Coup de Cœur du Jury 2025 avec

notre jeu de gestion de crise **BlackOut - 20 minutes pour reprendre le contrôle** prochainement disponible



🏆 Top 3 de l'année : ce que vous avez le plus utilisé



Merci à tous pour **votre confiance** et **votre engagement** ! Ensemble, nous préparons une année **2026 ambitieuse**, avec de nouveaux projets et fonctionnalités pour **renforcer la cybersécurité** et la sensibilisation.

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.



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 : Asahi victime d'un rançongiciel — paralysie de la production et risque de pénurie

Le brasseur japonais Asahi Group Holdings a été la cible d'un **rançongiciel massif** qui a paralysé une grande partie de ses systèmes informatiques, impactant la production et la distribution de ses bières emblématiques. L'attaque a touché les **30 usines japonaises**, entraînant des retards dans la prise de commandes, l'expédition, les services clients et menaçant de provoquer une pénurie de bière sur le marché japonais.

À l'origine de l'incident : un groupe de cybercriminels surnommé **Qilin** a pénétré les systèmes d'Asahi, exfiltrant environ **27 Go de données** (près de 9 300 fichiers) et chiffrant les machines afin de réclamer un rançon. La faille exacte permettant l'intrusion n'a pas été rendue publique, mais ce type d'attaque montre que **les systèmes IT et les processus opérationnels sont étroitement liés**, et qu'une vulnérabilité peut rapidement paralyser toute une chaîne logistique.

 Les points clés à retenir :

- Plus de **30 usines japonaises affectées**
- **27 Go de données exfiltrées** par le groupe Qilin
- Risque de **pénurie de bière** sur le marché japonais
- Une illustration concrète de **l'impact opérationnel et économique** d'une cyberattaque industriel

 **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.

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.