WAVESTONE

Bilan de la sécurité des sites web en France

Analyse des 1029 failles identifiées dans les sites des grandes entreprises…

Yann FILLIAT
yann.filliat@wavestone.com
Responsable de l'offre Audit de Sécurité

Gérôme BILLOIS
gerome.billois@wavestone.com
Senior Manager
@gbillois

Dans un monde où la capacité à se transformer est la clé du succès,
nous éclairons et guidons nos clients dans leurs décisions les plus stratégiques

Des clients leaders
dans leur secteur

2 500 collaborateurs
sur 4 continents

Parmi les leaders du conseil
indépendant en Europe,
n°1 en France

Paris | London | New York | Hong Kong | Singapore* | Dubai*
Brussels | Luxembourg | Geneva | Casablanca
Lyon | Marseille | Nantes

* Partenariats stratégiques

Réussir sa **transformation numérique** grâce à la **confiance numérique**

400+
Experts & Consultants Cybersécurité

1,000+
Missions par an dans plus de **20** pays

Nos clients
COMEX, Métier, CDO, CIO, CISO, BCM

UNE EXPERTISE EPROUVEE

- Stratégie et Conformité
- Transformation métier sécurisée
- Architecture et programme sécurité
- Identité, Fraude et Services de Confiance
- Tests d'intrusion & Réponse à incident
- Continuité d'Activité & Résilience

NOS DIFFERENCIATEURS

- Connaissance des risques métier
- Méthodologie AMT pour les schémas directeurs
- Radars Innovation et Startups
- CERT-W

Wavestone : un retour d'expérience unique sur les audits de sécurité

Périmètres d'interventions variés : sites web, tests d'intrusion physiques, ingénierie sociale, revue de configuration, de code, etc.

Essentiellement des très grandes entreprises françaises, présentes sur le marché national ou international

Banque/Assurance, Distribution, Médical, Énergie, Service, Télécom, Transport et Institutions Publiques

Un benchmark des failles des sites web

Tests d'intrusion de sites web réalisés entre juin 2015 et juin 2016 sur 84 sites sur Internet et 43 sites sur des réseaux privés d'entreprise.

De multiples secteurs d'activités : banque, santé, ministère, énergie, services, télécom et transport.

Une confidentialité préservée : les données de nos clients sont anonymisées, l'analyse est uniquement statistique.

Des tests respectant la même méthodologie, pour des résultats comparables.

Des failles incluant le contrôle d'accès, la qualité du chiffrement, la diffusion d'informations techniques superflues, le traitement des communications, etc.

Malgré les efforts d'anticipation consentis dans les entreprises, les tests sont généralement réalisés sur des versions déjà en production.

3 constats marquants sur la sécurité web

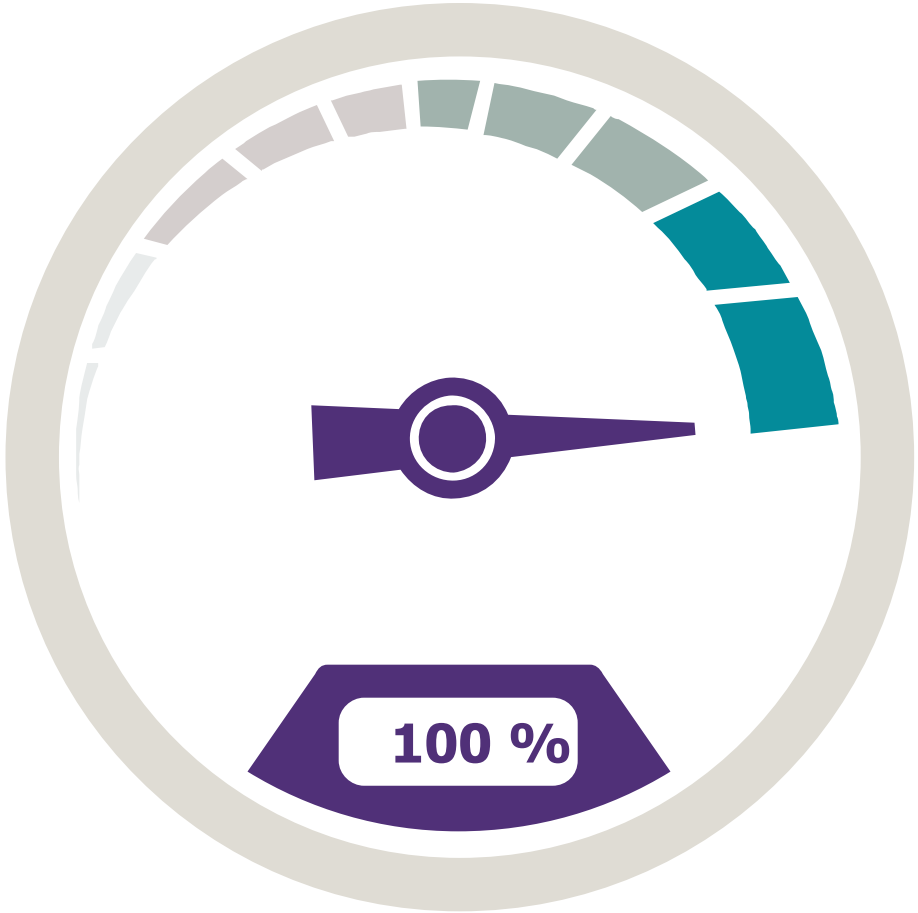
1. **100%** des sites web testés sont vulnérables, et ceci quel que soit le contexte ou le secteur
2. **50 %** des sites accessibles à tous depuis Internet ont au moins une faille grave
3. **75 %** des sites web internes réservés aux collaborateurs ont au moins une faille grave

4 zones à risque lors de la conception d'un site web

parmi le TOP 10 Wavestone des failles les plus rencontrées

1. **Contrôle d'accès**
   Un attaquant peut, avec un compte utilisateur, accéder aux données de tous les utilisateurs
2. **Fichiers**
   Le dépôt de fichiers permet fréquemment à un attaquant de prendre le contrôle du site web
3. **Sessions**
   Un attaquant peut, à partir d'un onglet ouvert, agir sur un site ouvert dans un autre onglet
4. **Langage**
   Le langage de développement ne change pas le nombre de failles… mais leur criticité !

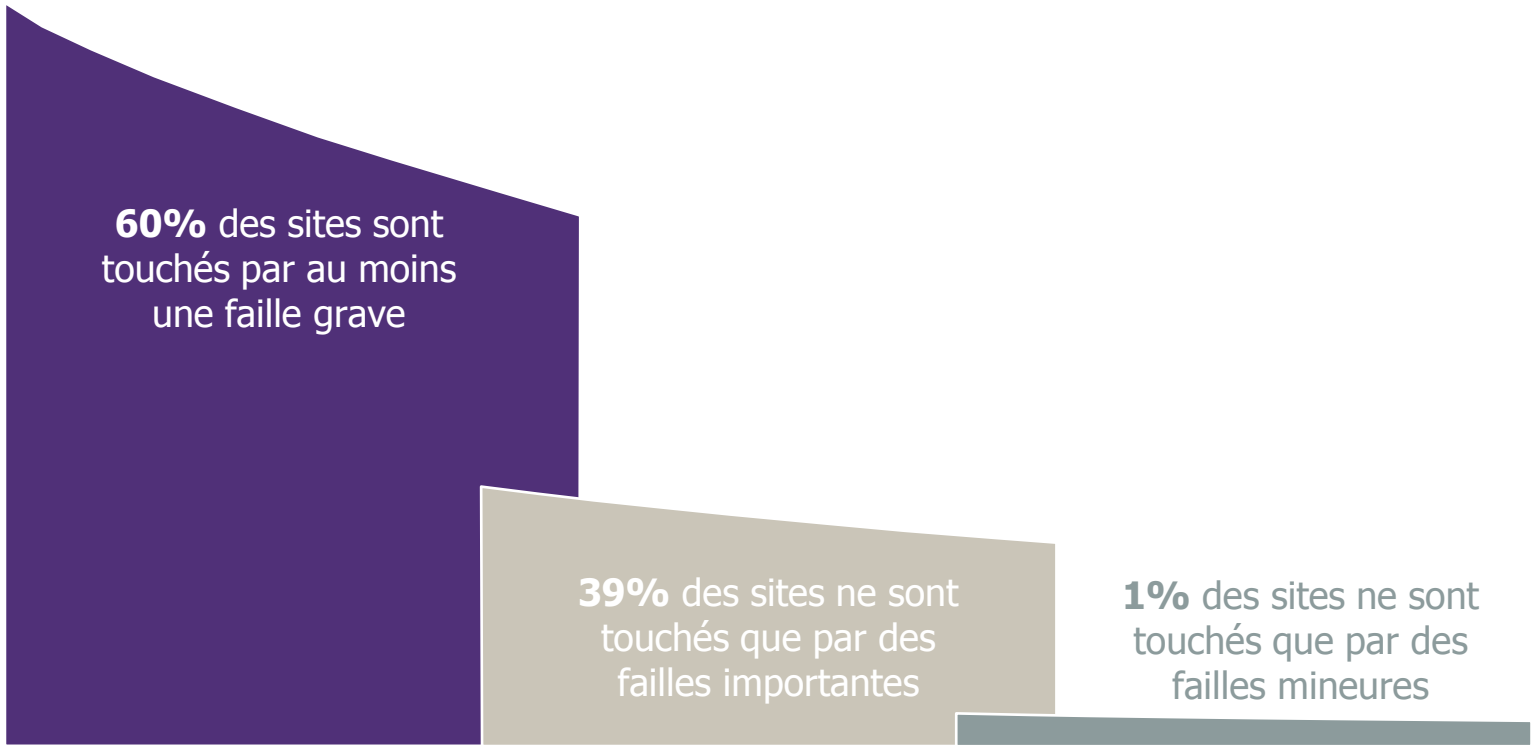
#1 : Tous vulnérables !



Le chiffre

100% Parmi les 128 sites web testés, **au moins une** faille de sécurité a été découverte lors de chacun des tests

Des failles graves dans 60% des cas



Faille grave
Permet d'accéder à l'ensemble du contenu du site et/ou de compromettre les serveurs

Accès à l'ensemble des données du site, exécution de code par le serveur, utilisateur A ayant accès aux données de B, etc.

Faille importante
Permet d'accéder aux informations d'autres utilisateurs mais en nombre limité ou de manière complexe

Vol de session d'un utilisateur, faiblesses dans le chiffrement, possibilité de faire réaliser des actions à l'insu de l'utilisateur, etc.

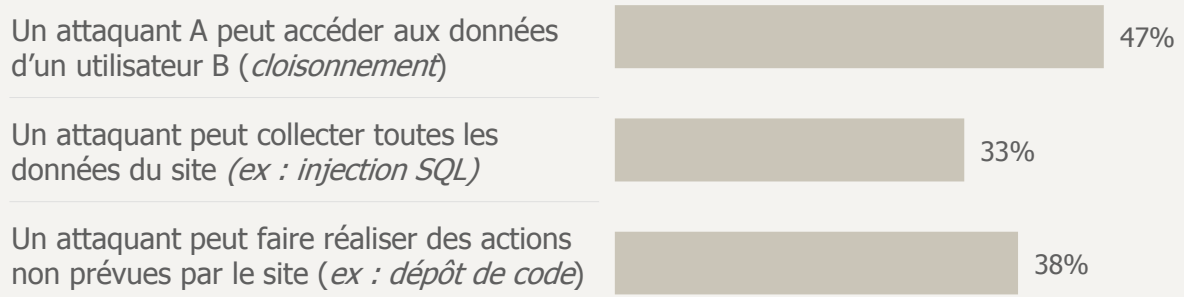
Faille mineure
Permet principalement d'obtenir des informations pour continuer l'attaque

Messages techniques superflus, absence de sécurisation des cookies, déconnexion utilisateur non efficace, etc.

Des failles graves dans les sites sur Internet, comme en interne

#2 : 50% des sites accessibles à tous depuis Internet ont au moins une faille grave

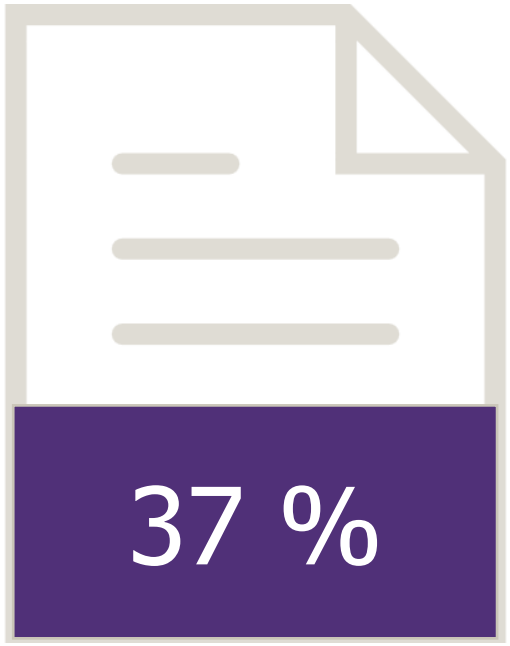
#3: 75% des sites web internes réservés aux collaborateurs ont au moins une faille grave



Un contrôle d'accès pas toujours contrôlé…

44% des tests réalisés en mode **boite grise** (utilisation d'un compte utilisateur standard) ont permis de contourner le cloisonnement applicatif pour accéder à des données ou des fonctions (escalade horizontale ou verticale) non autorisées

Dépôt de fichier ?
Attention danger !



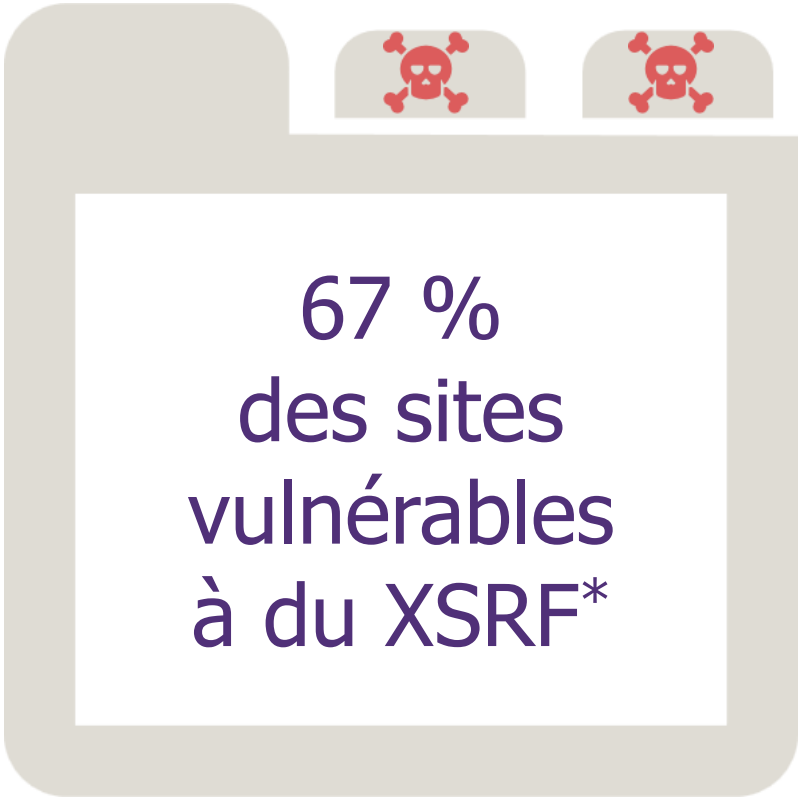
Dans **37%** des 68 cas où une fonctionnalité de type « dépôt de pièce jointe » était offerte, une faille a permis de déposer et d'exécuter du code sur le serveur

C'est une voie royale pour rebondir depuis ce serveur vers d'autres composants du SI

Surfer sur plusieurs sites en parallèle nuit gravement à la sécurité

2/3 des sites sont vulnérables à du CSRF* (ou XSRF*) :

- ➔ Pendant l'utilisation d'un site web sensible, vous décidez d'ouvrir un nouvel onglet pour surfer.
- ➔ Le site web de ce nouvel onglet, s'il contient une attaque, est capable de réaliser des actions à votre insu sur le site web sensible : *modifier votre adresse de contact pour réinitialiser le mot de passe par exemple…*



*CSRF ou XSRF : Cross Site Request Forgery

Le langage ne change pas le nombre de failles… mais leur criticité

Java

39%

de failles sur les sites

PHP

44%

de failles sur les sites

Java

40%

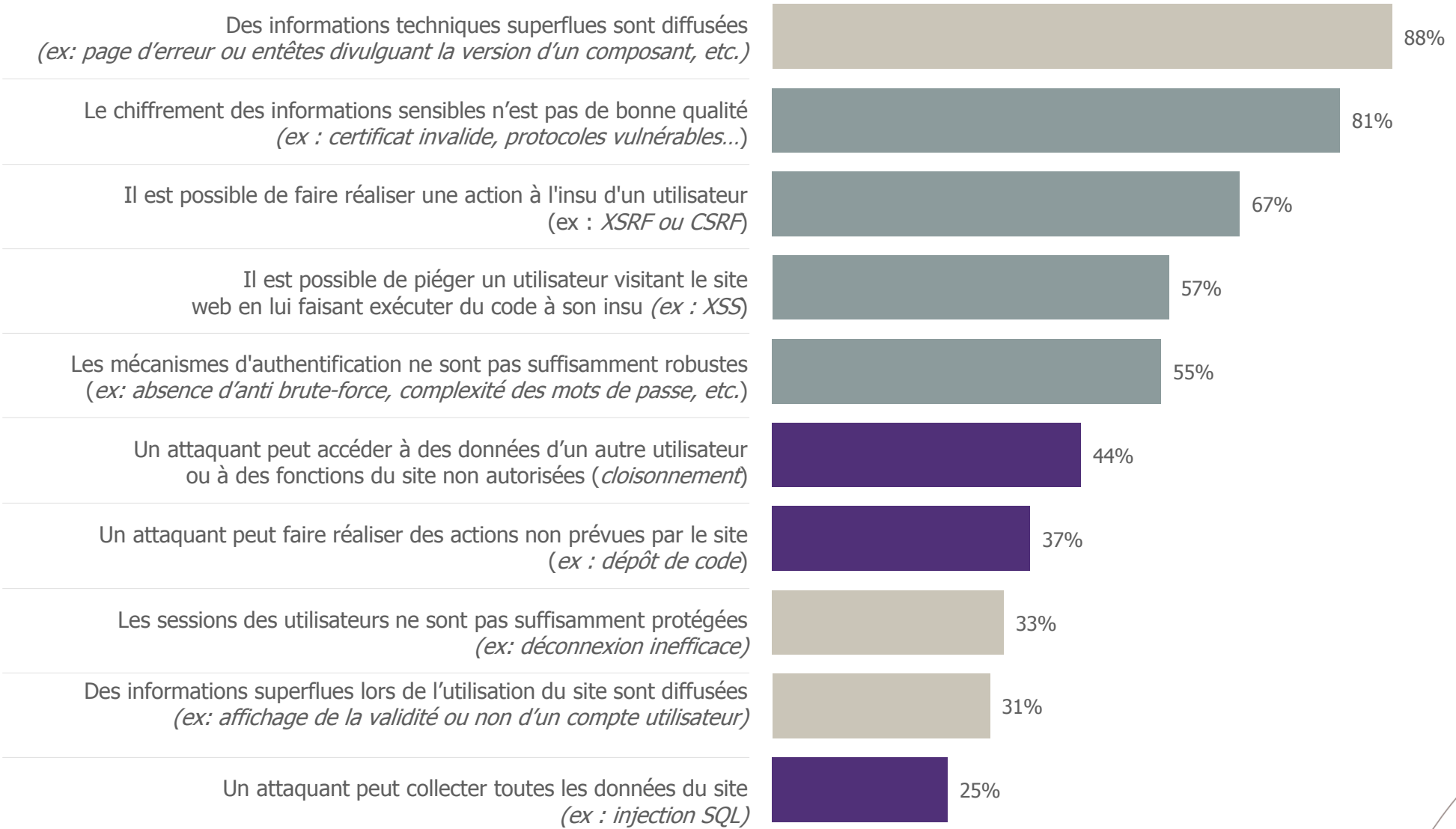
des sites présentent une faille grave

PHP

75%

des sites présentent une faille grave

Top 10 des failles découvertes



Oui, et maintenant ?

Des causes bien connues

Le constat est sans appel : une faille grave découverte sur près de 60% de sites web déjà en production…

La gestion actuelle des projets ne laisse pas beaucoup de place à la sécurité : mise en production urgente, projet dont on apprend l'existence à sa sortie, etc.

L'intégration de la sécurité dès le début du projet est l'une des clés à maîtriser pour améliorer ce chiffre.

Chamboulées par des nouvelles méthodes

Le rythme ne cesse de s'accélérer avec l'essor des méthodes agiles, DevOps…

Pourrait-on réaliser un test tous les 15 jours alors qu'il n'est pas possible aujourd'hui d'en faire un seul avant la mise en production ?

C'est pourtant une opportunité d'appliquer ce qui n'a jamais été possible : intégrer la sécurité en continu dans le processus de développement en rapprochant les contrôles des développeurs.

Qui nécessitent une organisation adaptée !

Car la réponse ne viendra pas uniquement d'investissements sur des nouveaux composants de sécurité, de contrôles a posteriori, etc.

Il est plus que jamais nécessaire d'investir dans les compétences des équipes, en particulier des développeurs, pour que la sécurité soit bien plus qu'une étape dans des processus peu suivis, mais bien une réalité de chaque instant.

WAVESTONE

Yann FILLIAT
Manager – Responsable offre audit de sécurité

M +33 (0)6 24 76 08 67
yann.filliat@wavestone.com

Etienne CAPGRAS
Manager – Responsable offre audit de sécurité

M +33 (0)6 67 49 45 35
etienne.capgras@wavestone.com

Gérôme BILLOIS
Senior Manager

M +33 (0)6 10 99 00 60
gerome.billois@wavestone.com

riskinsight-wavestone.com
@Risk_Insight

securityinsider-wavestone.com
@SecuInsider

wavestone.com
@wavestone_

PARIS

LONDON

NEW YORK

HONG KONG

SINGAPORE *

DUBAI *

BRUSSELS

LUXEMBOURG

GENEVA

CASABLANCA

LYON

MARSEILLE

NANTES

* Strategic partners

WAVESTONE