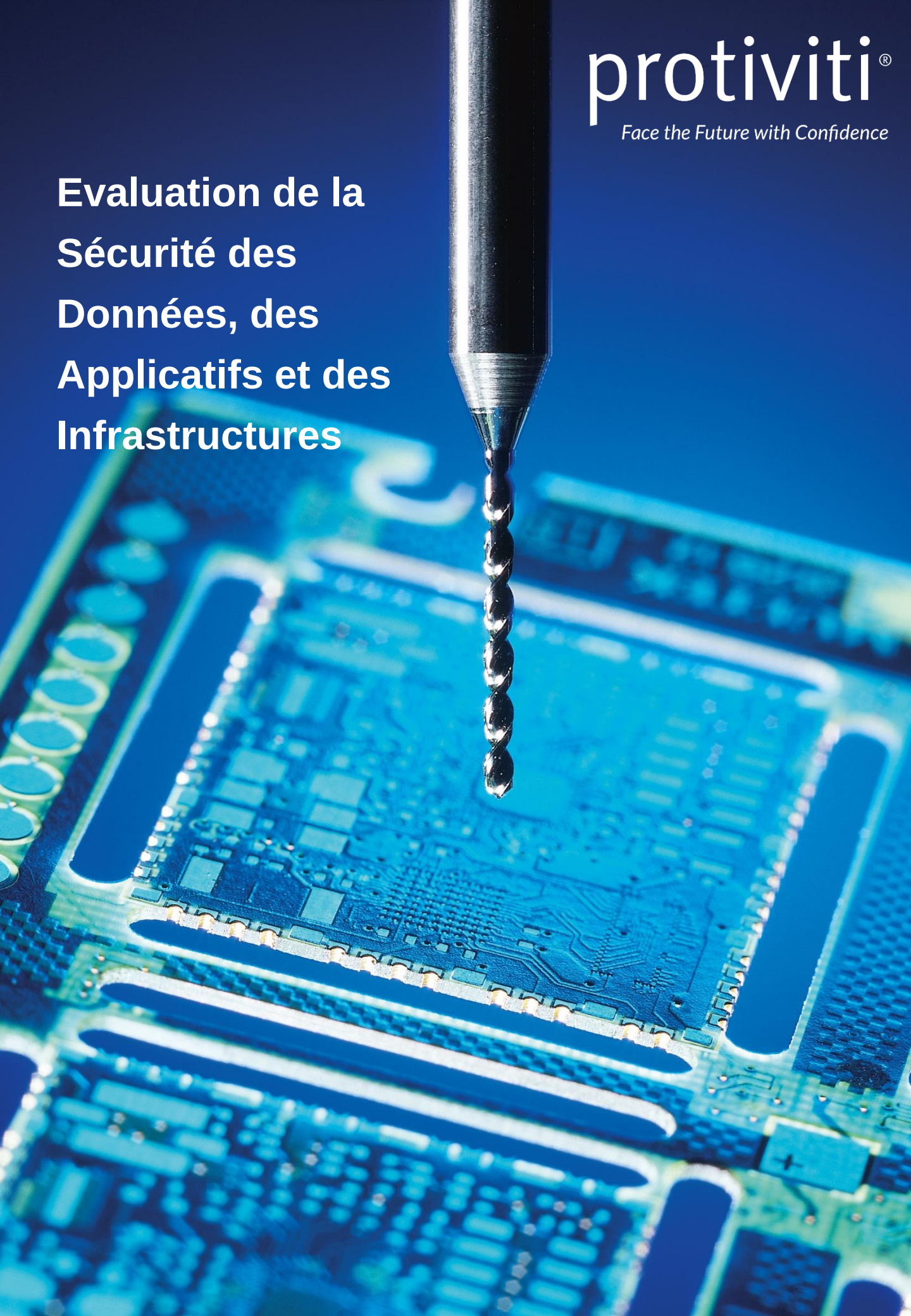
protiviti®

*Face the Future with Confidence*

# Evaluation de la Sécurité des Données, des Applicatifs et des Infrastructures



# L’interface applicative n’est que la partie émergée de l’iceberg!

Comprendre les défaillances des environnements applicatifs et des infrastructures doit être une priorité pour les intervenants opérationnels ainsi que pour le management.

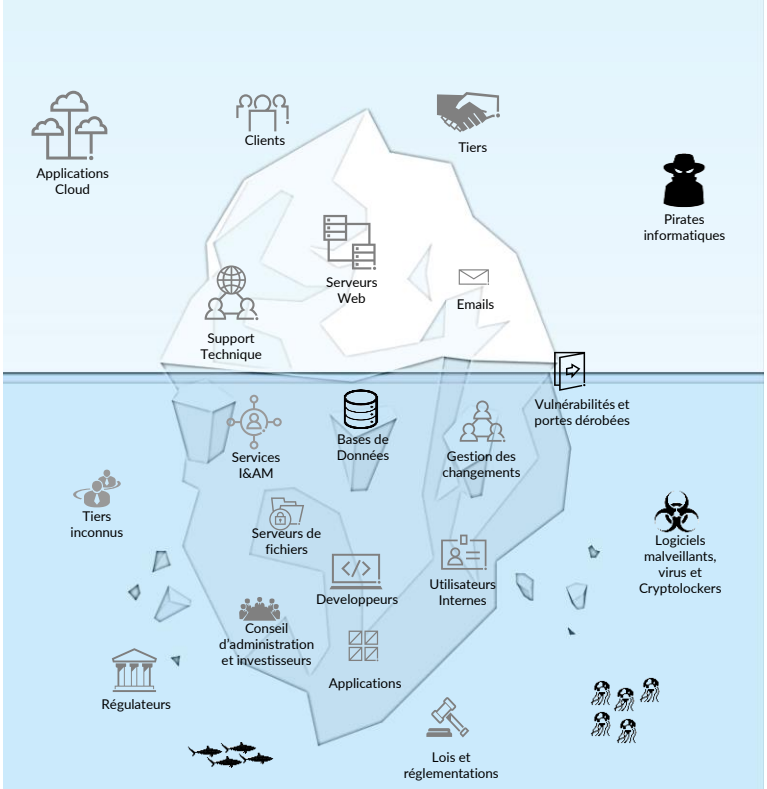
Les tests d’intrusion classiques ne permettent d'identifier que les failles techniques dans un environnement SI.

Les applications sont des interfaces d’accès et de traitements des données (métiers, personnelles, ...) et ne sont que la partie visible d’un Système d’Information (SI) plus complexe.

Un programme de cybersécurité efficace doit prendre en compte à la fois la sécurité des données, des applicatifs et des infrastructures. Les approches traditionnelles se sont largement appuyées sur des tests d'intrusion techniques effectués sur les interfaces applicatives ainsi que le matériel et les équipements sous-jacents. Bien que ces tests soient nécessaires et indispensables pour identifier les risques de piratage et d'intrusion, ils ne sont néanmoins plus suffisants pour une approche de cybersécurité à 360° qui doit être opérée dans environnement ouvert et de mobilité.

En effet une approche plus globale est nécessaire afin d'évaluer les risques liés à l'authentification des utilisateurs, la gestion des accès, les flux de données, le cycle de développement, le suivi des interconnexions et son audit, la résilience des plateformes applicatives, la protection des données notamment. Une telle approche comprend aussi l'identification des faiblesses liées aux manquements ou comportements jugés à risque de la part des parties prenantes autour du SI (utilisateurs, sous-traitants, ...).

Cette approche doit s’appuyer sur des référentiels reconnus dans le domaine de la sécurité SI et les règlementations en vigueur (NIST, ISO, ENISA, ANSII, RGPD, ...). Il est nécessaire également de réaliser des évaluations techniques de la sécurité au niveau de l’infrastructure : équipements réseaux, systèmes d’exploitation, connectivité, hébergement, bases de données, terminaux et équipements mobiles.




La partie immergée de « l’Iceberg SI » dissimule de nombreux risques et enjeux de cybersécurité

## Principaux défis

- Un appétit grandissant pour les applications nouvelles et/ou acquises qui dépasse la capacité des organisations à faire face aux risques SI
- L'attitude à l'égard de la gestion des risques SI doit évoluer afin de mieux apprécier les menaces provenant de l'intérieur même de la zone considérée comme "Zone de Confiance"
- L'absence d'inventaires précis et à jour des applicatifs et actifs SI
- Le besoin accru de partager les données avec les partenaires
- La capacité à intégrer la sécurité au sein du cycle de vie de développement des logiciels (SDLC sécurisé)
- La pénurie des compétences pointues et le besoin de suivre les nouveautés

Les missions autour de la sécurité SI devraient prendre en compte aussi les risques autour des applications, des systèmes, des processus, des lois et réglementations, des tiers et des utilisateurs.

## Par où commencer ?

Décider de la mise en place d’un plan d'action pour la sécurité SI n'est que le début du défi :

- Les organisations ont des centaines voire même des milliers d'applications en cours d’utilisation.
- Ces larges systèmes d’information sont si complexes qu’ils créent une grande part d’incertitude lors de la prise de décision de la part des responsables.
- Un grand nombre d'applications, un nombre conséquent d'utilisateurs, de multiples interfaces (internes et externes) créent un terrain propice à l'émergence de nouveaux risques SI et représente une grande surface d’attaque pour les utilisateurs malveillants.
- La cadence imposée par les départements métiers ne laisse pas assez de temps pour mener une évaluation des risques SI dans les règles de l’art.
- Une approche d'évaluation structurée, approfondie et maitrisée est essentielle pour s'assurer que les risques de sécurité SI sont identifiés selon les bonnes pratiques et normes reconnues.

# Plongeons sous la surface !

## Connaissez-vous bien votre architecture SI ?

Les questions suivantes sont utiles pour mesurer la maturité de votre programme d'évaluation de la sécurité du SI :

- Disposez-vous d'une source unique, précise et à jour de tous les actifs SI (applicatifs, base de données, etc.) avec un responsable affecté à chaque actif listé ?
- Comment vos utilisateurs accèdent-ils aux applications ? Comment déterminez-vous leurs besoins métiers au niveau des applications ?
- Quelles sont les données sensibles qui quittent votre organisation ? Sont-ils transférés en toute sécurité et pouvez-vous identifié la personne émettrice ainsi que les raisons du transfert ?
- Votre politique de cybersécurité et les procédures qui en découlent sont-elles conformes aux normes, standards et réglementations locales, européennes et internationales en vigueur ?
- A quel détail connaissez-vous le niveau de sécurité de vos tiers et des personnes externes qui interagissent avec vos systèmes ?
- Quelle est la robustesse de votre réseau local et cloud ? Est-ce que vous avez testé votre plan de cyber-résilience ?
- Vos processus et systèmes sont-ils sécurisés dès la phase de conception ?
- Avez-vous identifié vos processus à risques au regard des réglementations en vigueur ?
- Vos employés bénéficient-ils d'une formation régulière les sensibilisant aux risques liés aux SI et aux cyber-attaques ?

## Trois solutions pour répondre à vos besoins

### 1. Evaluation des risques pour la sécurité des données et des applications

Les entreprises ont besoin d'une évaluation large et approfondie de leur patrimoine applicatif, centrée sur l'identification des risques ayant un impact tangible sur leur activité en termes de réputation, de pertes financières, d'actions en justice, de sanctions réglementaires et de continuité d'activité.

Il est essentiel de mettre en place un programme d'évaluation des risques pour la sécurité des données et des applications afin d'évaluer avec précision leur exposition aux risques et de démontrer aux conseils d'administration et aux organismes de réglementation qu'ils sont gérés de manière sécurisée et proactive.

Protiviti a mis en place un programme d'évaluation de la sécurité des données et des applications qui a fait ses preuves auprès de larges organismes, les aidant ainsi à identifier les risques SI significatifs tout au long du cycle de vie d'un actif. Notre méthodologie flexible peut bien s'adapter à des organisations de tailles variables.

### 2. Evaluation des risques liés aux infrastructures

Comme pour l'évaluation des risques liés à la sécurité des données et des applications, Protiviti a développé un programme d'évaluation des risques liés à la sécurité des infrastructures SI qui a fait ses preuves auprès de plusieurs types d'organisations.

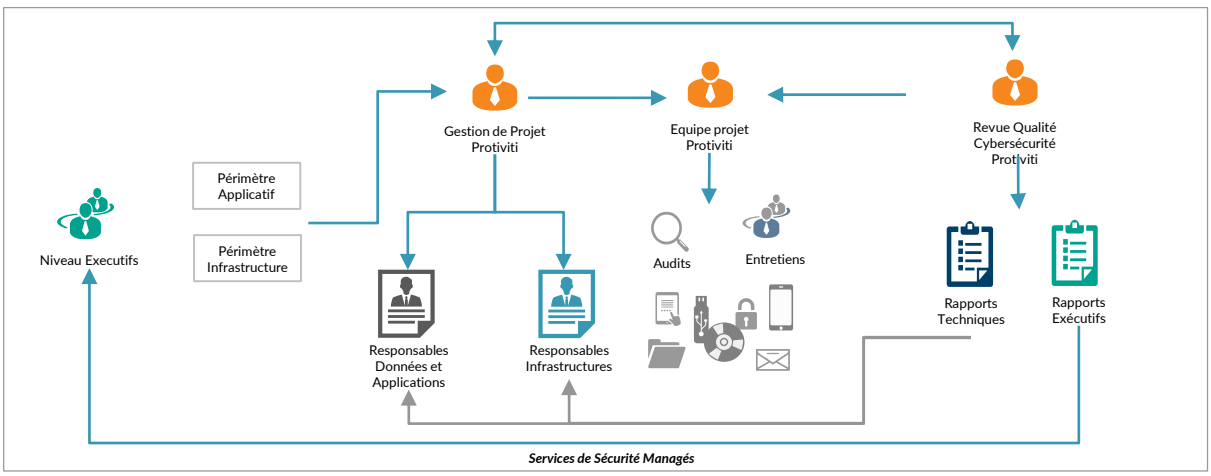
Notre méthodologie peut être appliquée aussi bien pour des infrastructures SI hébergées en interne que pour celles hébergées au niveau du cloud.

L'évaluation des risques de sécurité de l'infrastructure SI couvre également l'évaluation de la sécurité des terminaux fixes, des appareils mobiles ainsi que des objets connectés.

### 3. Services de Sécurité Managés chez Protiviti

Pour des programmes impliquants un très grand nombre d'actifs SI dans le périmètre de la mission s'étalant sur plusieurs années, nos services de sécurité managés constituent une solution adéquate à mobiliser pour la gestion et l'exécution des travaux.

Nos clients ont ainsi accès au réseau mondial Protiviti, composé de consultants hautement qualifiés en cybersécurité supporté par une équipe juridique, associés à un PMO expérimenté et dédié à la mission ainsi qu'à une fonction transverse d'assurance qualité (QA) centralisée pour la revue des travaux et de la méthodologie.



*Face the Future with Confidence*

## Contacts

**Nuvin Goonmeter**

Managing Director
nuvin.goonmeter@protiviti.fr

**Anis Hammami**

Manager
anis.hammami@protiviti.fr

protiviti.fr

PRO-013119