



## Offensive Security Center

Eprouvez vos systèmes en conditions réelles

L'un des plus grands challenges de la sécurité des entreprises est de déterminer si les politiques, outils et configurations mis en place fournissent le niveau de sécurité nécessaire à leurs besoins. Par son activité au sein de l'OSC (Offensive Security Center), Deloitte permet aux entreprises d'évaluer leur sécurité d'une manière pragmatique, au travers d'approches réalistes, ciblant notamment le métier et mettant en scénario des menaces actuelles.

### Une contextualisation forte des menaces

Fort d'une expertise pointue en cybersécurité, Deloitte complète son approche par une contextualisation des risques au regard du secteur d'activité (banque, assurance, énergie, etc.) ainsi que des enjeux stratégiques des clients.

Cette démarche permet de traduire les vulnérabilités techniques en risques et vecteurs de menaces sur les actifs de l'entreprise, fournissant ainsi les éléments de décision nécessaires à la direction.

### Une constante évolution

Les tests d'intrusion sont devenus une composante à part entière de la stratégie de défense de toutes les entreprises dans leur lutte contre la cybercriminalité. Cette dernière évolue constamment avec l'émergence de nouvelles technologies, et de vecteurs d'attaque (SCADA, BYOD, IoT,...). Conscient de ces constats au sein de l'OSC, les équipes Deloitte étudient les tendances et nouvelles menaces afin d'adapter leurs approches et fournir des méthodologies pertinentes et réalistes en adéquation avec les nouveaux risques encourus par les entreprises.

### Un réseau de connaissance mondial

Les équipes Deloitte du réseau mondial communiquent, échangent et travaillent de concert pour assurer un niveau de technicité et de connaissance répondant aux challenges auxquels nos clients font face. De plus, afin de stimuler les échanges, les équipes Deloitte participent de manière constante aux événements majeurs de la scène Cyber Hacking, tels que les Cyber Olympics (vainqueur 2016), Black Hat, Hack In The Box, etc.

## Des offres techniques avant tout

### Campagnes d'évaluation sécurité

Les campagnes d'évaluation sécurité se traduisent généralement par des audits sur un large périmètre, devant être réalisés dans un délai court et pour lesquels le rendu doit être homogène (tant sur la forme que sur la pertinence du fond). Fort d'une équipe de taille importante et expérimentée, Deloitte a l'habitude de répondre aux exigences liées à ce type d'audits.

### Application Security Assurance

L'analyse de la sécurité logicielle permet à une entreprise de maîtriser ses risques au travers d'une approche continue sur le cycle de développement et d'une capitalisation forte des résultats.

### Cov'Ops

Une approche Covert Operations permet d'évaluer le niveau de maturité en termes de sécurité de votre organisation à travers des scénarios d'incidents réalistes à tous les niveaux (humain, physique, technique)

### Evaluation de la sécurité de la chaîne production (SCADA)

L'évaluation de la sécurité de la chaîne de production permet de mesurer l'efficacité des dispositifs de protection des équipements industriels de tous les niveaux, du réseau de l'actionneur aux interconnexions avec le réseau d'entreprise .

### Cyberintelligence

Une approche qui consiste à collecter, mettre en corrélation et enrichir des données issues des différentes couches du web (de surface – Deep...) afin d'identifier les menaces existantes ou émergentes à l'encontre de nos clients

### Evaluation de la sécurité de la chaîne de paiement

Notre méthodologie d'évaluation de la sécurité de la chaîne de paiement permet d'identifier de manière proactive son exposition à des scénarios de fraude. Ceci permet notamment de servir de vecteur de sensibilisation fort auprès du top management de l'entreprise.

### Audit de code

BYOD

Audit d'architecture

Sécurité applicative

Interne / Externe

Real Team

Bonnes pratiques

Cyberintelligence

Revue de configuration

Cov'Ops

### Les plus Deloitte



Expertise et passion



Intégration des composantes métiers



Cycle de formation continue des collaborateurs OSCP, OSCE

Contactez-nous pour plus de détails ainsi que le reste de nos offres.

## Vos contacts :

### Michael Bittan

#### Associé

Leader des activités | Cyber Risk Services  
mbittan@deloitte.fr

### Adel Hamdi

#### Senior Manager

Cyber Risk Services  
ahamdi@deloitte.fr

PARTENAIRE  
OFFICIEL



Deloitte fait référence à un ou plusieurs cabinets membres de Deloitte Touche Tohmatsu Limited, société de droit anglais (« private company limited by guarantee »), et à son réseau de cabinets membres constitués en entités indépendantes et juridiquement distinctes. Pour en savoir plus sur la structure légale de Deloitte Touche Tohmatsu Limited et de ses cabinets membres, consulter [www.deloitte.com/about](http://www.deloitte.com/about). En France, Deloitte SAS est le cabinet membre de Deloitte Touche Tohmatsu Limited, et les services professionnels sont rendus par ses filiales et ses affiliés.

Deloitte  
185, avenue Charles-de-Gaulle - 92524 Neuilly-sur-Seine Cedex

© Deloitte Conseil - Une entité du réseau Deloitte  
Studio graphique Neuilly