# Tests d'intrusion d'Axians

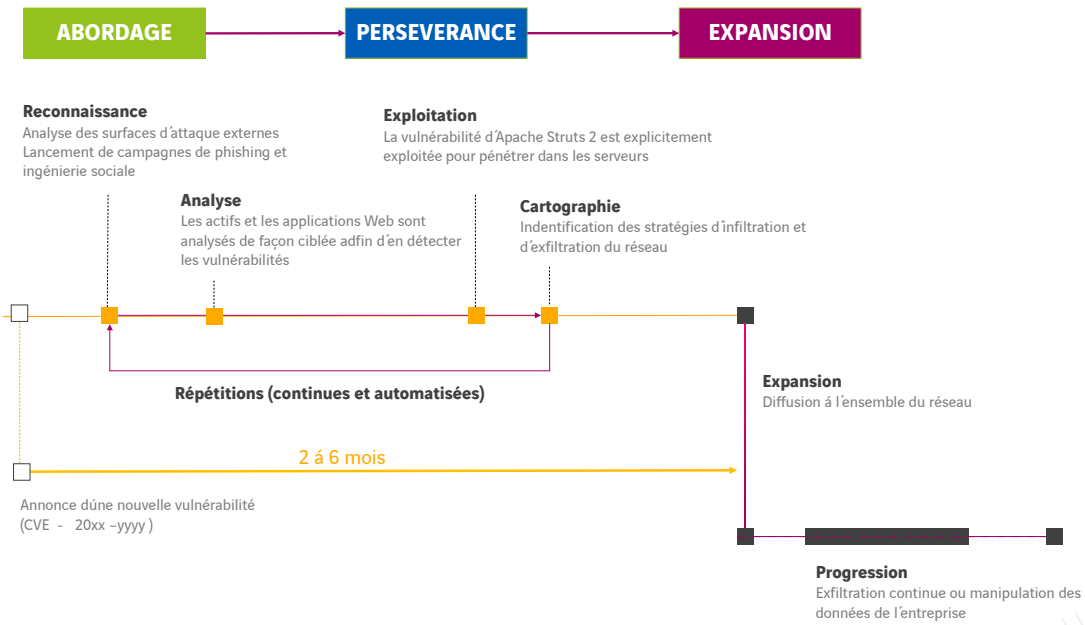
Grâce à notre service, vous validez en continu la posture de sécurité de votre entreprise et pouvez la présenter avec concision à votre direction.

**DEPLOYEZ-VOUS VOS MESURES DE CYBERSECURITE A BON ESCIENT ?**

# Tests d'intrusion d'Axians

Le traitement des données dans les environnements cloud agiles, les applications web et business avec accès nomade, les terminaux et les postes exposés offrent une surface d'attaque sans précédent à la cybercriminalité organisée. Il est donc d'autant plus urgent, pour les experts en sécurité et les autorités de régulation, de mettre en œuvre des stratégies de cyberdéfense validant, y compris aux yeux de leurs adversaires, l'infrastructure de l'entreprise et contrôlant ses vulnérabilités. Traditionnellement, les experts de la cybersécurité procèdent à des tests d'intrusion manuels et en analysent les résultats qui seront ensuite présentés sous forme de rapport. Ce type de validation de sécurité, statique et ponctuelle, ne répond plus aux exigences de l'infrastructure informatique actuelle dont l'évolution est dynamique. De même, les tests d'intrusion se concentrant sur des données et environnements critiques sont désormais obsolètes car la réalité des attaques de ransomware « couronnées de succès » montre que celles-ci ont été préparées en toute discrétion sur le réseau pendant des semaines, voire des mois, et qu'elles proviennent de systèmes considérés comme non critiques.

## Décomposition d'une cyberattaque : abordage - persévérance - expansion




Les hackers préparent longuement les cyberattaques et les attaques de ransomware et observent les infrastructures de l'entreprise pendant des périodes prolongées afin de frapper au moment opportun. Par conséquent, vous devez également surveiller l'infrastructure de votre entreprise sans relâche et dans la durée pour pouvoir intervenir au bon moment !

## Les services d'Axians – parés à surmonter tous les défis !

À partir de la plateforme de tests d'intrusion automatisés de Pentera, Axians offre la possibilité de soumettre votre environnement de production à une validation de sécurité continue – contrôlée, sécurisée et transparente !

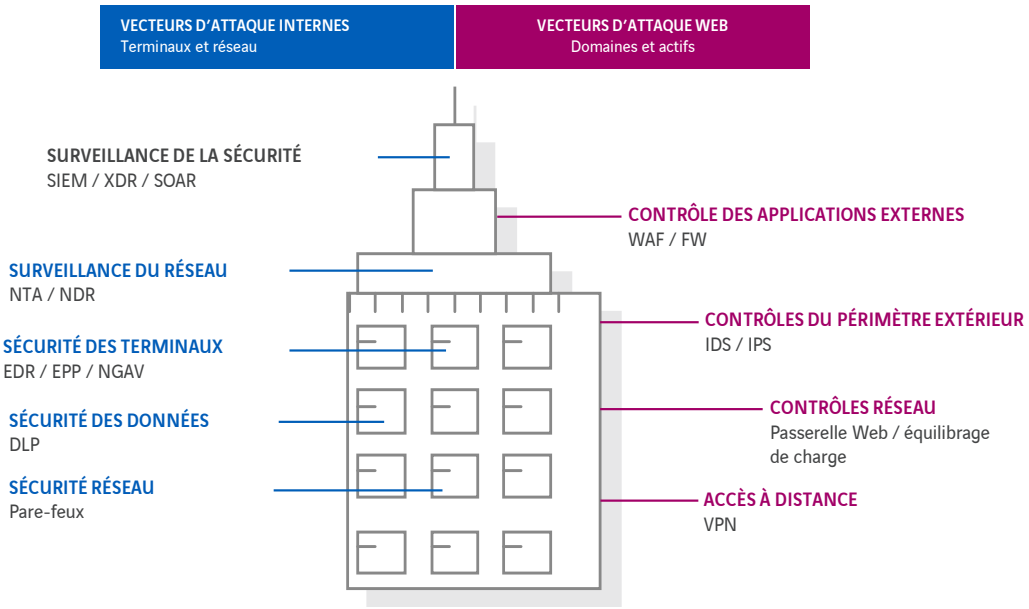
Axians vous indique quelles conséquences une cyberattaque peut réellement avoir sur vos données et processus stratégiques et vous aide à répondre aux questions suivantes :

- **Mon entreprise peut-elle être compromise par une attaque de ransomware ?** Dans l'affirmative, quelles en seraient les conséquences immédiates et comment combler cette faille de sécurité ?
- **Les programmes et solutions de cybersécurité sont-ils correctement mis en œuvre**, afin de garantir une protection appropriée face aux attaques ?
- **En cas d'attaque, les processus de recours hiérarchique sont-ils respectés** et les fournisseurs de services externes et internes respectent-ils leurs contrats de prestations ?

# Notre offre de service

Nous effectuons un contrôle global et permanent des infrastructures de votre entreprise afin de détecter les failles de sécurité sans interrompre la productivité de vos employés ni entraîner une mobilisation massive des ressources par le service informatique. Vous recevez quotidiennement des rapports détaillés et des recommandations d'actions ciblées sur les vulnérabilités avérées.

## Un service exhaustif de validation de sécurité et de tests d'intrusion




Validation de sécurité complète de l'ensemble des vecteurs d'attaque et ressources numériques

Les scénarios de test d'intrusion suivants sont donnés à titre d'exemple et sont ajustés de façon modulaire en fonction des besoins individuels lors d'un entretien de conseil.

- Vérification de la sécurité des **systèmes d'information opérationnels**

(p. ex. serveurs, clients, solutions de sécurité des terminaux)

- Vérification de la sécurité des **solutions de cybersécurité et des systèmes de contrôle**

(p. ex. pare-feux, accès à distance et VPN, environnements cloud, services du SOC)

- Vérification de la sécurité des **services et applications Web**

(p. ex. boutiques en ligne, banque en ligne, services Web et applications en ligne)

# Aperçu de nos offres PenTests

Tests d'intrusion interne ou externe, PenTests des applications Web, contrôle ponctuel ou continu des vulnérabilités : afin de garantir qu'aucune faille de sécurité ne passe inaperçue. Notre offre comprend différents types de tests d'intrusion qui peuvent par ailleurs être associés en fonction des projets et des besoins. N'hésitez pas à nous consulter.

## Tests d'intrusion pour applications Web

- Vérification technique des applications Web (y compris de l'infrastructure du serveur sur laquelle est installée l'application), du point de vue d'un hacker expérimenté
- Les tests d'intrusion sont basés sur le Guide sur les tests de sécurité des applications Web de l'OWASP (Open Web Application Security Project)
- Les PenTesters réalisent des « exploits éthiques » et enrichissent leurs tests de façon structurée en y intégrant des attaques spécifiques inspirées de leur longue expérience

## Tests d'intrusion pour API Web

- Vérification technique des API Web (y compris de l'infrastructure du serveur hébergeant l'API) par un hacker expérimenté
- Les tests d'intrusion sont basés sur le Guide sur les tests de sécurité des applications Web de l'OWASP et sur la Directive de l'OWASP sur les 10 principaux risques de sécurité des API
- Les PenTesters réalisent des « exploits éthiques » et enrichissent leurs tests de façon structurée en y intégrant des attaques spécifiques inspirées de leur longue expérience

## Tests d'intrusion des applications mobiles

- Vérification technique des applications mobiles sur la base du référentiel technique MASVS (norme de vérification de la sécurité des applications mobiles de l'OWASP) qui définit les exigences en matière de sécurité des applications mobiles

## Tests d'intrusion interne

- Validation continue de la sécurité, en totale conformité avec le Cadre MITRE ATT&CK. Notre offre est disponible sous forme de service permanent ou de programme de démarrage ponctuel. Nous aurons le plaisir de vous apporter des conseils personnalisés et de vous soumettre une offre
- Émulation ransomware et évaluation de la sécurité de l'AD

## Tests d'intrusion de la surface d'attaque externe et identification des actifs critiques

- Validation de sécurité continue des contrôles de périmètres défensifs tels que le contrôle des applications externes (WAF), l'accès à distance (SSL/VPN) et les contrôles de périmètre (pare-feu), comprenant une « surveillance de la fuite d'informations d'identification » (générées par Pentera)

**Cela vous intéresse ?**

Dans le cadre d'un entretien qui ne vous engage en rien, nous adaptons précisément les offres PenTest à votre entreprise.


**VOTRE INTERLOCUTRICE**

Renata Rekic (Presales Consultant)

Courriel : renata.rekic@axians.com

07/2023

axians

Axians IT Services AG · Arlesheim · Zurich · Romanel-sur-Lausanne · Martigny
Tél. : +41 61 716 70 70
Courriel : info-ch.security@axians.com · www.axians.ch