

## TESTS D'INTRUSION ET AUDITS DE SÉCURITÉ

La réalisation de tests d'intrusion et d'audits de sécurité fait partie intégrante d'une démarche proactive de gestion des risques. Concrètement, ce type de service permet de répondre aux questions suivantes:

- Quel est l'état actuel de la sécurité de mon organisation ?
- Est-ce que les mesures de sécurité en place sont adéquates ?
- Est-ce que mon organisation peut faire mieux pour assurer sa sécurité ? Si oui, comment ?

### SERVICES OFFERTS

Voici un bref aperçu des différents services offerts :

#### Applicatif

- Test d'intrusion d'applications Web (Java, .Net, PHP, JS, RoR)
- Test d'intrusion d'applications mobiles (Java, Objective-C)
- Test d'intrusion de Web Services / API (XML, SOAP, JSON, REST)
- Audit de code source (OWASP, CWE-25, PCI-DSS #6.3)

#### Infrastructure

- Test d'intrusion d'infrastructures réseau externe / Internet
- Test d'intrusion d'infrastructures réseau interne / LAN
- Audit d'architecture réseau / segmentation
- Audit d'architecture réseau sans-fil
- Audit d'architecture réseau Cloud (Microsoft, AWS)

#### Système

- Audit de système Windows (7/8/10, 2008/2012)
- Audit de système Linux/Unix (RedHat, Debian, SuSe)
- Audit de base de données (Oracle, MSSQL, PostgreSQL, MySQL)
- Audit de système ERP (SAP, Oracle, etc.)
- Audit TOIP / VOIP (Cisco, Avaya, Alcatel, SIP, H.323)
- Audit de plateforme de virtualisation (VMware, Xen, Hyper-V)
- Audit de solutions de sécurité (Pare-feu, VPN, Proxy)
- Audit des mots de passe (AD, LDAP, Applications)

#### Organisation

- Audit de sécurité organisationnel (ISO 27001/27002, CIS, etc.)
- Campagne d'hameçonnage ciblée (phishing)

### À PROPOS

Vumetric est une société indépendante certifiée ISO 9001 spécialisée en cybersécurité.

Voici quelques-unes des raisons qui expliquent pourquoi notre offre se démarque de la concurrence et qu'un nombre croissant d'organisations optent pour nos services :

- Expérience et réputation
- Indépendance et impartialité
- Meilleures pratiques
- Équipe d'experts
- Innovation et R&D
- Approche pragmatique
- Aucune sous-traitance
- Éthique professionnelle

### NOS CLIENTS

- Finance & Assurance
- Gouvernement
- Commerce en ligne
- Commerce de détail
- Manufacturier
- Technologie
- Villes et municipalités

## COMMENT S'ASSURER D'UN SUCCÈS ?

Le domaine des tests d'intrusion et d'audits de sécurité est complexe et il existe une grande variation dans la qualité et la profondeur des différentes offres de services disponibles sur le marché. À titre informatif, voici certains critères à considérer lors de la sélection d'un fournisseur de services de tests d'intrusion et d'audits de sécurité :

### Fournisseur

- Est-il indépendant de tout fabricant de solutions ou logiciels ?
- S'appuie-t-il sur des standards reconnus (ex.: ISO 9001, ITIL, etc.) ?
- Possède-t-il une assurance erreur et omission en vigueur ?
- Est-il possible d'obtenir des références de clients satisfaits ?

### Services

- Est-ce que les tests et audits de sécurité font partie intégrante de l'offre de services ?
- Existe-t-il une distinction entre les tests d'infrastructures et d'applications ?
- Est-ce que l'offre peut être adaptée en fonction de nos besoins spécifiques ?

### Ressources

- Depuis combien de temps effectuent-ils ce type de projet ?
- Possèdent-ils des certifications de sécurité reconnues et pertinentes (ex.: CISSP, CISA, CEH, CSSLP, GPEN, GWAPT, etc.) ?
- Sont-ils en mesure de fournir un certificat de recherche d'antécédents criminels négatif ?
- Sont-ils en mesure de présenter les constats et recommandations dans un langage clair et concis ?

### Encadrement

- Quels sont les moyens mis en oeuvre afin de limiter l'impact potentiel des tests sur la bonne conduite de nos opérations et la stabilité de nos infrastructures ?
- Quelle est la politique concernant la confidentialité des informations obtenues ?

### Méthodologie

- Utilisent-ils des cadres méthodologiques et standards reconnus (ex.: OSSTMM, OWASP, CVE, CVSS, CWE) ?
- Est-ce que les tests consistent uniquement à utiliser des outils automatisés (ex.: Nessus) ?

### Rapport

- Est-il possible d'obtenir un exemple de rapport ?
- Est-ce que les rapports sont générés automatiquement par un outil ?
- Est-ce que les rapports contiennent une section de type sommaire exécutif ?