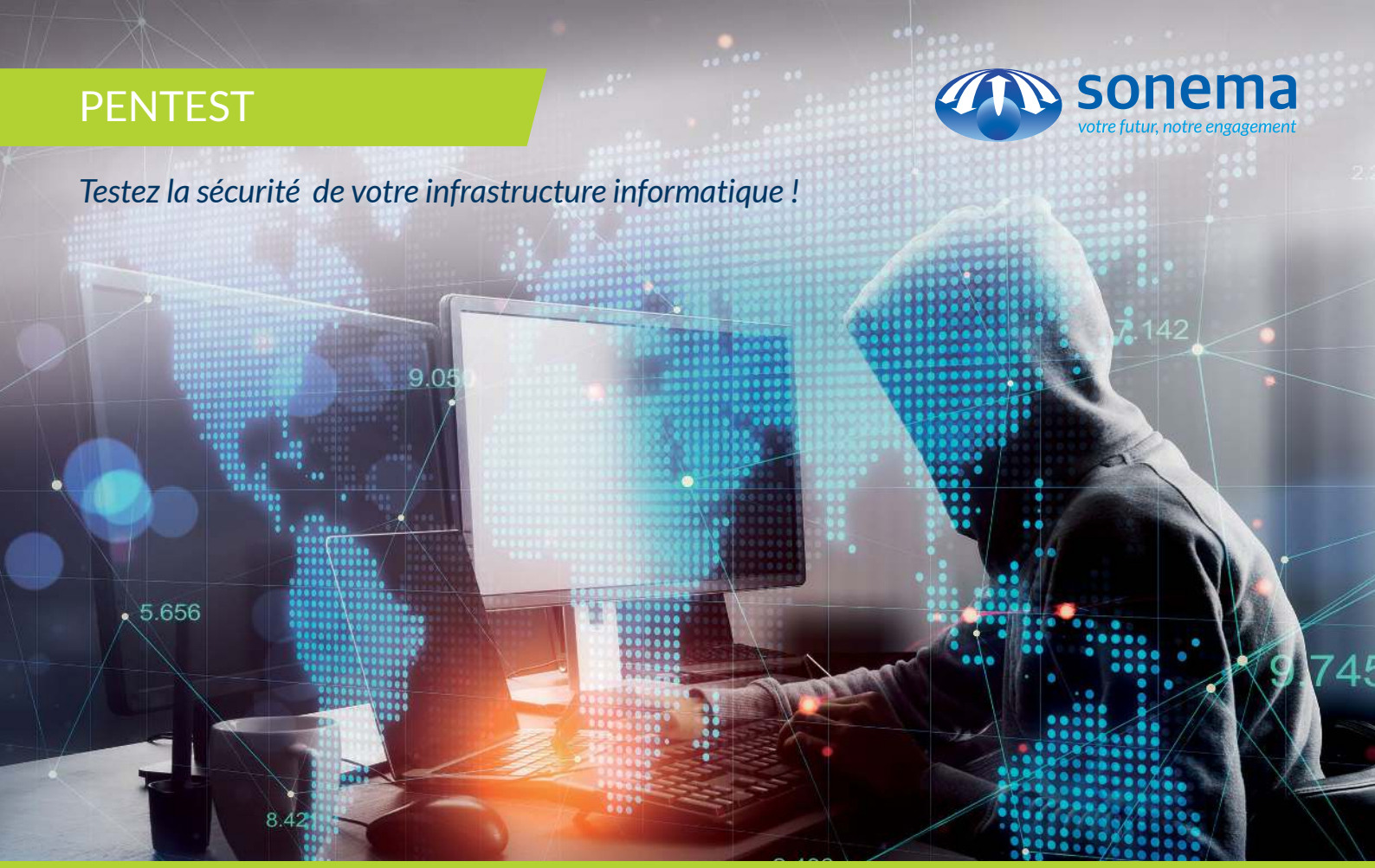
PENTEST

sonema
votre futur, notre engagement

Testez la sécurité de votre infrastructure informatique !



Mesurez votre niveau de protection grâce à des tests d'intrusions sur votre réseau et votre Système d'Information (SI)

LA PROTECTION ADÉQUATE DES SYSTÈMES ET DE L'INFORMATION

- Vérifier et connaître le niveau de sécurité de l'infrastructure technologique (postes, serveurs, etc.)
- Anticiper les menaces qui pourraient peser sur l'organisation
- Identifier les failles critiques et atténuer les risques avant qu'ils ne se matérialisent
- Assurer la conformité aux standards PCI-DSS lors d'audits de sécurité règlementaires

MAXIMISER LA SÉCURITÉ ET MINIMISER LES RISQUES SUR VOTRE SI

Sécurité et protection

- Tests de pénétration avancés et analyse des réponses du SI face à des cybermenaces
- Vérification des impacts réels des intrusions
- Protection à jour et performante pour réduire l'impact sur les processus métier essentiels

Performance et conformité

- Analyse des réponses du SI face à des cyber menaces réelles
- Evolution de l'infrastructure réseau pour prévenir des attaques
- Garantie de conformité aux réglementations

Démarche globale de sécurité

- Rapports détaillés des vulnérabilités et des risques auxquels l'organisation est exposée
- Accompagnement à la remédiation
- Mise en place de correctifs adaptés

DES OFFRES COMPLÉMENTAIRES

Procédure d'évaluation de la résilience de vos Systèmes d'Information par simulation d'attaques malveillantes :

1	2	3	4	5	6
Définition des objectifs et du périmètre	Scan du périmètre ciblé Identification des vecteurs d'attaques potentiels	Exploitation des vulnérabilités détectées Escalade de privilèges Mouvement latéral	Simulation d'accès aux données sensibles	Suppression des outils déposés sur le système	Hiérarchisation des risques par ordre de criticité Mesures correctives associées
PLANNING	CARTOGRAPHIE ET RECONNAISSANCE	EXPLOITATION	PERSISTANCE	NETTOYAGE DES TRACES	RAPPORT ET RESTITUTION

TESTS MANUELS

Simulations ponctuelles d'attaques exécutées par des experts en sécurité visant l'exploitation des potentielles failles

3 TYPES DE TESTS D'INTRUSION

BLACK BOX Attaques Externes	L'expert ne dispose d'***aucun accès autorisé*** = Tests depuis Internet sans droit d'accès
GREY BOX Attaques Intermédiaires	L'expert dispose d'***accès limités*** = Tests avec des droits utilisateur restreints
WHITE BOX Attaques Internes	L'expert bénéficie d'un ***accès complet*** = Tests avec des droits administrateur

Tests exécutés une fois ou de manière récurrente selon une fréquence définie et basés sur des guides de bonnes pratiques *Penetration Testing Execution Standard (PTES).*

Identification des vulnérabilités exploitables depuis l'intérieur et l'extérieur du Système d'Information

Contrôle du respect des normes
= Évaluation du niveau de conformité
= Mesure des écarts

TESTS AUTOMATISÉS

Simulations continues et globales d'attaques exécutées par des machines virtuelles

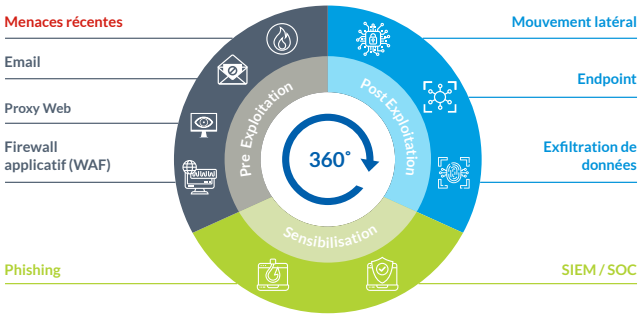
3 MODES D'ANALYSE

Pré Exploitation | ***Post Exploitation*** | ***Sensibilisation***

Tests exécutés via des technologies et outils *Breach & Attack Simulation (BAS)* et réalisés sur une base de *Common Vulnerability Exposure (CVE)* = liste publique de failles de sécurité informatique auxquelles un identifiant CVE est attribué.

Validation continue de la sécurité du Système d'Information

9 VECTEURS D'ATTAQUES



LA RÉPONSE SONEMA AUX EXIGENCES TECHNOLOGIQUES ET RÈGLEMENTAIRES

SÉCURITÉ | TRAÇABILITÉ | VISIBILITÉ | CONFORMITÉ

A propos de Sonema

Partenaire proactif de nos clients, nous développons des solutions télécom sur mesure et évolutives pour les accompagner au quotidien dans leurs projets. Notre état d'esprit d'engagement fondé sur une forte compréhension de leurs enjeux, leur permet de se concentrer sur leur coeur de métier et leurs innovations business.

Plus d'information ?

Contactez notre équipe commerciale :
+377 93 15 93 15 ou
sales@sonema.com

SONEMA

7, Avenue d'Ostende
98000 Monaco
www.sonema.com