AUDIT ET CONSEIL CYBERSÉCURITÉ

sonema
votre futur, notre engagement

Évaluez et renforcez la sécurité de vos systèmes d'information !

Nos experts vous accompagnent pour évaluer et mettre en place votre stratégie de sécurité

UNE STRATÉGIE DE CYBERSÉCURITÉ EFFICACE DOIT RÉPONDRE À 4 CHALLENGES

- Mieux connaître votre environnement et ses vulnérabilités
- Définir et appliquer une politique de sécurité pour protéger vos applications et vos données
- Vérifier régulièrement l'efficacité et la cohérence de la politique de sécurité mise en place
- Appliquer des mesures de protection adaptées aux risques potentiels

LA RÉPONSE SONEMA ADAPTÉE AUX SPÉCIFICITÉS DE VOTRE ENVIRONNEMENT

Diagnostic Sécurité

- Observation de l'exposition aux risques
- Identification des failles et vulnérabilités
- Évaluation des mesures de sécurité

Audit et Analyse

- Analyse du niveau de criticité des vulnérabilités
- Priorisation des actions correctives
- Recommandations personnalisées pour réponse aux exigences règlementaires

Accompagnement et Conseil

- Participation à la mise en place de votre stratégie de cybersécurité
- Aide à la mise en conformité règlementaire
- Préconisation de contre-mesures et de solutions de gestion des risques

NOS 3 OFFRES POUR UNE DÉMARCHE DE SÉCURITÉ GLOBALE

AUDIT TECHNIQUE

Diagnostic des mesures de sécurité et de la résilience des configurations

AUDIT D'ARCHITECTURE	Observation des dispositifs de sécurité = Vérification du dimensionnement réseau = Analyse des flux
AUDIT DE CONFIGURATION	Revue des configurations des équipements de sécurité et des postes de travail

- → Identification des failles de sécurité
- → Recommandations d'architecture et de configuration hautement sécurisées

AUDIT ORGANISATIONNEL

Vérification de la conformité vis-à-vis des référentiels normatifs ou règlementaires

ISO 27001 — PCI DSS*

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

** Payment Card Industry Data Security Standard*

- → Compte-rendu de l'analyse des écarts
- → Recommandations de corrections

TESTS D'INTRUSION - PENTESTS **

Évaluation de la résilience de vos systèmes d'information par simulation d'attaques malveillantes

TESTS MANUELS

Simulations ponctuelles d'attaques **par des experts en sécurité** visant l'exploitation des vulnérabilités identifiées

3 TYPES DE TESTS D'INTRUSION

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

- → Identification des vulnérabilités exploitables depuis l'intérieur et l'extérieur du système d'information

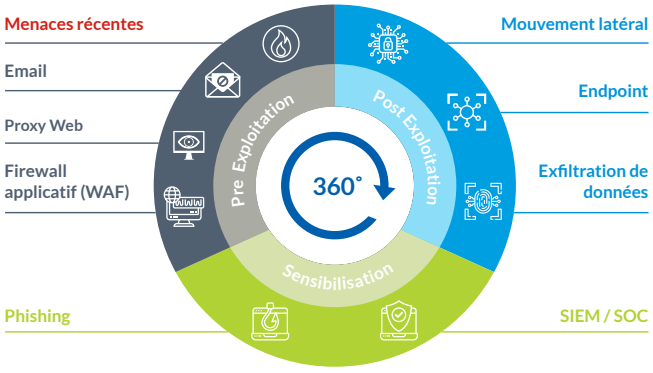
TESTS AUTOMATISÉS

Simulations continues et globales d'attaques **par des machines virtuelles et agents logociels (BAS***)**

3 MODES D'ANALYSE

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

9 VECTEURS D'ATTAQUES



*** PENTESTS : Penetration Testing - *** BAS: Breach & Attack Simulation*

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