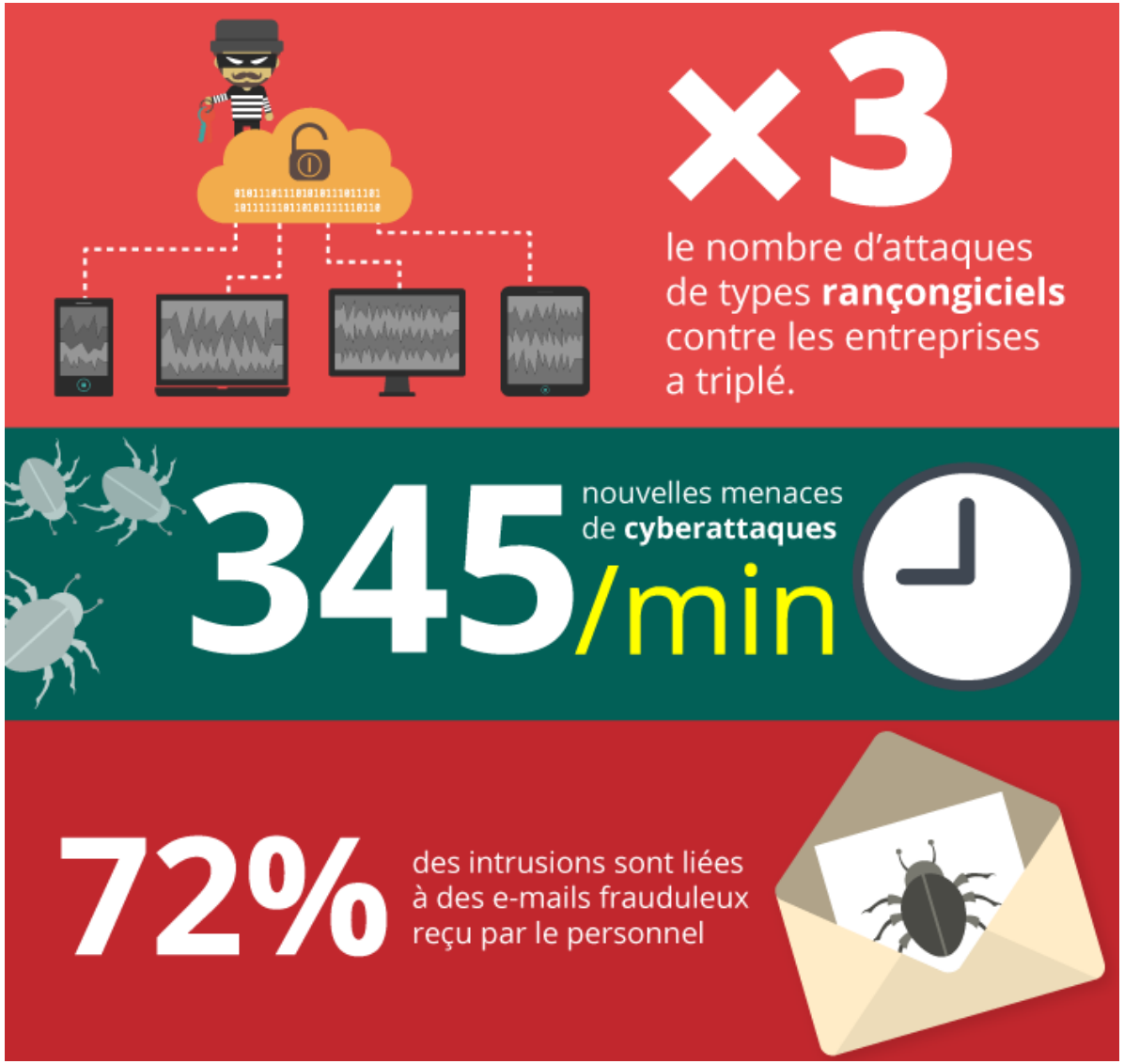
Pole Cyber Sécurité

By L@ Suite Californie

La Cyber Sécurité en Chiffres



Le constat est sans appel. **La pénurie d'experts en cybersécurité est confrontée à l'augmentation et à l'évolution des nouvelles technologies.** Des menaces plus nombreuses et plus sophistiquées apparaissent et les entreprises peinent à se réorganiser.

Comme à l'image des fondations d'un bâtiment, la cyber constitue à la fois la structure et la clé de voûte de l'IT permettant ainsi son bon fonctionnement.

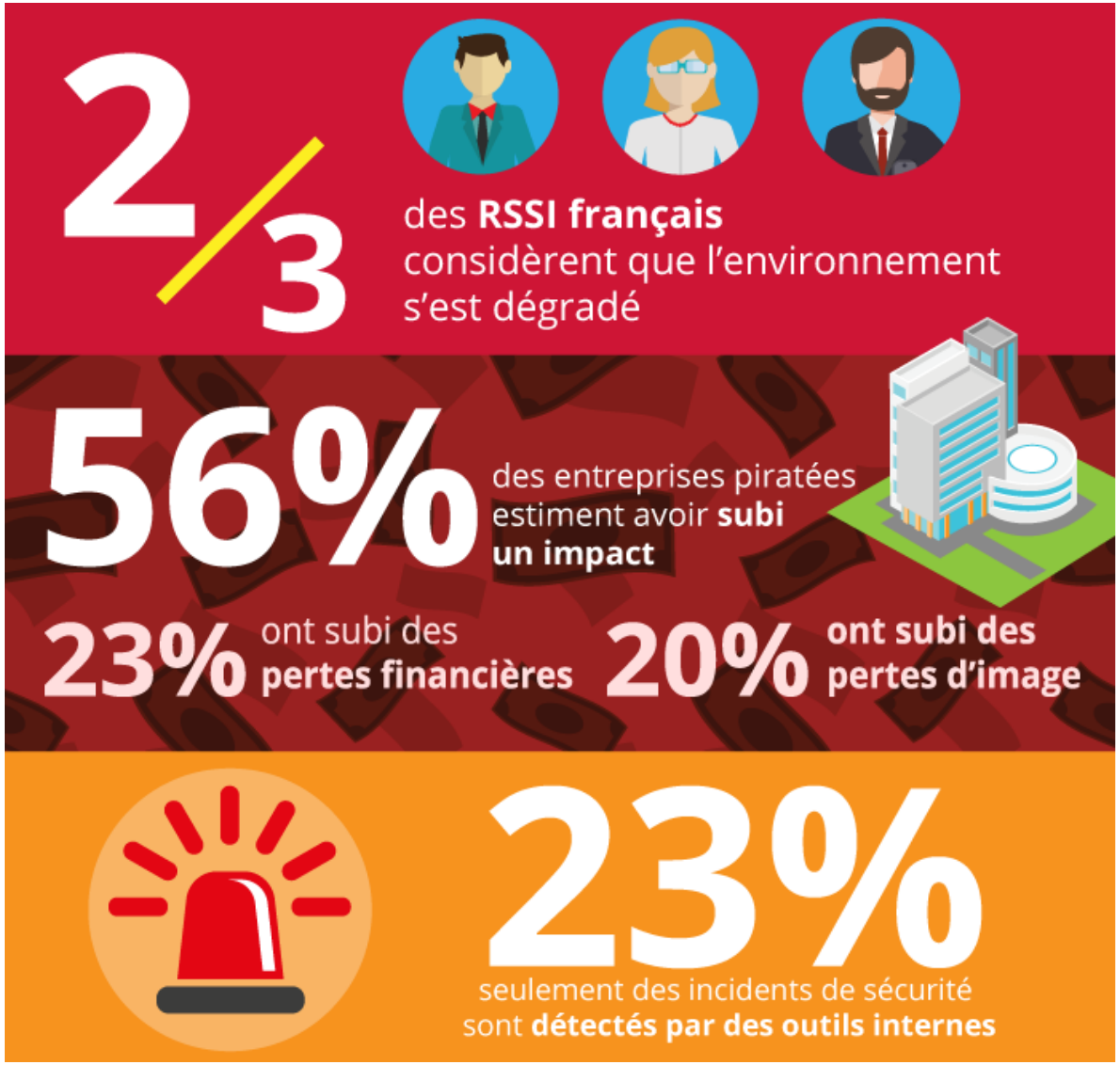
Au fil des années, la cyber s'est transformée en structure porteuse plus «intelligente», offrant des possibilités et des opportunités nouvelles aux différents métiers des entreprises.

La Cyber Sécurité en Chiffres

Près de 80% des salariés déclarent connaître les principaux enjeux de la cybersécurité mais seule la moitié déclare les bonnes pratiques au quotidien.

78% des salariés interrogés déclarent utiliser des mots de passe identiques pour plusieurs plateformes (entre autres nombreux comportements problématiques déclarés).

« Face à l'accélération des cyber-attaques, ce constat est particulièrement sévère et soulève l'urgence nécessité pour les entreprises d'ajuster leur stratégie et de s'armer d'outils adaptés pour mobiliser leurs salariés. Rappelons que les assureurs estiment que 70 à 90% des cyber attaques sont dues à des défaillances humaines et que depuis janvier 2018, le Forum Economique Mondial (‘Davos') appelle les dirigeants à se saisir directement du sujet de la culture de la cybersécurité. », commente Sylvan Ravinet, fondateur de CaptainCyber.



Méthodologies d’attaques

#1 – Prise d’information passive
Récupération d’informations sensibles sur les systèmes du périmètre initial à partir de ressources Internet (informations publiques, OSINT, etc.).

#2 – Prise d’information active
Récupération d’informations sensibles directement sur les systèmes du périmètre initial (scans réseaux, prise d’empreinte, recherche de vulnérabilités, etc.).

#3 – Vérification des rebonds possibles
Analyse des nouveaux systèmes adjacents accessibles depuis les systèmes compromis (scans de vulnérabilités, exploitation optionnelle).

#4 – Vérification des failles
2eme pentest (+1 mois) après correction des failles

Nos Compétences

Les tests Néo sont réalisés par des **consultants expérimentés** qui suivent une **méthodologie rigoureuse**.

Pour une mise en situation optimale et une pertinence maximale, **Néo est capable de coupler les tests d'intrusion applicatifs à une analyse des sections sensibles du code de l'application ciblée.**
La qualité de nos rapports, clairs, concis, et didactiques, est appréciée tant par les Directions Générales, que par les experts techniques.

Néo développe ses propres scripts d'intrusion et maîtrise les logiciels utilisés.
Les tests sont réalisés manuellement par nos experts avec une prise en compte réelle des risques métiers et de la logique "business" de chaque application.

Tests d’intrusion

Un test d’intrusion permet d’identifier les vulnérabilités avant qu’elles ne soient exploitées par des attaquants

Différents tests :

- Tests d’applications Web et API
- Tests d’infrastructure externe (internet, extranet)
- Tests VPN
- Tests d’intrusion spécifiques aux infrastructures
- Tests basés sur un parcours RedTeam

Comment ?

Différentes approches :

- **Boîte noire :** tests réalisés sans information afin de simuler les actions d'un attaquant
- **Boîte grise :** tests réalisés à partir de comptes d'accès afin de simuler le comportement d'un utilisateur
- **Boîte blanche :** tests réalisés avec une connaissance approfondie de l'environnement (schémas, code source, docu…(uniquement sur devis))

le type de test est en fonction de la connaissance de l'entreprise de son SI et de sa volonté

L'offre

NEO BASIC

300€

•2 systèmes
(connexion internet ou VPN + site web)
• Audit
• **Black box**
• Simulation d'attaques
• Résultats complets
• Cartographie 100%
• Détection de tous types de failles
• Liste des failles et correctifs à appliquer

• **Aucun frais d'installation**
•Sans engagement
•Envoi des rapports en PDF

NEO PLUS

1000€

•5 systèmes
(audit pentest initial + 1 audit après correction +1 mois maximum)
• **Black box**
• Simulation d'attaques
• Résultats complets
• Cartographie 100%
• Détection de tous types de failles
• Liste des failles et correctifs à appliquer

• **Aucun frais d'installation**
•Sans engagement
•Envoi des rapports en PDF

NEO FULL

Sur Devis

Contactez-nous pour définir vos besoins et obtenir un devis personnalisé.
contact@arobase972.com
Ou au 0696 484 438