Comment se préparer le plus efficacement possible à une cyberattaque ?

A — Mettre en place des solutions techniques (pare-feu, antivirus …)

B — Sensibiliser ses équipes aux menaces

C — Préparer l'ensemble des ses équipes à réagir (test d'intrusion, exercice de cyber crise …)

EXA

CORRESPONDANT MAZARS

CONSEIL

SYSTÈME D'INFORMATION

AUDIT ET CAC

EXPERTISE COMPTABLE

L'IMPORTANCE DU TEST D'INTRUSION DANS LE DIAGNOSTIC CYBER D'UN SYSTÈME D'INFORMATION

Forum Cybersécurité du 3 mars 2021

Qui sommes nous ?

Exa est cabinet pluridisciplinaire indépendant disposant de plus de 40 années d'expérience. Implanté à Saint-Denis de la Réunion et à Paris, Exa est reconnu pour la qualité de ses équipes – 9 associés et plus de 70 collaborateurs – et la rigueur de ses travaux.

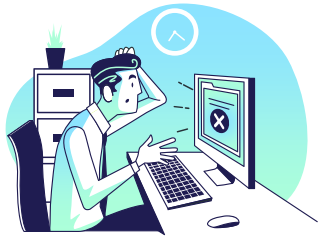
Depuis bientôt 15 ans, EXA a anticipé cette profonde mutation pour développer un savoir faire en matière d'audit des systèmes d'information au travers de la cellule dédiée «**Département Audit des Systèmes**» qui rassemble les spécialistes du contrôle interne informatique et de l'analyse de données informatiques.

- Audit informatique
- Support au CAC
- Assistance maitrise d'ouvrage
- Analyse de données
- Audit opérationnel et organisationnel
- Conseil
- Test d'intrusion

SOMMAIRE

01 – LES RISQUES CYBER

Les facteurs de risque



Manque de sensibilisation des collaborateurs (ingénierie sociale)

Attaque ciblée avec un haut niveau technique se basant sur des vulnérabilités systèmes mais puisant sa force de propagation dans le facteur humain

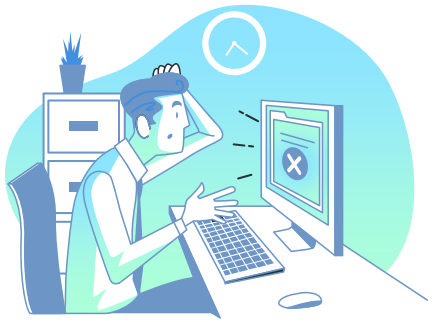
Faiblesse de l'infrastructure du système d'information ou mauvaise configuration des défenses

02 – COMMENT SE PROTÉGER

COMMENT SE PROTEGER

Problème Vs Solution

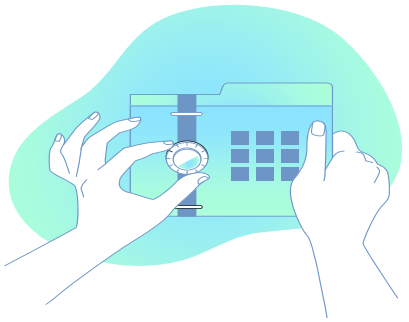
Problème



La plupart du temps pour fonctionner, une attaque informatique à besoin de deux points essentiels :

- Une **faiblesse** du système,
- Une **action non maitrisée** d'un ou plusieurs employés.

Solution



Pour limiter les risques de cyberattaque, il convient de vérifier **régulièrement** son niveau de protection **technique** et ne pas faire l'impasse sur la **formation** et la **sensibilisation** de ses collaborateurs

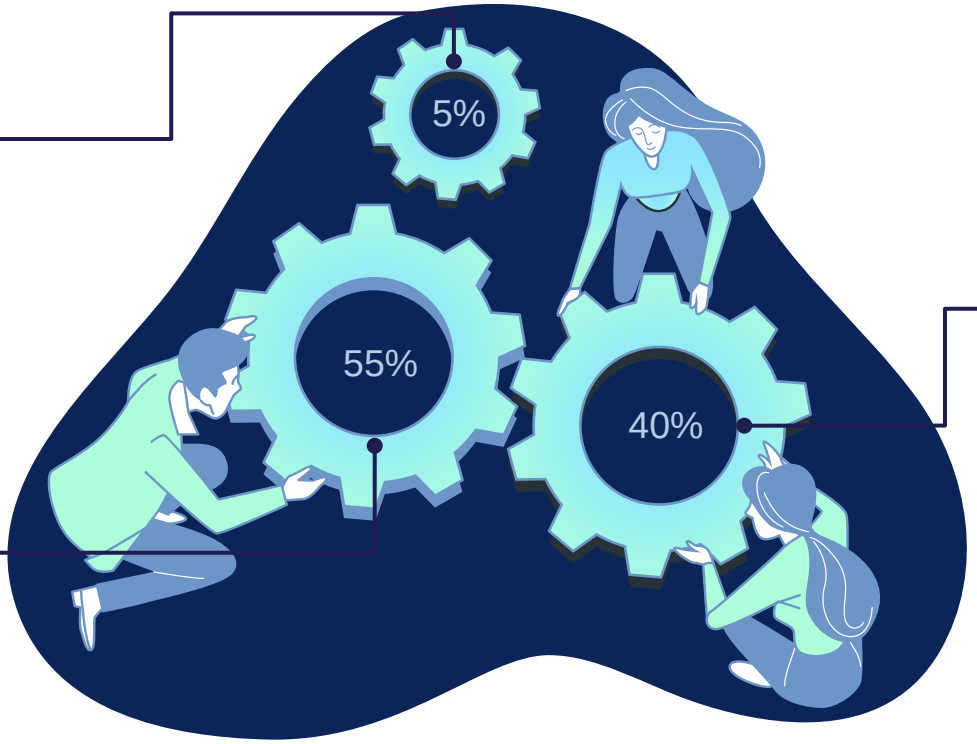
COMMENT SE PROTEGER

MISE EN ŒUVRE TECHNIQUE

Mettre en place des solutions techniques de défense

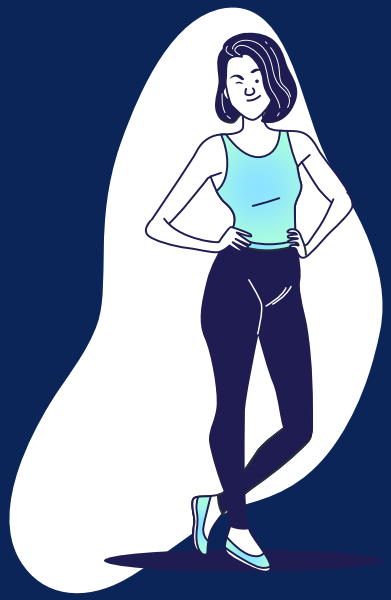
ANTICIPATION

Se préparer à subir une cyber attaque



SENSIBILISATION

Former les collaborateurs



03 – LES ÉQUIPES DE CYBERSECURITÉ

BLUE TEAM

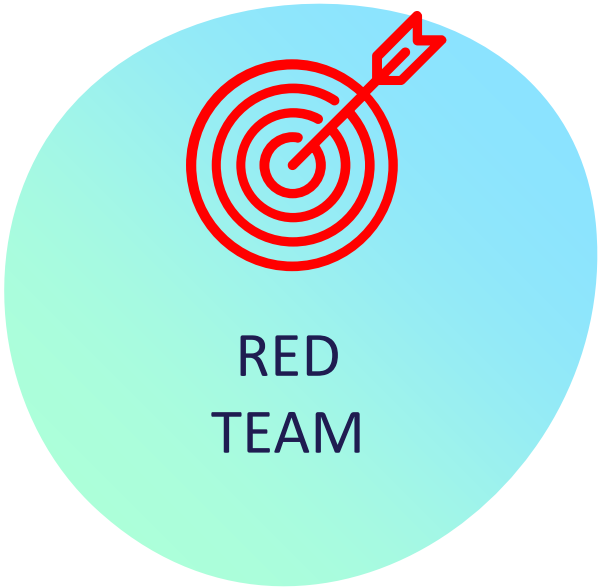
- Blue Team (Équipe défensive) : Elle met en place la défense de l'entreprise et est en charge de protéger activement l'entreprise (Centre sécurité opérationnelle(SOC), RSSI…)
- Elle a pour mission notamment :
  - La gouvernance
  - La gestion des risques
  - La réponse à incident
  - Intelligence de la menace
- Souvent internalisée, elle pratique peu d'exercices d'attaque

Equipe offensive

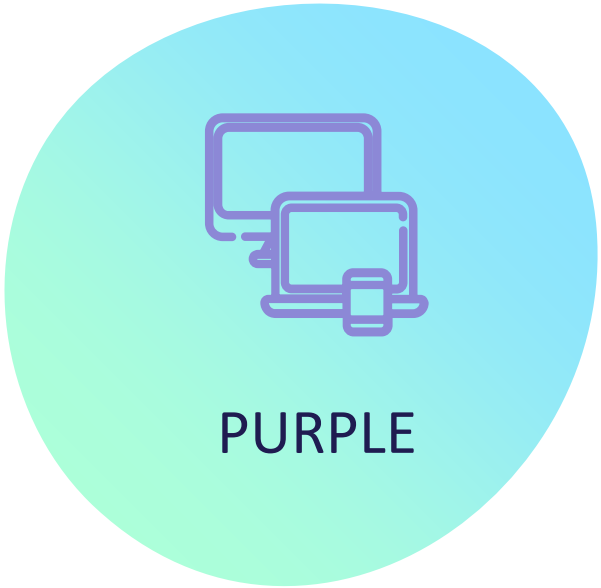
RED TEAM

- Red Team (Équipe offensive) : Elle mène le test d'intrusion. Elle utilise les techniques des attaquants pour arriver à ses fins. Bien sûr, rien d'illégal n'est entrepris mais les actions collent le plus possible à une véritable attaque informatique. Souvent, ce sont les groupes étatiques qui sont copiés

- L'équipe est souvent externe et contribue peu à la défense



PURPLE TEAM



- De ces deux équipes, en découle une troisième sous le nom de Purple team (Équipe intermédiaire). Cette équipe va conduire des tests d'intrusion mais va aussi contribuer à l'amélioration de la défense en apportant à la Blue Team des éléments pour mieux se défendre (indicateur de compromission, scenarii d'entrainement …)

- L'objectif est ici d'améliorer considérablement la défense avec des tests d'intrusion réguliers qui permettront de faire évoluer les mécanismes et techniques de sécurisation

Équipe cliente

CHEZ LE CLIENT

- Chez nos clients, le top management de l'entreprise va être notre principal interlocuteur pour la réalisation de nos prestations. En règle général, il signe la lettre de mission pour des prestations cybers.

- De plus, le client va lui-même décider de la portée des actions des équipes d'audit de sécurité sur son SI. Ainsi il va **maitriser toutes les données** mises à disposition des équipes de cybersécurité

Définition

Le PENTEST

Méthode d'évaluation de la sécurité d'un SI en mettant en évidence, au travers de preuves, les failles systèmes, applicatives et humaines d'une entreprise.

	BLACK BOX	GREY BOX	WHITE BOX
Moyens dont dispose l'attaquant	Pas d'informations	Peu d'informations	Toutes informations nécessaires
Objectif	Simulation d'attaque depuis l'extérieur	Simulation d'attaque de l'intérieur	Tester l'architecture complète

LE TEST D'INTRUSION

Un atout majeur

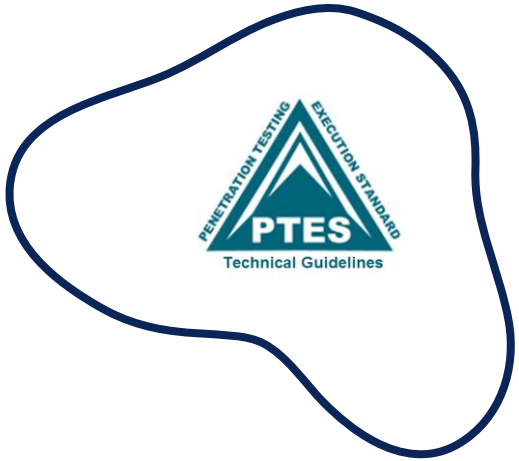
Elever le niveau de sécurité

La mise en place de tests d'intrusion permet **d'élever rapidement** le niveau de sécurité global

Se préparer

Le test d'intrusion permet de challenger sa protection informatique en **anticipant** la menace, en **sensibilisant** ses employés et en apportant une grand aide au déploiement de **solutions techniques** !

Méthodologie

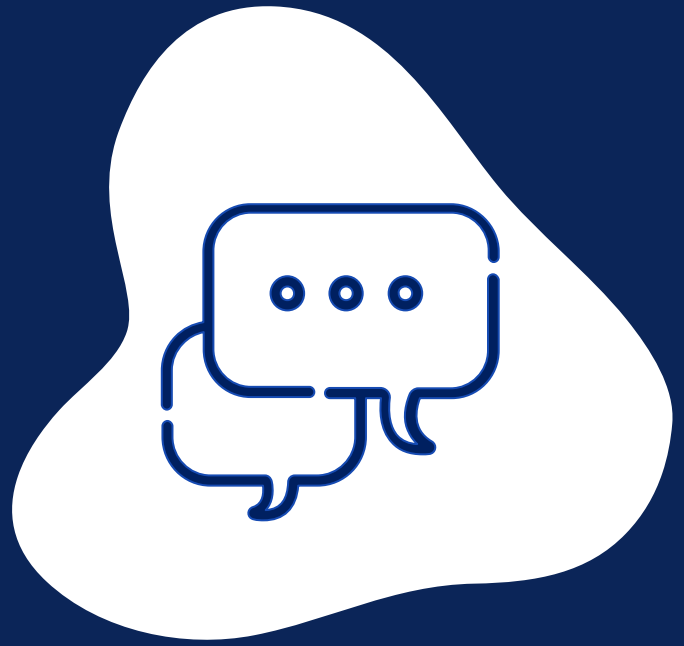


Pré-Engagement → Récolte d'informations → Analyse des faiblesses → Analyse des vulnérabilités → Exploitation → Post-Exploitation

Une nouvelle forme de test d'intrusion

Copier les actions d'un attaquant afin d'être au plus proche de la menace

- Orientation, découverte, énumération, OSINT
- Ingénierie sociale, phishing
- Backdoor, Evasion d'antivirus, développement de virus
- Obtention d'un accès physique et/ou logique



QUESTIONS

EXA

CORRESPONDANT MAZARS

CONSEIL

SYSTÈME D'INFORMATION

AUDIT ET CAC

EXPERTISE COMPTABLE

Pour toute question, merci de contacter :

Frédéric ANDRE
Associé
Frederic.andre@exaco.fr
06.92.68.20.99

Thomas LEONG-SHE
Manager DAS
Thomas.leong-she@exaco.fr
06.92.22.22.08

Tanguy MOREAU
Référent Cyber
tanguy.moreau @exaco.fr
06.92.50.79.27

Groupe Exa
4, Rue Monseigneur Mondon
97400 Saint-Denis
02.62.30.41.00