

# Technologies de l'information

**Cours:**

**Sécurité des systèmes  
informatiques**

**Séance # 11**

**Préparé par: Blaise Arbouet**



# DESS

# Objectifs de la séance

Se familiariser avec :

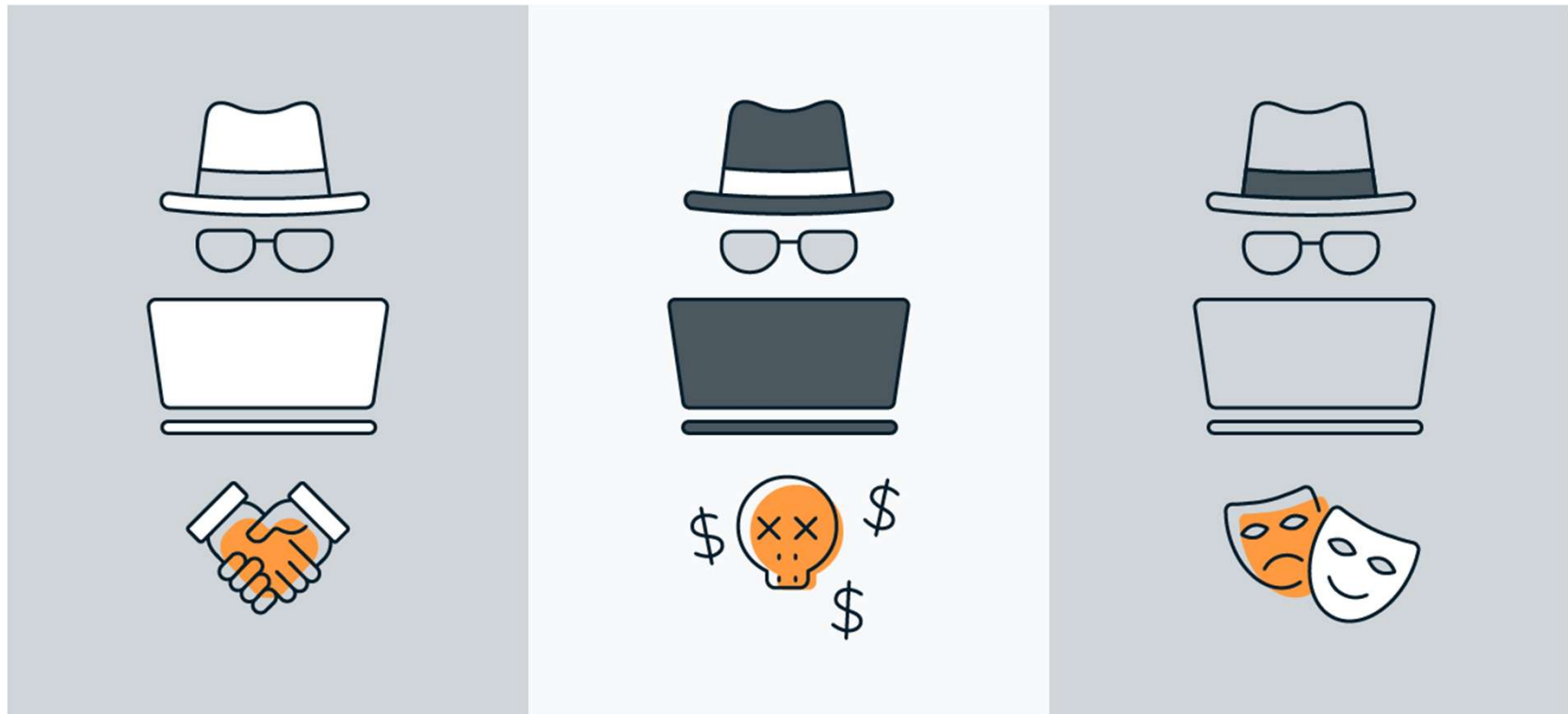
Les concepts de base entourant:

- les tests d'intrusion,
- la gestion de vulnérabilité,
- la sécurité infonuagique et
- les risques émergents

# Quelques concepts: Le piratage éthique

Le piratage éthique consiste à utiliser des compétences et des techniques de piratage pour tester la sécurité d'un système, d'un réseau ou d'une application, ainsi que pour identifier et corriger toute vulnérabilité ou faiblesse. Les hackers éthiques sont également connus sous le nom de hackers au chapeau blanc, car ils utilisent leurs compétences à des fins bonnes et éthiques, contrairement aux hackers au chapeau noir qui piratent pour des raisons malveillantes ou illégales. Le piratage éthique peut aider les organisations à améliorer leur posture de sécurité, à protéger leurs données et leurs actifs et à se conformer aux réglementations et normes.

# Types de pirates





## Pirates au chapeau noir (Black hat)

Les pirates au chapeau noir sont des cybercriminels qui piratent illégalement des systèmes dans un but malveillant. Chercher à obtenir un accès non autorisé aux systèmes informatiques est la définition du piratage chapeau noir.

Objectif: Gain financier

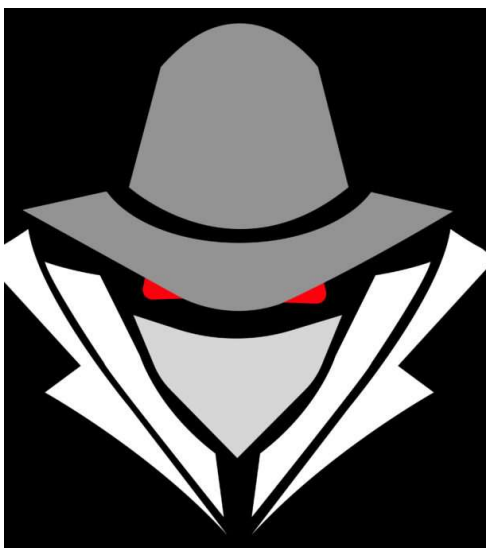
# Pirates au chapeau blanc (White hat)



Les hackers au chapeau blanc, également connus sous le nom de hackers de sécurité éthiques (Ethical hackers), identifient et corrigent les vulnérabilités. En piratant les systèmes avec la permission des organisations qu'ils piratent, les pirates informatiques tentent de découvrir les faiblesses du système afin de les corriger.

Objectif: contribuer à renforcer la sécurité globale d'Internet .

# Pirates au chapeau gris (Grey hat)



Les pirates au chapeau gris n'ont peut-être pas l'intention criminelle ou malveillante d'un pirate au chapeau noir, mais ils n'ont pas non plus la connaissance ou le consentement préalable de ceux dont ils piratent les systèmes.

Objectif: Signaler les failles découvertes . D'autres peuvent demander de l'argent en échange.

Note: Bog Bounty Program:

<https://www.cyber.gouv.qc.ca/services/programme-prime-bogues>



La liste peut  
s'allonger

## TYPES OF HACKERS



**Black Hat**  
Malicious hacker



**White Hat**  
Ethical hacker



**Gray Hat**  
Not malicious, but  
not always ethical



**Green Hat**  
New, unskilled  
hacker



**Blue Hat**  
Vengeful hacker



**Red Hat**  
Vigilante hacker

Image Credit: EverydayCyber



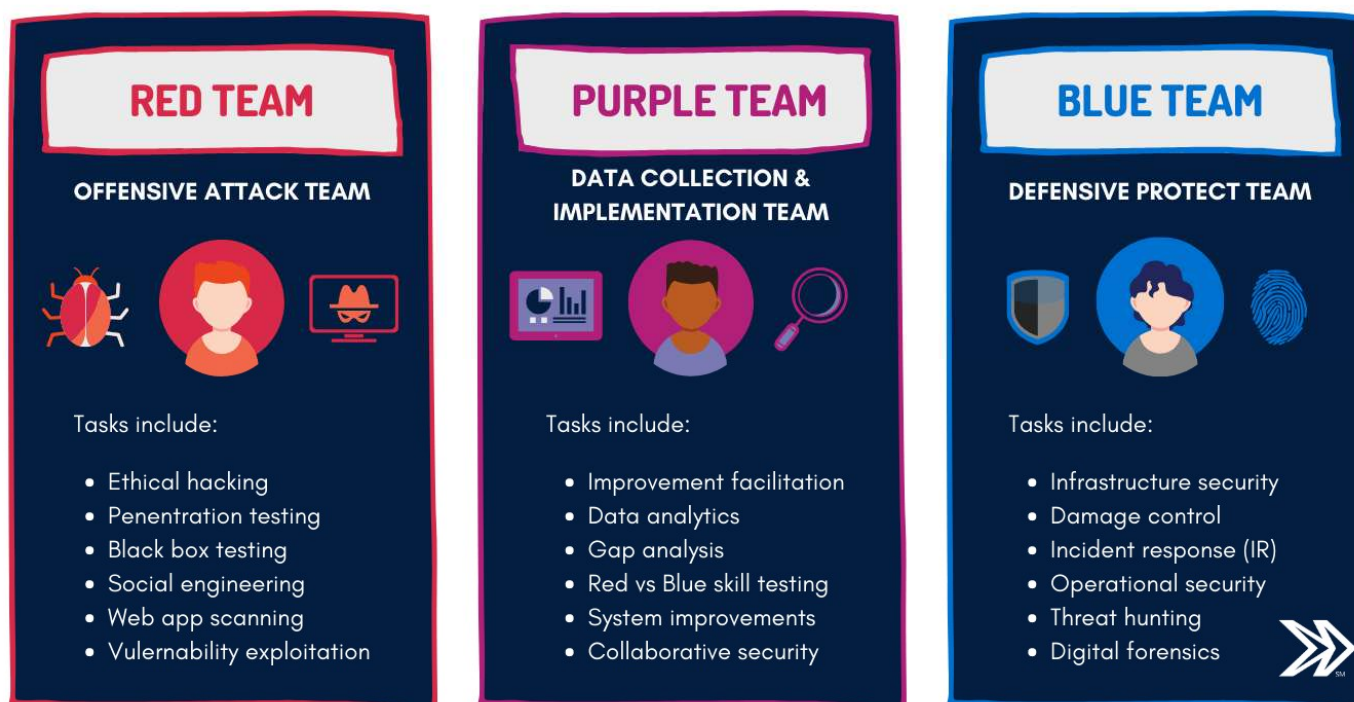
# Est-ce que le groupe Anonymous est?

- White Hat or Grey Hat Hacker?



Masque de Guy Fawkes vu lors d'une manifestation à Montréal des étudiants le 22 mai 2012, contre le projet de loi 78 dans le cadre des manifestations de 2012 au Québec.

# Les fameux groupes en cybersécurité



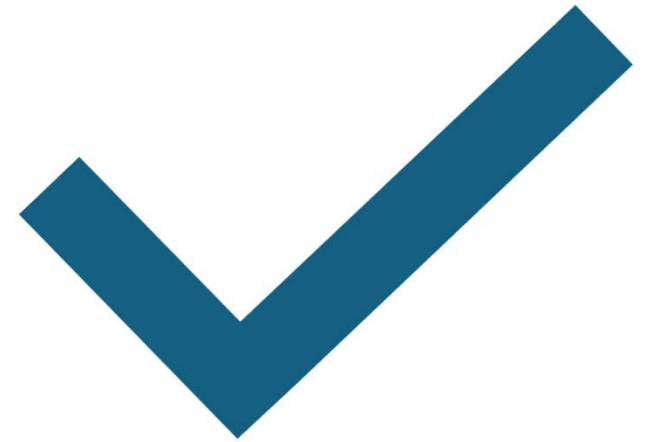
<https://www.linkedin.com/pulse/red-team-vs-purple-blue-sanjay-s-v/>

# C'est quoi un test d'intrusion

Les tests d'intrusion sont des simulations de cyberattaques réalisées pour évaluer la sécurité d'un système.

Objectif :

Identifier et exploiter les vulnérabilités pour comprendre les risques potentiels.



# Types de tests d'intrusion

	Black-Box <i>aka close box penetration testing</i>	Grey-Box <i>combination of black box and white box testing</i>	White-Box <i>aka open box penetration testing</i>
Goal	Mimic a true cyber attack	Assess an organization's vulnerability to insider threats	Simulate an attack where an attacker gains access to a privileged account
Access Level	Zero access or internal information	Some internal access and internal information	Complete open access to applications and systems
Pros	Most realistic <i>Testing is performed from point of view of attacker</i>	More efficient than black-box and saves on time and money <i>Testing is performed from point of view of attacker</i>	More comprehensive, less likely to miss a vulnerability and faster <i>Testing is performed from point of view of attacker</i>
Cons	Time consuming and more likely to miss a vulnerability	No real cons for this type of testing	More data (ex, source code) is required to be released to the tester and more expensive

SOURCE:



# Principaux avantages d'un pentest :

## Amélioration de la posture de sécurité

- Défense proactive
- Formation et préparation

## Identification des vulnérabilités de sécurité

- Simulation attaque réelles
- Priorisation de la remédiation

## Conformité aux normes de sécurité

- Respect de la réglementation
- Eviter de pénalités

# Qu'est-ce qu'un pentester ?

Ces sont des hackers éthiques, pentesters, personnel offensif, chercheurs en sécurité. Les titres se présentent sous de nombreuses formes, mais en bref : les tests de pénétration, pentesting ou pen test sont un domaine hautement spécialisé de la cybersécurité, nécessitant un mélange unique de compétences, de connaissances et de normes éthiques élevées.

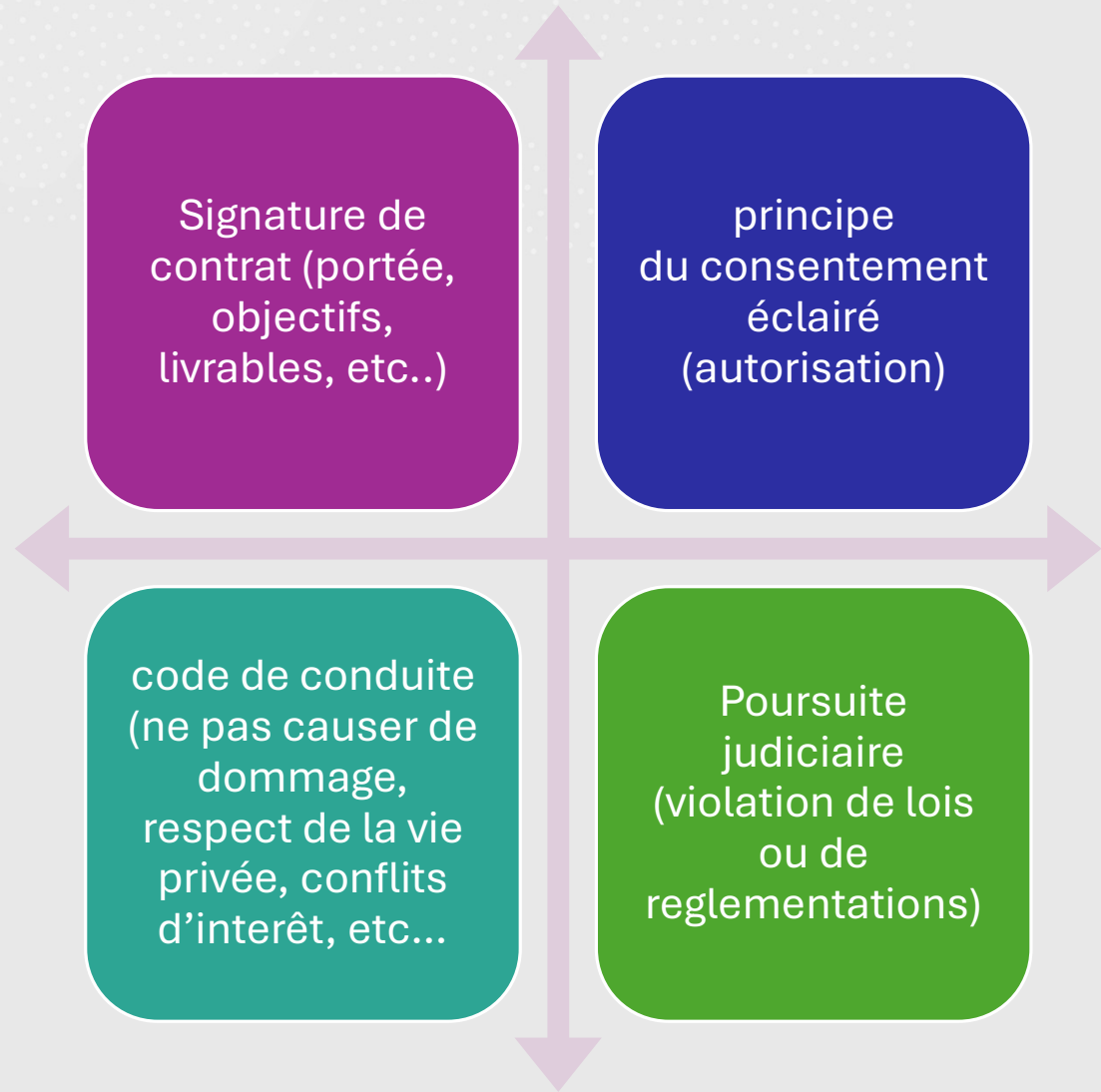
Les professionnels qui effectuent ces tests sont généralement des personnes ayant une compréhension approfondie des systèmes informatiques et des techniques de piratage.



# Phases d'un pentest



# Cadre juridique et éthique du piratage éthique





# Etape # 1: Pré-engagement



Définition des objectifs du test : L'équipe de tests d'intrusion et le client collaborent pour définir des objectifs clairs, conformes aux exigences de sécurité spécifiques de l'organisation.



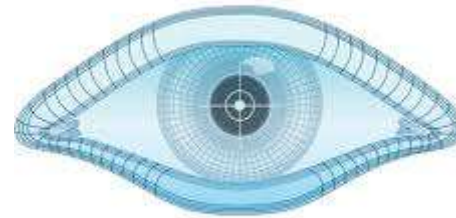
Détermination du périmètre du test : Le prestataire de services et le client définissent les systèmes, réseaux et applications concernés par le test. Ils identifient également les zones ou systèmes interdits, permettant ainsi aux deux parties de savoir à quoi s'attendre lors du processus de test. Cet accord définit les règles d'engagement.



Abordez les implications juridiques et contractuelles : Ils abordent ensuite les aspects juridiques, tels que les responsabilités potentielles et les autorisations requises pour le processus de test.

## Etape # 2: Reconnaissance

il s'agit de la première phase au cours de laquelle le pirate informatique éthique rassemble des informations sur la cible, telles que son nom de domaine, son adresse IP, la topologie du réseau, son système d'exploitation, ses services, ses applications et ses utilisateurs. . La reconnaissance peut être passive ou active, selon que le hacker éthique interagit ou non avec la cible. Certains des outils utilisés pour la reconnaissance sont Nmap, Wireshark, Shodan et Google Dorks.



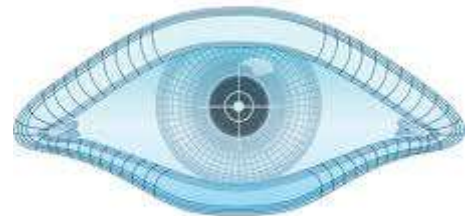
## Etape # 3: Analyse/Balayage/Découverte



le pirate informatique éthique analyse la cible à la recherche de vulnérabilités, telles que des erreurs de configuration, des logiciels obsolètes, des mots de passe faibles et des ports ouverts. L'analyse peut être effectuée manuellement ou automatiquement, à l'aide d'outils tels que Nessus, Metasploit, Burp Suite et ZAP

## Etape # 4: Exploitation

Le pirate informatique éthique exploite les vulnérabilités découvertes lors de la phase d'analyse et accède au système, au réseau ou à l'application cible. L'exploitation peut être effectuée à l'aide d'exploits existants ou en développant des exploits personnalisés à l'aide d'outils tels que Metasploit, Nmap, SQLmap et Hydra



## Etape # 5: Post-exploitation

Le pirate informatique éthique effectue des actions sur la cible après avoir obtenu l'accès, telles que l'augmentation des privilèges, le maintien de la persistance, l'installation de portes dérobées, l'exfiltration de données et la dissimulation. La post-exploitation peut être effectuée à l'aide d'outils tels que Mimikatz, PowerShell, Netcat et RDP.



## Etape # 6: Rapport

Le pirate informatique éthique documente et communique les résultats, tels que les vulnérabilités, les exploits, l'impact et les recommandations, à l'organisation cible. La création de rapports peut être effectuée à l'aide d'outils tels que Microsoft Word, Excel, PowerPoint et Snagit.



# Outils et techniques de pentest

## Outils courants :

- Nmap : analyse du réseau
- Metasploit : cadre d'exploitation
- Burp Suite : test d'applications Web
- Wireshark : analyse du trafic réseau
- John the ripper
- Kali Linux

## Techniques

- Ingénierie sociale, Injection SQL, Attaque XSS



## Exemple de rapport pentest





# Qu'est-ce que la gestion des vulnérabilités ?

Un processus continu d'identification, d'évaluation, de priorisation et d'atténuation des vulnérabilités dans les logiciels et les systèmes.

Éléments clés :

- Identification : Découvrir les vulnérabilités grâce à des analyses, des tests et une surveillance.
- Évaluation : Analyser et hiérarchiser les risques en fonction de leur gravité et de leur impact potentiel.
- Atténuation : Appliquer des correctifs, des mises à jour ou d'autres correctifs.
- Examen : Surveiller et réévaluer en permanence les nouvelles vulnérabilités.

# Processus de gestion des vulnérabilités

---

## 1) Identification des vulnérabilités

---

Analyses régulières à l'aide d'outils tels que Nessus, OpenVAS, Qualys

---

## 2) Évaluation des vulnérabilités

---

Déterminer la gravité à l'aide d'un système de notation des risques tel que CVSS (Common Vulnerability Scoring System).

---

## 3) Priorisation et correction

---

Traiter d'abord les vulnérabilités à haut risque avec des correctifs.

---

## 4) Vérification

---

Confirmer que les vulnérabilités ont été efficacement résolues.

---

## 5) Rapports et documentation

---

Créer un rapport détaillé pour les parties prenantes et examinez le processus de correction.

# Outils de gestion des vulnérabilités

---

Outils populaires :

---

Nessus : analyse complète des vulnérabilités

---

QualysGuard : sécurité basée sur le cloud

---

OpenVAS : scanner de vulnérabilité open source

---

Rapid7 InsightVM : gestion des vulnérabilités en temps réel

---

Caractéristiques des outils :

---

Analyse automatisée, alertes en temps réel, intégration de la gestion des correctifs

# Tests d'intrusion vs gestion de vulnérabilités

Aspect	Tests d'intrusion	Gestion de vulnérabilités
Objectif	Identifier les failles exploitables	Identifier et gérer toutes les failles
Fréquence	Périodique, annuelle ou semestrielle	Processus continu
Portée	Scénario d'une attaque simulée	Analyse approfondie de tous les systèmes
Outils	Nmap, Metasploit, BurpSuite	Nessus, Qualys, OpenVas
Résultat	Exploitation et évaluation des risques	Atténuation et correction des vulnérabilités

## Avantages d'une gestion efficace des vulnérabilités et des tests d'intrusion

### Posture de sécurité améliorée :

- Identifie de manière proactive les risques avant leur exploitation.

### Conformité réglementaire :

- Aide à respecter les normes telles que GDPR, PCI-DSS, HIPAA.

### Réduction du risque de violation :

- Atténue les menaces potentielles et minimise la surface d'attaque.

### Confiance renforcée :

- Renforce la confiance des clients dans la protection des données.

# Défis en matière de tests d'intrusion et de gestion des vulnérabilités

## Limitations des ressources :

- Contraintes de temps, de budget et de personnel qualifié.

## Menaces en constante évolution :

- De nouvelles vulnérabilités et de nouveaux vecteurs d'attaque apparaissent régulièrement.

## Faux positifs et négatifs :

- Des analyses inefficaces peuvent conduire à des vulnérabilités manquées ou à des alertes inutiles.

## Intégration aux processus métier :

- Équilibrer la sécurité avec l'efficacité opérationnelle.

# Bonnes pratiques de mise en œuvre

## Tests et analyses réguliers :

- Planifiez des tests d'intrusion et des analyses de vulnérabilité réguliers.

## Donner la priorité aux vulnérabilités à haut risque :

- Utilisez l'évaluation basée sur les risques pour vous concentrer en premier sur les problèmes critiques.

## Automatisez lorsque cela est possible :

- Tirez parti des outils automatisés pour une analyse et des rapports cohérents.

## Mettez à jour et corrigez les systèmes :

- Appliquez rapidement les mises à jour de sécurité pour réduire l'exposition.

## Surveillance continue :

- Mettez en œuvre une surveillance continue pour la détection des menaces en temps réel.

# Définition du cloud computing

---

Le cloud computing gère les ressources partagées par le biais de l'abstraction, ce qui permet une orchestration, une mise à disposition, une mise à l'échelle et une mise hors service rapides. Il fournit un modèle d'utilité à la demande avec des avantages tels que la collaboration, l'agilité, l'élasticité, la disponibilité, la résilience et la réduction des coûts.

---

Voici les définitions du cloud computing selon le National Institute of Standards and Technology (NIST) des États-Unis, l'International



## Définitions de base (suite)

---

**NIST SP 800-145 defines cloud computing as:** “[A] model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

---

---

**ISO/IEC 22123-1:2023 defines cloud computing as:** “[A] paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.”

# Définition selon AWS

Le **cloud computing** est le déploiement **à la demande** de puissance de calcul, de stockage, de bases de données, d'applications et d'autres ressources informatiques **par Internet**, avec une **tarification à l'utilisation**.



# Les avantages de l'infonuagique



Paielement à l'usage (CAPEX-OPEX)



Economies d'échelle massives



Capacité adaptée aux besoins de l'organisation



Vitesse et agilité



Accélérer l'innovation

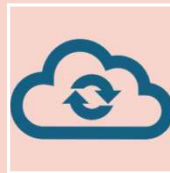


Déploiement mondial en quelques minutes

# Caractéristiques de l'infonuagique



**1) Le libre-service à la demande** signifie que les utilisateurs peuvent demander des services et des logiciels sophistiqués au fournisseur de services cloud qui provisionne automatiquement le service, généralement en quelques millisecondes ou secondes.



**2) L'accès au réseau étendu**, ce qui signifie que l'accès aux ressources cloud est disponible à partir de plusieurs types d'appareils et de plusieurs emplacements.

# Caractéristiques (suite)



## 3- Mise en commun des ressources



D'un point de vue technologique, on a besoin de trois ressources principales :



a) **le calcul** : la capacité à récupérer des instructions, à les décoder, à les exécuter et à stocker les résultats. Essentiellement la capacité à exécuter du code.



b) **le stockage** : vous devez pouvoir stocker un tas de bits quelque part : les données et le code.



c) **le réseau** : vous devez pouvoir déplacer un tas de bits partout.

## Caractéristiques (fin)

---

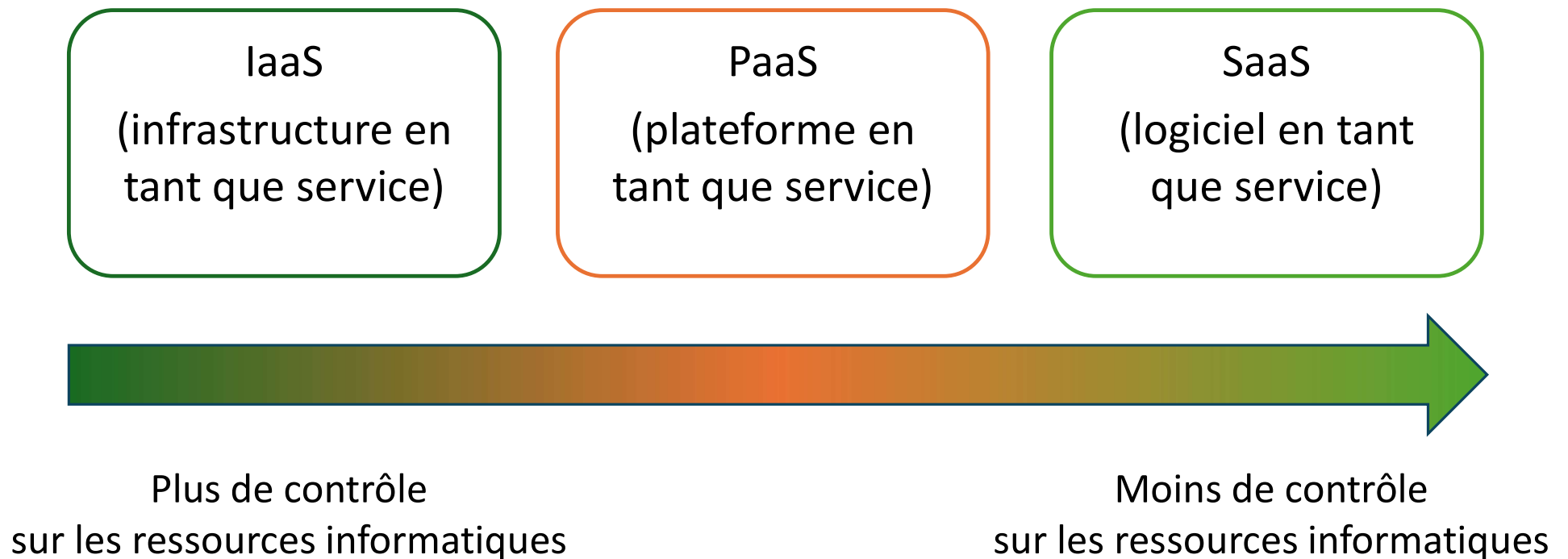
### 4) **Élasticité et évolutivité rapides.**

Vous avez la possibilité de provisionner et de déprovisionner rapidement des ressources dans le cloud.

---

5) **Le service mesuré**, ce qui signifie que le fournisseur de services cloud surveille de près votre utilisation du cloud et que vous ne payez que pour ce que vous utilisez.

# Modèles de service cloud





# IaaS

L'infrastructure en tant que service est un environnement dans lequel les clients peuvent déployer une infrastructure virtualisée : serveurs, appareils, stockage et composants réseau. En gros, cela permet à un client de recréer un centre de données physique entier sous forme de composants virtualisés : pare-feu virtuels, routeurs virtuels, serveurs virtuels, etc.



# Services IaaS populaires :

- AWS EC2.
- Rackspace.
- Google Compute Engine (GCE).
- Digital Ocean.
- Microsoft Azure.
- Magento 1 Enterprise Edition.





# PaaS

Platform as a Service fournit les services et fonctionnalités permettant aux clients de développer et de déployer des applications personnalisées. Les clients peuvent créer leurs propres applications personnalisées sans avoir à se soucier de toute la complexité sous-jacente comme les serveurs, le réseau et le stockage.

# Services PaaS populaires :

AWS Elastic Beanstalk.

Heroku.

Windows Azure (principalement utilisé comme PaaS).

Force.com.

Google App Engine.

OpenShift.

Apache Stratos.

Adobe Magento Commerce Cloud.





# SaaS

Et le logiciel en tant que service est un outil dans lequel un client peut louer l'accès à une application hébergée dans le cloud.

# Services SaaS populaires :

BigCommerce

Google Workspace,  
Salesforce.

Dropbox.

MailChimp.

ZenDesk.

DocuSign.


Slack.


Hubspot.



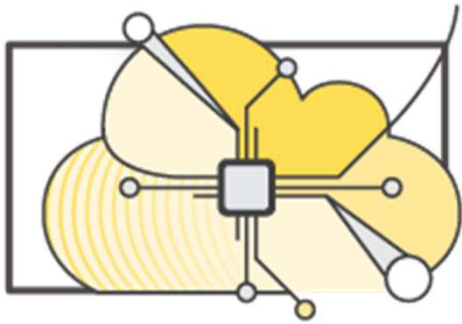
# Modèles de cloud en résumé

On-site	IaaS	PaaS	SaaS
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

 You manage

 Service provider manages

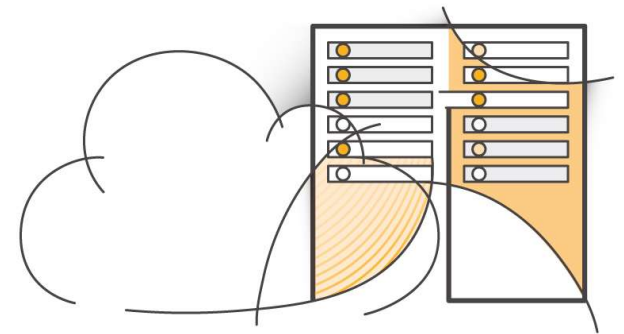
# Modèles de déploiement de cloud computing



**Cloud  
Public**



**Hybride**



**Sur site  
(cloud privé)**

# Le cloud public

Le cloud public désigne les services cloud accessibles à tous, c'est-à-dire au public. Un fournisseur de services cloud possède et exploite une infrastructure cloud ouverte à l'usage du grand public.





## Le cloud privé

Le cloud privé, en revanche, est une infrastructure cloud fournie pour une utilisation exclusive par un seul client. Les clouds privés peuvent être détenus et exploités par le client ou par un fournisseur de services cloud. Ils peuvent exister sur site ou hors site, et être physiquement ou logiquement séparés des autres clients.

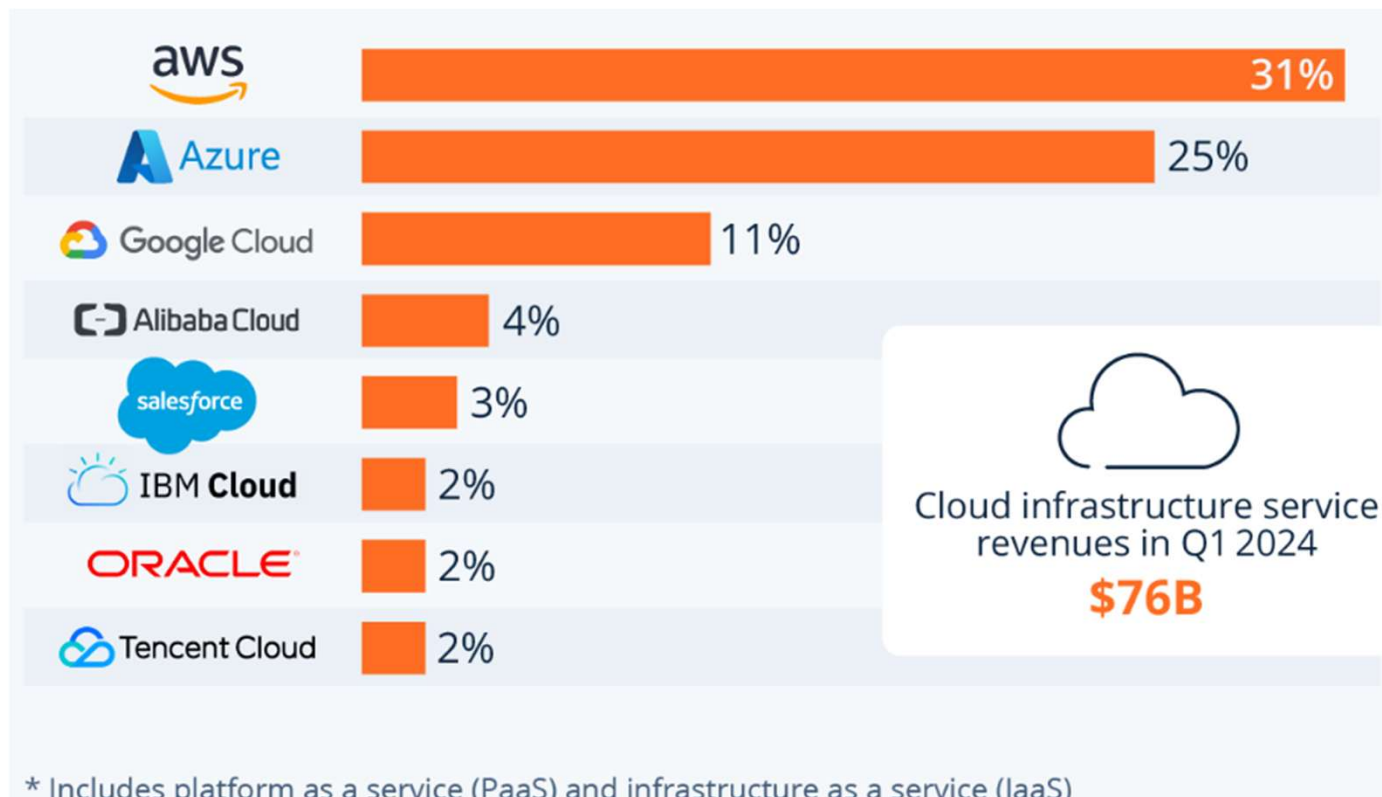
# Le cloud communautaire

Le cloud communautaire est une infrastructure cloud accessible uniquement à une petite communauté d'organisations partageant des préoccupations similaires (exigences similaires en matière de sécurité et de réglementation, par exemple).

# Le cloud hybride

Le cloud hybride est simplement une combinaison de cloud public, privé et communautaire. Par exemple, il est très courant que les grandes organisations disposent de leur propre cloud privé sur site dédié pour les données sensibles, et qu'elles utilisent également le cloud public pour les données et charges de travail moins sensibles. Elles ont donc un modèle hybride.

# Quid des fournisseurs infonuagiques?



**SOURCE:**  
**statista**

# Qu'est-ce que le modèle de responsabilité partagée ?

Pour mieux comprendre qui est responsable de la sécurité dans le cloud, nous devons faire référence à ce que l'on appelle le modèle de responsabilité partagée.

Le modèle de responsabilité partagée est un cadre qui permet de différencier quand le fournisseur de cloud est responsable de la sécurité et quand votre organisation est responsable de la sécurité, en fonction de ce qui est déployé dans le cloud.

# Responsabilités de sécurité des IaaS, PaaS et SaaS



Pour l'infrastructure en tant que service (IaaS), le CSP sécurise l'infrastructure de base, tandis que le CSC est responsable de tout ce qui est construit sur cette dernière.



La plateforme en tant que service (PaaS) se situe au milieu, le CSP sécurisant la plateforme et le CSC gérant leurs implémentations, y compris la configuration des fonctionnalités de sécurité.

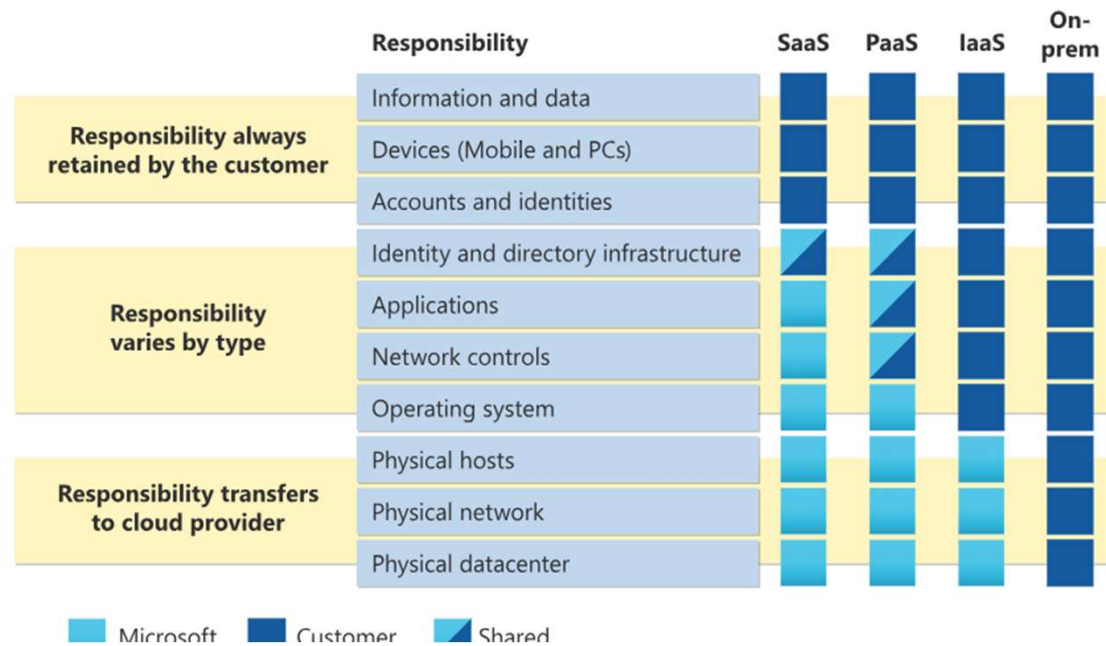


Dans le logiciel en tant que service (SaaS), le CSP assume la plupart des responsabilités de sécurité, laissant au CSC le soin de gérer les autorisations et les droits des applications.

## Rôles de courtiers infonuagiques (Cloud broker)

Cependant, la présence de courtiers ou d'intermédiaires cloud peut compliquer ces rôles. Dans ce cas, il serait judicieux de répartir les responsabilités de chacun à un niveau granulaire. Si un CSP présente des lacunes dans les contrôles de sécurité que le CSC ou les intermédiaires ne peuvent pas combler, optez pour un autre CSP.

# Répartition de la responsabilité chez Azure

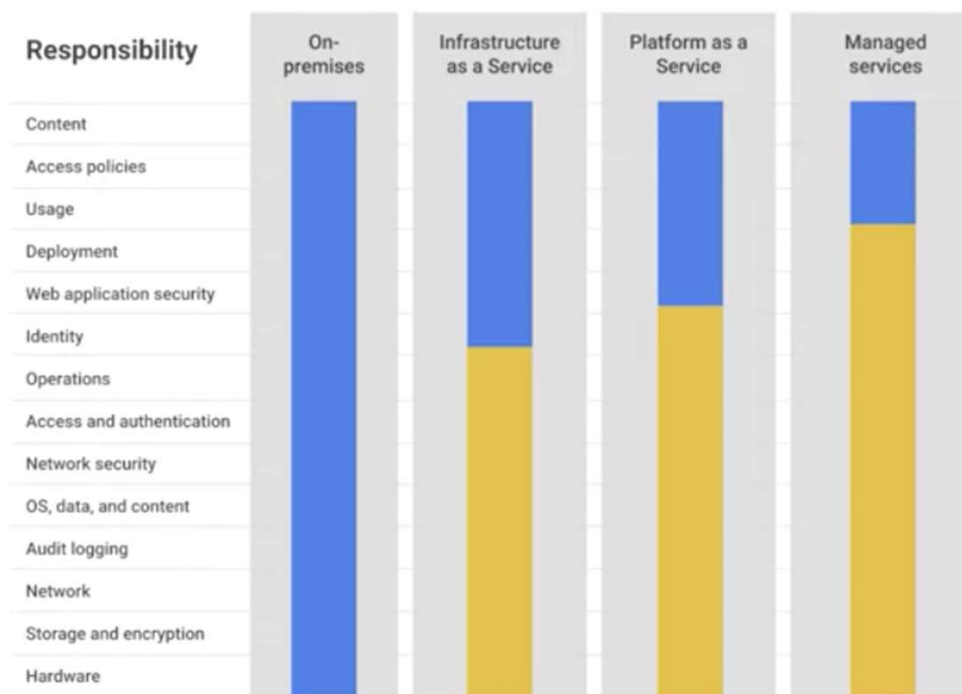




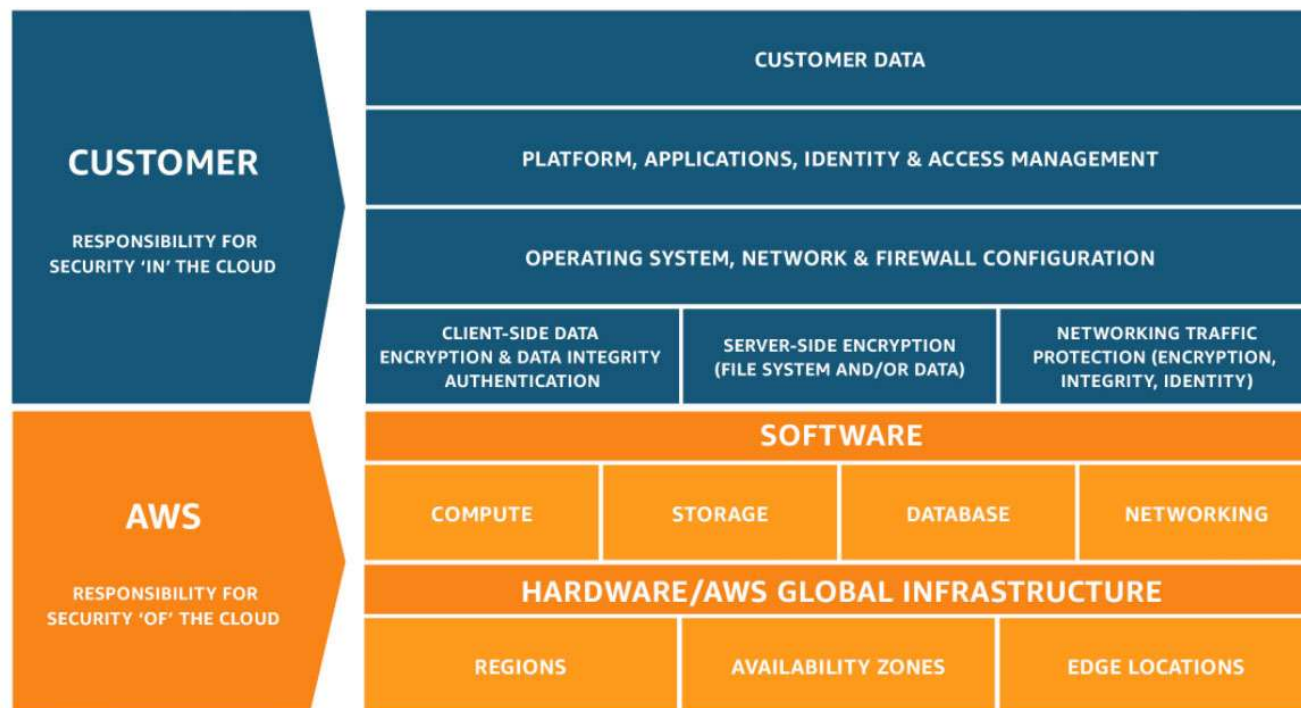
# Répartition de la responsabilité chez Google

- Google is responsible for managing its infrastructure security.
- You are responsible for securing your data.
- Google helps you with best practices, templates, products, and solutions.

■ Customer-managed  
■ Google-managed



# Répartition de la responsabilité chez AWS



# Risques émergents

Un risque émergent est un risque qui évolue dans des domaines et selon des modalités où le corpus de connaissances disponibles est faible.

Les risques émergents en cybersécurité évoluent rapidement en raison de l'adoption massive du numérique, de l'IA, de l'IoT, et de l'augmentation des attaques sophistiquées.

# Liste (1)

## **Attaques basées sur l'IA (offensive AI)**

- **Exemples** : Deepfakes pour l'ingénierie sociale, génération de malwares polymorphes par IA.
- **Risques** : Tromperie accrue, contournement des systèmes traditionnels de détection.

## **Vulnérabilités dans l'IoT et les objets connectés**

- **Exemples** : Appareils médicaux, domotique, capteurs industriels.
- **Risques** : Failles non corrigées, manque de mises à jour, surfaces d'attaque élargies.

# Liste(2)

## **Ransomwares en tant que service (RaaS)**

- **Tendance** : Industrialisation des ransomwares via des plateformes accessibles.
- **Risques** : Multiplication des attaques, impact économique croissant

## **Cyberattaques sur les chaînes d'approvisionnement (supply chain attacks)**

- **Exemples** : Attaques de type SolarWinds, compromission de bibliothèques logicielles.
- **Risques** : Dissémination des malwares via des partenaires de confiance.

## Cybersecurity Threats for 2030



# Références

- <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Foresight%20Cybersecurity%20Threats%20for%202030.pdf>
- <https://www.truesec.com/security/penetration-testing>
- <https://www.hackerone.com/knowledge-center/7-pentesting-tools-you-must-know-about>
- <https://www.fortinet.com/resources/cyberglossary/vulnerability-scanning-compare>
- <https://www.avast.com/c-hacker-types>
- <https://www.securitymetrics.com/blog/6-steps-penetration-test>
- <https://torii-security.fr/tests-dintrusion-tout-ce-quil-faut-savoir/>
- <https://www.getastra.com/blog/security-audit/penetration-testing-phases/>
- <https://www.securitymetrics.com/blog/6-steps-penetration-test>
- <https://www.microsoft.com/en-us/security/business/security-101/what-is-cloud-security>

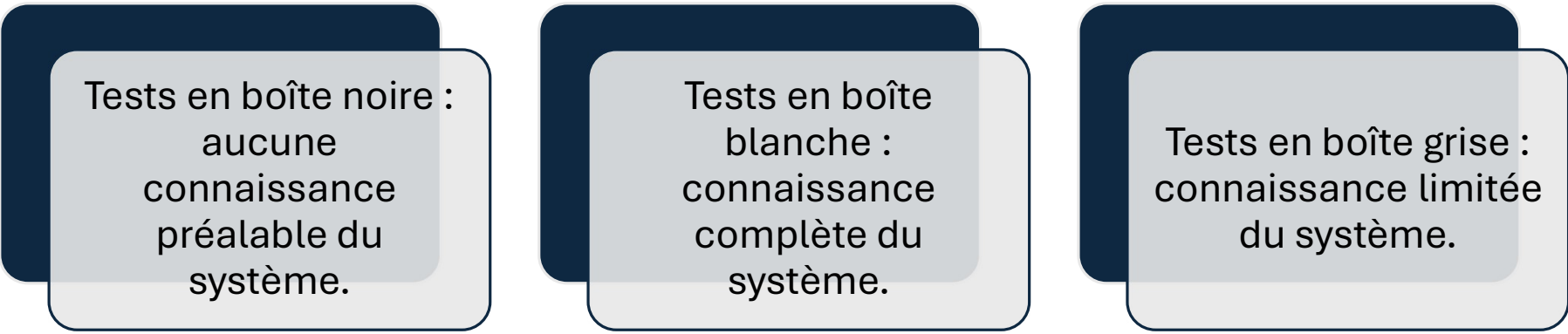
# Questions ?

En avez-vous?





# Types de tests d'intrusion



Tests en boîte noire :  
aucune  
connaissance  
préalable du  
système.

Tests en boîte  
blanche :  
connaissance  
complète du  
système.

Tests en boîte grise :  
connaissance limitée  
du système.