



La Cyber-Résilience à l'Ère de l'IA

➤ Protégez Vos Actifs Numériques

ETAT DES MENACES CYBER 2025

Évolution et tendances des cyber-risques actuels



Hameçonnage

1,9 Million

de consultations d'articles (+47%)



Violations de données

+82%

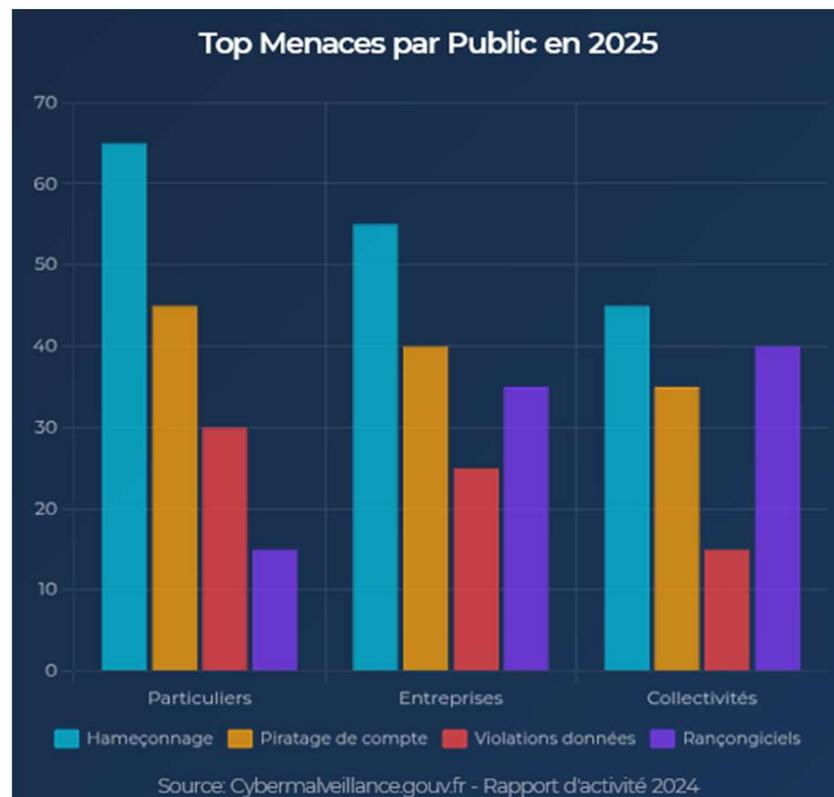
4ème menace pour les particuliers



Piratage de compte

+55%

2ème menace tous publics



Tendances clés

- › Multiplication et diversification des types de menaces
- › Forts impacts sur les jeunes publics (sextorsion, cyberharcèlement)

LA CYBERCRIMINALITE : UN BUSINESS FLORISSANT

Modèles économiques cybercriminels



Ransomware-as-a-Service (RaaS)

Location de ransomware prêt à l'emploi avec support technique
Modèle d'affiliation : 70/30% entre affiliés et développeurs



Marché noir des données

Vente de données personnelles et d'entreprises
Prix moyen : 40-200€ par 1000 enregistrements



Cyber-attaques pilotées par l'IA

Automatisation des attaques et contournement des défenses
Croissance de +225% en 2024 vs 2023



10,5Mds\$

Coût global des rançongiciels en 2025

15%

Croissance annuelle du marché cybercriminel

83%

Des groupes avec structure organisationnelle

70/30

Répartition revenu affilié/développeur RaaS

Tarifs observés sur le Dark Web

Accès VPN compromis	5-10€
DDoS à la demande (1h)	15-50€
Kit de phishing	20-80€
Accès admin compromis	1000-15000€

SCC IT MAKES SENSE

LES ACTEURS DES CYBERATTAQUES

Motivations, méthodes et cibles des principaux protagonistes

Groupes sponsorisés par États

Motivations :
Espionnage, sabotage, avantages géopolitiques

Méthodes :
APT 0-day Supply chain

Exemples :
APT28, Lazarus, Equation Group

Sophistication ★★★★★
Ressource ★★★★★

Secteurs ciblés

- › Défense & Aérospatiale
- › Infrastructures critiques
- › Gouvernements étrangers
- › R&D de haute technologie

Groupes cybercriminels

Motivations :
Profit financier, extorsion, vente de données

Méthodes :
Ransomware Phishing BEC

Exemples :
LockBit, Conti, BlackCat/ALPHV

Sophistication ★★★★★
Ressource ★★★★★

Secteurs ciblés

- › Services financiers
- › Santé
- › Commerce de détail
- › Toute entreprise rentable

Hacktivistes

Motivations :
Idéologique, politique, mobilisation sociale

Méthodes :
DDoS Defacement Doxing

Exemples :
Anonymous, KillNet, GhostSec

Sophistication ★★★★★
Ressource ★★★★★

Secteurs ciblés

- › Sites gouvernementaux
- › Multinationales controversées

Cybermercenaires & Opportunistes

Motivations :
Profit par service, revente d'accès, opportunisme

Méthodes :
Initial Access Vulnérabilités Infostealers

Exemples :
NSO Group, IABs, Script Kiddies

Sophistication ★★★★★
Ressources ★★★★★

Secteurs ciblés

- › Sur commande (tous secteurs)
- › PME vulnérables
- › Organisations avec accès VIP
- › Individus & Entreprises ciblés

PROTECTION DES DONNEES

Méthodes de sécurisation, bonnes pratiques et conformité réglementaire

Chiffrement

Données en transit (TLS/SSL), données au repos (AES-256), E2EE

RSA AES HSM

Contrôle d'accès

Authentification MFA, principe du moindre privilège, IAM

ZTA SSO RBAC

Protection contre la perte

Solutions DLP, classification des données, backup 3-2-1

DLP CASB EDR

Bonnes Pratiques

Formation & Sensibilisation

- › Formation récurrente
- › Tests de phishing
- › Culture de sécurité

Gestion des vulnérabilités

- › Patch management
- › Tests d'intrusion
- › Veille sécurité

Obligations Réglementaires

Amendes jusqu'à 4% CA
mondial ou 20M€

HIPAA (US)

Protection des données de
santé

NIS2 (UE)

Cybersécurité pour
infrastructures critiques

LPM (FR)

Protection des OIV et
OSE

L'IA COMME OUTIL DE DEFENSE

Comment l'intelligence artificielle révolutionne la cybersécurité défensive

Reconnaissance de Motifs

Détection d'anomalies basée sur l'apprentissage automatique

Machine Learning Analyse Comportementale

Surveillance en Temps Réel

Analyse continue des flux de données et détection instantanée

SIEM Big Data 24/7

Analyse Prédictive

Anticipation des menaces et des vulnérabilités potentielles

Deep Learning Threat Intelligence

Automatisation des Réponses

Réponse aux Incidents

- › Triage automatisé
- › Containment instantané
- › Workflows prédéfinis

Auto-défense Proactive

- › Adaptation dynamique
- › Systèmes auto-réparants
- › Remédiation guidée

60%

Réduction du
temps de
détection des
menaces

80%

Automatisation
des tâches de
sécurité
répétitives

IA vs Cybersécurité Traditionnelle

Apprentissage continu

S'améliore avec chaque incident

Réactivité instantanée

Réponse en millisecondes

Analyse Big Data

Traitement de millions d'événements

Détection contextuelle

Compréhension des relations

L'IA COMME OUTIL D'ATTAQUE

Comment les cybercriminels exploitent l'intelligence artificielle

Vecteurs d'Attaques Améliorés par l'IA



Deepfakes & Usurpation d'Identité

Création de contenu trompeur indétectable pour l'œil humain

Usurpation Biométrique Fraude Audio/Vidéo



Phishing Intelligent

Personnalisation automatisée basée sur les données sociales des cibles

Spear Phishing Ingénierie Sociale

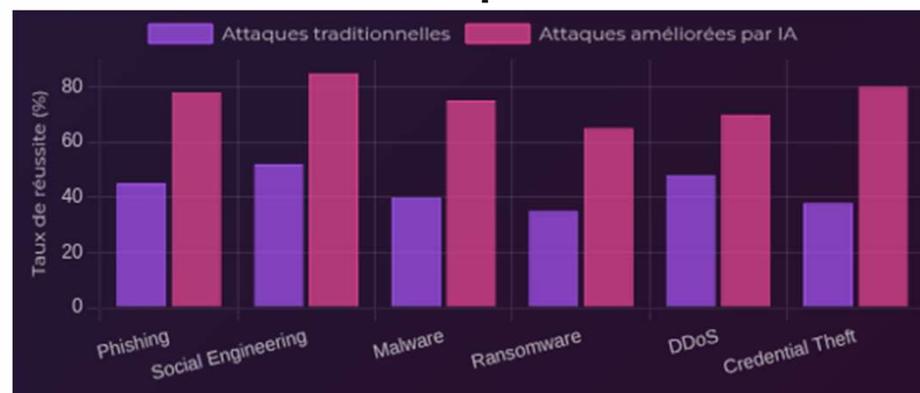


Empoisonnement des Données

Corruption des ensembles d'apprentissage des systèmes de défense

Attaques par Adversité Manipulation ML

Taux de Réussite des Attaques avec IA



Malwares Avancés par IA

Polymorphisme Intelligent

- > Mutation de code automatique
- > Contournement d'antivirus
- > Adaptation aux environnements

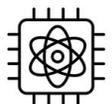
Ransomwares Contextuels

- > Ciblage précis des données
- > Demandes de rançons adaptatives
- > Analyse du "prix" optimal

TENDANCES FUTURES DE LA CYBER

Évolutions technologiques, menaces émergentes et réglementations

Technologies Émergentes en Cybersécurité



Informatique Quantique & Post-Quantique

Développement d'algorithmes résistants aux ordinateurs quantiques

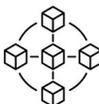
Cryptographie Post-Quantique Algorithmes Quantiques



IA Générative Défensive

Systèmes autonomes de défense intelligents adaptables

Défense Automatisée Détection Avancée



Technologies Décentralisées

Applications blockchain pour authentification et intégrité des données

Identité Décentralisée Smart Contracts

Menaces Émergentes à Surveiller

Attaques sur l'IoT 2.0

- > Smart cities vulnérables
- > Objets connectés

Menaces Multi-Cloud

- > Exfiltration inter-clouds
- > Attaques sur les APIs

Supply Chain 2.0

- > Attaques firmware précoces
- > Compromission des puces

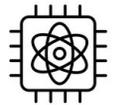
Cyberattaques XR

- > Vol d'identité métavers
- > Manipulation sensorielle

RECOMMANDATIONS

Évolutions technologiques, menaces émergentes et réglementations

Stratégie & Organisation



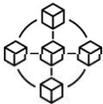
Approche Globale de Sécurité

Stratégie Zero-Trust et défense en profondeur



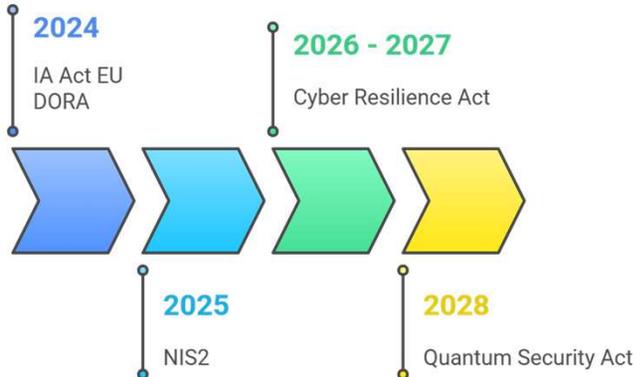
Sensibilisation & Formation

Formation régulière des équipes et simulations d'attaques



Gouvernance & Conformité

Mise en place d'un cadre réglementaire adapté



Mesures Techniques & Opérationnelles

Gestion des Accès

- ✓ Authentification multi-facteurs (MFA)
- ✓ Gestion des identités privilégiées (PAM)

Mises à Jour

- ✓ Patch management automatisé
- ✓ Veille sur les vulnérabilités

Détection & Réponse

- ✓ Solutions EDR/XDR avancées
- ✓ Monitoring continu (24/7)

Données

- ✓ Chiffrement de bout en bout
- ✓ Classification automatique

Cloud Security

- ✓ CASB & CSPM
- ✓ Sécurité conteneurs/microservices

DevSecOps

- ✓ Tests de sécurité automatisés
- ✓ Sécurité par conception



Merci

sgiai-checa@fr.scc.com

SCC France
Stand D12