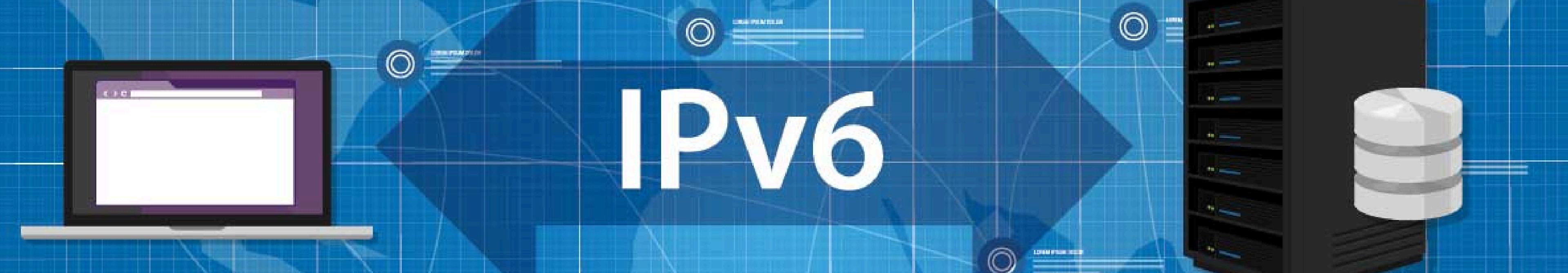


Veille Technologique : Systèmes, Réseaux et Sécurité Informatique

Exploration des protocoles réseau, vulnérabilités et sécurité. Je suis passionné par l'innovation et la cybersécurité proactive.

Cette présentation résume les principaux thèmes de ma veille technologique et les outils que j'utilise.





IPv6

Evolutions des Protocoles

Adoption croissante de l'IPv6

L'IPv6 est utilisé par 33% des internautes.

Il offre un espace d'adressage plus vaste et une meilleure gestion des adresses.

Le protocole QUIC (HTTP/3)

QUIC offre des performances et une sécurité accrues.

Il réduit la latence et améliore la fiabilité des connexions.



Nouvelles Vulnérabilités et Contre-mesures



DNS mal sécurisé

Les DNS mal sécurisés créent une porte ouverte pour les attaques.



Techniques modernes d'attaque

Attaques via protocoles obsolètes comme FTP.



Importance croissante

Outils de chiffrement et de surveillance actives.



Avancées en Cloud



Synergie
Synergie entre
infrastructures locales
et cloud.



Sécurité des
données
Sécurité des données
et conformité
réglementaire en mode
hybride.



Gestion
automatisée
Gestion automatisée
des environnements
multi-cloud avec IaC.

Infrastructure as Code (IaC)

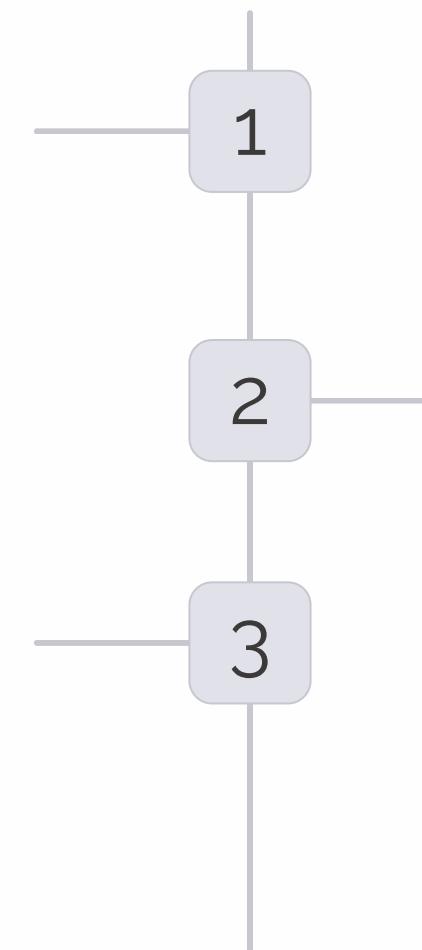
Automatisation et Infrastructure as Code (IaC)

Approche déclarative vs impérative

Gestion des configurations.

Modularité et réutilisabilité

Configurations.



Réduction des erreurs humaines

Outils comme Ansible.

Logiciels espions : 21 pays s'engagent à lutter contre la prolifération des armes numériques

Le « processus de Pall Mall », lancé par la France et le Royaume-Uni en 2024, a abouti à la signature d'un « code de bonnes pratiques ». Non contraignant, il a le mérite d'aborder des sujets cruciaux, liés notamment à l'usage abusif des logiciels espions.



Outils de Veille

- 1
- 2
- 3

Twitter

Tendances en temps réel et annonces professionnelles.

Flux RSS

Agrégation de news spécialisées (sécurité, réseaux).

Reddit et Newsletters

Discussions techniques et approfondissements.

Résultats et Perspectives

Identification rapide
Menaces émergentes.

Adaptation proactive
Évolutions technologiques.

Meilleures pratiques
Sécuriser et optimiser les infrastructures.

PRINCIPALES MENACES DE CYBERSÉCURITÉ



Ransomiciel
Les rançongiciels sont actuellement considérés comme la menace la plus préoccupante.

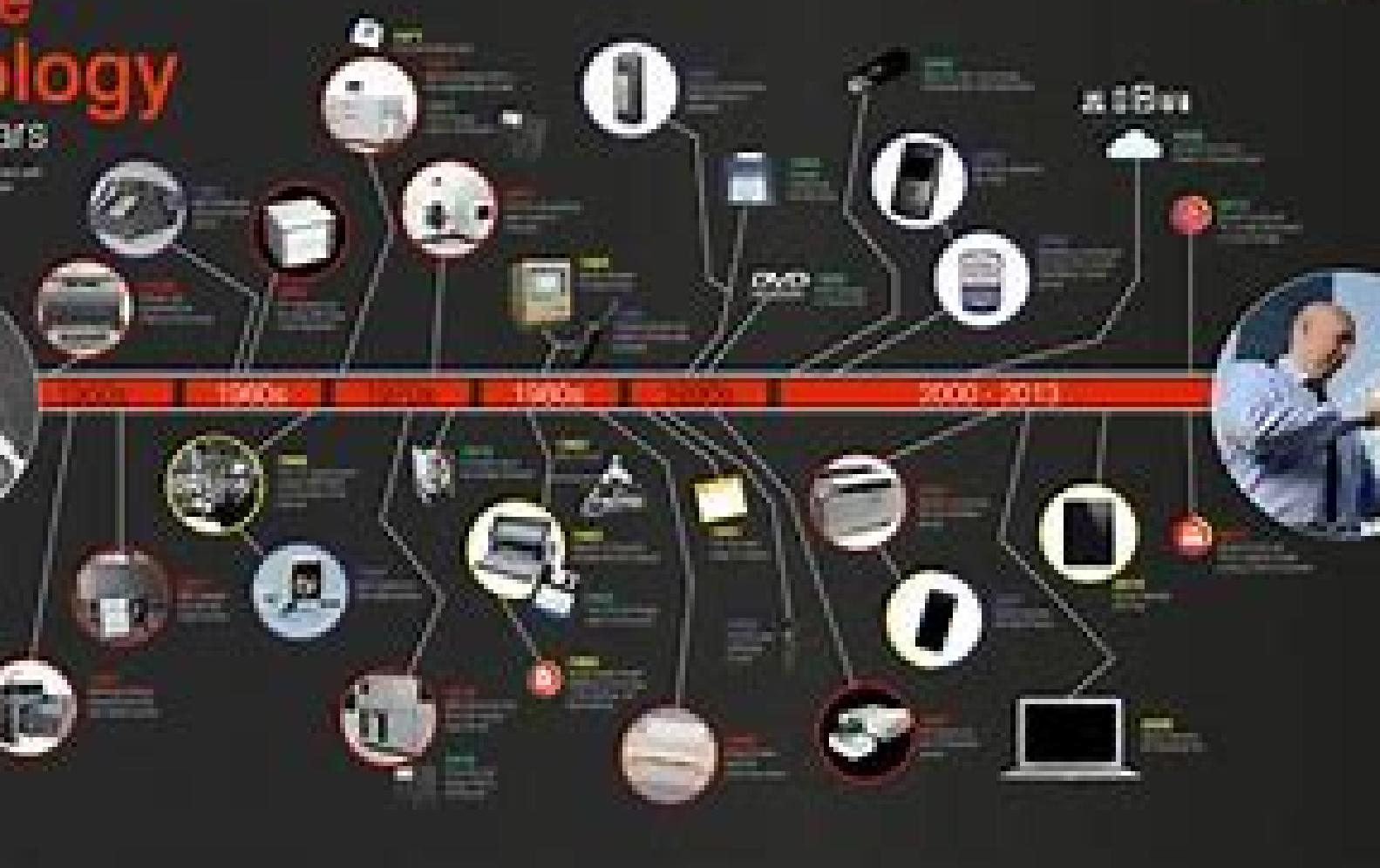


Cryptojacking
Un criminel utilise secrètement l'ordinateur de la victime pour générer de la crypto-monnaie. Au cours du premier trimestre 2021, les malwares de cryptominer ont augmenté de 117%.



Menaces contre les données
85% des violations de données impliquent un facteur humain. L'ingénierie sociale et les erreurs font aussi partie des causes principales.

Sources :
Agence de l'Union européenne pour la cybersécurité (ENISA) 2021, Parlement européen 2021





Conclusion

La veille technologique comme un atout stratégique. Elle est essentielle pour rester informé.

Importance de l'apprentissage continu dans l'univers des systèmes et réseaux. "Anticiper pour mieux protéger et innover."