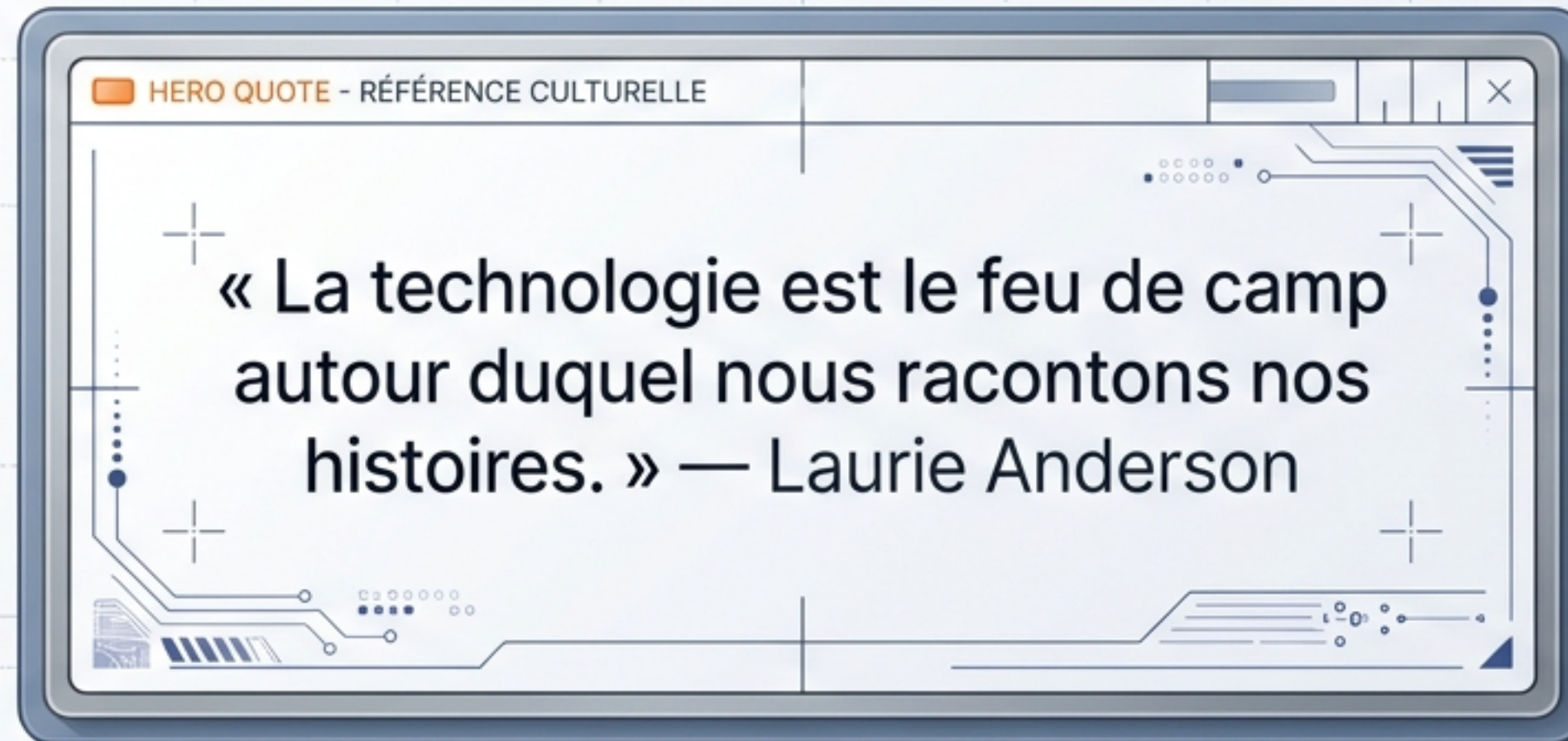


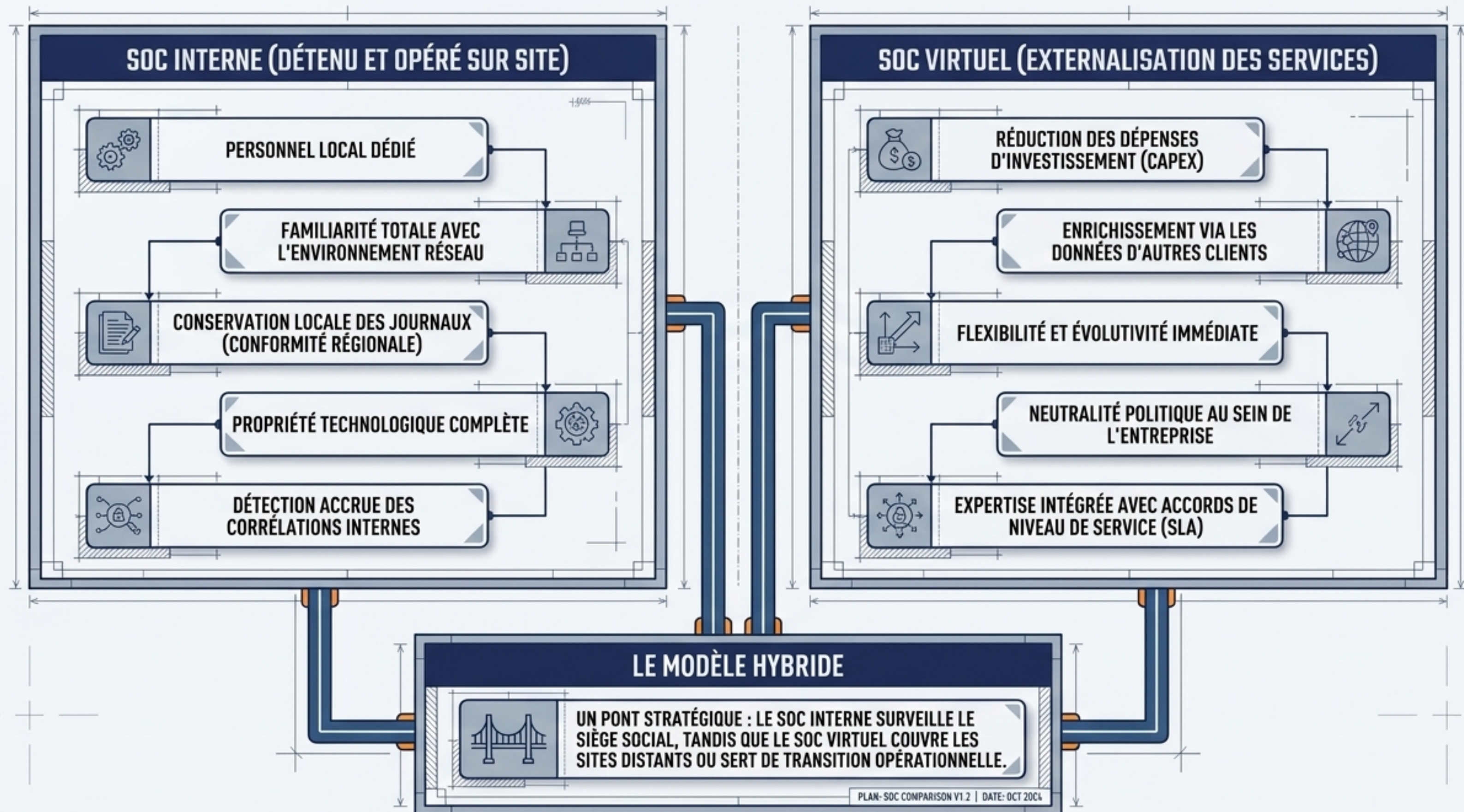
L'Architecture Technologique du SOC

Le plan directeur pour la conception des fondations, des réseaux et des terminaux d'un centre d'opérations de sécurité.

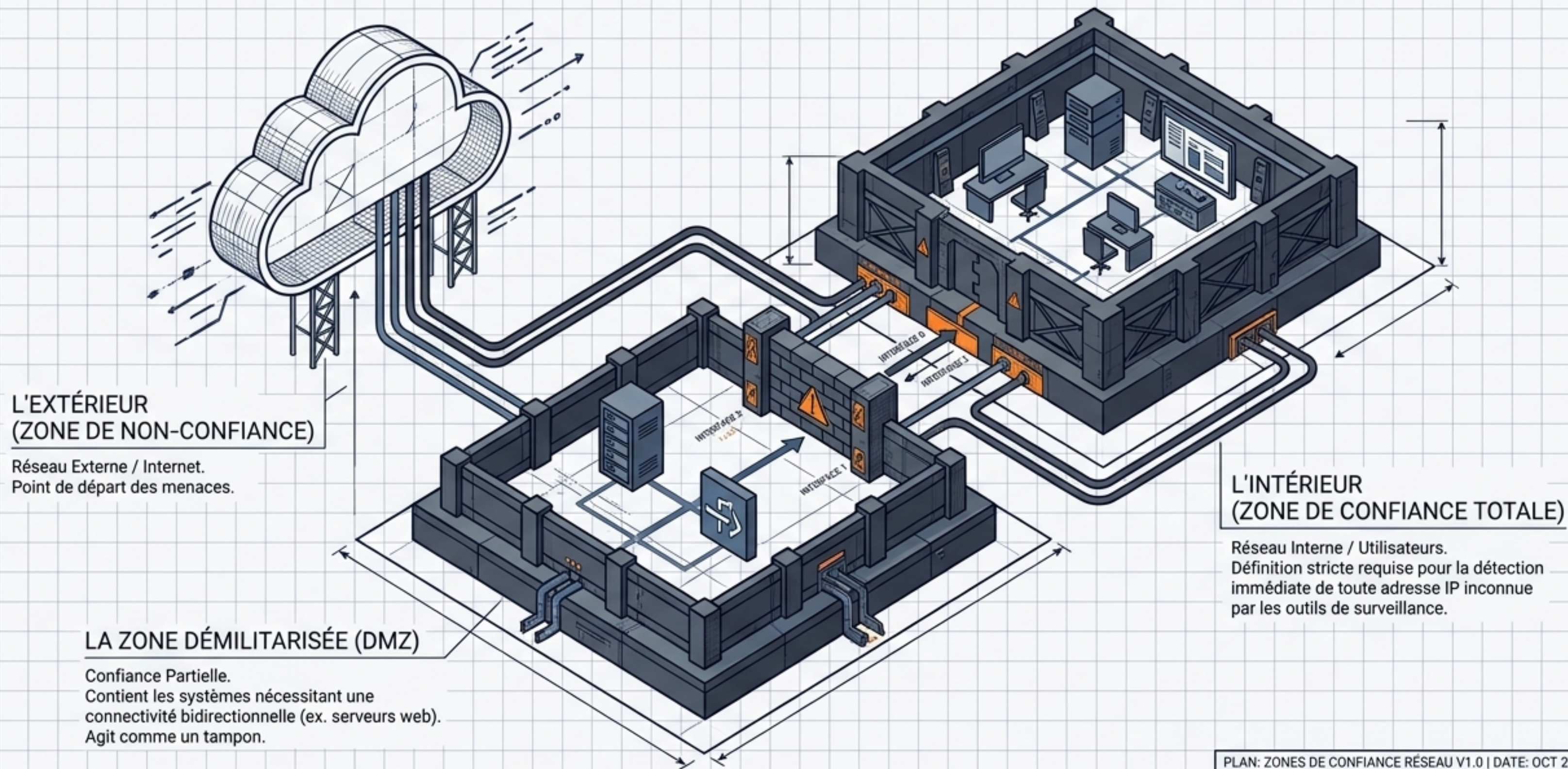


Un guide de référence visuel pour les architectes SOC.

MATRICE DIAGNOSTIC DE MODÈLES SOC – ANALYSE COMPARATIVE



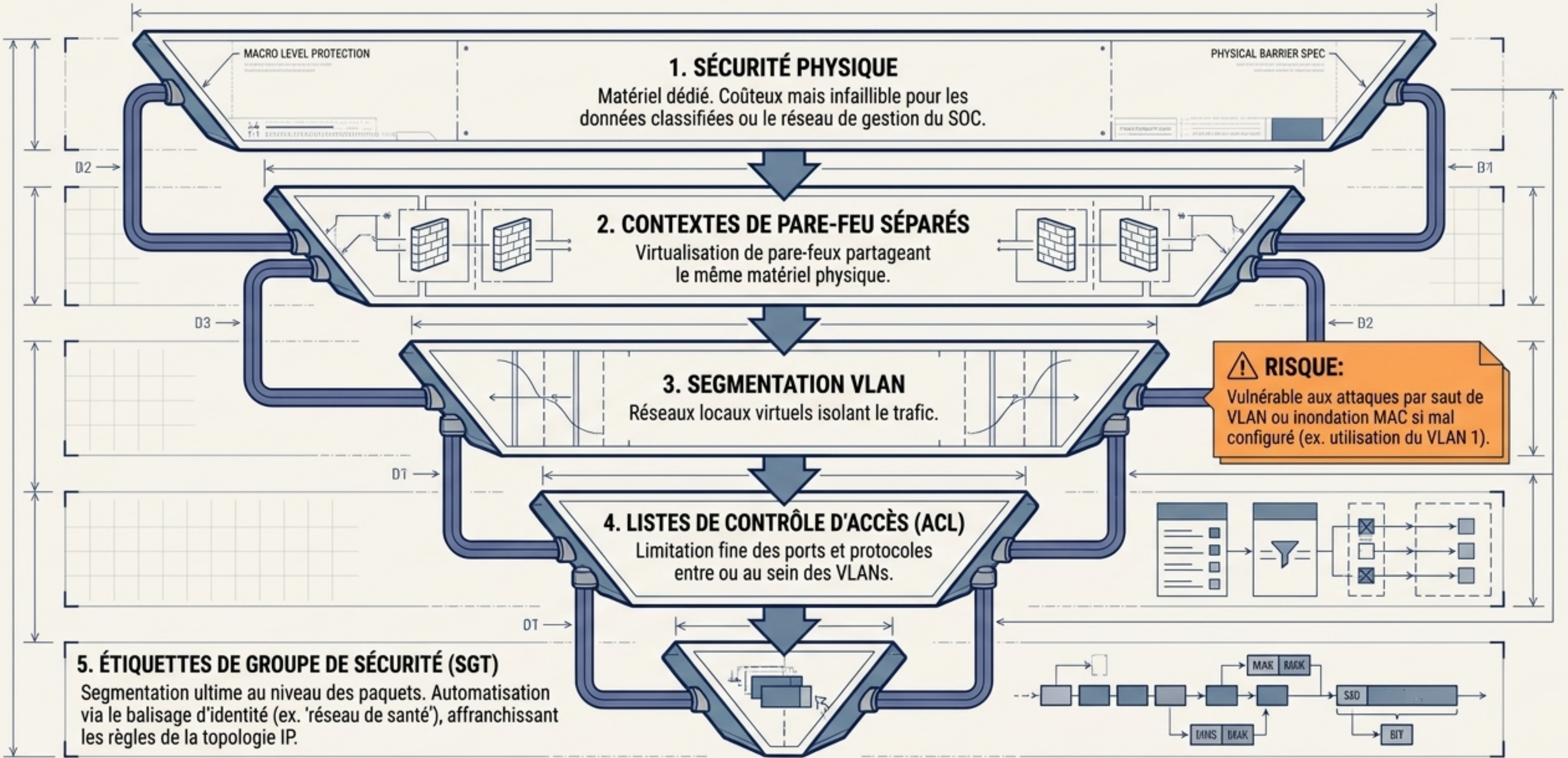
ARCHITECTURE DES ZONES DE CONFIANCE RÉSEAU – SCHÉMA STRUCTUREL



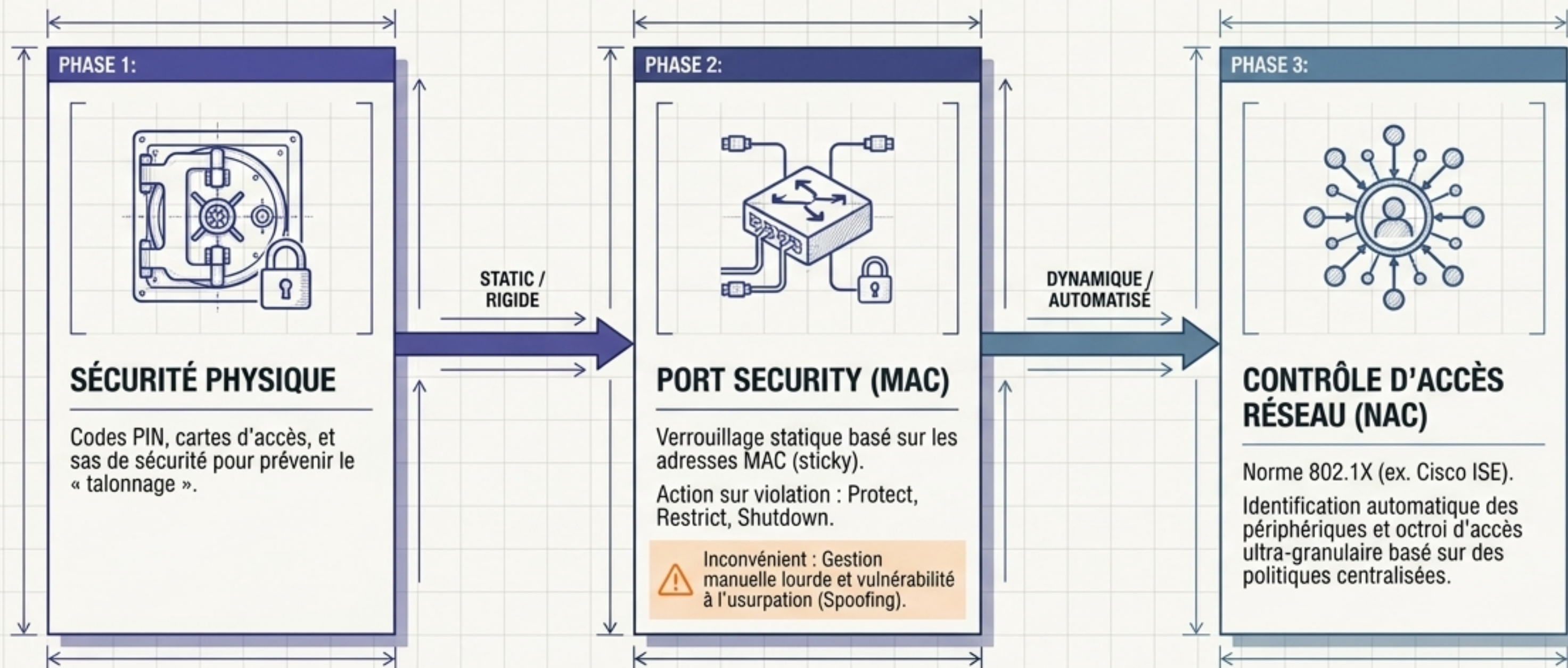
PLAN: ZONES DE CONFIANCE RÉSEAU V1.0 | DATE: OCT 2024

SCHÉMA DIAGNOSTIC

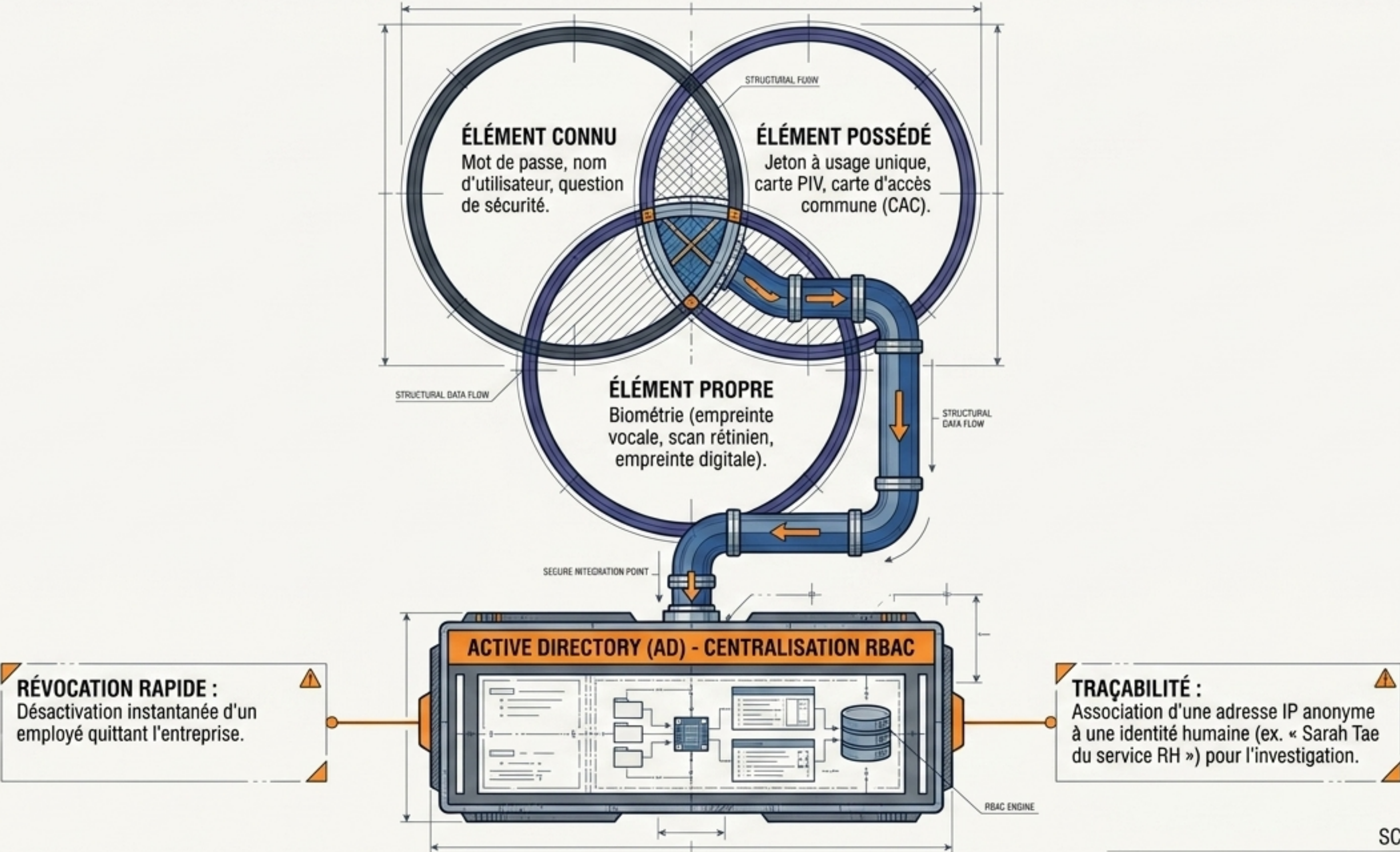
SECURITY CORE – DIAGRAMME STRUCTUREL DE SEGMENTATION RÉSEAU



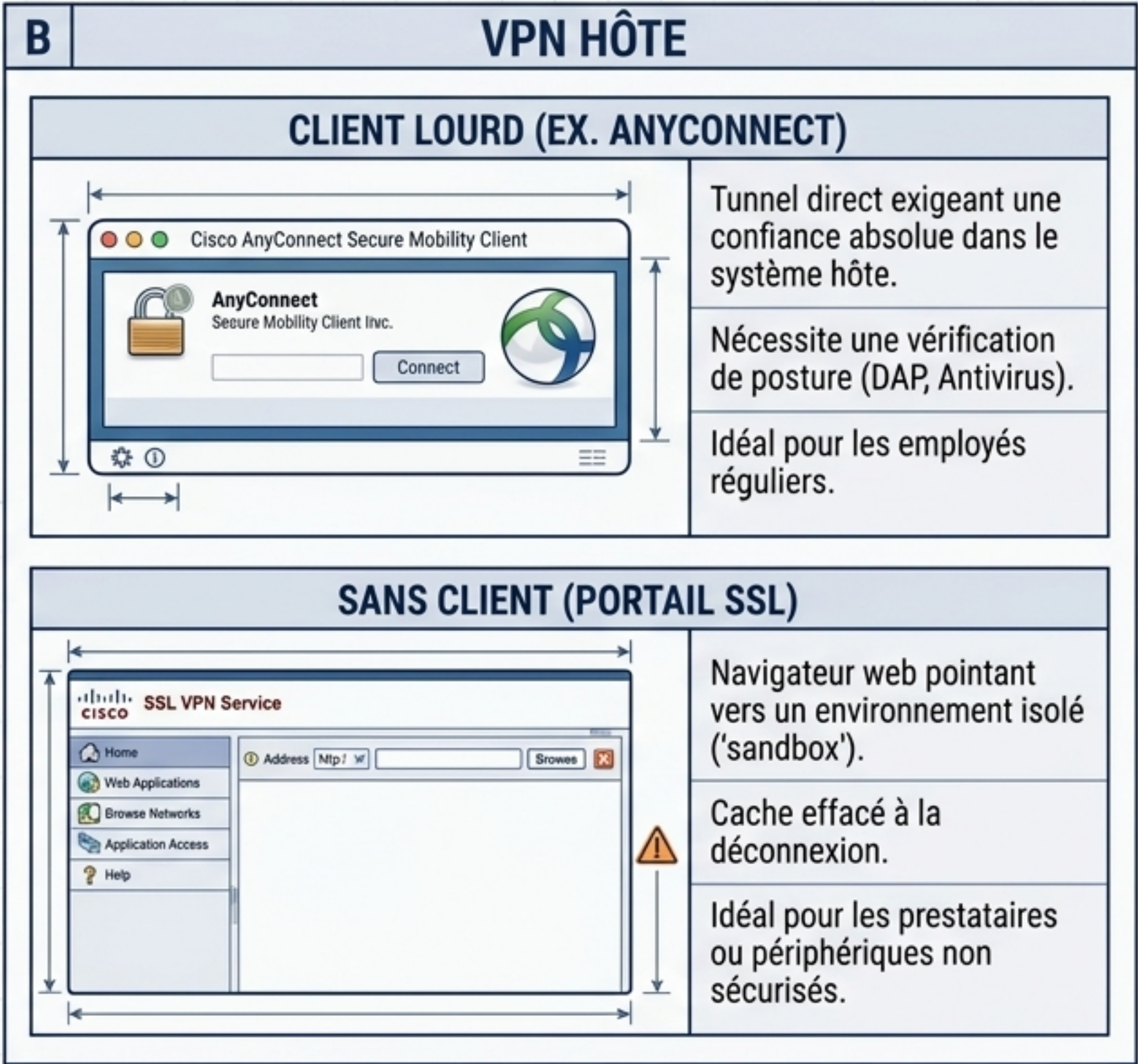
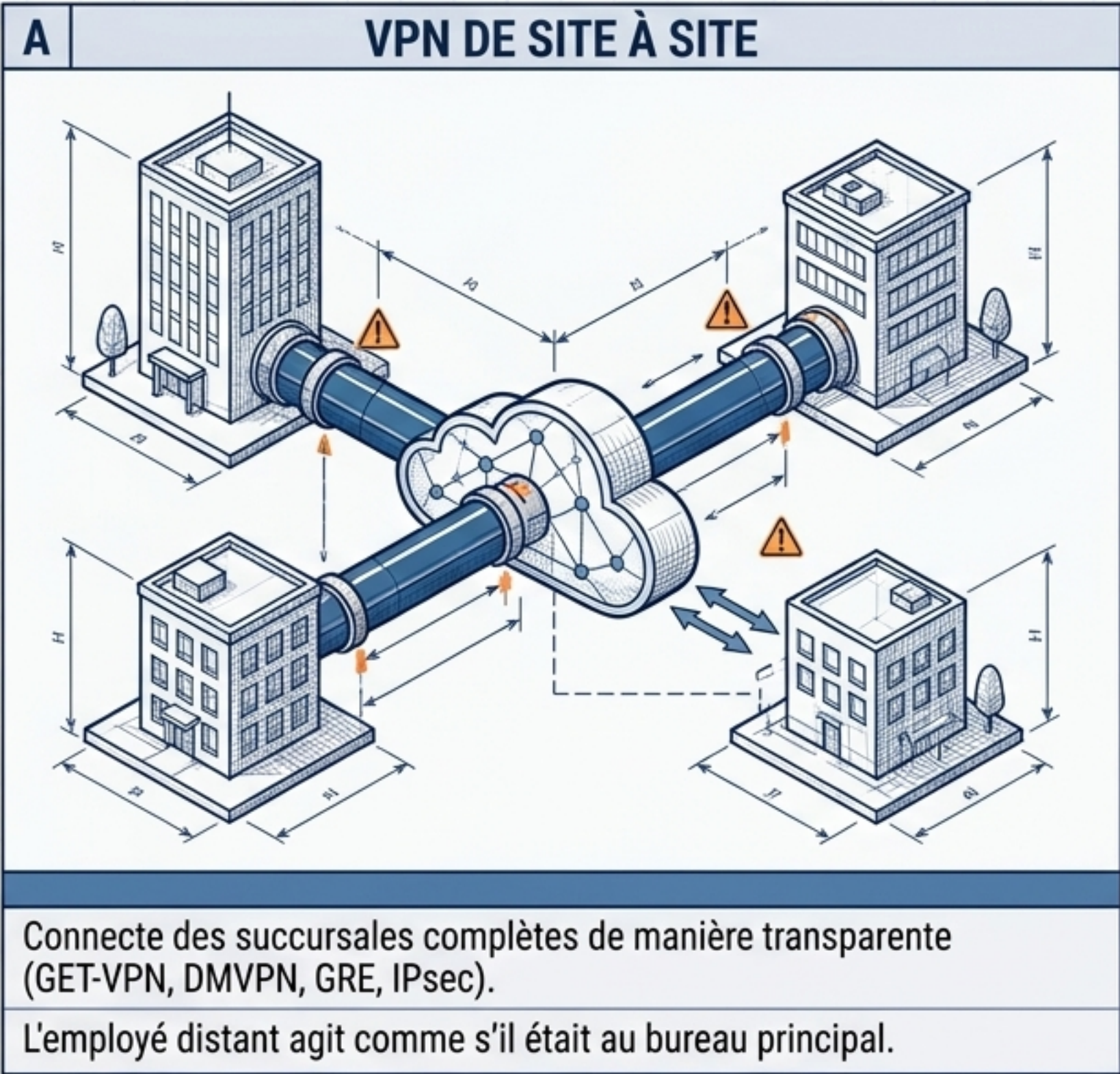
ÉVOLUTION DU CONTRÔLE D'ACCÈS – LIGNE DE TEMPS STRUCTURELLE



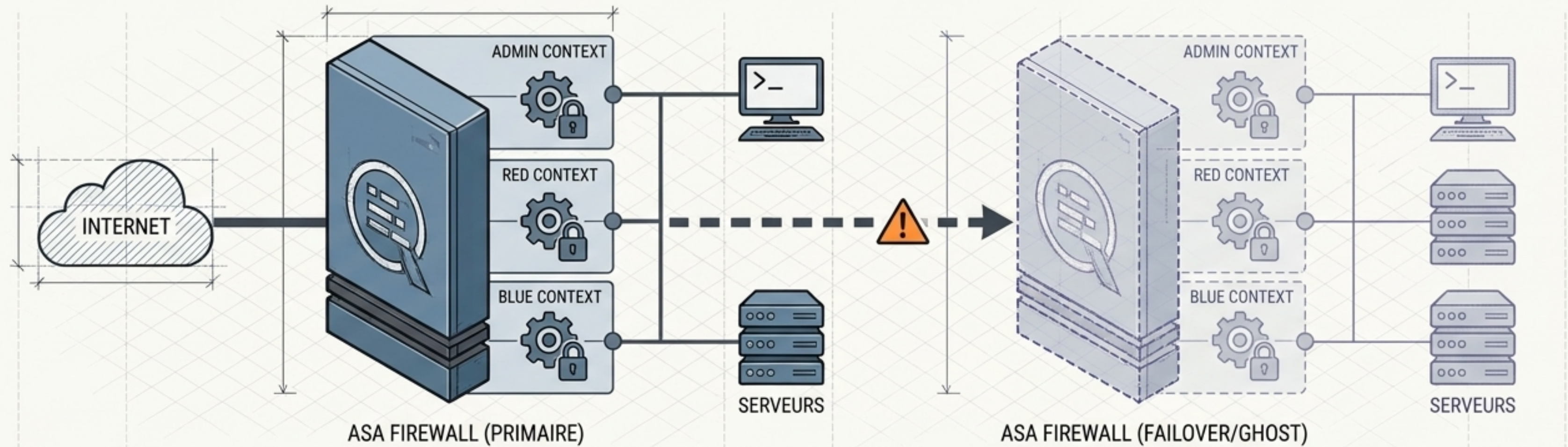
MULTI-FACTEUR D'AUTHENTIFICATION (MFA) – DIAGRAMME STRUCTUREL ET CENTRALISATION AD



STRATÉGIES VPN : COMPARAISON STRUCTURELLE - DIAGRAMME DE DIAGNOSTIC



DISPONIBILITÉ ÉLEVÉE (HA) - DIAGRAMME MATÉRIEL ET NIVEAUX DE SERVICE (SLA)



BASULMENT (HA) : MATÉRIEL REDONDANT AVEC LA MÊME VERSION DE CODE.
BASULMENT AUTOMATIQUE BASÉ SUR LE DÉLAI DE SYNCHRONISATION.
ATTENTION AU COÛT DES DOUBLES LICENCES.

INTERVENTION :
JOUR OUVRABLE
SUIVANT

INTERVENTION :
8 HEURES

INTERVENTION :
1 HEURE

RÈGLE D'ARCHITECTURE : DISTINGUER IMPÉRATIVEMENT LE SUPPORT LOGICIEL
DE LA GARANTIE MATÉRIELLE.

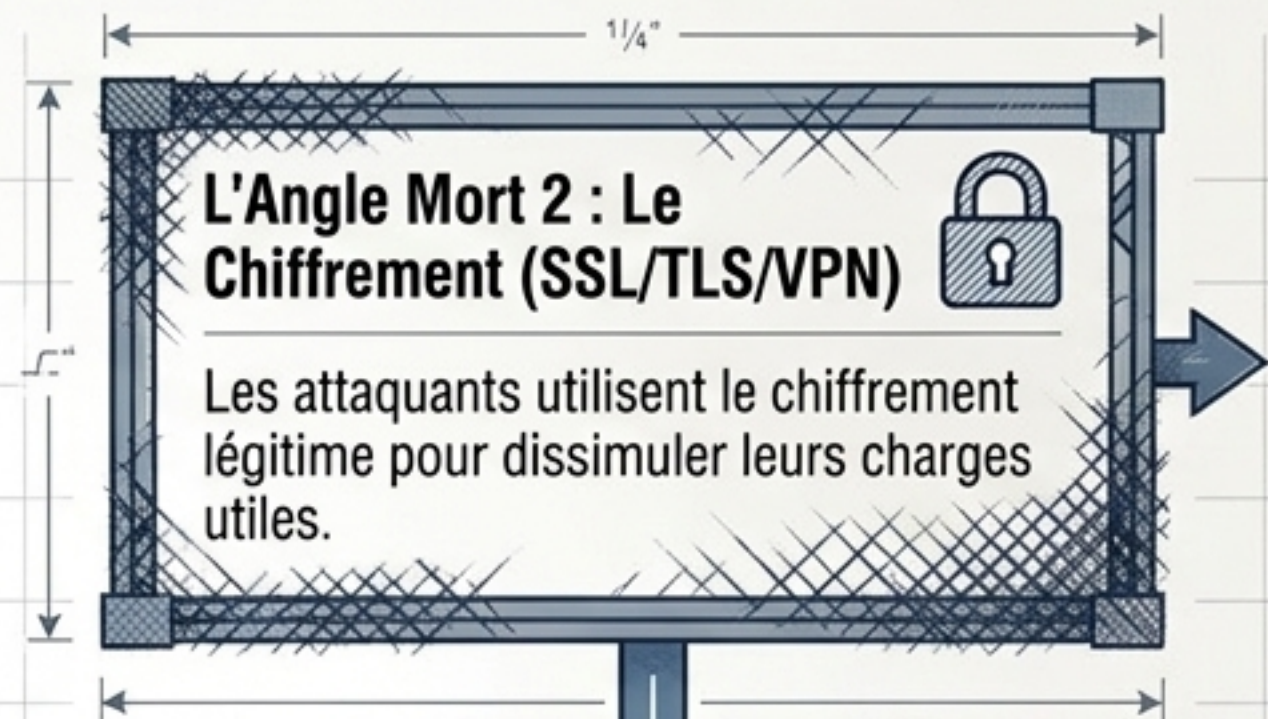
TÉLÉMÉTRIE RÉSEAU : CARTE DES FLUX DE DONNÉES - DIAGRAMME DE DIAGNOSTIC



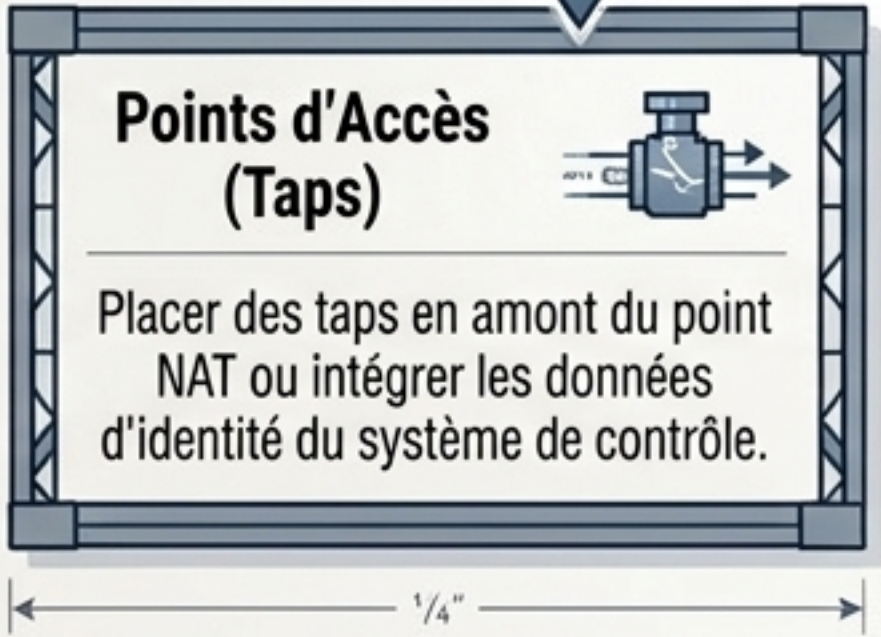
PLAN : TÉLÉMÉTRIE RÉSEAU CARTE DES FLUX

V1.0 | DATE : OCT 2024 | SCHÉMA DIAGNOSTIC

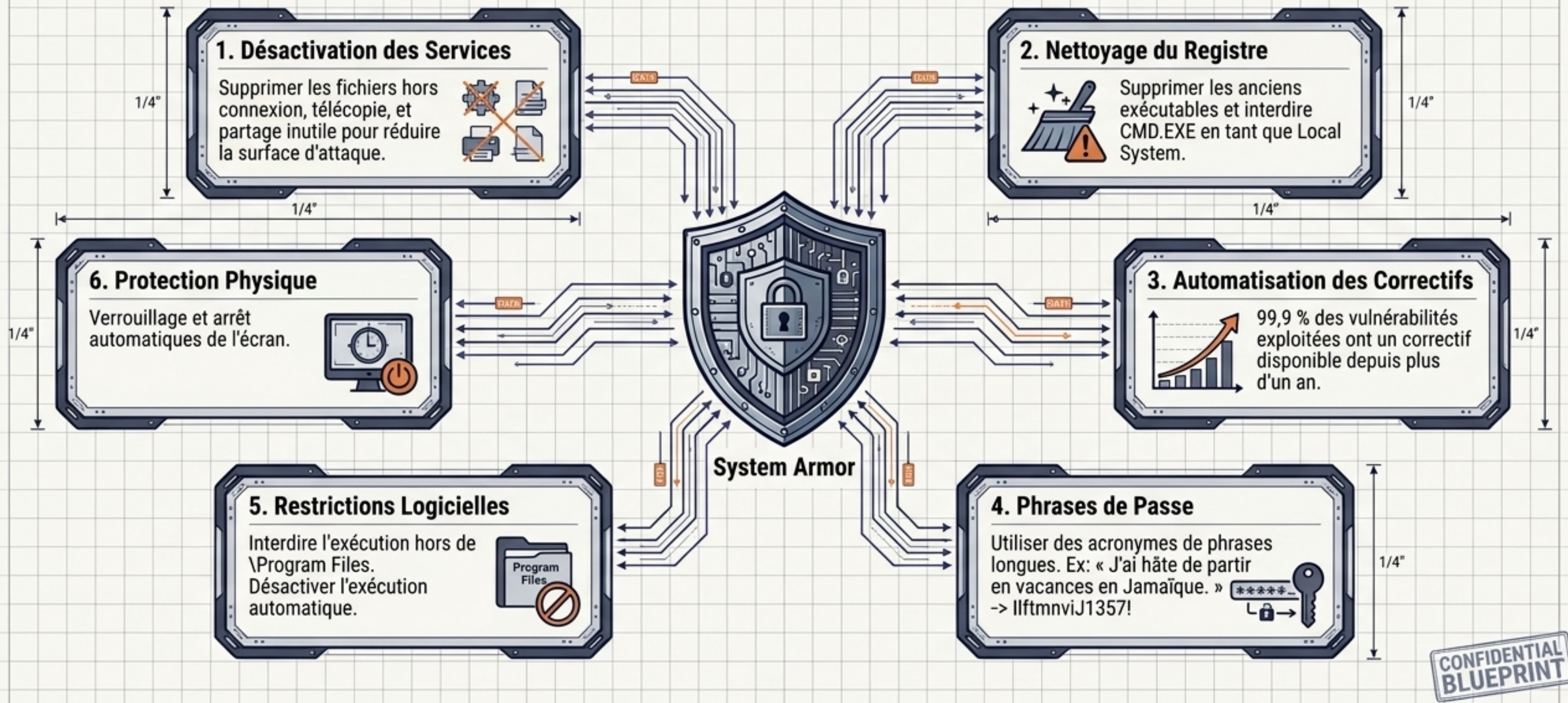
LES ANGLES MORTS (BLIND SPOTS)



LES SOLUTIONS : ÉCLAIRAGE (ILLUMINATING)



Objectif : Standardisation matérielle et OS pour automatiser les correctifs.



CONFIDENTIAL
BLUEPRINT

ANALYSE COMPARATIVE : ANTIVIRUS VS. DÉTECTION AVANCÉE (AMP)

ANTIVIRUS TRADITIONNEL

La première ligne de défense



MÉCANISME

Basé sur les signatures (reconnaissance de motifs connus).



CIBLE

Menaces de base, logiciels malveillants courants, attaques historiques.



VERDICT

Indispensable mais insuffisant. Sans lui, les capteurs avancés sont saturés par le bruit des attaques basiques.

DÉTECTION AVANCÉE (AMP)

Advanced Malware Protection



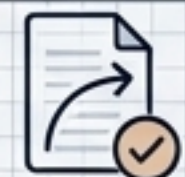
MÉCANISME

Analyse comportementale, polymorphisme, modification du démarrage.



CIBLE

Menaces Persistantes Avancées (APT), Zero-Day, menaces inconnues.



VERDICT

Trajectoire de fichier, remédiation automatique, et télémétrie.

☐ File Detection	Fingerprint (SHA-256)
☐ MKORTEN-M-DOFB detected foto1298171648.zip as Downloader:Trojan-tpd Quarantine: Successful	2023-03-13 13:23:46.07...
☐ MKORTEN-M-DOFB detected foto1298171648.zip as Downloader:Trojan-tpd Quarantine: Successful	2023-03-13 15:22:48.67...
☐ MKORTEN-M-DOFB detected foto1298171648.zip as Downloader:Trojan-tpd Quarantine: Successful	2023-03-13 15:27:36.07...

Analyze

Restore File

All Computers

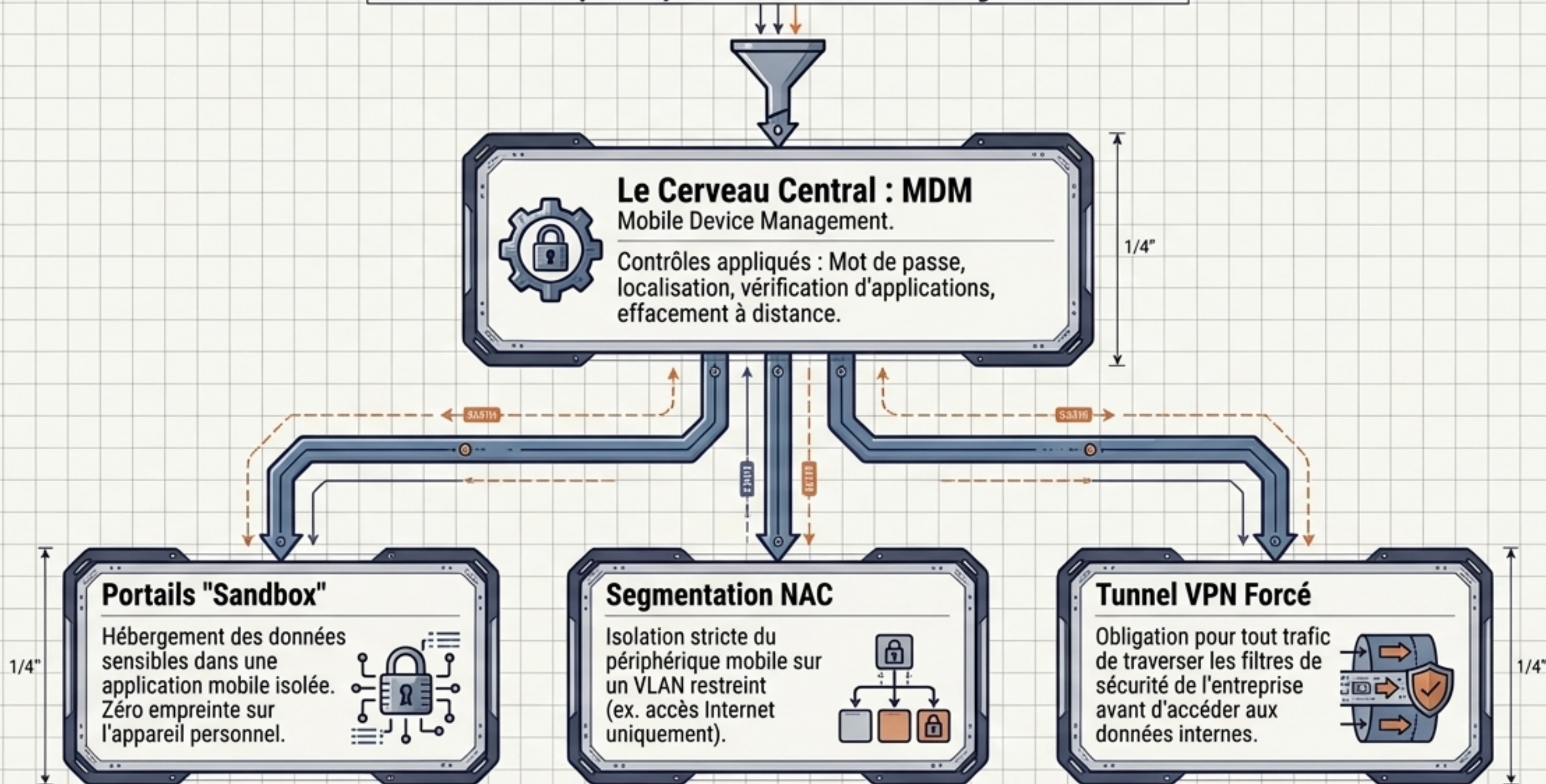
Add to Whitelist

File Trajectory

Figure 9-8 Cisco AMP Removing Six Trojans

Le Défi Mobile : BYOD, systèmes fermés (iOS), et réseaux hybrides.

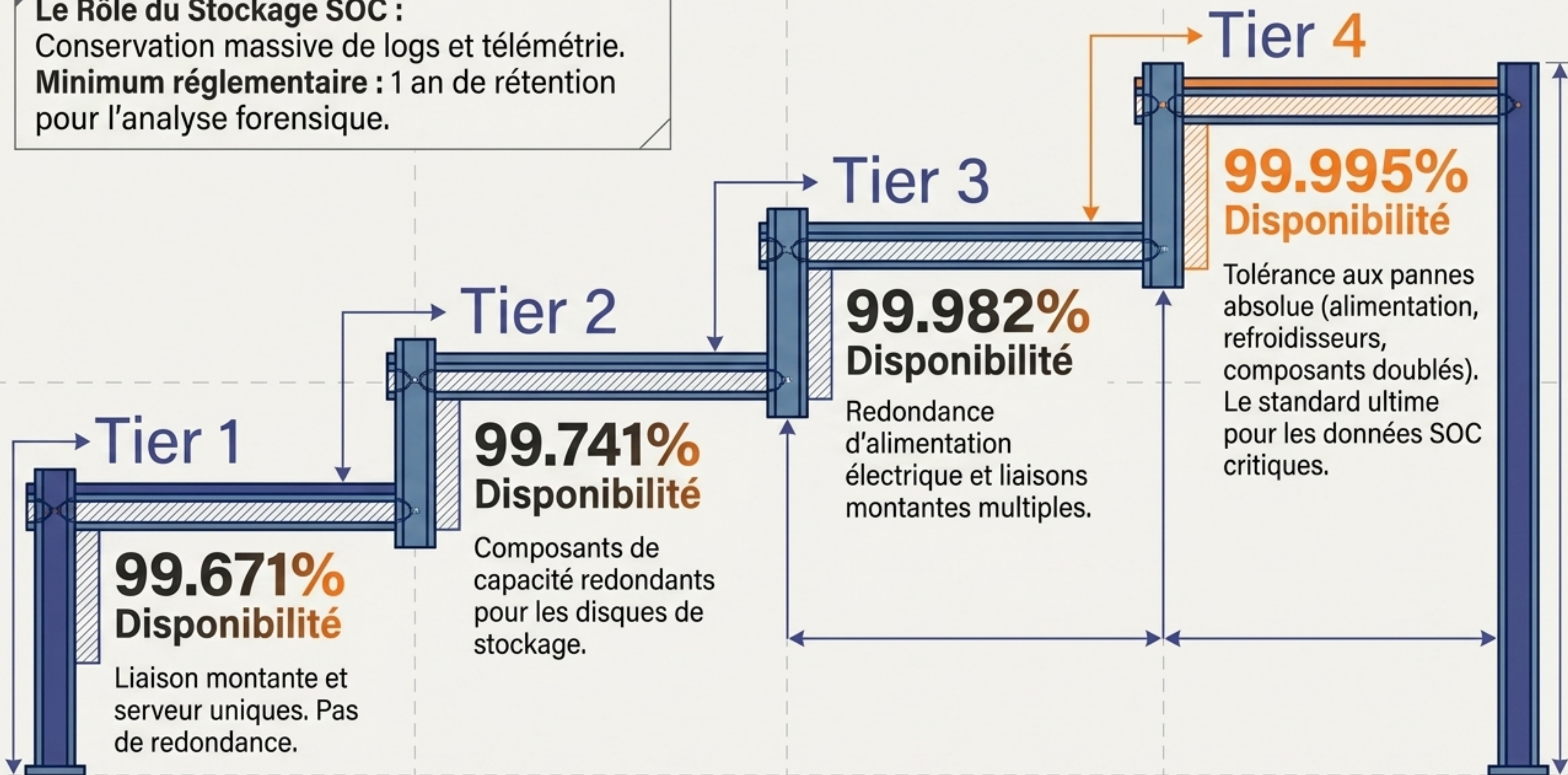
CONFIDENTIAL
BLUEPRINT



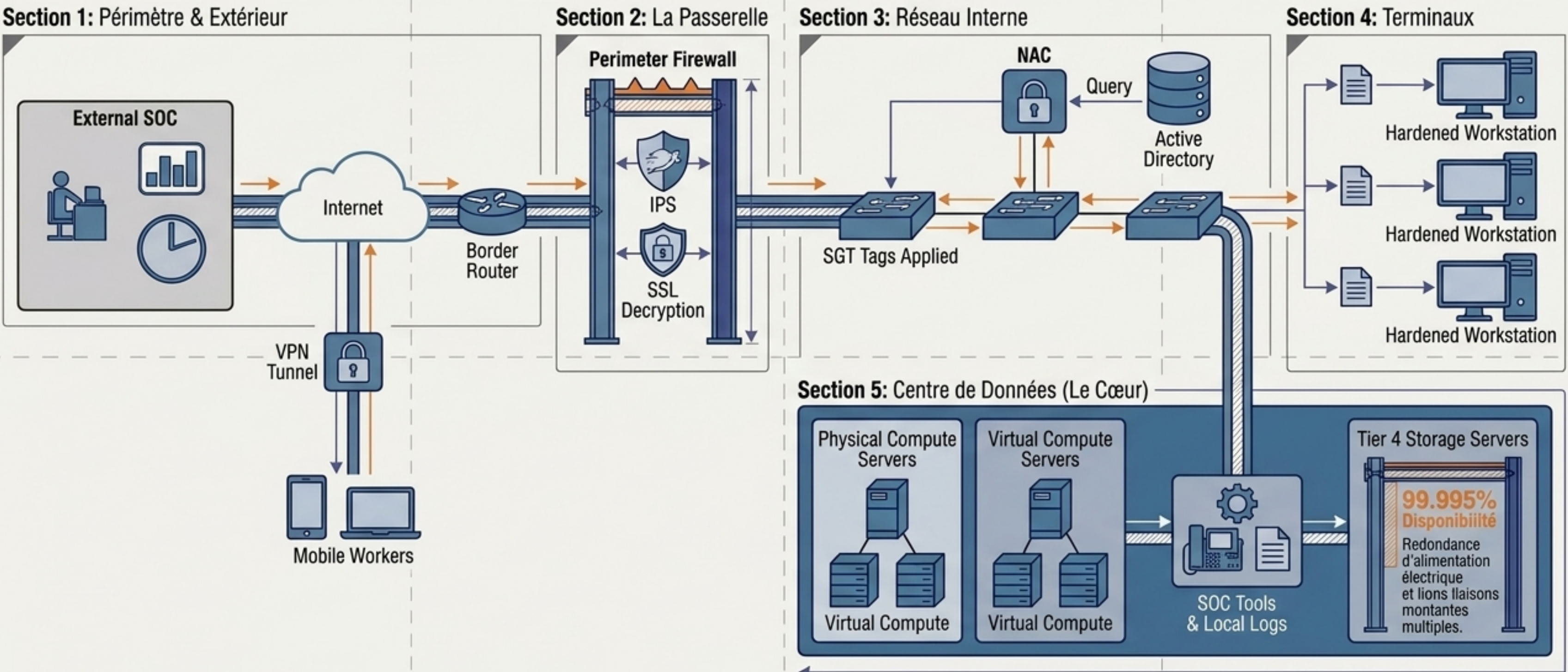
Le Rôle du Stockage SOC :

Conservation massive de logs et télémétrie.

Minimum réglementaire : 1 an de rétention pour l'analyse forensique.



ARCHITECTURE GLOBALE DU SOC : INTÉGRATION MULTICOUCHE



Conclusion : Un SOC moderne ne repose pas sur un seul produit, mais sur une architecture de couches superposées, de la segmentation physique au comportement des terminaux.

CONFIDENTIAL BLUEPRINT
PROJECT
DATE : OCT 2024