

Pilotage d'un Système d'Information

Bloc 1 - Titre : Administrateur
système réseaux et sécurité

Montpellier Ynov
Campus



Contexte du projet

Recensement des besoins

Rédaction de l'ensemble des spécifications

Diagramme de Gantt

Diagramme de charges

Proposition d'amélioration du SI

Conclusion

Contexte



Un hôpital en 2024

-  581 incidents de sécurité
-  représentent 10 % des victimes de cyberattaques
-  Coût moyen jusqu'à 10 M€ (remédiation)
-  Pertes de revenus d'exploitation : jusqu'à 20 M€ estimées

Objectif :

-  Gouvernance de la sécurité
-  Sécurité des réseaux
-  Sécurité des systèmes et services
-  Pentest et validation

Données de santé
hautement sensible



Conformité
HDS



Spécifications techniques

Architecture globale



Liste des principales catégories de spécifications :

- Architecture réseau & sécurité périphérique
- Systèmes d'authentification et gestion des accès
- Protection et chiffrement des données
- Surveillance, détection et réponse
- Plan de continuité d'activité et reprise après sinistre

Cahier des charges



Contexte & Objectif

- Protection des données médicales sensibles
- Conformité réglementaire (RGPD, ISO 27001, normes santé)
- Sécurisation de l'infrastructure hospitalière contre les cybermenaces



Infrastructure Cible

- Réseau segmenté avec 11 VLANs dédiés
- Infrastructure virtualisée (4 serveurs ESXi)
- Services critiques identifiés et priorisés
- Équipements réseau et sécurité (Firewalls, IDS/IPS, 802.1X)



Exigence de sécurité

- Confidentialité et intégrité des informations médicales
- Continuité des services critiques (24/7)
- Traçabilité des accès aux données sensibles
- Détection et réponse aux incidents



Livrables

- PSSI adaptée au contexte hospitalier
- Documentation des configurations réseau et systèmes
- Plan de Reprise d'Activité (PRA)

Contexte CHYNOV

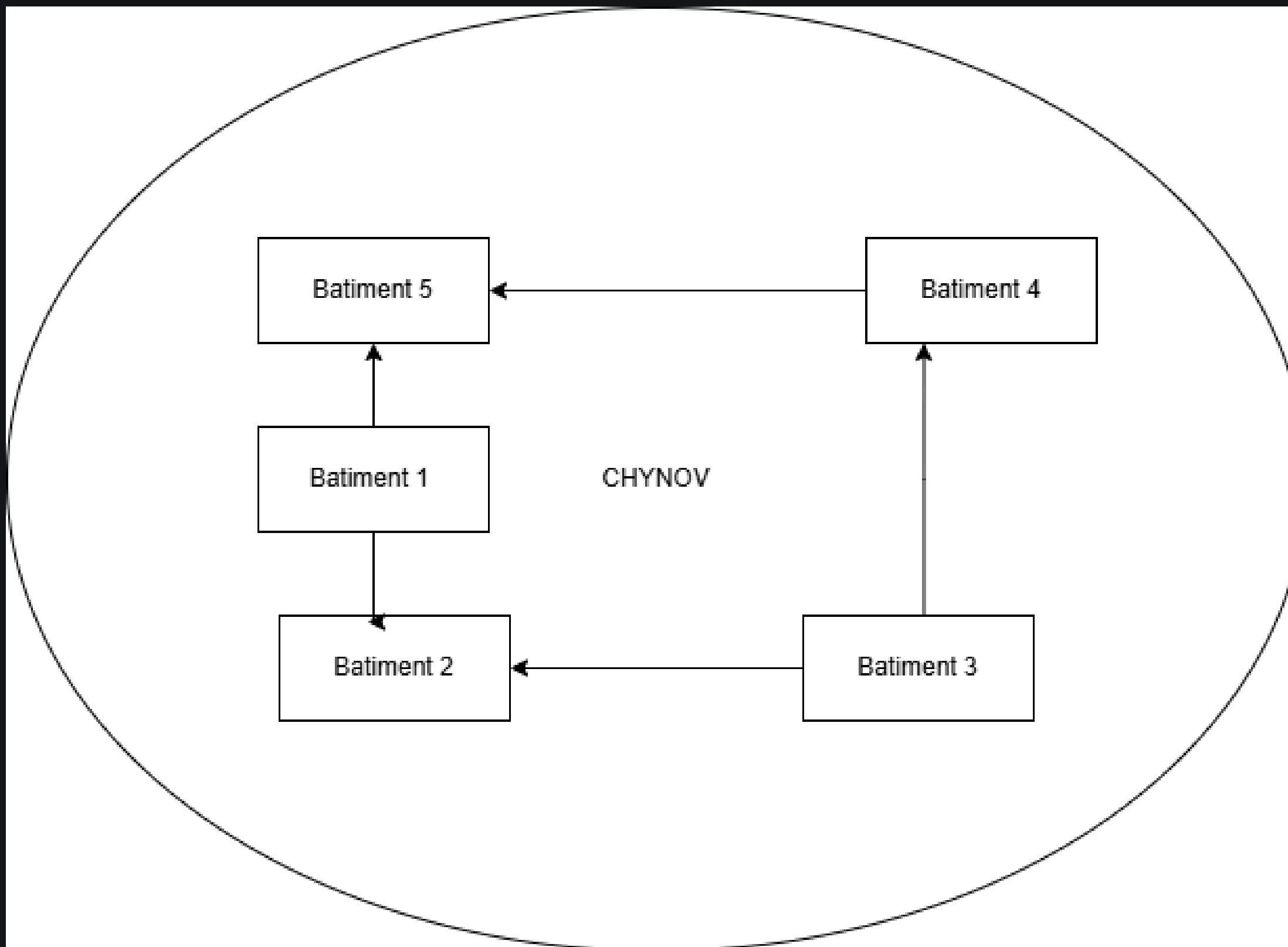
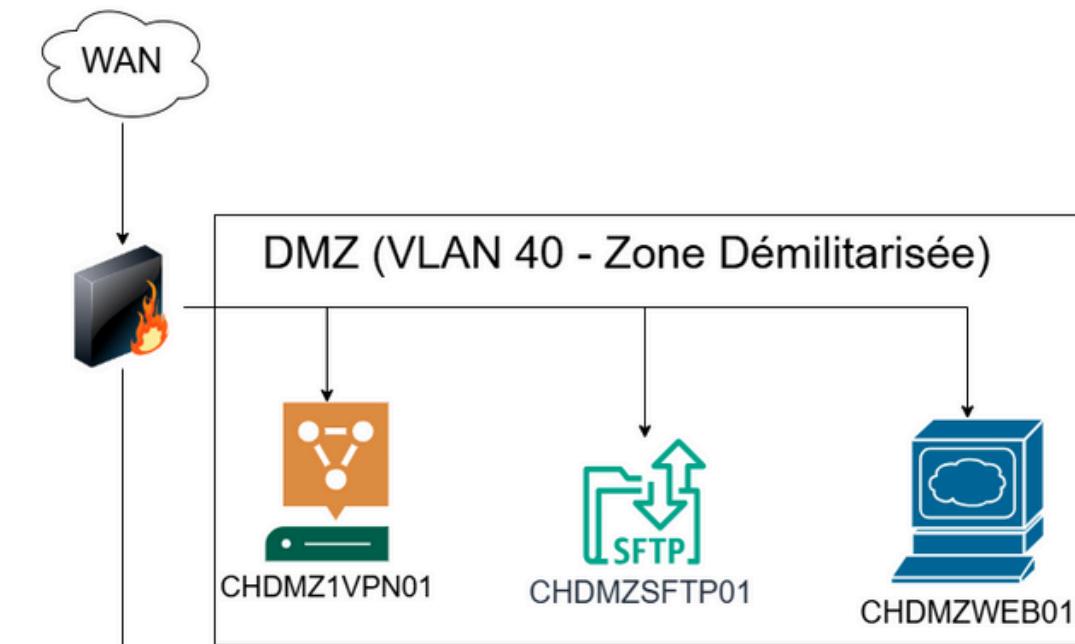


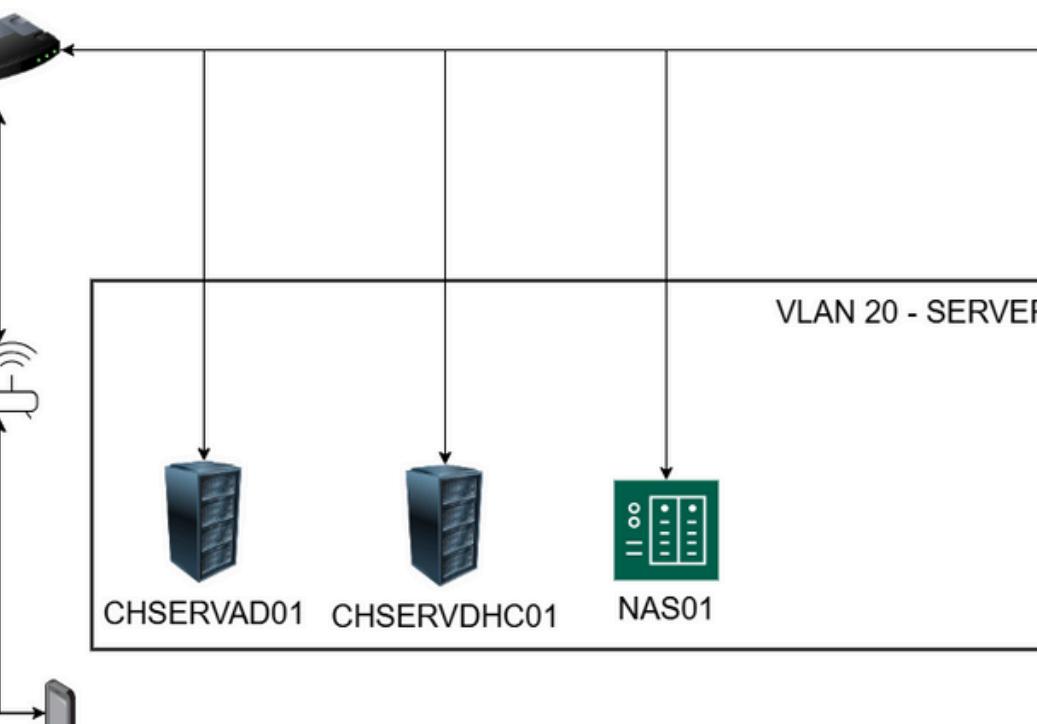
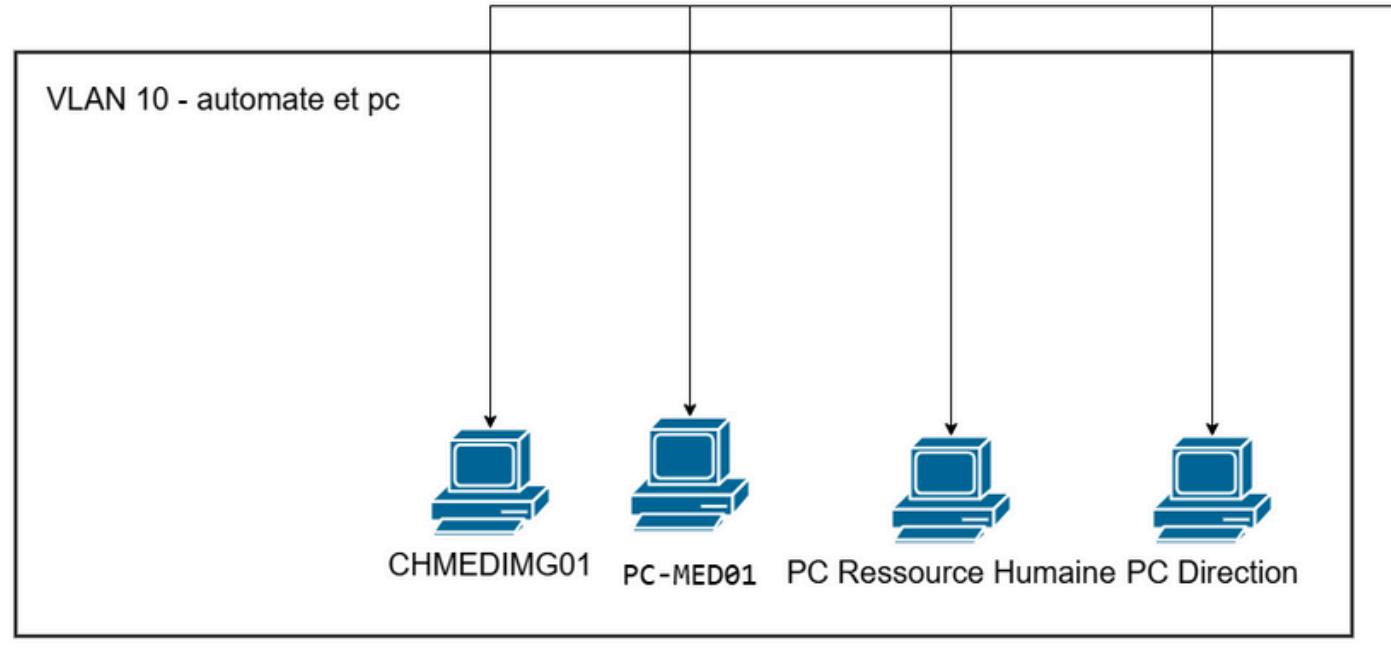
Schéma du réseau initial

Légende des composants du réseau initial (CHU – avant sécurisation)

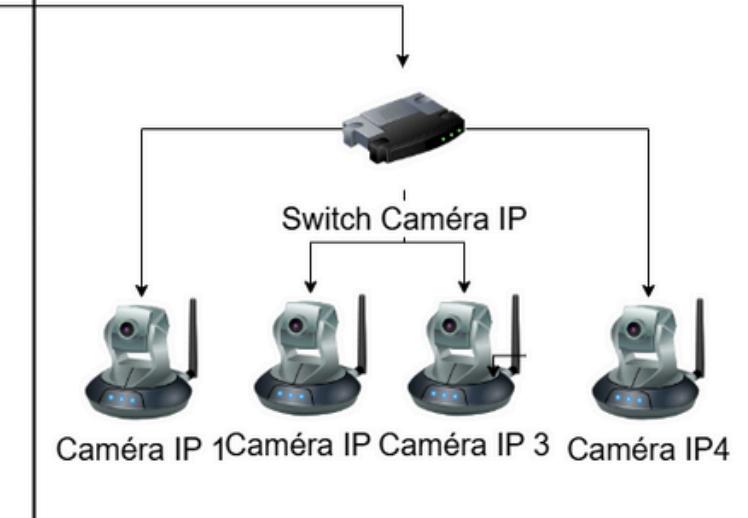
- CHMEDIMG01 : Poste d'imagerie médicale
- PC-MED01 : Poste personnel médical
- PC Ressource Humaine : Poste administratif RH
- PC Direction : Poste direction
- CHSERVAD01 : Contrôleur de domaine (Active Directory)
- CHSERVDHC01 : Serveur DHCP
- NAS01 : Serveur de stockage réseau (NAS)
- Caméra IP 1 à 4 : Caméras de vidéosurveillance connectées
- Switch : Switch principal non administrable
- Switch Caméra IP : Switch secondaire pour équipements IoT
- Point d'accès Wi-Fi : Réseau Wi-Fi partagé patients/personnels/visiteurs
- Réseau utilisé : 192.168.0.0/24



192.168.0.0/24



VLAN 30 - Videosurveillance



Analyse des Risques

N°	Élément analysé	Mode de défaillance	Effets potentiels	G	P	D	Criticité
1	CHSERVAD01	Compromission, élévation de priviléges	Contrôle total du réseau, compromission d'identités	10	8	5	400
2	VLAN PATIENT / VLAN GUEST	Accès non autorisé au réseau interne	Risque de pivot et fuite de données	8	7	6	336
3	DMZ	Exploitation des services exposés	Intrusion externe, exfiltration	9	6	5	270
4	équipement de sûreté	Équipements compromis	Perte de vidéos, porte d'entrée réseau	6	7	6	252
5	CHSERVSAG01	Corruption ou vol de données	Pertes comptables, arrêt de gestion	9	6	4	216
6	CHADMIPS01	IDS désactivé / mal configuré	Intrusions non détectées	10	5	4	200
7	CHSERVBKP01	Corruption ou indisponibilité	Impossible de restaurer après attaque	9	5	4	180
8	VLAN Déploiement	MAJ véroées ou malveillantes	Infection généralisée du SI	8	5	4	160
9	Machines médicales	Défaillance ou piratage d'équipements	Arrêt d'examens, perte de données patient	9	4	4	144
10	VLAN ADM	Défaillance des services de base	Rupture de connectivité, d'authentification	7	6	3	126

TABLE 2 – Analyse des modes de défaillance, de leurs effets et de leur criticité.

Analyse des Risques : Matrice des risques – État initial du SI

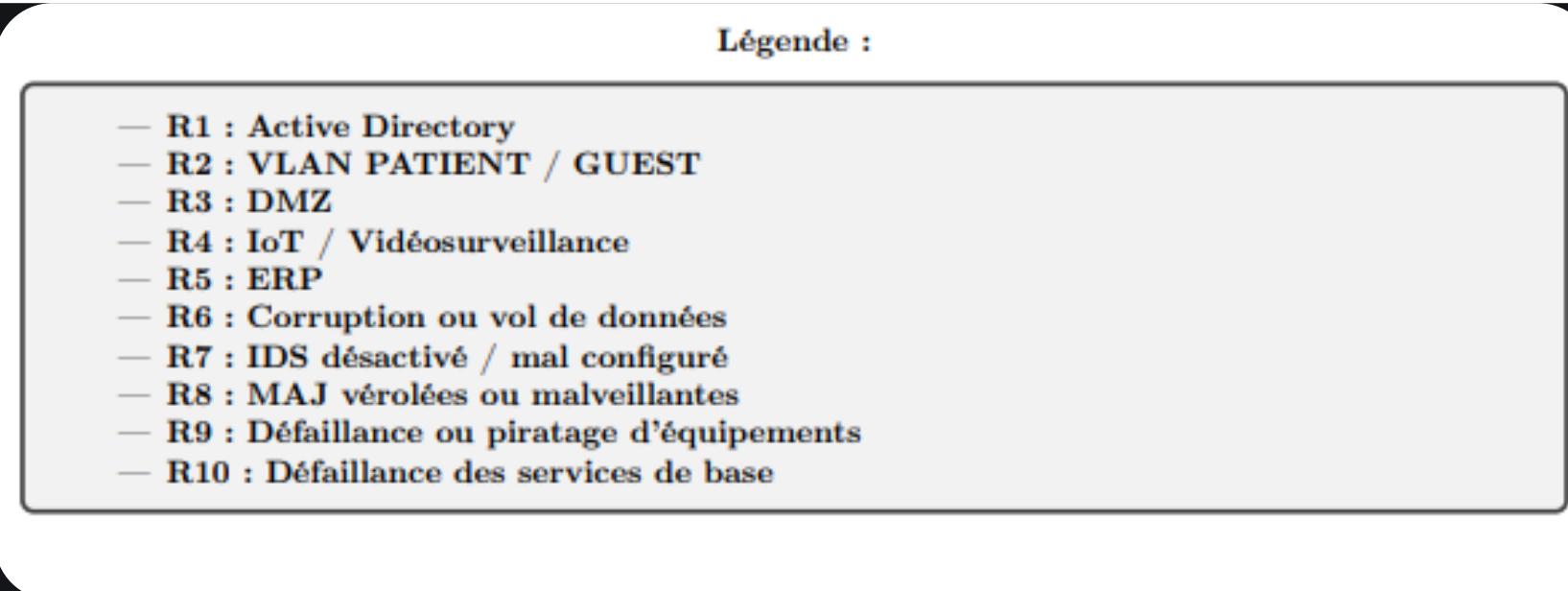
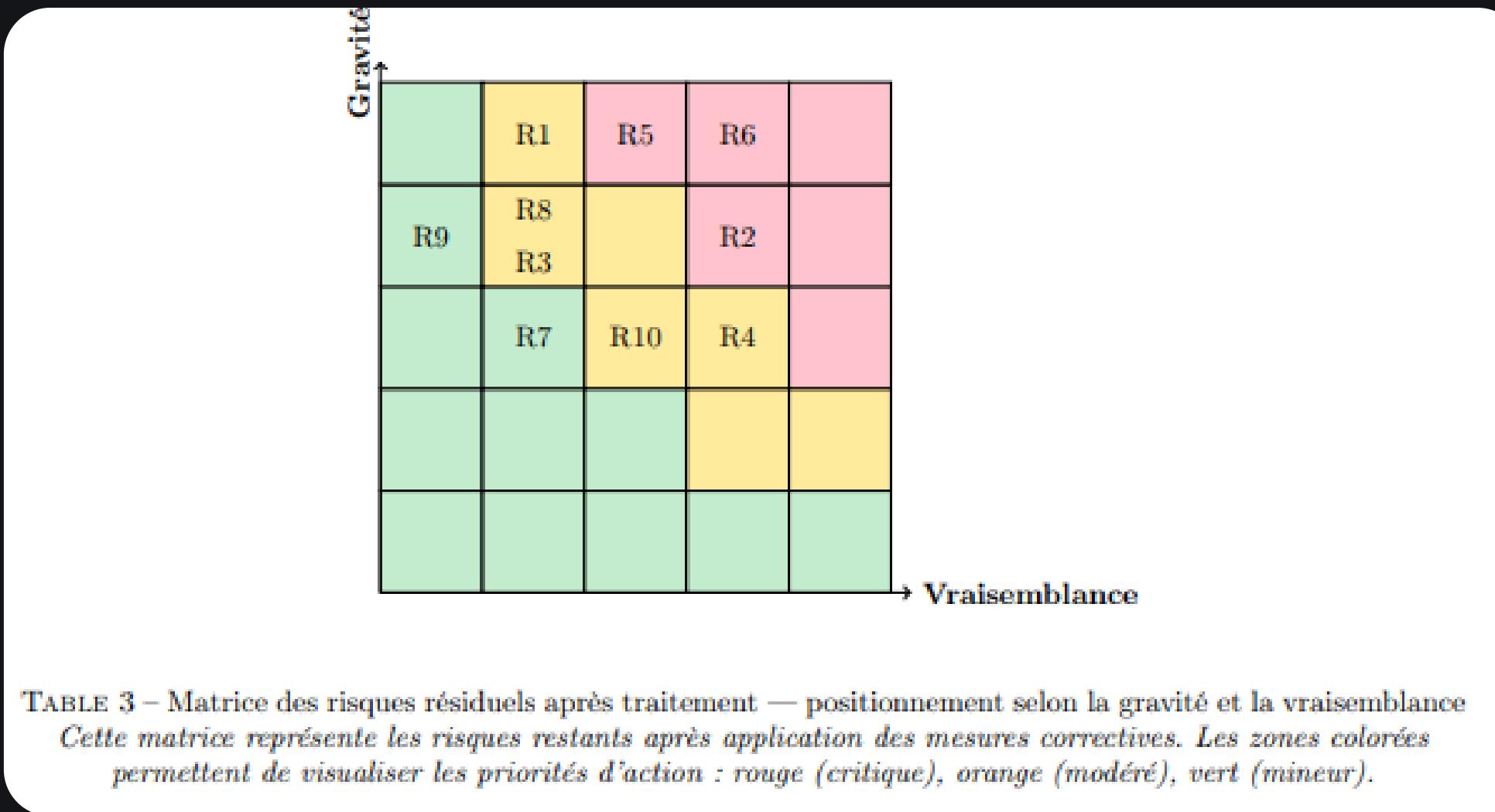


Diagramme de Gantt



CHynov

Read-only view, generated on 09 May 2025



Instagantt

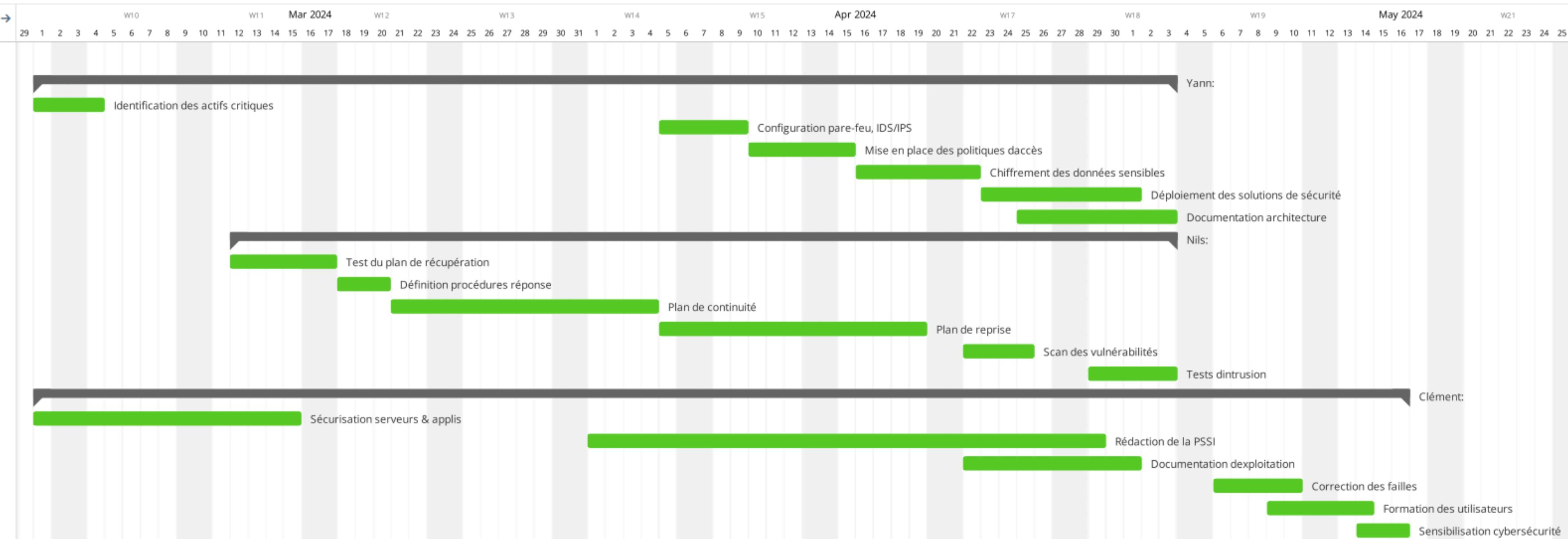
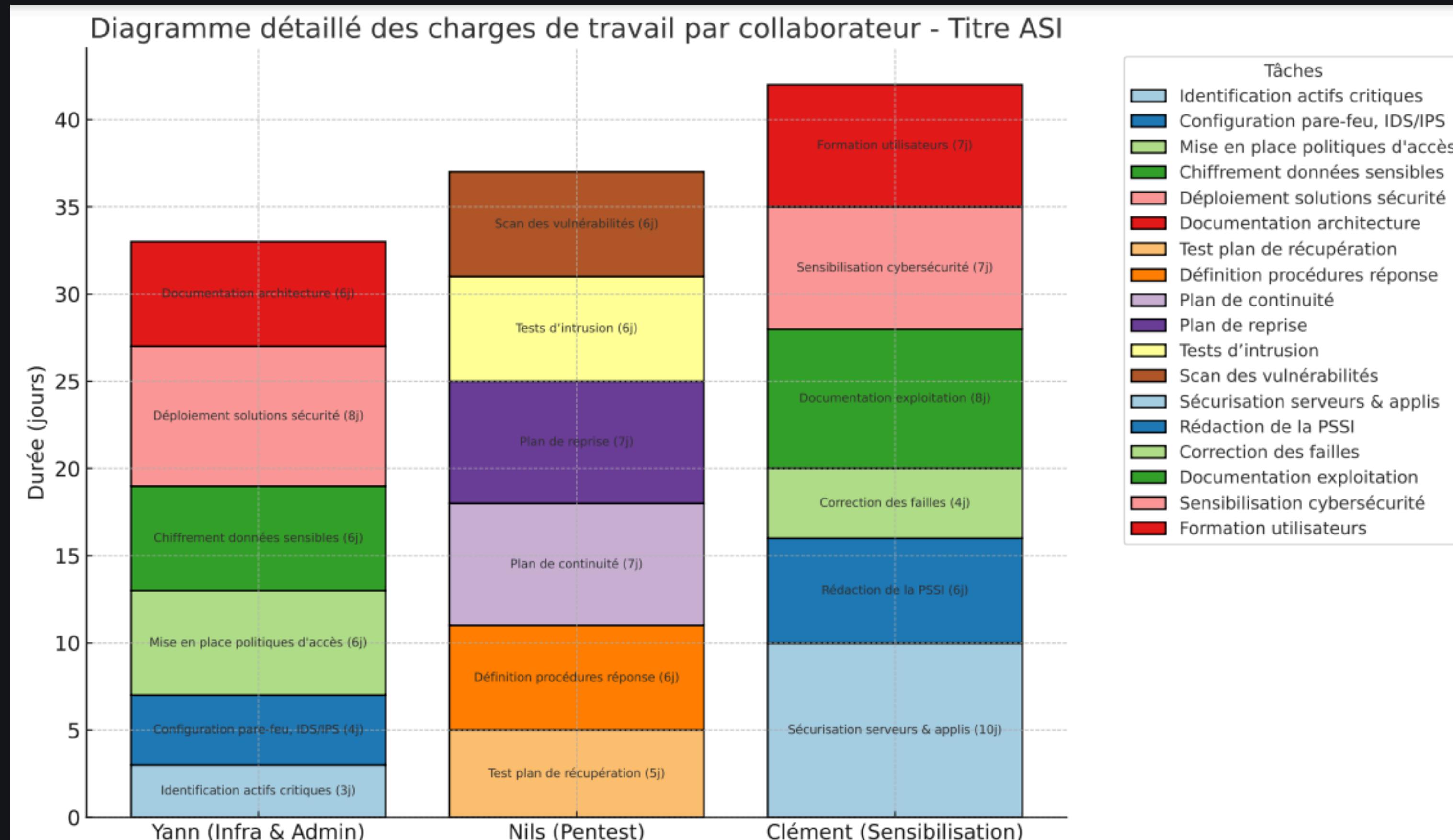


Diagramme de charges



Recensement des besoins

Gouvernance de la Sécurité

Liste des principaux objectifs :



Élaboration d'une PSSI



Politique & Gestions des comptes



Définir les objectifs de la sécurité (CIA)



Rôles & Responsabilités



Conformité (Iso, NIS2, Doc Santé RGPD)

Amélioration du SI

(Gouvernance de la Sécurité)



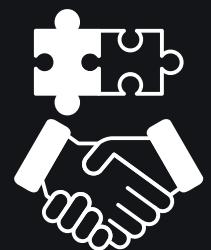
Gestion des utilisateurs du SI



Protection des Données



Architecture du Système d'Information



Intégration avec
Systèmes de Santé Nationaux

POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION



Mesures de Sécurité

- Gestion des Identités et des Accès
- Cycle de Vie des Identités
- Sécurisation de l'infrastructure hospitalière contre les cybermenaces



Sensibilisation et Formation

- Programme de Sensibilisation
- Actions Générales
- Ateliers Sensibilisation

Recensement des besoins

(sécurité réseau)



Configurer des pare-feu, IDS/IPS.



Pentest



Politiques d'accès strictes (2FA, Groupes...).

AMÉLIORATION DU SI

(réseaux)



Cloisonnement par VLAN



Jumpbox



Norme : 802.1X



Révision des comptes
utilisateurs / des accès



MFA via VPN pour zone
sensible

RECENSEMENT DES BESOINS

Sécurité des systèmes / services



Identifier les actifs critiques



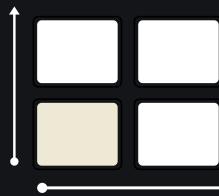
Réaliser un pentest



Évaluer les menaces et vulnérabilités



Sensibilisation du Personnel



Estimer les impacts avec la matrice de criticité

Amélioration du SI

sécurité système et services

Sécurité physique

 Identifier les actifs et zones critiques

 Évaluer menaces et vulnérabilités

 Badgeuse

 Test Intrusion physique

 Plus de caméras

Sécurité logique

 Fire-Wall

 EDR / XDR

 Segmentation

 WAF

Recensement besoin

Pentest

Identifier les failles



Test intrusion



Rapport pentest



Respecter les
Exigences réglementaires (RGPD, HDS).



PSSI claire et appliquée



Remédiation testée

AMÉLIORATION DU SI

(pentest)

Rapport Pentest



Migration des équipements



Vérification Patch fréquent



Veille Cyber (Cert santé...)



Sensibilisation Employés



Amélioration constante

Amélioration du SI

CONCLUSION

KPI pertinents



Gouvernance :

Taux de disponibilité entre 98 % et 99,99 % sur 1 an



Sécurité Réseau :

100 % des ports non utilisés fermés ou filtrés



Pentest

100 % des vulnérabilités critiques corrigées sous 30 jours

Métier Acteur clés



RSSI

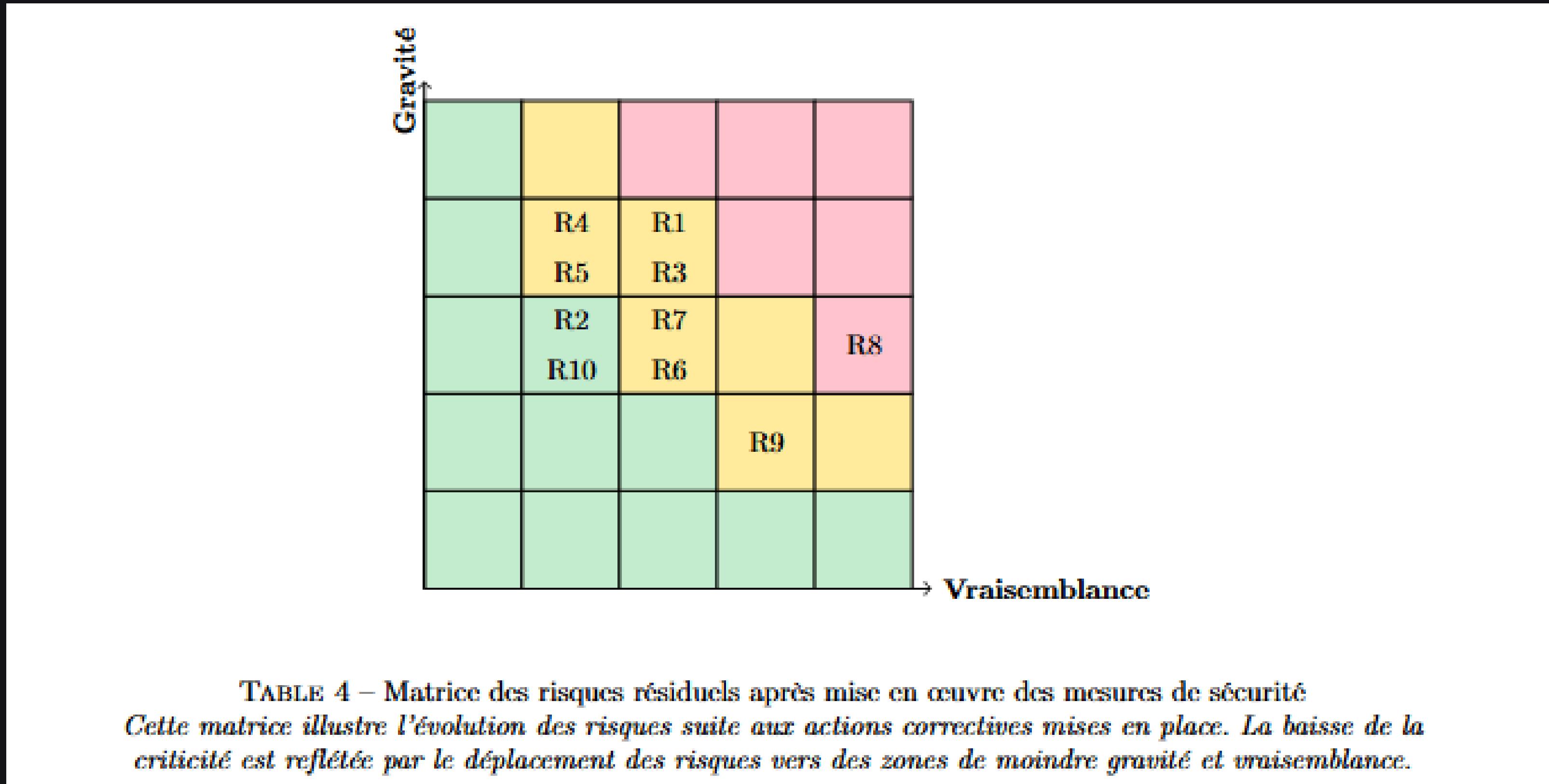


Dev Ops



Admin Sys

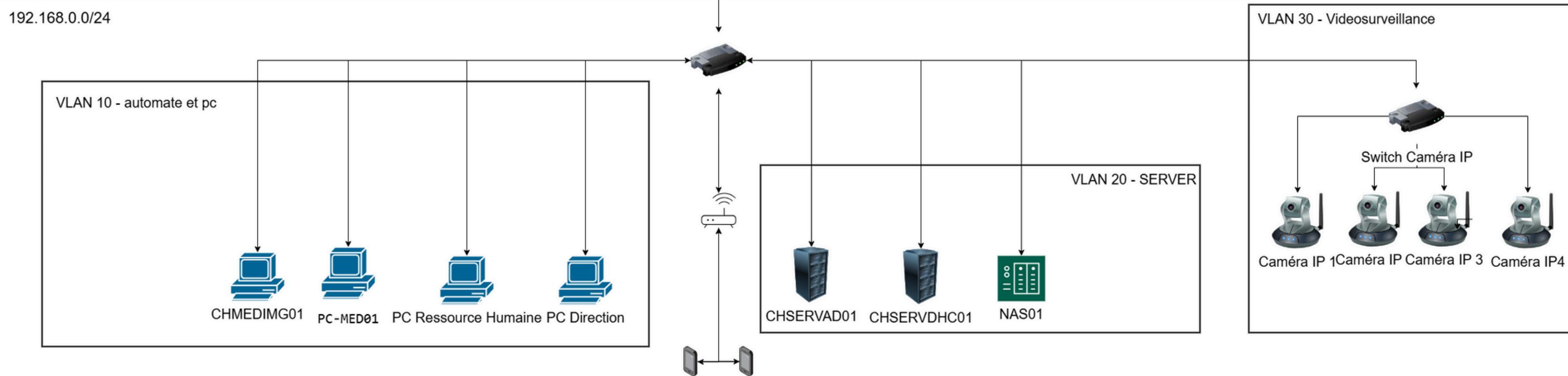
Risques résiduels après amélioration du SI



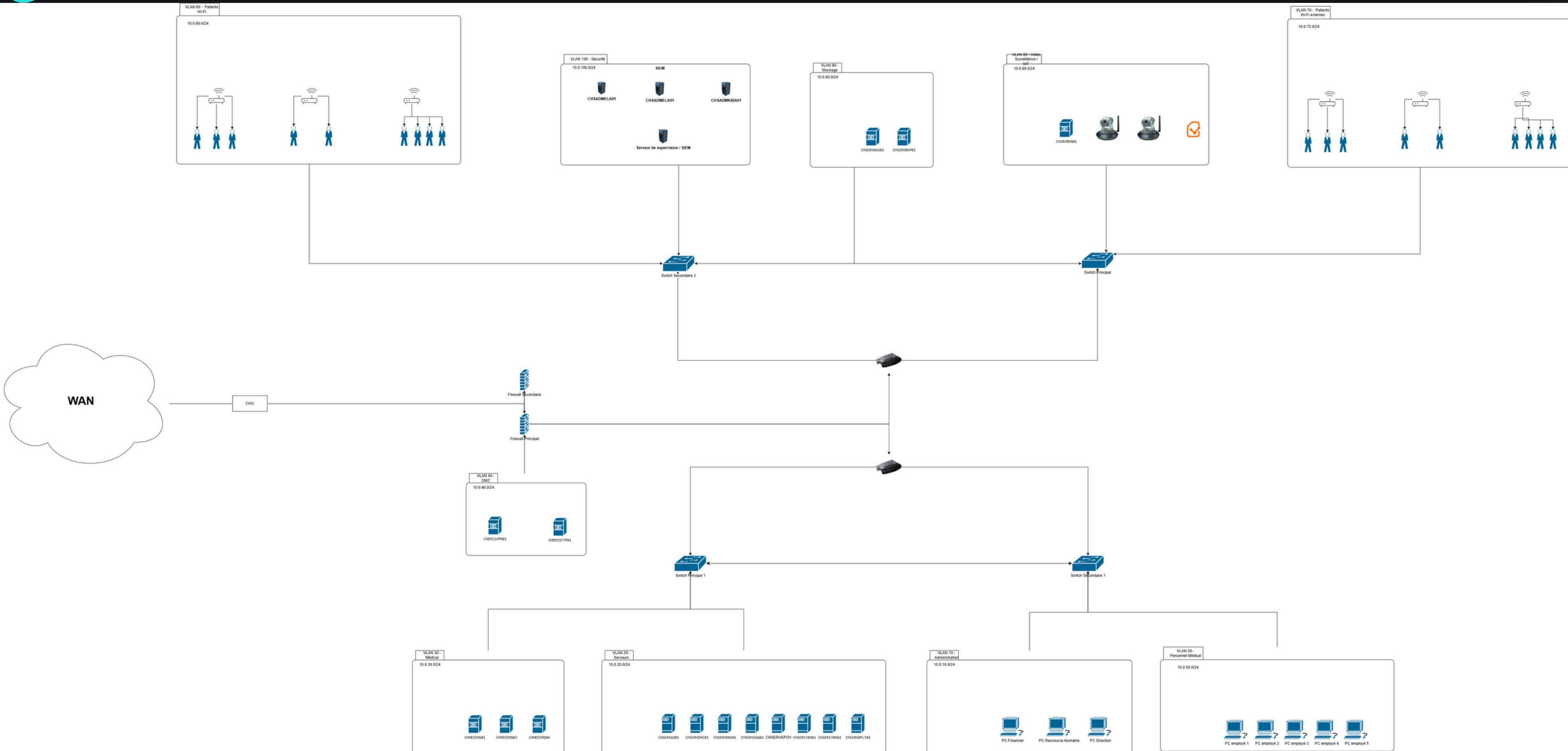
SCHEMA initial du SI

Légende des composants du réseau initial (CHU – avant sécurisation)

- CHMEDIMG01 : Poste d'imagerie médicale
- PC-MED01 : Poste personnel médical
- PC Ressource Humaine : Poste administratif RH
- PC Direction : Poste direction
- CHSERVAD01 : Contrôleur de domaine (Active Directory)
- CHSERVDHC01 : Serveur DHCP
- NAS01 : Serveur de stockage réseau (NAS)
- Caméra IP 1 à 4 : Caméras de vidéosurveillance connectées
- Switch : Switch principal non administrable
- Switch Caméra IP : Switch secondaire pour équipements IoT
- Point d'accès Wi-Fi : Réseau Wi-Fi partagé patients/personnels/visiteurs
- Réseau utilisé : 192.168.0.0/24



SCHEMA RESEAU 2.0



Recensement des besoins en matière de coûts

Un réseau de taille moyenne :

- Planification et design réseau : 8 heures à 60 €/heure = **480 €**
- Installation physique : 15 heures à 60 €/heure = **900 €**
- Configuration des équipements : 15 heures à 60 €/heure = **900 €**
- Configuration logicielle : 15 heures à 60 €/heure = **900 €**
- Tests et validation : 8 heures à 60 €/heure = **480 €**
- Documentation et formation : 8 heures à 60 €/heure = **480 €**
- Total estimé : **4.140 €**
- Nous serions aux alentours de **18.000 € pour trois techniciens supérieur.**

Budget global

- Infrastructure réseau : 84.000€ (*Estimation*)
- Matériel : 180.000€ (*Estimation*)
- Logiciel métiers (SIH / DPI) : 112.000€ (*Estimation*)
- Sécurité et conformité : 64.000€ (*Estimation*)
- Main-d'œuvre spécialisée : 18.500€ (*Estimation*)
- Total : 520.500€ (*Estimation*)

Avez-vous des questions ?

Budget et effectifs des plus gros centres hospitaliers

CHU	Budget Total	Effectifs
Montpellier	900 millions d'euros	11 683 agents
Paris	7,8 milliards d'euros	100 000 agents
Marseille	1,37 milliard d'euros	12 000 agents

IoMT

L'IoMT fait référence à l'ensemble des systèmes connectés, qui offrent des moyens innovants d'améliorer les soins aux patients et de donner aux médecins l'accès à des données en temps réel.

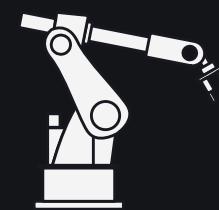
La surveillance à distance des patients



bracelets connectés

Les diagnostics avancés

Avec IA → diagnostiquer les maladies à leur stade précoce



La chirurgie robotisée

Budget global

1. SIH (Système Information Hospitaliés -> GLIMS (Clinisys) : Cout ->
500 000€
2. DPI (Dossier patient Informatisé)-> ORBIS (Dedalus) : Cout -> [
3. Investissement initial : $(1,9 \text{ M€} / 74000) \times 10000 \approx 257000 \text{ €}$
4. Coûts d'exploitation annuels : $(5,6 \text{ M€} / 74000) \times 10000 \approx 757000 \text{ €}$
5. Coût total annuel estimé : environ 1 million d'euros*]

 **Tableau des coûts estimés – SIH du CHU fictif (10 000 utilisateurs)**

Composant	Coût initial (€)	Coût annuel (€)	Coût sur 3 ans (€)	Coût sur 5 ans (€)
ORBIS (DPI)	257 000	757 000	2 528 000	3 785 000
GLIMS (SIL)	300 000	200 000	900 000	1 300 000
Skello (Badgeuse)	0	6 000	18 000	30 000
Caméras de surveillance	21 516,99	2 000	27 516,99	31 516,99
Total estimé	578 516,99	965 000	3 473 516,99	5 146 516,99

Coûts

1. Infrastructure réseau : 84 000 €

Le coût de l'infrastructure réseau dépend de la taille de l'établissement et des équipements nécessaires. Bien que les documents spécifiques sur les coûts détaillés soient limités, le rapport de la Cour des comptes souligne l'importance d'une planification rigoureuse pour éviter les surcoûts dans les projets SIH .

2. Matériel : 180 000 €

Ce poste comprend les serveurs, postes de travail, équipements médicaux connectés, etc. Selon le rapport de la Cour des comptes, les investissements en matériel doivent être planifiés avec soin pour éviter des dépenses excessives .

3. Logiciels métiers (SIH/DPI) : 112 000 €

Les logiciels métiers incluent le Système d'Information Hospitalier (SIH) et le Dossier Patient Informatisé (DPI). Le rapport de la Cour des comptes met en évidence que des spécifications techniques mal définies peuvent entraîner des coûts supplémentaires significatifs .

4. Sécurité et conformité : 64 000 €

La sécurité des données est cruciale dans un environnement hospitalier. Le rapport de la Cour des comptes souligne que des spécifications techniques inadéquates peuvent entraîner des surcoûts, notamment en matière de sécurité .

5. Main-d'œuvre spécialisée : 18 500 €

Ce poste couvre les coûts liés à l'ingénierie réseau, la sécurité, la formation et l'intégration. Le rapport de la Cour des comptes indique que des retards et des surcoûts peuvent survenir en raison de spécifications techniques mal définies, affectant ainsi les coûts de main-d'œuvre

Sources :

- https://sante.gouv.fr/IMG/pdf/Analyse_des_charges_et_ressources_SIH_-_donnees_2012_-_mai_2014.pdf
- <https://drees.solidarites-sante.gouv.fr/publications-communique-de-presse-documents-de-reference/panoramas-de-la-drees/241120-Panorama-CNS24>
- <https://cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-010.pdf>

Vecteur et Surface d'attaque

Surface d'attaque du CHU :

- Réseau interne non cloisonné (VLANs absents ou mal configurés)
- Postes utilisateurs peu durcis (droits admin locaux, MAJ absentes)
- Services exposés (RDP, SMB, WebApp sans WAF)
- Utilisateurs non sensibilisés (phishing, usage de mots de passe faibles)

Vecteurs d'attaque identifiés

- Phishing ciblé → récupération de credentials utilisateurs
- Exploitation de vulnérabilités (Zerologon, EternalBlue, etc.)
- Mauvaise configuration → partages ouverts, ports non filtrés
- Élévation de privilèges → via tokens, LSA, ou Kerberos
- Mouvement latéral → rebond via PSEexec, SMB, RDP vers contrôleur de domaine

Pentest

Outils Utilisés

Openvas : Détection des vulnérabilités

Nmap : Scan de port

Metasploit : test de payloads

Faille exploitée : Zerologon

Connexion au contrôleur de domaine sans mot de passe via Netlogon.

Un attaquant peut réinitialiser le mot de passe du contrôleur, puis prendre le contrôle total du domaine Active Directory.

car NETLOGON accepte des zéros comme authentification à cause d'un bug.

Conséquence on écrase le mot de passe

Machine Cible

OFADMDC01

Active Directory Windows
Server 2012

Normes sécurité Hôpital

Obligatoire

HDS : certification hébergement de données de santé

RGPD : données personnelles sensibles, DPIA, droits des patients

OIV / OSE : Certains Grands CHU

En cours

NIS2 : infrastructures critiques → cybersécurité renforcée

Audit technique externe périodique obligatoire : recommandé par la Cour des comptes (devrait devenir une norme)

Programme CaRE (750 M€) : les financements sont accordés uniquement si l'établissement fournit des preuves :
d'audit de sécurité,
de mise en place d'un PRA,
de segmentation réseau et d'un annuaire sécurisé.

Certification HAS (Haute Autorité de Santé) : inclut une grille cybersécurité avec exigences sur accès, sauvegardes, traçabilité et continuité.

Fortement recommandé

ISO 27001/27799 : sécurité de l'information + spécificité santé

Référentiel ANS : pratiques sécurité réseau, MFA, cloisonnement

Doctrine numérique santé : cadre stratégique et conformité nationale

802.1X

802.1X

Permet d'authentifier les utilisateurs via un serveur RADIUS

Empêche le branchement de clients inconnus

Différents protocoles de communication pour s'adapter aux besoins (EAP TLS, MSCHAP v2)

Outil : Machine Debian contenant un Freeradius (Linux)

Plus complexe de mise en place mais meilleure scalabilité sur long terme

Pourquoi ?

UN AD gère au niveau Logique
802.1X gère au niveau physique

IPS / IDS / XDR / EDR

Technologie	Rôle principal	Position	Exemples concrets	OUTILS / PRIX
IDS (Intrusion Detection System)	Déetecte les attaques réseau	Passif, en écoute	Alerte sur un scan Nmap ou Zerologon	🔒 Open Source : Snort – Gratuit 💼 Payant : Cisco Secure IDS – ~3k/an
IPS (Intrusion Prevention System)	Bloque les attaques en temps réel	Actif, inline	Coupe une attaque brute-force RDP automatiquement	🔒 Open Source : Suricata – Gratuit 💼 Payant : FortiIPS – ~4 000 €/an
EDR (Endpoint Detection & Response)	Supervise et protège les <i>postes de travail</i>	EDR agit sur le poste : (plutôt passif) il voit et répond à ce qui s'y passe.	Déetecte un exécutable suspect lancé sur une machine médicale	🔒 Open Source : Wazuh – Gratuit 💼 Payant : CrowdStrike Falcon – ~100 €/poste/an
XDR (Extended Detection & Response)	Corrèle les alertes de <i>plusieurs sources</i> (EDR + réseau + logs)	XDR relie tout : il combine les alertes de plusieurs sources pour reconstruire une attaque complète.	Relie une attaque mail + exécution + mouvement latéral sur AD	🔒 Wazuh + TheHive – Gratuit 💼 Payant : Microsoft Defender XDR – ~5 000 €/an (selon taille)

PSSI

Grandes Sections

🎯 Objectifs

Protéger les données de santé, assurer la continuité des soins, respecter RGPD/HDS

📍 Périmètre

SI complet : DPI, PACS, biomédicaux, réseau, utilisateurs, partenaires

🧠 Principes clés

Risques (EBIOS), confidentialité, intégrité, disponibilité, traçabilité

🏛️ Gouvernance

Comité SSI, RSSI, DPO, DSI, rôles définis, budget alloué

🔧 Mesures

Accès, MFA, chiffrement, cloisonnement, sauvegardes, PRA, EDR, IDS/IPS

⌚ Suivi & audit

Audits, indicateurs, veille, révision tous les 2 ans

Pourquoi est-elle adaptée au contexte hospitalier :

Elle tient compte des spécificités critiques du secteur santé :

📊 Données hautement sensibles

🕒 Disponibilité 24/7 pour garantir la continuité des soins

👤 Multiplicité des profils utilisateurs (soignants, administratifs, externes)

⚖️ Contraintes réglementaires fortes : RGPD, HDS, NIS2, HAS

WAF / FIREWALL

WAF

(Web Application Firewall) est un pare-feu applicatif

un WAF est utile pour :

Protéger les applications médicales (ex : portail patient, webmail, intranet)

Compenser des failles de développement non corrigées rapidement

Intercepte les tentatives d'injections SQL, XSS...

● **WAF open source** ModSecurity, NAXSI

● **WAF Payant Imperva WAF** environ 3 000 à 10 000 €/an pour PME / hôpital moyen

Firewall

Firewall – Pare-feu Réseau
contrôle traffic entrant et sortant

Firewalls open source
pfSense (FreeBSD, très utilisé en prod)
OPNsense (fork amélioré de pfSense)

Firewalls payants
Stormshield (français, certifié ANSSI)
Fortinet FortiGate
Palo Alto Networks

Stormshield SN210 : ~1 200 € + abonnement annuel
FortiGate 60F : ~700 € + licence UTM à partir de 400 €/an
Palo Alto PA-220 : ~1 500 € + support

JUMPBOX / BASTION

JUMPBOX

Simple Machine de rebond
(Ici Windows 10)

permet d'ajouter une couche de sécurité supplémentaire,
via la connexion une connexion VPN pour se connecter

Beaucoup moins coûteux économiquement qu'un bastion

BASTION

Ensemble de machines

Supervision, contrôle, enregistrement
et filtrage des accès

Plateforme sécurisée
d'accès administrateur centralisé

💡 Wallix Bastion, BeyondTrust,
Teleport, Guacamole

Identity & Access

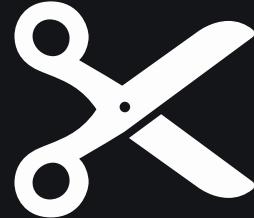
IAM (Identity & Access Management)

Ensemble des mécanismes permettant de gérer, sécuriser et tracer les accès utilisateurs au SI.

- 🔐 Authentification forte (MFA et VPN pour JUMPBOX, certificat (EAP TLS pour 802.X))
- 👥 Comptes centralisés via Active Directory
- 📁 Groupes AD par rôle (médecins, admins, biomédicaux, etc.)
- ⌚ Cycle de vie des identités automatisé via le SIRH (*Système d'Information des Ressources Humaines*)
- 📅 Revue Mensuels des droits + suppression des comptes désactivés après 90 jours d'inactivité

Protocole LDAP

GANTT et charge de Travail



Découpage structuré des tâches)

Le projet a été segmenté en grandes phases : analyse des risques, rédaction PSSI, mise en place des mesures, tests (pentest), documentation.



Jalons clés et points de contrôle

Intégration de jalons :
Livraison du schéma réseau
Validation de la PSSI
Résultats du pentest
Documentation finale

Répartition réaliste des ressources)

Chaque membre a été affecté selon ses forces



Anticipation des risques de planning



Délais de rendu en parallèle des cours
Problèmes techniques sur machines virtuelles
Solution :
Répartition hebdomadaire et points réguliers

KPI pertinent

KPI	Objectif / Seuil cible	Intérêt
 % de comptes inactifs désactivés sous 90 jours		100% Réduction du risque lié aux comptes dormants
 % d'accès critiques protégés par MFA		100% Sécurisation des systèmes vitaux (DPI, PACS, AD)
 % de comptes à privilège revus trimestriellement		100% Gouvernance des accès sensibles
 % du personnel formé à la cybersécurité	≥ 90 % / an	Renforcement de la culture sécurité (critère HAS)
 % de logs critiques conservés > 12 mois		100% Traçabilité et conformité HDS / PGSSI-S
 Temps moyen de réponse à un incident de sécurité	< 4h	Réactivité opérationnelle du CSIRT
 % de serveurs conformes au référentiel de durcissement	≥ 95 %	Réduction du risque d'exploitation
 % de flux internes/externe chiffrés	≥ 95 %	Protection des communications (RGPD / ANSSI)

DevOps & intégration continue

⚙ 1. Métier de DevOps & Spécificités

Pont entre développement et réseaux

Objectifs : automatisation, collaboration, livraison continue, résilience

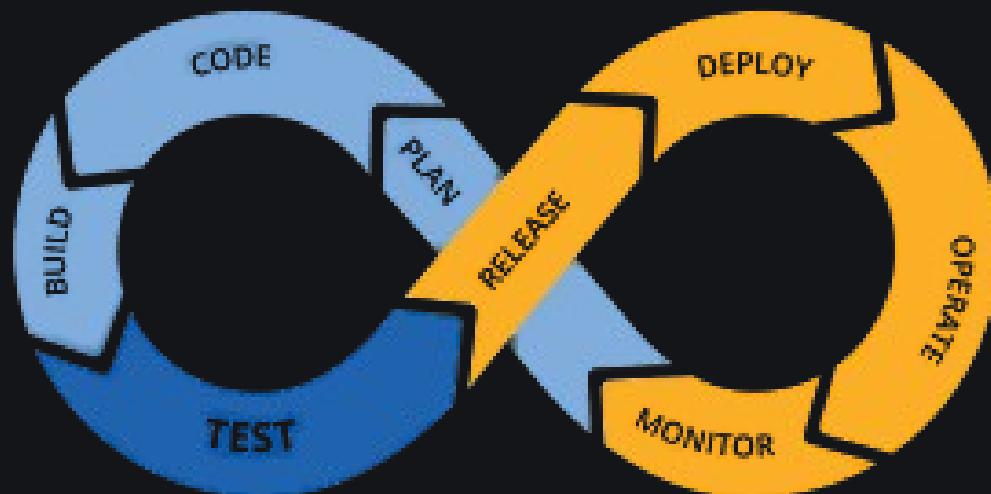
Spécificités : CI/CD, Ansible...

🛠 2. Outil d'intégration continue recommandé

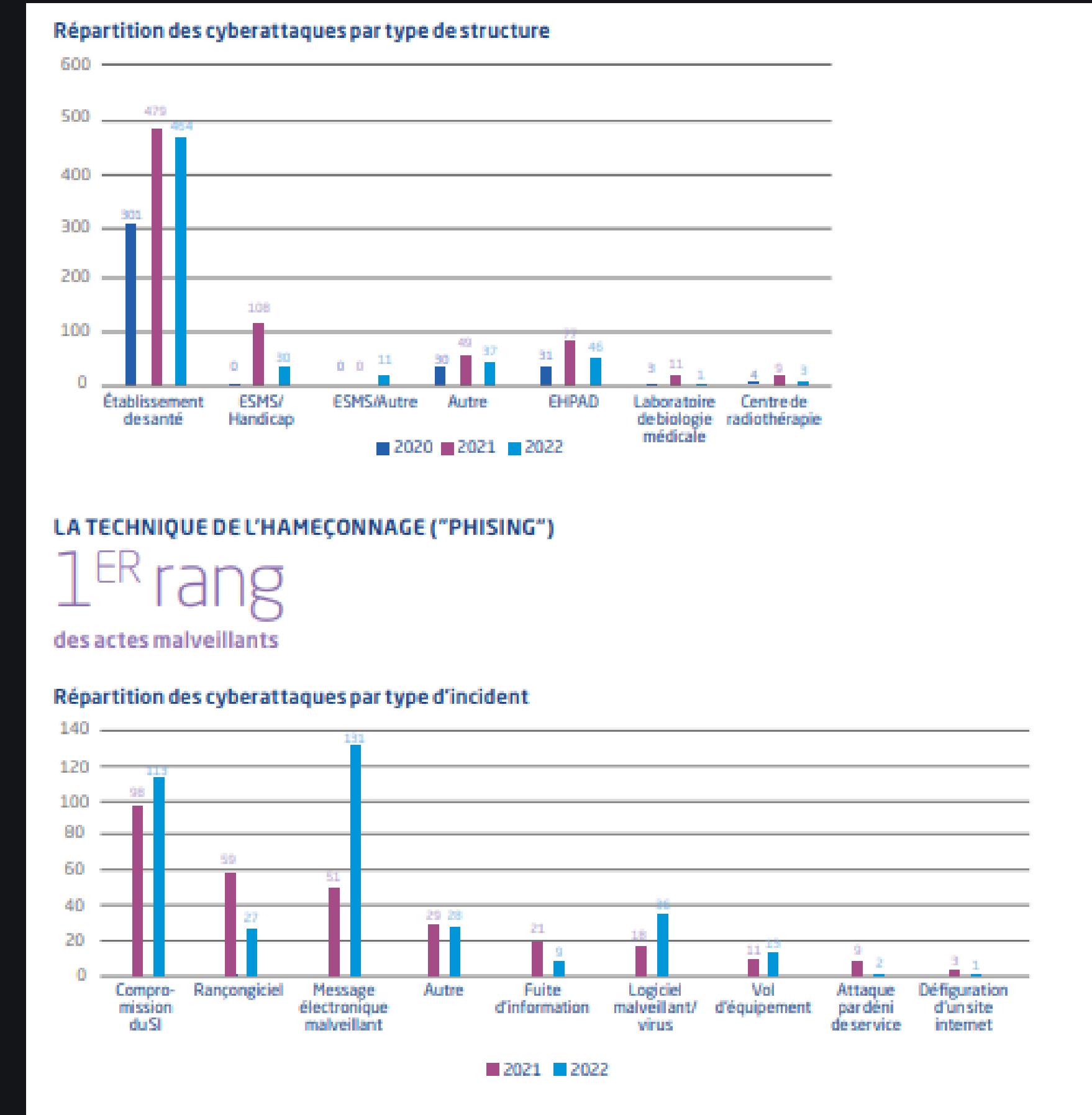
GitLab CI/CD ou GitHub Actions (simples, intégrés à Git)

Jenkins (personnalisable, très utilisé en entreprise)

Exemple de pipeline :



LE RISQUE CYBER des établissements de santé EN CHIFFRES



Source : <https://www.grand-est.ars.sante.fr/media/125985/download?inline>

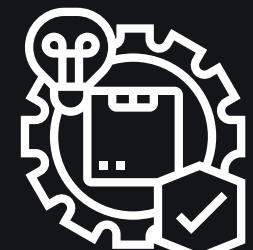
La méthode EBIOS Risk Manager



Expression des Besoins et Identification des Objectifs de Sécurité



La méthode EBIOS, méthode d'analyse de risque française de référence, permet aux organisations de réaliser une appréciation et un traitement des risques



Une démarche collaborative et agile

Concept de sécurité	Mise en œuvre dans le projet
Défense en profondeur	Superposition des protections : firewall, VLANs, 802.1X, IDS/IPS, segmentation logique et physique.
Sécurité périphérique	Firewall principal en frontal entre le WAN et l'architecture interne.
Segmentation logique (VLANs)	11 VLANs isolés : utilisateurs, serveurs, caméras, biomédical, administration, etc.
Segmentation physique	Cloisonnement par switchs physiques selon les zones critiques.
Contrôle d'accès (AAA)	Authentification 802.1X, Active Directory centralisé, gestion des groupes par rôle.
Authentification forte (MFA)	VPN + MFA pour l'accès distant sécurisé (zone sensible via Jumpbox).
Gestion des accès	Comptes revus mensuellement, suppression après 90 jours d'inactivité.
Bastion / Jumpbox	Poste intermédiaire pour administrer les serveurs (Windows 10 avec VPN).
Détection d'intrusion (IDS/IPS)	Outils open source comme Snort ou Suricata pour surveillance réseau.
Sécurité des terminaux (EDR/XDR)	Utilisation de Wazuh ou CrowdStrike pour la supervision des postes.
PSSI et gouvernance	Politique formelle, comité SSI, rôles définis (DPO, RSSI, DSI).
Tests d'intrusion (Pentest)	Exploitation de la faille Zerologon avec Metasploit sur l'AD.
Plan de continuité (PRA/PCA)	Documenté et testé pour les services critiques.
Sensibilisation et formation	Ateliers, formations internes et campagnes anti-phishing.
Surveillance et veille	Veille CERT Santé, indicateurs de sécurité (MFA, logs, accès dormants).
Chiffrement des flux	Chiffrement des communications internes et externes (95% des flux).

TABLE 1 – Résumé des mécanismes de sécurité déployés dans le SI du CHYNOV

VOL / PERTE D'UN PC PORTABLE, D'UN SMARTPHONE OU D'UNE TABLETTE – REFLEXES



VOL / PERTE D'UN PC PORTABLE, D'UN SMARTPHONE OU D'UNE TABLETTE – REFLEXES

EN CAS DE VOL/PERTE D'EQUIPEMENT¹ CONSTATE, CERTAINS POINTS SONT A CONSIDERER :

OBJECTIFS DE L'ATTAQUE

L'objectif peut être de récupérer des informations sensibles/confidentielles à des fins malveillantes.

Il peut toutefois s'agir d'un vol opportuniste ne ciblant pas précisément le contenu de l'équipement¹.

RISQUES

- VOL DE DONNEES SENSIBLES/CONFIDENTIELLES
- PERTE DEFINITIVE DE DONNEES (SI ABSENCE DE SAUVEGARDE)
- PERTE FINANCIERE
- PREPARATION D'ATTAQUE CIBLEE

LES BONNES PRATIQUES

- Rester vigilant : ne pas laisser votre équipement sans surveillance notamment dans des lieux publics
- Utiliser un mot de passe fort et toujours verrouiller sa session en cas d'absence
- Chiffrer les données sensibles avec un outil dédié
- Sauvegarder les données sur un autre support

¹ Par « équipement », on désigne les appareils mobiles suivants : ordinateur portable, tablette et smartphone.



VOL / PERTE D'UN PC PORTABLE, D'UN SMARTPHONE OU D'UNE TABLETTE – REFLEXES

ATTENUER L'IMPACT DU VOL D'UN EQUIPEMENT

PREVENTION

1. Noter le numéro de série de l'équipement

Le numéro de série de l'équipement est unique et permet son identification. Il sera demandé en cas de dépôt de plainte pour vol ou déclaration de perte.

2. Sauvegarder régulièrement les documents

La sauvegarde régulière des documents sur un support externe (disque dur externe, USB...) facilite la reprise d'activité et évite la perte de données. Il est fortement conseillé de chiffrer ce support externe.

3. Permettre le verrouillage et l'effacement à distance des données de l'équipement

L'utilisation d'une solution de MDM est recommandée. Cette solution doit au minimum disposer des fonctionnalités suivantes :

- verrouillage à distance de l'équipement en cas de perte ou de vol (blocage des accès non autorisés à l'appareil sans avoir à supprimer les données)
- effacement de l'intégralité des données enregistrées sur un appareil ou uniquement les informations sensibles de la structure
- localisation/suivi des smartphones et des tablettes : utilisation de la fonctionnalité GPS, 3G/4G ou WiFi pour localiser l'appareil

4. Sécuriser les mots de passe

- Utilisation de mots de passe non rejouables (One Time Password)
- Utilisation des gestionnaires de mots de passe tel que l'outil gratuit KeePass

5. Chiffrer le contenu de l'équipement

- Chiffrement des données sensibles (avec un mécanisme de chiffrement conseillé par l'ANSSI)
 - Utilisation des solutions permettant de chiffrer le disque en partie ou totalement (mode de chiffrement conseillé afin d'éviter la récupération des informations liées à l'architecture interne données d'authentification...) telles que :
 - Cryhod² : Windows XP, Vista, Seven, Windows 2003 et 2008
 - STORMSHIELD Data Security (SDS)² : Windows 7 & 8.1
 - ZoneCentral v5.0 build 960² : Windows 2000, XP, Vista, Seven, 2003, 2008 (32 et 64 bits)
 - BitLocker² : Windows Enterprise (solution gratuite)
 - VeraCrypt (solution gratuite)

6. Sensibiliser les utilisateurs à l'égard des équipements mis à leur disposition et les former à la protection des documents qu'ils contiennent

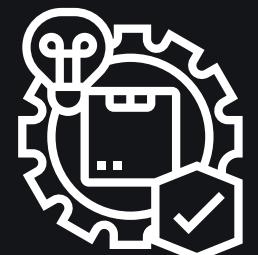
BACK UP



Stockage à chaud



Stockage à froid (2 sites extérieur privé)



chiffrement logique (AES 256), Hardening des machines,

Systeme de Supervision



- Interface utilisateur conviviale
- Intégration avec Nagios
- Large éventail de plugins et extensions
- Gestion centralisée de la supervision
- Personnalisable et extensible
- Visualisation graphique des données
- Surveillance multi-plateforme
- Rapports et analyses avancées



- Complexité de configuration
- Courbe d'apprentissage
- Performance affectée par le nombre d'hôtes et de services
- Coût élevé pour les versions commerciales
- Besoin de compétences techniques pour l'administration
- Documentation parfois limitée
- Notifications parfois excessives
- Intégration avec d'autres outils parfois complexe



- Open-source et gratuit
 - Large éventail de plugins et extensions
 - Surveillance en temps réel
 - Grande communauté de support
 - Personnalisable et extensible
 - Surveillance multi-plateforme
 - Détection rapide des pannes
 - Fonctionnalités avancées de reporting
- Configuration complexe
 - Courbe d'apprentissage raide
 - Interface utilisateur basique
 - Notifications fréquentes et bruyantes
 - Coût élevé pour les versions commerciales
 - Scalabilité limitée sans plugins tiers
 - Documentation parfois insuffisante
 - Intégration avec d'autres outils complexe



SIEM



- Elasticsearch



- Logstash



- Kibana



- Withsecure