Certification ASI – Bloc 1

Matrice AMDEC – Cybersécurité du CHU

Administrateur Systèmes, Réseaux et Sécurité

Réalisé par :

Clément Garcia
Nils Jaudon
Yann Blanc

IPSSI / Ynov Informatique
15 avril 2025

Version du document validée par Michel Gournier : 2.7

Table des matières

1 Contexte

Dans le cadre du projet Ynov, cette analyse AMDEC a été conduite pour le CHU fictif en vue de déterminer les principaux risques en termes de cybersécurité. L'idée est de disposer d'un cadre pour évaluer l'impact potentiel de chaque scénario de défaillance, la probabilité de sa survenance, ou le risque de ne pas le détecter – afin de savoir où mobiliser en priorité nos efforts.

2 Analyse des risques

N°	Élément analysé	Mode de défaillance	Effets potentiels	G	P	D	Criticité
1	CHSERVAD01	Compromission, élévation de privilèges	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	equipement de sureté	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 vérolées 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.

Légendes :

- **Gravité (G)** : Impact potentiel sur le fonctionnement du CHU (1 à 10)
- **Probabilité (P)** : Fréquence d'occurrence (1 à 10)
- **Détection (D)** : Difficile à détecter (1 à 10)
- **Criticité (C)** : G × P × D

3 Acceptabilité des risques et actions correctives proposées

Dans le contexte hospitalier, l'acceptabilité d'un risque dépend de plusieurs facteurs : la gravité pour les patients, l'impact sur la continuité des soins, et les obligations réglementaires (RGPD, HDS, etc.).

Nous avons défini un seuil de criticité à ne pas dépasser. Ainsi :

— Les risques avec une criticité supérieure à 150 sont considérés comme **non acceptables**.
— Ils nécessitent obligatoirement une action immédiate.
— Les autres sont surveillés, mais peuvent être tolérés temporairement.

Les actions correctives proposées pour les risques critiques sont :

— **R1 – AD** : Mise en place du MFA, audits réguliers, durcissement.
— **R2 – VLAN PATIENT** : Séparation stricte VLAN, filtrage inter-réseaux, portail captif.
— **R3 – DMZ** : Surveillance SIEM, tests de pénétration réguliers.
— **R6 – IDS/IPS** : Redondance, supervision continue.
— **R7 – Sauvegardes** : Tests de restauration, externalisation hors ligne.

3.1 Matrice des risques – État initial du SI

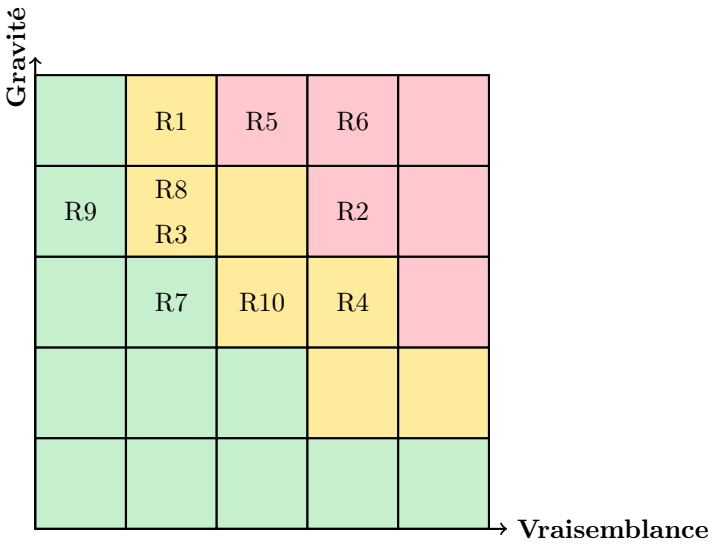

Table 3 – Matrice des risques résiduels après traitement — positionnement selon la gravité et la vraisemblance
Cette matrice représente les risques restants après application des mesures correctives. Les zones colorées permettent de visualiser les priorités d'action : rouge (critique), orange (modéré), vert (mineur).

Légende :

— **R1 : Active Directory**
— **R2 : VLAN PATIENT / GUEST**
— **R3 : DMZ**
— **R4 : IoT / Vidéosurveillance**
— **R5 : ERP**
— **R6 : Corruption ou vol de données**
— **R7 : IDS désactivé / mal configuré**
— **R8 : MAJ vérolées ou malveillantes**
— **R9 : Défaillance ou piratage d'équipements**
— **R10 : Défaillance des services de base**

3.2 Matrice des risques – Risques résiduels après amélioration du SI

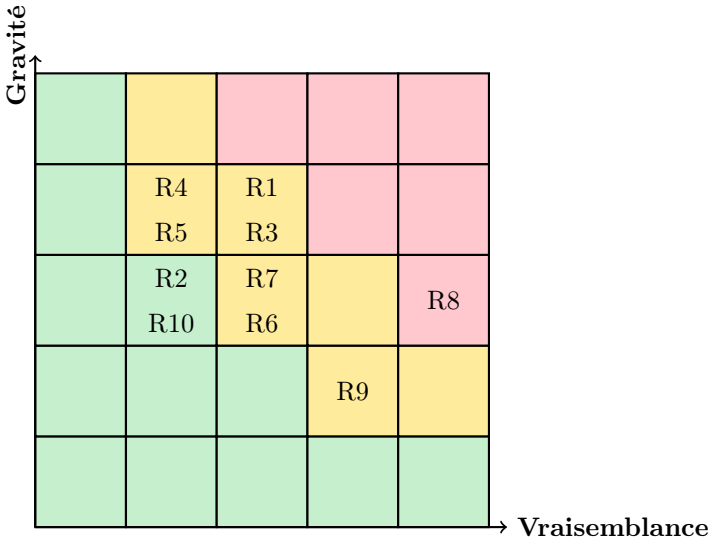

TABLE 4 – Matrice des risques résiduels après mise en œuvre des mesures de sécurité
Cette matrice illustre l'évolution des risques suite aux actions correctives mises en place. La baisse de la criticité est reflétée par le déplacement des risques vers des zones de moindre gravité et vraisemblance.

Légende :

- **R1 : Active Directory**
- **R2 : VLAN PATIENT / GUEST**
- **R3 : DMZ**
- **R4 : IoT / Vidéosurveillance**
- **R5 : ERP**
- **R6 : Corruption ou vol de données**
- **R7 : IDS désactivé / mal configuré**
- **R8 : MAJ vérolées ou malveillantes**
- **R9 : Défaillance ou piratage d'équipements**
- **R10 : Défaillance des services de base**

4 Niveaux de disponibilité attendus selon la criticité des applications

Dans un établissement comme un CHU, certaines applications doivent être disponibles en permanence, tandis que d'autres tolèrent de courtes interruptions. Selon la criticité des services analysés dans la matrice AMDEC, il est essentiel de définir un niveau de disponibilité chiffré pour chaque catégorie.

Niveau de criticité	**Disponibilité cible**	**Indisponibilité max / an**	**Indisponibilité max / mois**
Très critique	99.999 %	5 min 15 s	25,9 s
Critique	99.99 %	52 min 34 s	4 min 23 s
Importante	99.9 %	8 h 45 min	43 min 49 s
Modérée	99 %	3 j 15 h 36 min	7 h 18 min
Faible	95 %	18 j 6 h	36 h

Table 5 – Tableau de correspondance entre criticité des services et objectifs de disponibilité.

5 Conclusion

L'analyse AMDEC de l'infrastructure du CHU met clairement en évidence plusieurs points critiques à ne pas méconnaître. Certaines parties comme le serveur Active Directory, la DMZ, les VLAN patients/invités sont à haut risque (à propos de la gravité et de la probabilité d'occurrence) et leur détection fait défaut, ce qui rend leur dangerosité encore plus grande.

Ce qu'on en retire, c'est qu'il convient de prioriser des actions concrètes : authentification forte à mettre en place, isolation des VLAN sensibles, renforcement des services exposés et surveillance assurée par un bon SIEM, à mettre en œuvre rapidement pour empêcher les impacts en cas d'attaque.

Au final, la matrice est un vrai outil de pilotage. Elle permet d'identifier clairement les priorités et de concentrer les efforts du système de sécurité là où ces derniers sont vraiment nécessaires, tout en restant adaptable dans le temps face à des risques émergents, la mise à jour de l'infrastructure ou les protections mises en place.

6 Annexes et ressources

Voici les principales ressources consultées et utilisées pour la rédaction de ce livrable :

- **EBIOS - Risque Manager** :
  `https://cyber.gouv.fr/publications/la-methode-ebios-risk-manager-le-guide`
- **Grille de criticité et disponibilité (source pédagogique)** :
  `https://pressbooks.pub/methodes/chapter/criticite-des-applications/`
- **Documentation ITIL et ISO 27005 (inspiration méthodologique)** :
  `https://www.iso.org/standard/80585.html`