Document d’Architecture Technique (DAT)

Mardi 10 juin 2025

MONTPELLIER ynov CAMPUS

1. Présentation générale

Ce projet se déroule dans le cadre d'un Centre Hospitalier Universitaire (CHU) fictif, réparti sur cinq bâtiments. Il sert de support à l'évaluation des compétences de la section cybersécurité, et mobilise plusieurs axes clés : gouvernance de la sécurité, tests d'intrusion, sécurité des systèmes d'exploitation et sécurité des réseaux.

L'objectif est de renforcer l'infrastructure numérique de l'hôpital contre les cybermenaces. Le projet comporte plusieurs volets :

- Élaboration d'une PSSI (Politique de Sécurité des Systèmes d'Information) adaptée à un hôpital. Même dans un cadre fictif, cette politique doit être crédible, alignée sur les normes en vigueur (ex. : ISO 27001) et adaptée aux enjeux du secteur santé.

- Sécurisation du réseau : définition et mise en place de protections réseau telles que des règles de pare-feu, IDS/IPS, segmentation, 802.1X, jumpbox, et des indicateurs de performance (KPI) pour le suivi.

- Sécurité des systèmes et applications critiques : durcissement des serveurs (notamment bases de données contenant des données sensibles), conformité avec la directive NIS2, et sécurisation des applications métiers.

- Pentest : réalisation d'un test d'intrusion sur les systèmes de sécurité de l'hôpital afin d'identifier les vulnérabilités. Le projet se conclut par une analyse des faiblesses du SI et des recommandations d'amélioration.

1.3 Périmètre

Infrastructure fictive : Toutes les mesures se basent sur un schéma hospitalier, permettant de simuler un vrai hôpital sans manipuler de données réelles.
Aspects étudiés :

- Politique de sécurité (gouvernance)
- Sécurité réseau (firewalls, IDS/IPS, segmentation, etc.)
- Sécurisation des systèmes d'exploitation et des applications sensibles
- Tests d'intrusion et recommandations

1. Nos Vlans

VLAN ID	Nom	Fonction	Plage IP
10	ADM (Administration)	Gestion RH, finance, services généraux	10.0.10.0/24
20	SERV (Serveurs critiques)	Centralisation des services essentiels	10.0.20.0/24
30	MED (Médical - Équipements)	Appareils biomédicaux, logiciels métiers	10.0.30.0/24
40	DMZ (Zone publique)	Services accessibles depuis l'extérieur	10.0.40.0/24
50	USER (Personnel médical)	Réseau dédié aux PC des médecins, infirmiers	10.0.50.0/24
60	PATIENT (Wi-Fi patients)	Réseau isolé pour les patients connectés	10.0.60.0/24
70	GUEST (Invités externes)	Wi-Fi pour visiteurs et conférenciers	10.0.70.0/24
80	VIDÉO (Surveillance & IoT)	Caméras de surveillance, badgeuses	10.0.80.0/24
90	STOCKAGE (NAS & Backup)	Serveurs de fichiers et sauvegardes	10.0.90.0/24
100	SÉCURITÉ (IDS/IPS & Firewall)	Détection et monitoring de sécurité	10.0.100.0/24
110	Infirmier	Pour Infirmier	10.0.110.0/24
666	Blackhole	Confinement	10.0.666.0/24

1. Nom des Machines Virtuelles

Service / Fonction	Nom de la Machine	Remarques
KPI (Monitoring / Stats)	CHSERVKPI01	Gestions des certificats (autorité de certification interne)
Active Directory	CHSERVAD01	Serveur Active Directory
ERP / Logiciel de gestion (Sage)	CHSERVSAG01	Gestion comptable et administrative
FreeRADIUS (Debian)	CHADMFRAD01	Authentification réseau
Serveur DHCP	CHSERVDHC01	Attribution des IP
Serveur DNS	CHSERVDNS01	Résolution de noms
SIEM (ELK Stack)	CHSADMELA01	Serveur ELK principal
	CHSADMELTS01	Logstash
	CHSADMKIBA01	Kibana
Sauvegarde / Backup	CHSERVBKP01	Serveur de sauvegarde
Serveur de déploiement (Ansible, WSUS, etc.)	CHSERVDPLY01	Gestion des déploiements
SAN / Serveur de fichiers	CHSERVNAS01	Stockage centralisé
Jumpbox Windows	CHSERVJBX01 / CHSERVJBX02	Accès sécurisé aux systèmes
SFTP (DMZ - sécurisé externe)	CHDMZSFTP01	Transferts sécurisés externes

Machines médicales	**CHMEDIMG01 / CHMEDIMG03 / CHMEDIMG04**	**Systèmes d'imagerie médicale**
IDS / IPS	**CHADMIPS01**	**Détection et prévention des intrusions**
OpenVPN	**CHDMZ1VPN01**	**Accès VPN sécurisé**
Badgeuse (Gestion des accès)	**CHSRVBDG01**	**Gestion des badges**

2. Infrastructure Physique

Serveurs

Dell PowerEdge R740xd x4

Réseau & Sécurité

- **Switches : Cisco SG550X (x4)**
- **Firewall : Stormshield (x2)**
- **Sondes de Sécurité : Darktrace**
- **Points d'accès Wi-Fi : Aruba (x30)**

Autres Équipements

- **Badgeuse : Gestion des accès**

Schémas Réseau (Draw.io)