



République Tunisienne
Ministère de l'Enseignement Supérieur et de la Recherche
Scientifique
Université de Carthage
**Institut National des Sciences Appliquées
et de Technologie**



RAPPORT DE PROJET

Système de Gestion d'une Flotte de Robots Hospitaliers

Filière : Réseaux & Télécommunications

Matière : Programmation Orientée Objet

Module : Java

Niveau universitaire : 2ème année

Groupe : RT2/1

Élaboré par :

Feriel Ferah · Lina Cherif

Encadré par : Dr. Amira Dkhil

Date de remise : 2026

Année universitaire 2025–2026

1. Concept et Positionnement

Ce projet conçoit une flotte intelligente de robots hospitaliers répondant à deux enjeux critiques de l'e-santé moderne : la protection du réseau informatique face aux cyberattaques (ransomware, intrusions) et l'automatisation du triage médical aux urgences.

- D'une part, l'idée du « robot sécurité » s'inscrit dans une urgence sanitaire majeure soulignée par l'Académie nationale de médecine. En France, la vulnérabilité du secteur s'est intensifiée avec **1 582 établissements touchés en 2021**, soit une augmentation spectaculaire qui concerne désormais **un établissement sur six**. Ces offensives, qui ont doublé entre 2020 et 2021, ne se limitent plus au vandalisme mais paralysent des structures critiques : l'hôpital d'Armentières a dû fermer ses urgences pendant 24 heures en 2024. Les conséquences documentées sont alarmantes, allant de l'annulation d'opérations chirurgicales à l'impossibilité d'effectuer des transfusions par effacement de données, transformant ces actes numériques en véritables mises en danger de la vie d'autrui, voire en homicides potentiels.
- D'autre part, le « robot triage » répond à la mauvaise organisation chronique des hôpitaux tunisiens, en particulier dans les services d'urgence. Notre approche s'inspire également du modèle grec du dossier médical national. Dans ce système, chaque hôpital conserve son propre dossier médical, mais chaque patient possède un identifiant national unique. Lorsqu'un médecin souhaite accéder aux antécédents d'un patient, il s'authentifie via son empreinte professionnelle, puis utilise l'identifiant national pour se connecter au réseau national de santé. Il peut ainsi consulter l'intégralité du dossier médical du patient : opérations passées, maladies chroniques, consultations antérieures, etc. Après la consultation, le médecin se reconnecte au réseau et « pousse » les nouvelles informations (diagnostic, examens prescrits, compte rendu) directement dans le dossier médical national du patient, assurant ainsi une mise à jour centralisée et partagée en temps réel.

Deux spécialisations complémentaires

RobotSecurite	RobotTriage
Surveille le réseau 24h/24. Détecte intrusions, DDoS, brute force. Active le mode dégradé anti-ransomware. Chiffre les données avec AES-256 simulé. Journalise dans un audit trail légal.	Robot autonome de triage. Mesure tension, température, SpO2, pouls. Analyse vision IA (YOLO + HSV). Calcule le niveau ESI (1–5) international. Déploie le kit d'urgence en cas de Code Blue.
Station fixe — surveillance via réseau, jamais physique	Mobile — se déplace vers le patient, retour autonome à la station

2. Diagramme de Classes

Hiérarchie d'héritage (3 niveaux)

```
Robot    [ABSTRAITE]
  attributs : id, x, y, energie, heuresUtilisation, enMarche,
  historiqueActions
  méthodes : demarrer(), arreter(), verifierEnergie(),
  verifierMaintenance()
  abstraites : deplacer(x,y) • effectuerTache()
  ↳ RobotConnecte [ABSTRAITE] implements Connectable
    attributs : connecte, reseauConnecte
    méthodes : connecter(), deconnecter(), envoyerDonnees()
    ↳ RobotTriage
      kitUrgence, analyseur, baseDossiersMedicaux,
modeDegrade
    ↳ RobotSecurite
```

robotsIsoles

niveauAlerte, etatSysteme, sessionsActives, auditTrail,

Classes de domaine et interfaces

Type POO	Nom	Rôle
Interface	Connectable	connecter / deconnecter / envoyerDonnees
Classe concrète	SignesVitaux	Encapsule pouls, tension, température, SpO2
Classe concrète	DossierMedical	Dossier patient MyHealth (âge, catégories de risque)
Classe concrète	KitUrgence	Stock individuel par élément, réapprovisionnement
Classe concrète	AnalyseurUrgence	Moteur de règles ESI en 3 étapes (vision + constantes + dossier)
Classe concrète	GestionnaireHospitalier	Pilote ArrayList<Robot>, polymorphisme sélection + alerte

3. Réponse aux Exigences POO

3.1 Héritage et redéfinition de méthodes

La hiérarchie repose sur trois niveaux d'abstraction. La classe Robot impose un contrat via deux méthodes abstraites. RobotConnecte y ajoute la couche réseau. Chaque classe concrète redéfinit déplacer() et effectuerTache() différemment :

- RobotSecurite.deplacer() lève systématiquement une RobotException — ce robot est une station fixe qui surveille le réseau, pas les couloirs.
- RobotTriage.deplacer() calcule la distance euclidienne, vérifie l'énergie (0,3 %/unité) et incrémente les heures d'utilisation (1 h par 10 unités).
- RobotTriage.effectuerTache() exécute un protocole de triage en 9 étapes détaillées ci-dessous.

3.2 Gestion de la criticité par énumérations

Énumération	Valeurs	Effet dans le code
NiveauESI	ESI_1 (Code Blue) ... ESI_5	ESI_1 → UrgenceVitaleException + kit déployé
NiveauAlerte	VERT / ORANGE / ROUGE / CRITIQUE	ROUGE → déconnexion réseau + mode dégradé
EtatSysteme	NORMAL / ALERTE / DEGRADE / URGENCE	DEGRADE → robots en fonctionnement local
Role	INFIRMIER / TECHNICIEN / MEDECIN / ADMIN	Contrôle d'accès hiérarchique RBAC
ElementKit	DEFIBRILLATEUR, MASQUE_O2, GARROT...	Stock individuel, rapport infirmiers à la station

3.3 Hiérarchie d'exceptions personnalisées

Exception	Hérite de	Déclencheur
RobotException	Exception	Classe racine du projet
EnergieInsuffisanteException	RobotException	Énergie < seuil requis pour l'action

Exception	Hérite de	Déclencheur
MaintenanceRequiseException	RobotException	Heures d'utilisation > 100
UrgenceVitaleException	RobotException	ESI_1 confirmé — Code Blue
AuthenticationException	RobotException	Code médecin invalide (RobotTriage)
AuthentificationEchoueeException	RobotException	Identifiants SHA-256 incorrects (RBAC)
CompteVerrouilleException	RobotException	≥ 3 tentatives de connexion échouées
AccesNonAutoriseException	RobotException	Rôle insuffisant pour l'action demandée
DonneesAltereesException	RobotException	Données reçues sans chiffrement AES valide
HoneypotException	RobotException	Accès à la ressource piège — intrusion confirmée
SessionExpireeException	RobotException	Token inconnu ou expiré

3.4 Polymorphisme — GestionnaireHospitalier

Le gestionnaire pilote une `ArrayList<Robot>` et illustre le polymorphisme à deux niveaux :

- Sélection intelligente : parcourt la flotte et retourne le robot le plus apte selon l'énergie disponible, l'état NORMAL et le type de mission (RobotTriage pour triage, RobotSecurite pour surveillance).
- Alerte générale : appelle `arreter()` et `deconnecter()` sur chaque robot via leur type commun, sans connaître leur classe concrète.

4. Fonctionnalités Innovantes

4.1 RobotSecurite — Cinq mécanismes de cybersécurité

Mécanisme	Implémentation
RBAC + SHA-256	Authentification par hachage SHA-256. Rôles hiérarchiques (INFIRMIER < TECHNICIEN < MEDECIN < ADMIN). Verrouillage compte après 3 échecs. Tokens UUID de session.
IDS	Détection DDoS par fenêtre glissante 60 s (> 50 requêtes = ORANGE). Détection de robots isolés tentant de reprendre leur activité réseau. Escalade automatique du niveau d'alerte.
Mode Dégradé	Détection ransomware → déconnexion réseau principal → isolation de tous les robots connectés → maintien des urgences vitales en local. Inspiré des cyberattaques de 2024 (Armentières, Guy's Hospital).
Honeypot	Ressource piège DOSSIER_PATIENT_VIP_CONFIDENTIEL : aucun utilisateur légitime ne l'accède jamais. Tout accès = intrusion confirmée à 100% → HoneypotException + NiveauAlerte.ROUGE.
Audit Trail	Journal horodaté (acteur, rôle, action, données). Inviolable (List non modifiable à l'export). Exportable comme preuve légale — conforme au caractère pénal des cyberattaques hospitalières.

4.2 RobotTriage — Protocole de triage en 9 étapes

#	Étape	Détail technique
1	Détection patient	Simulation caméra panoramique — position aléatoire dans la salle d'attente
2	Authentification	Lecteur d'empreinte digitale biométrique → identification patientId
3	Scan vision IA	YOLO + HSV : saignement massif, amputation, inconscience, agitation
4	Tension artérielle	Brassard cylindrique embarqué → [systole, diastole] en mmHg
5	Température + SpO2	Thermomètre infrarouge frontal + oxymètre de pouls digital
6	Dossier MyHealth	Chargement antécédents (CategorieRisque) — désactivé en mode dégradé
7	Calcul ESI	Moteur de règles 3 étapes : critères immédiats, score de base, surclassement
8	Actions & kit	ESI_1 → déploiement complet du kit ; ESI_2-5 → orientation adaptée
9	Audit + Dashboard	Journal horodaté + transmission JSON au tableau de bord de la salle d'admission

Le mode dégradé est activable via `activerModeDegrade()` : le robot se déconnecte et travaille sur capteurs seuls, sans accès à MyHealth — réponse directe au risque de cyberattaque paralysant les SI hospitaliers.

5. Synthèse de la Couverture POO

Exigence du sujet	Localisation dans le code
Classe abstraite Robot	Robot.java — méthodes abstraites <code>deplacer / effectuerTache</code>
Héritage 3 niveaux	Robot → RobotConnecte → RobotTriage / RobotSecurite
Interface Connectable	RobotConnecte implements Connectable (3 méthodes)
Exceptions personnalisées (hiérarchie)	12 exceptions héritant de RobotException
Énumérations pour la criticité	NiveauESI, NiveauAlerte, Role, EtatSysteme, ElementKit...
Polymorphisme GestionnaireHospitalier	ArrayList<Robot>, sélection et <code>alerteGenerale()</code> polymorphes
Contrôle d'accès / sécurité	RBAC SHA-256 (RobotSecurite) + code médecin (RobotTriage)
Interface graphique Swing	Dashboard, centre de commande, console de logs temps réel
Actualité — enjeu réel	Mode dégradé anti-ransomware + audit trail légal

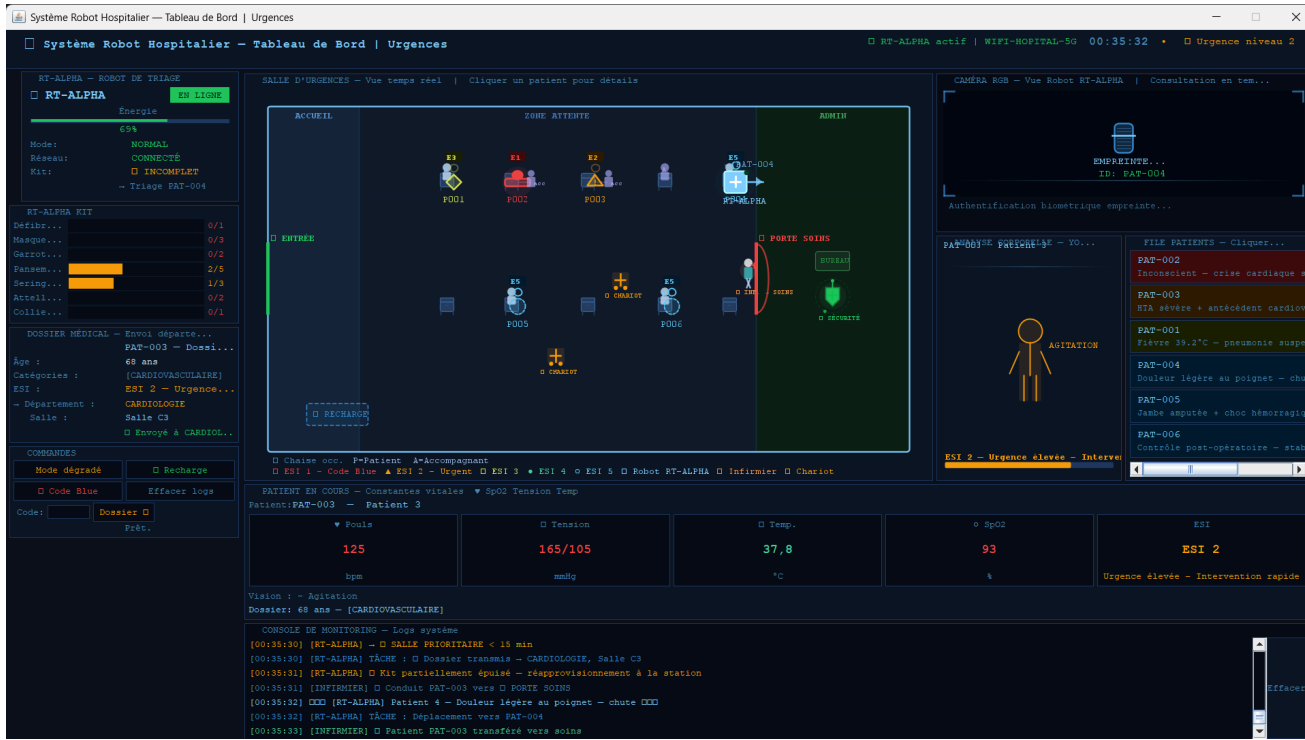
Conclusion

Le projet aboutit à la conception d'une flotte de robots hospitaliers capable de répondre simultanément aux enjeux de la cybersécurité et de l'automatisation médicale en milieu hospitalier. En s'appuyant sur une architecture Java rigoureuse, l'implémentation valide l'ensemble des exigences de la programmation orientée objet, notamment à travers une hiérarchie d'héritage à trois niveaux, l'utilisation du polymorphisme pour la gestion de flotte et la mise en place d'une structure complexe de douze exceptions personnalisées.

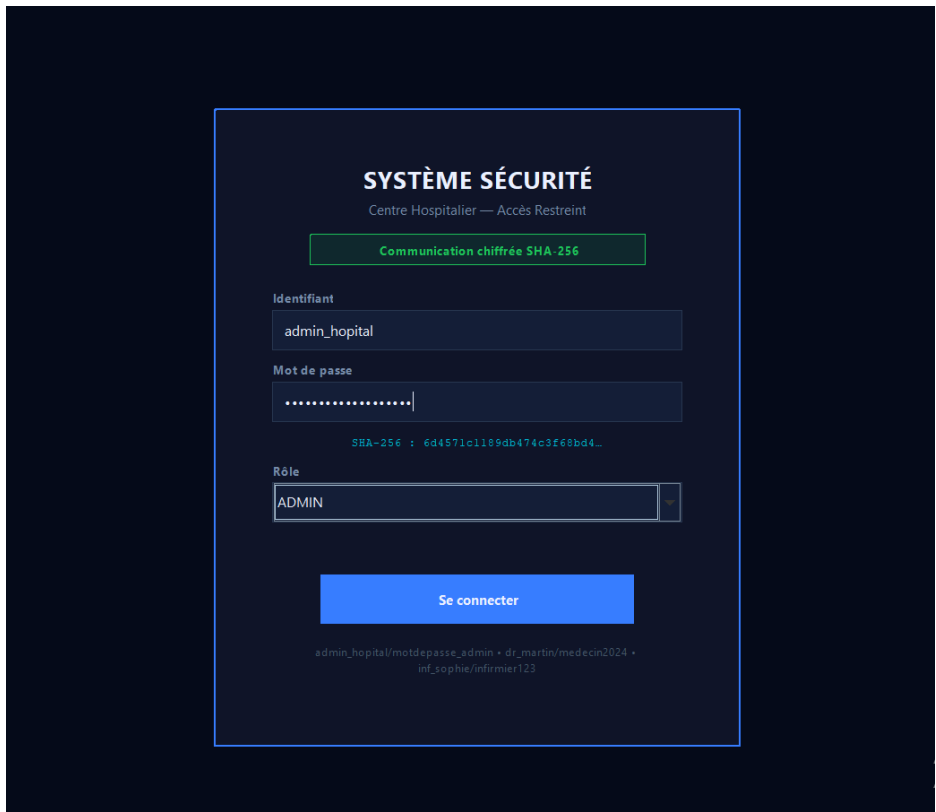
L'originalité du système réside dans son ancrage dans l'actualité sanitaire, illustré par le développement d'un "mode dégradé" anti-ransomware et d'un protocole de triage ESI intelligent, offrant ainsi une solution résiliente et opérationnelle face aux crises numériques et médicales contemporaines.

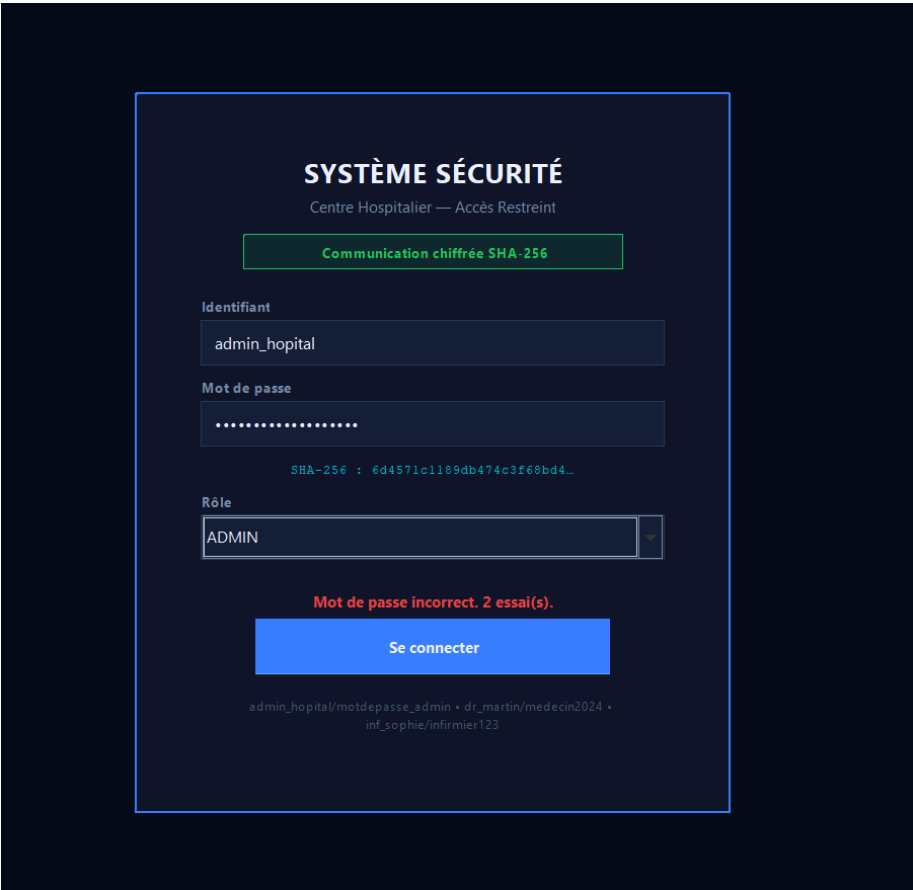
Captures d'écrans

1. Robot Triage



2. Robot Sécurité





CyberSec Hospitalier — Système de Sécurité

CyberSec Hospitalier

Surveillance & Sécurité

SHA-256Session : -Déconnexion

Carte & Robots

Centre Commande

Mode Degrade

Console / Logs

HoneyPot

Légende :

Opérationnel

En alerte

Critique/Isolé

Sécurité (fixe)

Double-clic sur un robot pour y accéder.

Cardiologie

CABD-01

Neurologie

NEUR-01

Oncologie

ONCO-01

Pédiatrie

PED-01

Radiologie

RAD-01

Chirurgie

CHIR-01

CHIR-02

Réanimation

REA-01

REA-02

Urgences

URG-01

Laboratoire

LABO-01

Pharmacie

PHAR-01

Administration

SEC-01

Maintenance

MAINT-01

Hygiène/Entretien

HYG-01

ID	Département	Étage	Énergie	État	Mission	Accès min.	Isolé
CHIR-02	Chirurgie	Étage 2	12%	Critique	BATTERIE CRITIQUE	MEDECIN	-
PED-01	Pédiatrie	Étage 1	80%	Normal	Ronde de soins	INFIRMIER	-
REA-01	Réanimation	Étage 2	98%	Normal	Surveillance continue	MEDECIN	-
REA-02	Réanimation	Étage 2	33%	Critique	ISOLÉ - comportement suspect	ADMIN	OUI
RAD-01	Radiologie	Étage 1	74%	Normal	Transport IRM	TECHNICIEN	-
LABO-01	Laboratoire	RDC	86%	Normal	Prises de sang - analyses	TECHNICIEN	-

Accéder (double-clic)

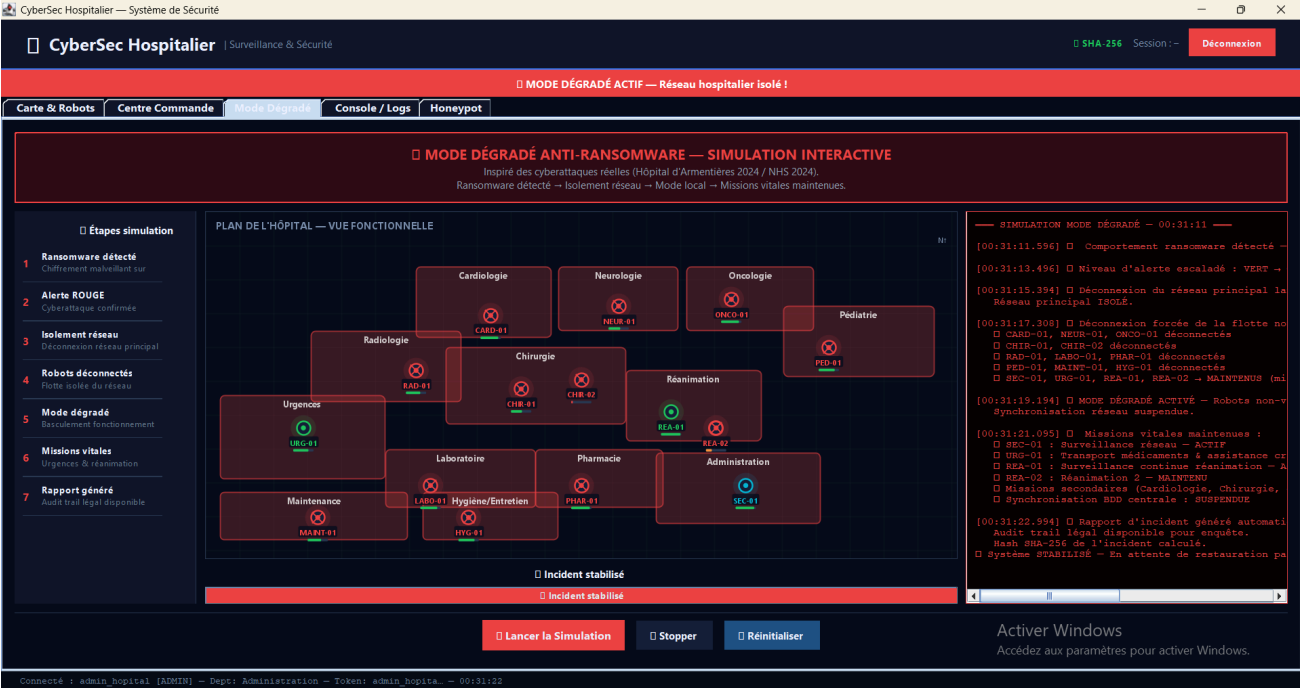
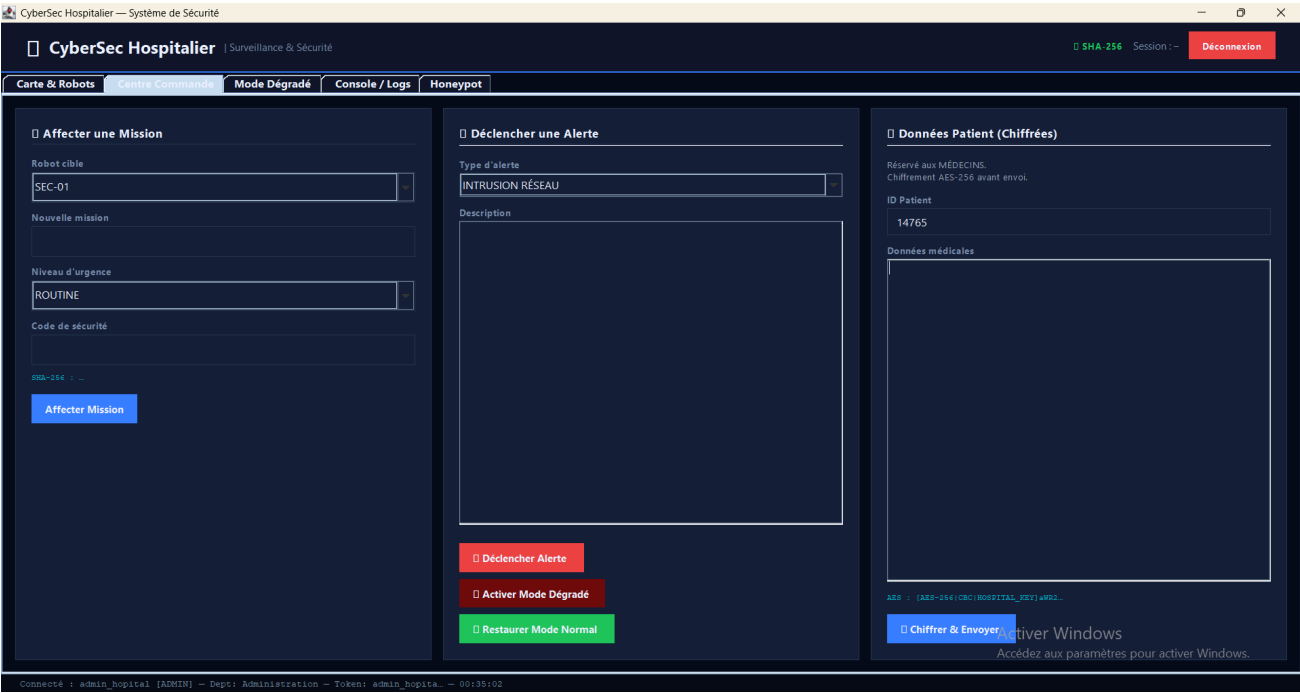
Isoler robot

Rétablir (Admin)

Activer Windows

Accédez aux paramètres pour activer Windows.

Connecté : admin_hopital (ADMIN) - Dept: Administration - Token: admin_hopital_ - 00:00:07



CyberSec Hospitalier — Système de Sécurité

CyberSec Hospitalier

Surveillance & Sécurité

SHA-256Session : Déconnexion

Carte & Robots

Centre Commande

Mode Dégradé

Console / Logs

HoneyPot

Légende :

- Opérationnel
- En alerte
- Critique/Isolé
- Sécurité (fixe)

Double-clic sur un robot pour y accéder.

Cardiologie

CARD-01

Neurologie

NEUR-01

Oncologie

ONCO-01

Pédiatrie

PED-01

Radiologie

RAD-01

Chirurgie

CHIR-01

Chirurgie

CHIR-02

Réanimation

REA-01

Réanimation

REA-02

Urgences

URG-01

Laboratoire

LABO-01

Pharmacie

PHAR-01

Administration

SEC-01

Maintenance

MANT-01

Hygiène/Extinction

HTG-01

ID	Département	Étage	Énergie	État	Mission	Accès min.	Isolé
CHIR-02	Chirurgie	Étage 2	12%	ARRÊTÉ (mode dégradé)	BATTERIE CRITIQUE	MEDECIN	-
PED-01	Pédiatrie	Étage 1	80%	ARRÊTÉ (mode dégradé)	Ronde de soins	INFIRMIER	-
REA-01	Réanimation	Étage 2	98%	VITAL — Maintenu	Surveillance continue	MEDECIN	-
REA-02	Réanimation	Étage 2	33%	VITAL — Maintenu	ISOLÉ — comportement suspect	ADMIN	OUI
RAD-01	Radiologie	Étage 1	74%	ARRÊTÉ (mode dégradé)	Transport IRM	TECHNICIEN	-
LABO-01	Laboratoire	RDC	86%	ARRÊTÉ (mode dégradé)	Prises de sang — analyses	TECHNICIEN	-

Accéder (double-clic)

Isoler robot

Rétablir (Admin)

Connecté : admin_hopital [ADMIN] — Dept: Administration — Token: admin_hopita. — 00:36:02

Activer Windows

Accédez aux paramètres pour activer Windows.

CyberSec Hospitalier — Système de Sécurité

CyberSec Hospitalier

Surveillance & Sécurité

SHA-256Session : Déconnexion

Carte & Robots

Centre Commande

Mode Dégradé

Console / Logs

HoneyPot

Console de Monitoring

Effacer

Télécharger Logs

Audit Trail (Admin)

[00:28:46.080] [SYSTEM] Démarrage cybersécurité hospitalière. SHA-256 actif.
[00:28:46.082] [HONEYPOT] Ressource piége 'DOSSIER_PATIENT_VIE_CONFIDENTIEL' armée.
[00:30:17.626] [SECURITE] Connexion : admin_hopital [ADMIN] — Dept: Administration
[00:31:11.094] [MODE_DEGRADE] Simulation lancée par admin_hopital
[00:31:41.111] [MODE_DEGRADE] Stoppe.
[00:31:41.111] [MODE_DEGRADE] Réinitialisé.
[00:32:26.797] [HONEYPOT] INTRUSION par ATTAQUANT_EXT

Enregistrer

Enregistrer dans : Disque local (C:)

bac2024

lin cherif

bac2025

matlab

bac2026

MathWorks_MATLAB_R2023a

bdd

MinGW

Dev-Cpp

msys64

inetpub

PerlLogs

Nom du fichier : audit_20260423_003304.txt

Type de fichier : Tous les fichiers

EnregistrerAnnuler

Connecté : admin_hopital [ADMIN] — Dept: Administration — Token: admin_hopita. — 00:33:22

Activer Windows

Accédez aux paramètres pour activer Windows.

[Carte & Robots](#)
[Centre Commande](#)
[Mode Dégradé](#)
[Console / Logs](#)

ATTENTION : INTRUSION HONEYPOT

PIÈGE DÉCLANCHÉ !

ATTACQUANT EXT
a tenté d'accéder à une ressource confidentielle inexistante.

Intrusion enregistrée dans l'audit trail légal.
Niveau d'alerte : **ROUGE**

Compris