LOUIS70 CONSEIL

Sécurité • Stratégie • Discrétion

ANALYSE DE RISQUES EBIOS RISK MANAGER

Étude de sécurité du système d'information

Objet d'étude :

EHPAD Les Tilleuls — Établissement fictif à des fins de démonstration

Commune de Beaumont-sur-Vingeanne (21), 48 résidents

Référence mission : L70C-2026-EHPAD-002
Méthode : EBIOS Risk Manager (ANSSI, 2018)
Date : avril 2026

Classification : CONFIDENTIEL — Diffusion restreinte

Sommaire

Cadrage de l'étude

Contexte et périmètre

L'EHPAD Les Tilleuls a sollicité LOUIS70 CONSEIL pour conduire une analyse de risques selon la méthode EBIOS Risk Manager publiée par l'ANSSI en 2018. Cette méthode, référence nationale en matière d'analyse de risques numériques, permet d'identifier les risques pesant sur un système d'information, d'évaluer leur vraisemblance et leur gravité, et de définir les mesures de traitement adaptées.

Le périmètre de l'étude couvre l'ensemble du système d'information de l'établissement : logiciel métier de gestion des soins (Osiris Care), postes de travail, infrastructure réseau, sauvegardes, et accès distants du prestataire informatique.

Comité de pilotage

Rôle	Fonction	Organisme
Responsable de l'étude	Consultant SSI	LOUIS70 CONSEIL
Commanditaire	Directrice	EHPAD Les Tilleuls
Référent métier soins	Infirmière coordinatrice	EHPAD Les Tilleuls
Référent SI	Responsable administrative	EHPAD Les Tilleuls
Expert technique	Prestataire informatique	Société externe (confidentiel)

Valeurs métiers retenues

Les valeurs métiers sont les éléments essentiels dont la compromission aurait un impact direct sur la mission de l'établissement. Elles ont été identifiées lors des entretiens de cadrage.

ID	Valeur métier	Description	Responsable	Criticité
VM1	**Continuité des soins**	Accès permanent au dossier résident, prescriptions, traçabilité des actes	Infirmière coord.	CRITIQUE
VM2	**Confidentialité des données de santé**	Protection des données médicales et personnelles des résidents (RGPD, secret médical)	Direction	CRITIQUE
VM3	**Intégrité des prescriptions**	Fiabilité des informations de prescription et de dosage médicamenteux	Médecin coord.	CRITIQUE
VM4	**Disponibilité administrative**	Accès aux données RH, comptabilité, communication externe	Resp. administrative	MODÉRÉ
VM5	**Réputation et conformité**	Image de l'établissement, relations avec l'ARS, conformité réglementaire	Direction	MODÉRÉ

Atelier 1 — Cadrage et socle de sécurité

1.1 Biens supports

Les biens supports sont les composants du système d'information qui supportent les valeurs métiers. Leur identification permet de délimiter précisément le périmètre technique de l'étude.

ID	Bien support	Type	Valeurs métiers	État
BS1	Logiciel Osiris Care	Application métier	VM1, VM2, VM3	Obsolète v2019
BS2	Serveur local (NAS + données)	Infrastructure	VM1, VM2, VM3	Sans sauvegarde externe
BS3	Postes de travail (10 postes)	Matériel	VM1, VM2, VM4	2 postes Win7 EOL
BS4	Réseau LAN / Wi-Fi	Réseau	VM1, VM2, VM3, VM4	Switch non managé
BS5	Accès Internet / VPN prestataire	Réseau	VM4, VM5	Sans MFA
BS6	Messagerie (Gmail partagé)	Application	VM4, VM5	Non chiffrée
BS7	Tablettes Android (2)	Matériel	VM1	Android 9 EOL
BS8	Téléphonie fixe	Matériel	VM4	Hors périmètre numérique

1.2 Socle de sécurité

Le socle de sécurité regroupe les mesures de sécurité déjà en place ou imposées par la réglementation. Il constitue la ligne de base sur laquelle s'appuie l'analyse.

Mesure	Référentiel	Statut	Niveau
Antivirus sur postes de travail	ANSSI hygiène #6	Partiel	FAIBLE
Sauvegarde locale nocturne (NAS)	ANSSI hygiène #28	En place	MODÉRÉ
Contrat de maintenance informatique	Bonne pratique	En place	MODÉRÉ
Registre des traitements RGPD	RGPD art. 30	Incomplet	FAIBLE
Politique de mots de passe	ANSSI hygiène #10	Absente	FAIBLE
Charte informatique utilisateurs	ANSSI hygiène #1	Absente	FAIBLE
Journalisation des accès	HDS, RGPD art. 32	Absente	FAIBLE
Segmentation réseau	ANSSI hygiène #19	Absente	FAIBLE
Authentification multifacteur	ANSSI hygiène #11	Absente	FAIBLE
Plan de reprise d'activité (PRA)	Bonne pratique secteur santé	Absent	FAIBLE

Constat : le socle de sécurité est très lacunaire. Sur 10 mesures élémentaires, 2 sont en place, 2 sont partielles, 6 sont absentes. L'établissement part d'un niveau de protection quasi nul, ce qui élève mécaniquement la vraisemblance de l'ensemble des scénarios de risque.

Atelier 2 — Sources de risque

2.1 Identification des sources de risque

Les sources de risque (SR) sont les entités susceptibles de porter atteinte aux valeurs métiers de l'établissement. EBIOS RM distingue les sources intentionnelles (attaquants) et non intentionnelles (erreurs, accidents).

ID	Source de risque	Description	Type	Pertinence
SR1	**Cybercriminel opportuniste**	Attaquant externe cherchant un gain financier rapide (ransomware, vol de données revendables). Cible prioritairement les structures faiblement protégées.	Intentionnelle	ÉLEVÉE
SR2	**Prestataire informatique**	Accès légitime mais non encadré au SI. Risque d'action malveillante ou d'erreur lors d'interventions distantes non tracées.	Intentionnelle / accidentelle	MODÉRÉE
SR3	**Personnel interne négligent**	Agent commettant des erreurs involontaires : clic sur phishing, mauvaise manipulation, perte de matériel contenant des données.	Non intentionnelle	ÉLEVÉE
SR4	**Ancien personnel**	Ex-employé conservant des accès actifs ou la connaissance de mots de passe. Risque accru si départ conflictuel.	Intentionnelle / accidentelle	MODÉRÉE
SR5	**Intervenant extérieur malveillant**	Bénévole, famille de résident, prestataire non informatique ayant un accès physique aux locaux et équipements.	Intentionnelle	FAIBLE
SR6	**Sinistre physique**	Incendie, inondation, panne électrique prolongée. Non intentionnel mais impact potentiellement total sur la disponibilité.	Non intentionnelle	MODÉRÉE
SR7	**Éditeur logiciel défaillant**	Cessation de maintenance d'Osiris Care v2019 : absence de correctifs de sécurité, vulnérabilités non comblées.	Non intentionnelle	ÉLEVÉE

2.2 Sources de risque retenues pour l'étude

Après évaluation de la pertinence au regard du contexte de l'établissement, les sources SR1, SR3 et SR7 sont retenues comme prioritaires pour la construction des scénarios. SR2 et SR4 sont retenues à titre secondaire. SR5 et SR6 sont conservées en surveillance.

Atelier 3 — Scénarios stratégiques

3.1 Présentation

Les scénarios stratégiques décrivent les chemins d'attaque de haut niveau par lesquels une source de risque peut atteindre les valeurs métiers. Ils sont construits à partir des couples Source de risque / Valeur métier les plus critiques, en identifiant les biens supports intermédiaires.

3.2 Cartographie des chemins d'attaque

ID	Source	Valeur cible	Chemin d'attaque	Vrais.	Gravité
SS1	**SR1 Cybercriminel**	VM1 Continuité soins	Phishing → poste compromis → propagation réseau → chiffrement NAS (ransomware)	3/4	4/4
SS2	**SR1 Cybercriminel**	VM2 Confidentialité	Exploitation vuln. Win7 → accès Osiris Care → exfiltration données résidents	3/4	4/4
SS3	**SR3 Personnel négligent**	VM3 Intégrité prescriptions	Phishing → compromission compte → modification involontaire données prescription	4/4	4/4
SS4	**SR2 Prestataire**	VM2 Confidentialité	Accès distant non tracé → consultation/copie données hors mission	2/4	3/4
SS5	**SR4 Ancien personnel**	VM1 Continuité soins	Compte orphelin actif → connexion non autorisée → suppression ou altération données	2/4	4/4
SS6	**SR7 Éditeur défaillant**	VM1, VM3	Vulnérabilité Osiris Care non corrigée → exploitation par attaquant externe	3/4	4/4
SS7	**SR6 Sinistre physique**	VM1 Continuité soins	Incendie local technique → destruction serveur + NAS → perte totale données	1/4	4/4

Échelle de vraisemblance et de gravité : 1 = Faible, 2 = Modéré, 3 = Élevé, 4 = Critique. Les scénarios SS1, SS2, SS3 et SS6 sont prioritaires (vraisemblance ≥ 3 et gravité = 4).

Atelier 4 — Scénarios opérationnels

4.1 Présentation

Les scénarios opérationnels déclinent les scénarios stratégiques en séquences techniques détaillées. Ils décrivent pas à pas comment un attaquant ou un événement accidentel peut compromettre les biens supports pour atteindre les valeurs métiers.

4.2 Scénario opérationnel SO1 — Attaque ransomware par phishing

Source de risque : SR1 (cybercriminel opportuniste) | Scénario stratégique : SS1

Étape	Action	Description technique	Bien support visé
1	Reconnaissance	L'attaquant identifie l'EHPAD via LinkedIn, site web, annuaires ARS. Collecte des adresses mail du personnel.	Sources ouvertes (OSINT)
2	Envoi phishing	Mail imitant l'ARS ou un fournisseur (facture, document urgent). Pièce jointe .docx malveillante ou lien vers faux portail.	BS6 Messagerie
3	Compromission poste	Un agent ouvre la pièce jointe. Macro VBA exécute un téléchargeur. Cheval de Troie installé sur BS3.	BS3 Poste de travail
4	Persistance	Le malware crée une tâche planifiée, désactive l'antivirus. Connexion à un C2 (Command & Control) distant.	BS3, BS4 Réseau
5	Mouvement latéral	Exploitation du réseau non segmenté. L'attaquant atteint le serveur et le NAS via les partages réseau.	BS4 LAN, BS2 NAS
6	Exfiltration (optionnel)	Copie des données Osiris Care vers serveur externe avant chiffrement (double extorsion).	BS1 Osiris Care, BS2
7	Chiffrement	Déclenchement du ransomware. Chiffrement du NAS, des postes, du logiciel métier. Demande de rançon.	BS1, BS2, BS3
8	Impact final	Arrêt total du SI. Impossibilité d'accéder aux dossiers résidents. Risque patient direct.	VM1, VM2, VM3

Facteurs aggravants spécifiques à l'EHPAD Les Tilleuls : absence de segmentation réseau (propagation instantanée), NAS sans sauvegarde externe (pas de restauration possible), aucun plan de reprise d'activité, personnel non sensibilisé au phishing.

4.3 Scénario opérationnel SO2 — Compromission par compte orphelin

Source de risque : SR4 (ancien personnel) | Scénario stratégique : SS5

Étape	Action	Description technique	Bien support visé
1	Identification	Ex-employé (aide-soignante partie en décembre 2025) conserve son identifiant et mot de passe Osiris Care.	BS1 Osiris Care
2	Connexion distante	Connexion via l'interface web Osiris Care accessible depuis l'extérieur sans MFA.	BS1, BS4 Réseau

3	Accès données	Consultation et copie de dossiers résidents (données de santé, informations personnelles).	VM2 Confidentialité
4	Altération possible	Modification de données de prescription ou de traçabilité des soins, sans alerte ni traçabilité.	VM3 Intégrité
5	Non détection	Absence de journalisation : l'incident n'est pas détecté. Aucun log ne permet la reconstruction.	VM2, VM3

4.4 Scénario opérationnel SO3 — Exploitation de vulnérabilité Windows 7

Source de risque : SR7 (éditeur défaillant) + SR1 (cybercriminel) | Scénario stratégique : SS6

Étape	Action	Description technique	Bien support visé
1	Détection de cible	Scan automatisé de plages IP identifie deux postes Windows 7 exposés (port RDP ouvert).	BS3 Postes Win7
2	Exploitation CVE	Exploitation d'une vulnérabilité RDP non corrigée (MS17-010 type EternalBlue ou équivalent post-2020).	BS3 Postes Win7
3	Élévation de privilèges	Obtention des droits administrateur local. Accès au compte Osiris Care ouvert en session.	BS1, BS3
4	Accès données soins	Lecture et exfiltration des données du logiciel métier directement depuis la session ouverte.	BS1, VM2
5	Persistance	Installation d'une backdoor. L'attaquant maintient un accès durable et discret au SI.	BS3, BS4

Atelier 5 — Traitement du risque

5.1 Stratégie de traitement

Pour chaque scénario de risque, quatre options de traitement sont possibles selon EBIOS RM : réduction (mise en place de mesures de sécurité), transfert (assurance cyber, externalisation), acceptation (risque jugé résiduel acceptable), ou refus (abandon de l'activité associée).

Au regard du contexte de l'EHPAD Les Tilleuls et de l'absence quasi totale de mesures existantes, la stratégie retenue est principalement la réduction pour tous les risques critiques et élevés, avec acceptation encadrée des risques résiduels modérés.

5.2 Plan de traitement des risques

Scénario	Vrais. init.	Gravité init.	Mesures de traitement	Vrais. cible	Gravité cible
SS1/SO1	3/4	4/4	Sensibilisation phishing + MFA + sauvegarde externalisée + segmentation réseau + EDR postes	1/4	2/4
SS2/SO3	3/4	4/4	Isolation immédiate postes Win7 + migration Windows 11 + gestion des correctifs	1/4	2/4
SS3	4/4	4/4	Formation personnel + procédure signalement + MFA + journalisation accès	2/4	3/4
SS4	2/4	3/4	MFA prestataire + traçabilité des interventions + contrat encadrant les accès	1/4	2/4
SS5/SO2	2/4	4/4	Purge comptes orphelins + procédure offboarding + MFA + journalisation	1/4	2/4
SS6/SO3	3/4	4/4	Migration Osiris Care + veille vulnérabilités + gestion des correctifs	1/4	2/4
SS7	1/4	4/4	Sauvegarde externalisée + PRA documenté + extincteur local technique	1/4	2/4

La mise en oeuvre des mesures de traitement permet de ramener l'ensemble des risques critiques à un niveau résiduel acceptable (vraisemblance ≤ 1/4 ou gravité ≤ 2/4). Le risque SS3 (personnel négligent / intégrité prescriptions) conserve une gravité résiduelle élevée en raison de sa nature intrinsèquement humaine -- seul un programme de sensibilisation continu peut agir sur ce vecteur.

Synthèse et feuille de route

Tableau de bord des risques résiduels

ID	Scénario	Vrais. init.	Grav. init.	Vrais. cible	Grav. cible
SS1	Ransomware par phishing	3/4	4/4	1/4	2/4
SS2	Exploitation Win7 / exfiltration	3/4	4/4	1/4	2/4
SS3	Négligence / intégrité prescriptions	4/4	4/4	2/4	3/4
SS4	Prestataire / accès non contrôlé	2/4	3/4	1/4	2/4
SS5	Compte orphelin / accès non autorisé	2/4	4/4	1/4	2/4
SS6	Vulnérabilité Osiris Care	3/4	4/4	1/4	2/4
SS7	Sinistre physique / perte données	1/4	4/4	1/4	2/4

Feuille de route — Mesures prioritaires

- IMMÉDIAT : Isolation postes Windows 7 — purge comptes orphelins — changement mots de passe constructeur
- M+1 : Mise en place MFA prestataire — activation journalisation Osiris Care — sauvegarde externalisée
- M+2 : Segmentation réseau VLAN — migration Windows 11 — exercice phishing personnel
- M+3 : Migration Osiris Care — charte informatique signée — procédure offboarding
- M+6 : PRA documenté et testé — sensibilisation annuelle — revue droits d'accès trimestrielle
- M+12 : Audit de suivi EBIOS RM — mise à jour du registre des risques

Conclusion

L'analyse EBIOS RM conduite sur l'EHPAD Les Tilleuls confirme et précise les résultats de l'audit organisationnel SSI mené en parallèle. Elle apporte une dimension supplémentaire en quantifiant la vraisemblance et la gravité des scénarios, et en permettant une comparaison avant/après traitement.

Le scénario ransomware (SS1/SO1) demeure le risque prioritaire absolu : vraisemblance initiale élevée (3/4), gravité maximale (4/4), chemin d'attaque entièrement documenté et réaliste au regard des capacités actuelles de l'établissement. Sa réduction à un niveau acceptable nécessite la mise en oeuvre simultanée de plusieurs mesures complémentaires.

La cohérence entre les deux études (audit SSI et EBIOS RM) renforce la fiabilité des recommandations. Les mesures proposées sont identiques dans leur essence, validées par deux approches méthodologiques distinctes.

Intervenir avec méthode. Décider avec lucidité. Agir avec discrétion.

Louis BONJEAN — LOUIS70 CONSEIL
contact@louis70conseil.fr | +33 6 89 17 57 62 | louis70conseil.fr
27 route de Souhières — 70270 Mélisey

Annexe A — Cartographie des chemins d'attaque

Lecture de la cartographie

Le tableau suivant représente la matrice SR × VM : pour chaque couple Source de risque / Valeur métier, il indique les biens supports intermédiaires mobilisés et le niveau de risque composite (vraisemblance × gravité). Cette lecture croisée permet d'identifier les biens supports les plus exposés et les valeurs métiers les plus menacées.

Source \ Valeur métier	VM1 Continuité soins	VM2 Confidentialité	VM3 Intégrité prescrip.	VM4 Disponibilité admin.	VM5 Réputation
SR1 Cybercriminel	BS3→BS4→BS1/BS2 **12/16**	BS3→BS1 **12/16**	BS3→BS1 **9/16**	BS3→BS4 **9/16**	—
SR2 Prestataire	BS5→BS1 **6/16**	BS5→BS1/BS2 **6/16**	BS5→BS1 **4/16**	BS5→BS6 **4/16**	—
SR3 Personnel négligent	BS3→BS4→BS1 **12/16**	BS3→BS1 **12/16**	BS3→BS1 **16/16**	BS3→BS6 **9/16**	—
SR4 Ancien personnel	BS1 direct **8/16**	BS1 direct **8/16**	BS1 direct **8/16**	—	—
SR6 Sinistre physique	BS2 destruction **4/16**	BS2 destruction **4/16**	BS2 destruction **4/16**	BS3 destruction **3/16**	—
SR7 Éditeur défaillant	BS1 vuln. **12/16**	BS1 vuln. **12/16**	BS1 vuln. **12/16**	—	—

Lecture : chaque cellule indique le chemin d'attaque (biens supports mobilisés) et le score de risque composite (vraisemblance × gravité sur 16). Score ≥ 9 = risque prioritaire. BS1 = Osiris Care, BS2 = NAS/serveur, BS3 = postes, BS4 = réseau, BS5 = accès distant, BS6 = messagerie.

Biens supports les plus exposés

Bien support	Désignation	Nb scénarios	Score max	Priorité
BS1	Logiciel métier Osiris Care	6/7	**16/16**	**CRITIQUE**
BS3	Postes de travail	5/7	**12/16**	**CRITIQUE**
BS4	Réseau LAN	4/7	**12/16**	**ÉLEVÉ**
BS2	Serveur / NAS	4/7	**12/16**	**ÉLEVÉ**
BS5	Accès distant prestataire	2/7	**6/16**	**MODÉRÉ**
BS6	Messagerie	2/7	**9/16**	**MODÉRÉ**

Annexe B — Registre des risques

Usage et mise à jour

Le registre des risques est un document vivant. Il constitue l'outil de suivi opérationnel de la démarche EBIOS RM. Il doit être mis à jour a minima annuellement, ou à chaque événement significatif (incident, changement d'organisation, évolution du SI, modification du périmètre).

Responsable de la mise à jour : référent SSI de l'établissement, avec validation de la direction. Version initiale établie par LOUIS70 CONSEIL — avril 2026.

ID	Scénario	V. init.	G. init.	Traitement	Mesure principale	V. cible / G. cible	Statut / Révision
SS1	Ransomware phishing	3/4	4/4	Réduction	MFA + sauvegarde ext. + EDR	1/4 / 2/4	À traiter — Avr. 2026
SS2	Exploitation Win7	3/4	4/4	Réduction	Isolation + migration Win11	1/4 / 2/4	À traiter — Avr. 2026
SS3	Négligence / prescriptions	4/4	4/4	Réduction	Formation + MFA + journalisation	2/4 / 3/4	À traiter — Avr. 2026
SS4	Prestataire non contrôlé	2/4	3/4	Réduction	MFA + traçabilité interventions	1/4 / 2/4	À traiter — Avr. 2026
SS5	Compte orphelin	2/4	4/4	Réduction	Purge comptes + offboarding	1/4 / 2/4	À traiter — Avr. 2026
SS6	Vuln. Osiris Care	3/4	4/4	Réduction	Migration logiciel métier	1/4 / 2/4	À traiter — Avr. 2026
SS7	Sinistre physique	1/4	4/4	Réduction	Sauvegarde ext. + PRA	1/4 / 2/4	À traiter — Avr. 2026

Ce registre est à compléter au fil de la mise en oeuvre : date de réalisation effective de chaque mesure, révision des niveaux de risque résiduels, ajout de nouveaux scénarios identifiés. La prochaine révision complète est prévue en avril 2027 ou après tout incident significatif.

Intervenir avec méthode. Décider avec lucidité. Agir avec discrétion.

Louis BONJEAN — LOUIS70 CONSEIL
contact@louis70conseil.fr | +33 6 89 17 57 62 | louis70conseil.fr
27 route de Souhières — 70270 Mélisey