Annexes

CABINET MEDICAL

BODSON Fabrice
COLLIGNON Thomas
THITEUX Lucas

MASI 2022 - 2023

Table des matières

1 Méthode EBIOS-RM 2018

1.1 Atelier 1 : Cadrage et socle de sécurité

1.1.1 Matrice RACI

Taches / Intervenants	Secrétaire	Docteur	Patient	Confrère	Plateforme externe
Gestion des rendez-vous	R	A, I	C		
Gestion des informations de contact des patients	R, A		C		
Gestion de l'agenda	R	A, I			
Dossier médical du patient		R	C, I	C	A

Figure 1 - Matrice RACI

1.1.2 Périmètre métier et technique

MISSION	Fournir une expertise médicale			
Business Value	Service de gestion de RDV	Informations de contact du patient	Suivi médical	Dossier médical
NATURE of BV	Processus	Information	Information	Information
Security need	High	High	Low	High
Support asset	Agenda Matériel informatique Secrétaire	Dossier du patient Matériel informatique Secrétaire	Dossier du patient Matériel informatique Médecin	Accès à la plateforme Matériel informatique Médecin
Accounting person / entity	Médecin	Secrétaire	Médecin	Plateforme en ligne

Figure 2 - Périmètre métier et technique

1.1.3 Évènements redoutés et gravité

Business Value	Feared Event	Consequences	Severity		Severity level	Consequences
Service de gestion de RDV	Agenda hors-service suite à une attaque	Impossibilité de travailler car il n'y a plus aucune organisation. Et impossibilité de gérer des RDV.	2		4 - Critique	Organization is unable to perform its missions, with potentially serious impact on security of persons and goods; it is unlikely that it will recover
	Perte des données suite à une attaque	Perte de toutes les informations concernant les RDV qui étaient encodés.	3		3 - Majeur	Strong degradation of performance, with potentially significant impact on security of persons and goods; recovery will be difficult
Informations de contact du patient	Perte des données suite à une attaque	Impossible de prendre contact avec le client	2		2 - Significatif	Degradation of performance, without impact on security of persons and goods; recovery will take place with light difficulties
	Vol ou manipulation des données	Integrité et confidentialité des données	4		1 - Mineur	No impact on the activity; recovery will take place without serious difficult
Suivi médical	Perte des données suite à une attaque	L'indisponibilité des données pour assurer le suivi d'un patient	2			
Dossier médical	Connexion à internet interrompue	Impossibilité de se connecter à la plateforme en ligne pour obtenir le dossier médical	4			
	Identifiants du médecin compromis	Confidentialité des dossiers médicaux en usurpant l'identité du médecin	3			
	Vol pour revente des données		3			

Figure 3 - Évènements redoutés et gravité

1.2 Atelier 2 : Sources de risques

1.2.1 Sources de risque et objectif visé

Risk Origin	Target Objective	MOTIVATION	RESSOURCES	Activity	Relevance
Vengeur	Interrompre les activités du cabinet, détruire des assets. Dénigrer le cabinet auprès des patients pour qu'ils n'aillent plus là bas	Fortement	Significatives	++++	Plutôt
Amateur	Tester ses compétences par défi, essayer d'obtenir un gain financier par la même occasion	Peu	Limitées	+	Peu
Crime organisé	Revente d'informations afin de les revendre	Assez	Importantes	++	Moyennement
Hacktiviste	Interrompre les activités du cabinet, détruire des assets. Dénigrer le cabinet auprès des patients pour qu'ils n'aillent plus	Assez	Significatives	++	Moyennement
Concurrent	Voler des informations de contact dans le but de voler des patients	Assez	Significatives	++++	Plutôt

Motivation	Ressources	Activités	Relevance
Fortement	Illimitées	++++	Très
Assez	Importantes	+++	Plutôt
Peu	Significatives	++	Moyennement
Très peu	Limitées	+	Peu

Figure 4 - SR et OV

1.2.2 Lien entre évènement redouté et les sources de risque

	SOURCE DE RISQUE	OBJECTIF VISE	PERTINENCE
1	Vengeur	Interrompre les activités du cabinet, détruire des assets. Dénigrer le cabinet auprès des patients pour qu'ils n'aillent plus là bas	Plutôt
2	Amateur	Tester ses compétences par défi, essayer d'obtenir un gain financier par la même occasion	Peu
3	Crime organisé	Revente d'informations afin de les revendre	Moyennement
4	Hacktiviste	Interrompre les activités du cabinet, détruire des assets. Dénigrer le cabinet auprès des patients pour qu'ils n'aillent plus là bas	Moyennement
5	Concurrent	Voler des informations dans le but de voler des patients	Plutôt

VALEUR METIER	EVENEMENT REDOUTE	GRAVITE	SR
Service de gestion de RDV	Agenda hors-service suite à une attaque	2	1, 4
Service de gestion de RDV	Perte des données suite à une attaque	3	1, 4
Informations de contact du patient	Perte des données suite à une attaque	2	1, 4
Informations de contact du patient	Vol ou manipulation des données	4	2, 3, 5
Suivi médical	Perte des données suite à une attaque	2	1, 4
Dossier médical	Connexion à internet interrompue	4	1, 4
Dossier médical	Identifiants du médecin compromis	3	2, 3, 5
Dossier médical	Vol pour revente des données	3	2, 3

Figure 5 - Lien ER et SR

1.3 Atelier 3 : Scénarios stratégiques

1.3.1 Niveau de menace

Category	Stakeholder	Dependance	Penetration	Maturity	Trust	Threat Level
Interne	Secretaire	2	4	1	2	4
	Médecin	4	3	2	2	3
Externe	Patient	3	1	1	1	3
	Confrère	2	1	1	1	2
	Plateforme	4	3	4	3	1

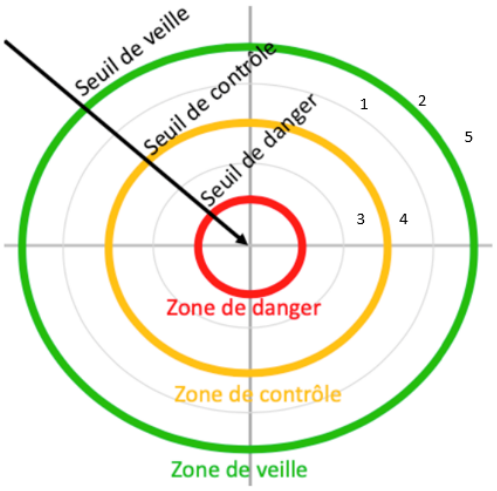
Figure 6 - Niveau de menace

1	Secrétaire
2	Médecin
3	Patient
4	Confrère
5	Plateforme

Figure 7a - Cible menace

Partie prenante	Chemins d'attaque	Mesures de sécurité	Menace initiale	Menace résiduelle
Secrétaire	Vengeur qui arrête de la prise de rdv par compromission (via une clé USB piégée, phishing) du pc de la secrétaire	Blocage des ports USB. Formation du personnel aux risques cyber.	4	1
Secrétaire	Le crime organisé et/ou concurrent offrent un pot de vin ou menacent pour accéder aux infos de contact des patients	Avantages extra-légaux. Clause contractuelle de non-divulgation.	4	1
Secrétaire	Pièce jointe piégée par l'envoi de mail frauduleux ou clé USB piégée pour atteindre les données de contact des clients.	Blocage des ports USB. Formation du personnel aux risques cyber.	4	1
Plateforme en ligne	Arrêt de l'activité générale dû à une coupure d'internet volontaire	Avoir une seconde ligne internet (redondance des câbles, boitier 4G).	1	0.75
Médecin	Pièce jointe piégée par l'envoi de mail frauduleux ou clé USB piégée pour obtenir les identifiants du médecin	Installation d'une solution de sécurité (AV). Formation du personnel aux risques cyber.	3	0.89
Médecin	Utilisation des identifiants du médecin ou d'une session ouverte pour voler des données des dossiers médicaux	Forcer le médecin à changer de mdp régulièrement. Double authentification. Monitoring des accès.	3	0.89

Figure 8b – Mesures de sécurité et menace résiduelle



1	Secrétaire
2	Médecin
3	Patient
4	Confrère
5	Plateforme

Figure 9c – nouvelle Cible menace

1.3.2 Scénarios stratégiques

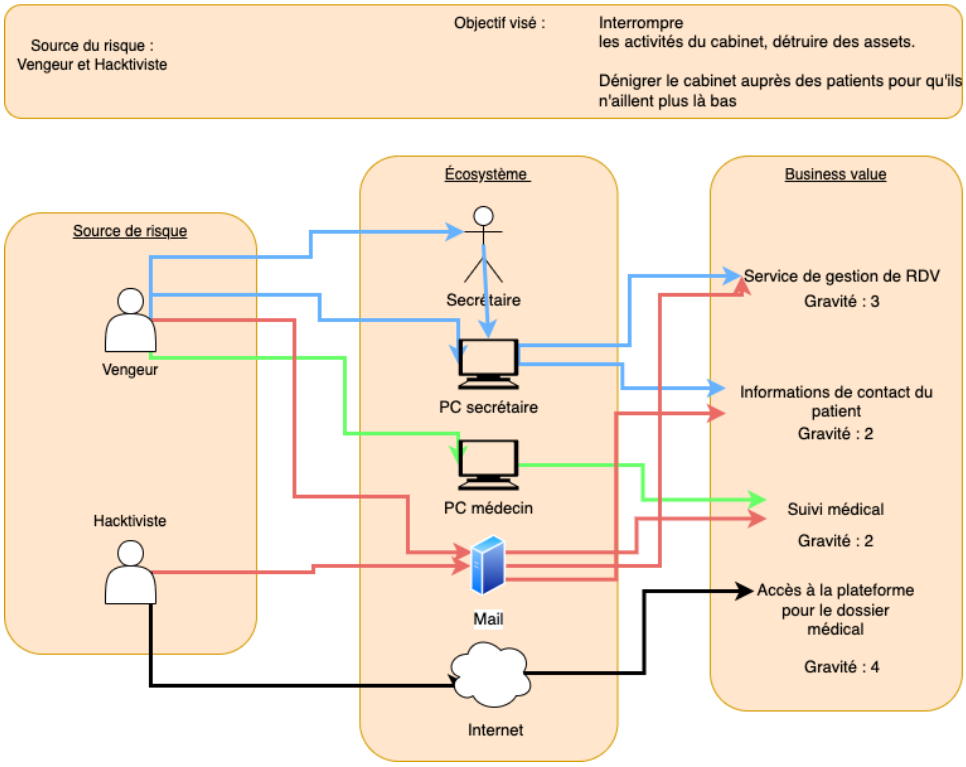


Figure 10 - Scénario stratégique 1

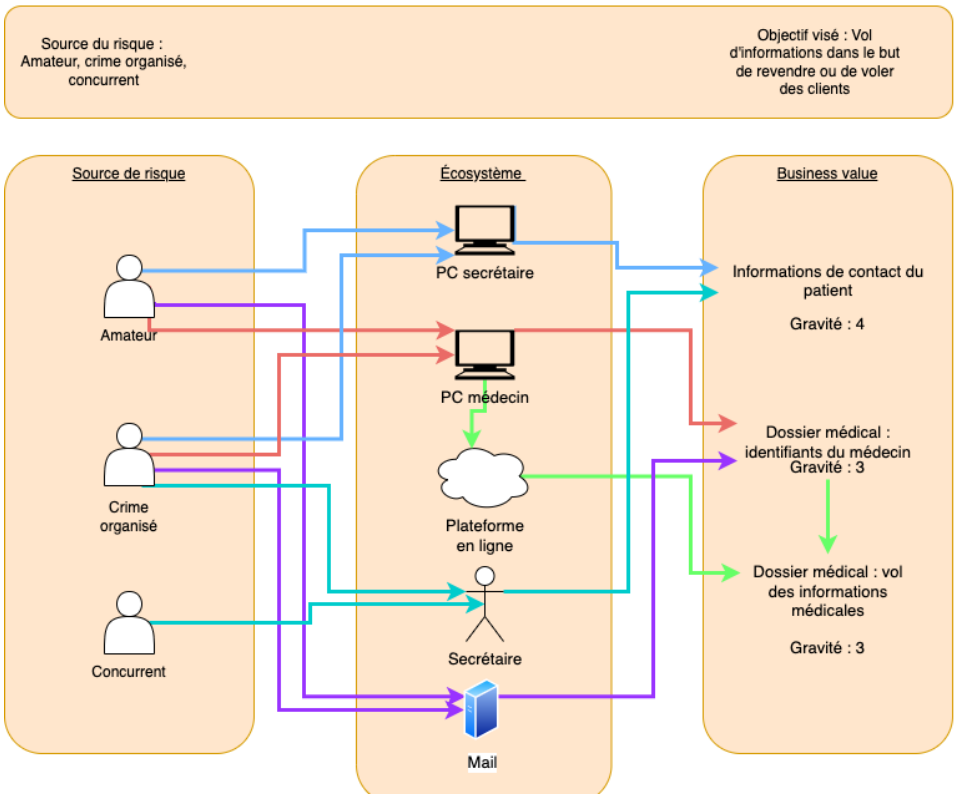


Figure 11 - Scénario stratégique 2

Category	Stakeholder	Dependance	Penetration	Maturity	Trust	Residual threat Level
Interne	Secretaire	2	3	2	3	1
	Médecin	4	2	3	3	0,888888889
Externe	Patient	3	1	1	1	3
	Confrère	2	1	1	1	2
	Plateforme	3	3	4	3	0,75

Figure 12 - Niveau de menace résiduel

1.4 Atelier 4 : Scénarios opérationnels

1.4.1 Scénarios organisationnels

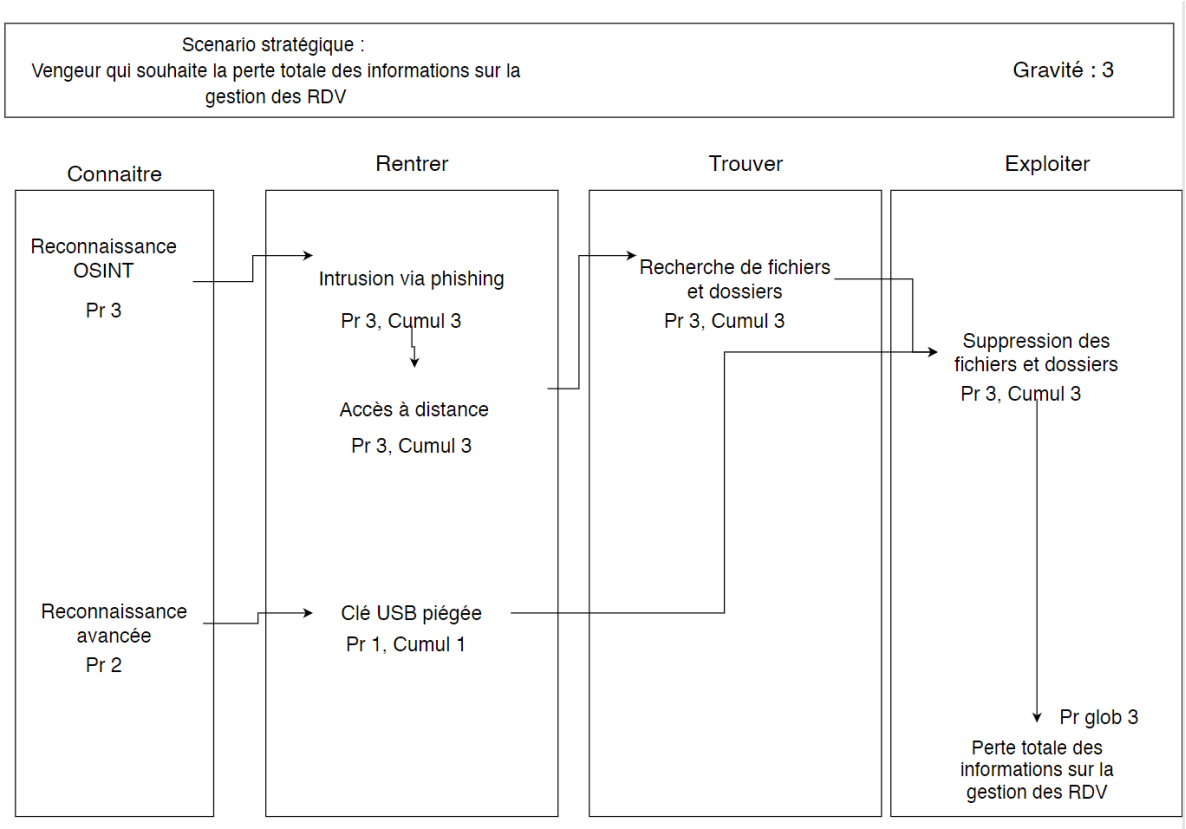


Figure 13 - Scenario du vengeur

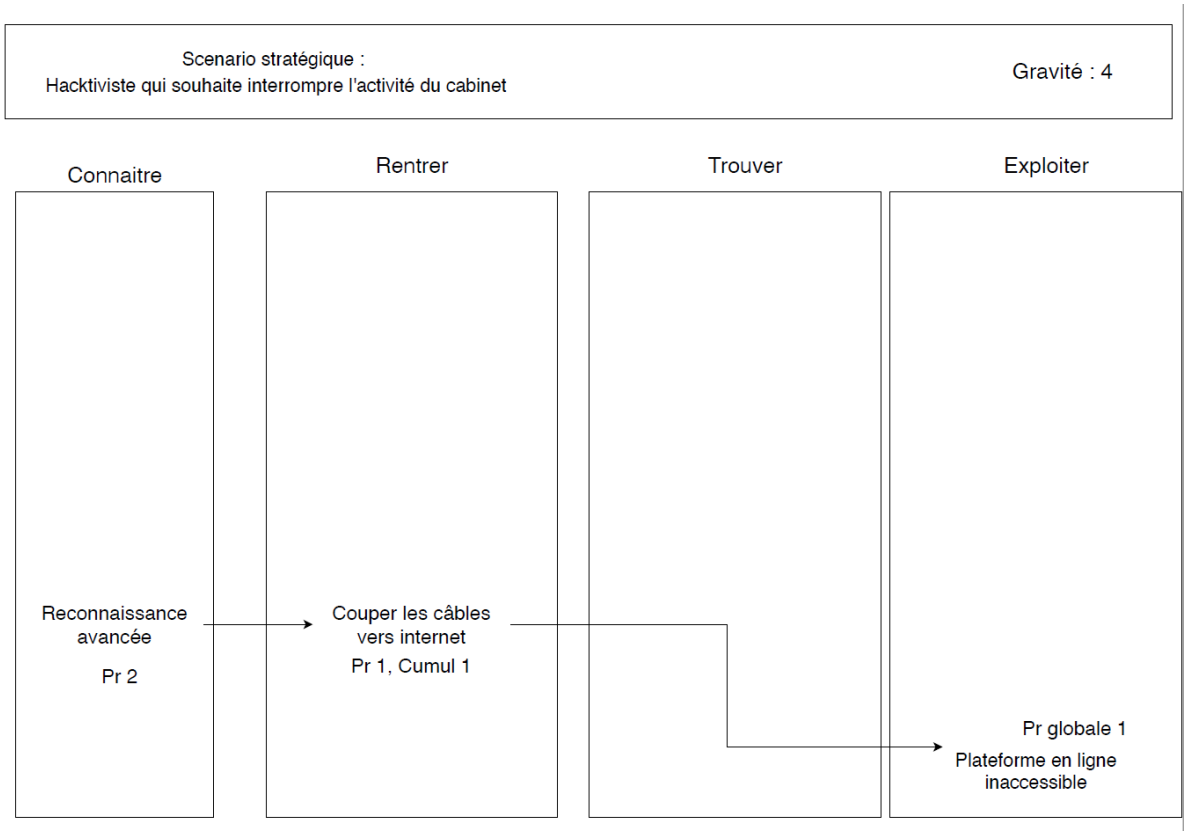


Figure 14 - Scenario du hacktiviste

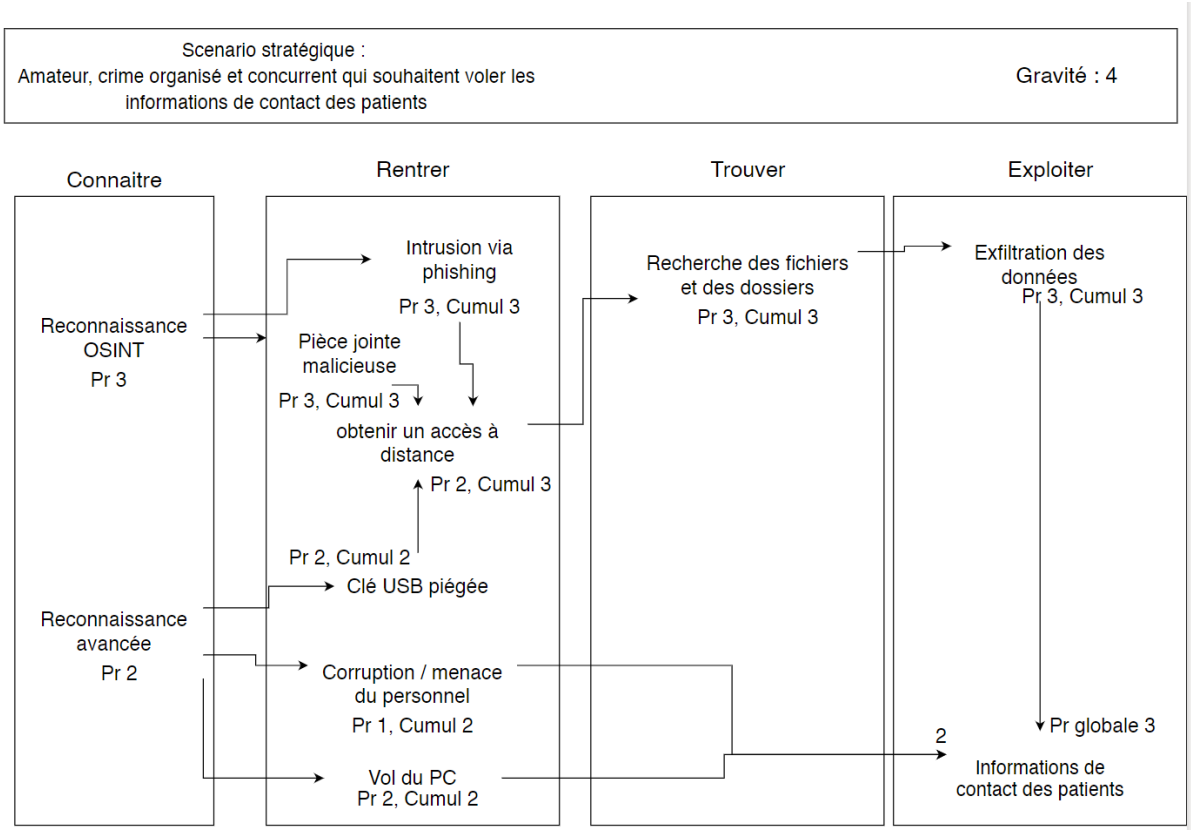


Figure 15 - Scenario du vol des informations de contact des patients

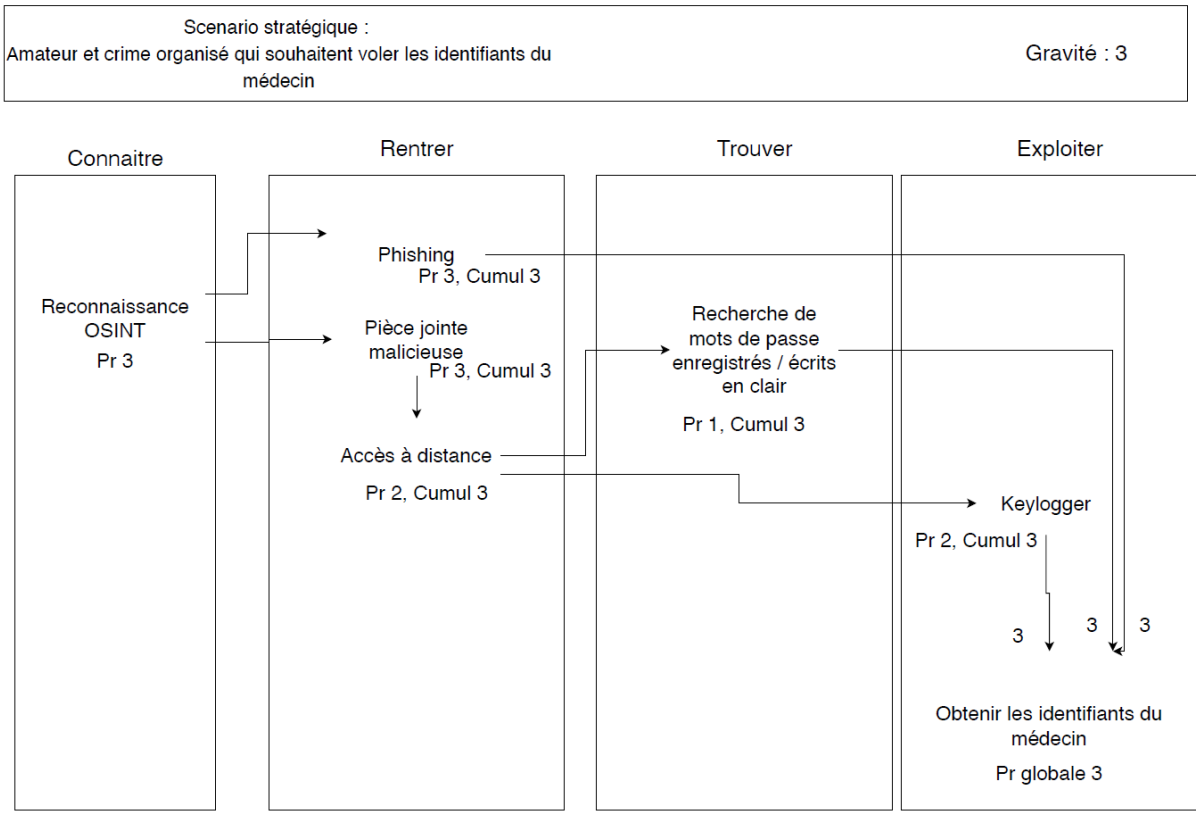


Figure 16 - Scenario du vol des identifiants du médecin

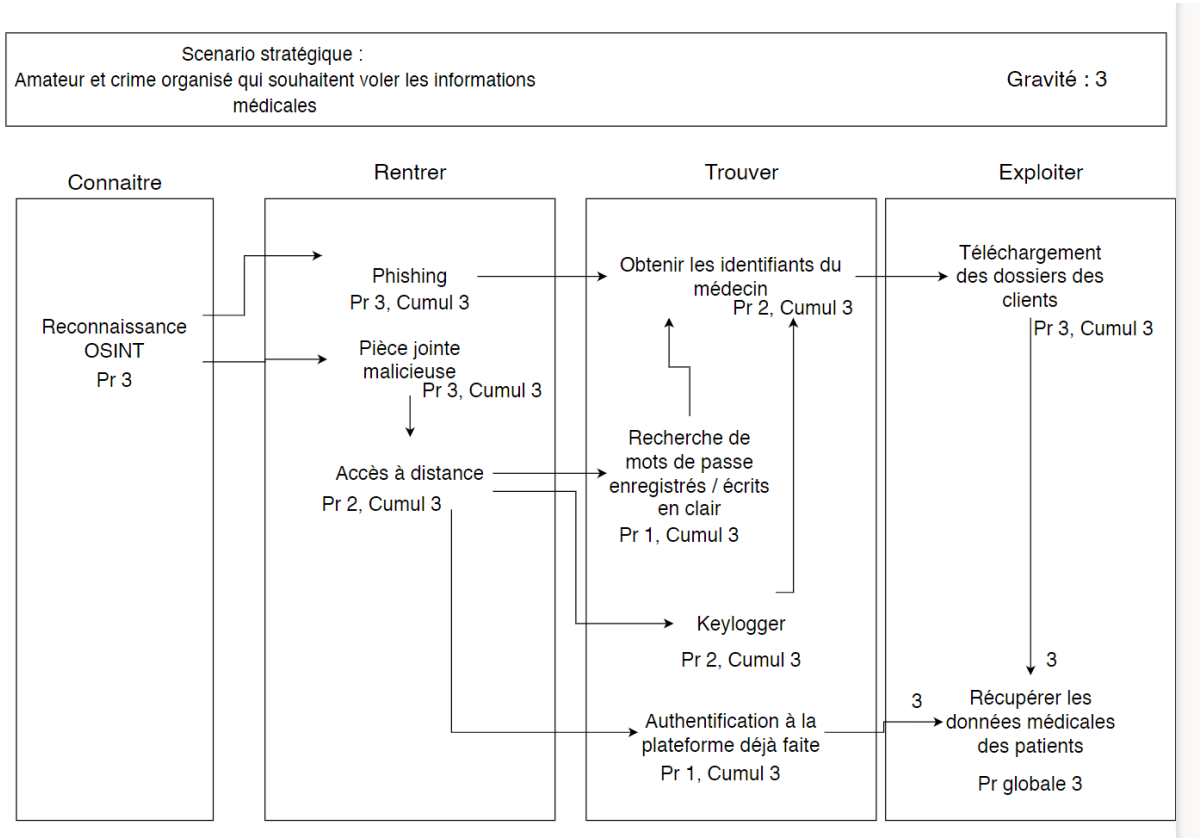


Figure 17 - Scenario vol des données médicales

1.5 Atelier 5 : Traitement du risque

R1	Vengeur qui souhaite la perte totale des informations sur la gestion des RDV	
	Gravité : 3	Pr : 3
R2	Hacktiviste qui souhaite interrompre l'activité du cabinet	
	Gravité : 4	Pr : 1
R3	Amateur, crime organisé et concurrent qui souhaitent voler les informations de contact des patients	
	Gravité : 4	Pr : 3
R4	Amateur et crime organisé qui souhaitent voler les identifiants du médecin	
	Gravité : 3	Pr : 3
R5	Amateur et crime organisé qui souhaitent voler les informations médicales	
	Gravité : 3	Pr : 3

Figure 18 risques retenus

Risk level	Risk acceptability	Strategies
Level 1	Acceptable	Maintain (or accept)
Level 2	Tolerable	Reject
Level 3	Unacceptable	Reduce (or modify)
		Transfer (or share)

Figure 19 échelle d'acceptabilité et stratégie de gestion de risque

Severity				
4	R2		R3	
3			R1, R4, R5	
2				
1				
Likelihood	1	2	3	4

Figure 20 matrice probabilité / gravité de nos risques

R1	Vengeur qui souhaite la perte totale des informations sur la gestion des RDV	Strategy : Reduce
	Gravité : 3 Pr : 3	
R2	Hacktiviste qui souhaite interrompre l'activité du cabinet	Strategy : Reduce
	Gravité : 4 Pr : 1	
R3	Amateur, crime organisé et concurrent qui souhaitent voler les informations de contact des patients	Strategy : Reject
	Gravité : 4 Pr : 3	
R4	Amateur et crime organisé qui souhaitent voler les identifiants du médecin	Strategy : Reject
	Gravité : 3 Pr : 3	
R5	Amateur et crime organisé qui souhaitent voler les informations médicales	Strategy : Reject
	Gravité : 3 Pr : 3	

Figure 21 stratégies de traitement de nos risques

Control	Affected risk scenarios	Responsible entity	Implementation difficulties	Cost/complexity
Governance				
Blocage des ports USB	R1	Prestataire IT	Matériel compatible	Peu
Forcer le changement de MDP régulièrement	R4, R5	Prestataire IT		Moyen
Proposer des avantages extra-légaux	R3	Secrétariat social	S'accorder sur les avantages	Moyen
Double authentification	R4, R5	Prestataire IT		Peu
Clause de non divulgation dans les contrats	R3	Secrétariat social		Peu
Prevention				
Mettre d'autres PC à disposition	R1, R2	Prestataire IT		Peu
Cryptage des données	R1, R3	Prestataire IT	Sélectionner le produit de chiffrement	Moyen
Formation du personnel	R1, R2	Prestataire IT		Moyen
Effectuer des simulations pour voir la réaction de la secrétaire face à un pot de vin	R3	Prestataire IT	Coût d'un consultant	Beaucoup
Detection				
IPS/AV/FW	R3	Prestataire IT		Beaucoup
Monitorer les accès	R4, R5	Prestataire IT		Beaucoup
Recovery				
Backup	R1, R2	Prestataire IT	Coût du processus	Beaucoup
Redondance de la ligne internet	R2	Prestataire IT		Moyen

Figure 22 Mesures de traitement de nos risques

R1	Vengeur qui souhaite la perte totale des informations sur la gestion des RDV	
	Gravité : 1	Pr : 1
R2	Hacktiviste qui souhaite interrompre l'activité du cabinet	
	Gravité : 1	Pr : 1
R3	Amateur, crime organisé et concurrent qui souhaitent voler les informations de contact des patients	
	Gravité : 2	Pr : 3
R4	Amateur et crime organisé qui souhaitent voler les identifiants du médecin	
	Gravité : 3	Pr : 1
R5	Amateur et crime organisé qui souhaitent voler les informations médicales	
	Gravité : 3	Pr : 1

Figure 23 nouvelles gravité et probabilité de nos risques

Severity				
4				
3	R4, R5			
2			R3	
1	R1, R2			
Likelihood	1	2	3	4

Figure 24 nouvelle matrice