DÉPARTEMENT CYBERDÉFENSE
Année universitaire 2019 – 2020
Rue André Lwoff, 56000 Vannes

Laurent GRAFF
Gabriel CHAMPIAT
Mike DA SILVA
Vincent NIEUTIN
Kévin MOREAU
Arthur GUYADER

Sécurité des architectures

Analyse de risque
EBIOS 2016

Référents ENSIBS : Julien Breyault, Yoann Prioux

Introduction

Ce rapport traite du projet d'Architecture sécurisée. Ce projet se découpe en 3 parties : Analyse de risque, Architecture technique de sécurité et enfin Analyse juridique de sécurité. Ce document est le dossier pour présenter notre partie analyse de risque autour de la méthode EBIOS Risk Manager.

Le contexte de notre analyse est le suivant :

- Une entreprise commerciale d'une douzaine de salariés qui vend et loue des biens nautiques dans son agence de Vannes où se trouve le stock. Elle est équipée en ordinateurs de type bureautique, lien internet ADSL par Box, mail et partage de fichiers local.
- Le dirigeant veut augmenter et diversifier sa clientèle au niveau européen en ouvrant un site de e-commerce pour prospecter de nouveaux clients, communiquer sur ses produits et ses offres, vendre et louer ses biens et services en ligne, suivre ses commandes et livraisons et suivre ses clients en ligne.
- Il veut une solution globale sécurisée et externalisée au plus bas coût de possession.
- Dans ces perspectives, les solutions cloud seront évaluées.
- Le dirigeant veut pouvoir suivre depuis son entreprise l'ensemble des opérations commerciales.
- Il ne connaît pas les pratiques en la matière de solution numérique sécurisée et craint la cyber-fraude compte tenu des affaires qu'il traite. Il a donc besoin d'être rassuré.
- Il décide de confier la maîtrise d'œuvre de ce projet à un cabinet spécialisé (vous) dans le cadre d'un appel d'offre.

L'analyse de risque se base sur la méthode EBIOS (2016) Risk Manager. Ce document rédigé par l'ANSSI a pour but la définition suivante :

"*Aider les organisations pour identifier et comprendre les risques numériques qui leur sont propres. Elle permet de déterminer les mesures de sécurité adaptées à la menace et de mettre en place de suivi et d'amélioration continue à l'issue d'une analyse de risque partagée au plus haut niveau."**

*https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/

Atelier 1 - Cadrage et socle de sécurité

Cet atelier a pour objectif de poser un cadre. Nous allons y définir les valeurs métiers, acteurs et impacts redoutés pour pouvoir cadrer cette étude.

MISSION	Vente et Location de biens nautiques					
Dénomination de la valeur métier	Location	Vente	Gestion site e-commerce	Communication	Livraison	Données relatives aux paiements
Nature de la valeur métier *(processus ou information)*	Processus	Processus	Processus	Information	Information	Information
Description	Activité consistant à : * Génération de devis * Ajouter/modifier/supprimer un bien * Suivre la/les commande(s) (bateaux) * Réalisation de transactions financières	Activité consistant à : * Génération de devis * Ajouter/modifier/supprimer un bien * Suivre la/les commande(s) (bateaux) * Réalisation de transactions financières	Activité de vente permettant de : * Authentification des utilisateurs (Interne / Externe) * Réalisation de transactions financières * Maintien du site e-commerce * Suivre la/les commande(s) (pièces)	Activité consistant à : * Communiquer sur des produits et des offres	Activité consistant à : * Suivre la commande (notifier le statut de la livraison)	Liste les informations relatives aux données de paiement : * Historique des transactions ayant eu lieu sur notre plateforme * Informations quant aux moyens de paiement proposé (paypal, CB, Chèque, Etc.) * Informations sur le client

Entité ou personne responsable *(INTERNE/EXTERNE)*	Commercial (INTERNE)	Commercial (INTERNE)	Prestataire (EXTERNE)		Responsable communication (INTERNE)	Prestataire (EXTERNE)	Service comptabilité + Prestataire (Externe)	
Dénomination du/des biens supports associés	Système bureautique	Système bureautique	Serveurs d'e-commerce	Système bureautique	Système bureautique	Serveur de Tracking	Système bureautique (Poste de comptabilité)	Serveur e-commerce
Description	Ordinateur portable avec windows 10. Le poste possède un accès privilégié au site pour permettre certaines actions, il possède aussi un outil de génération de devis	Ordinateur portable avec windows 10. Le poste possède un accès privilégié au site pour permettre certaines actions, il possède aussi un outil de génération de devis	Serveur d'e-commerce Debian 10 permettant de stocker le site d'e-commerce fait avec symfony ainsi que toutes les données avec une MongoDB (stockage d'objet JSON XML plus efficace)	Poste Windows 10, outil github pour la capitalisation ainsi qu'un IDE (VScode) pour développer et interagir avec le site web	Poste utilisateur Windows 10 avec un accès privilégié au site permettant l'affichage d'annonce de communication, il possède aussi un logiciel d'édition graphique tel que photoshop par exemple	Serveurs de tracking permettant de stocker les données de suivis des livraisons	Poste de comptabilité windows 10 avec une suite office	Serveur d'e-commerce Debian 10 permettant de stocker le site d'e-commerce fait avec symfony ainsi que toutes les données avec une MariaDB
Entité ou personne responsable	Prestataire (EXTERNE)	Prestataire (EXTERNE)	Prestataire (EXTERNE)	Prestataire (EXTERNE)	Prestataire (EXTERNE)	Prestataire (EXTERNE)	Service comptabilité (Interne)	Prestataire (Externe)

Les acteurs et biens supports associés sont définis, nous savons donc qui fait quoi et avec quoi. Nous allons donc pouvoir cadrer les différents impacts possibles au vus des différents éléments issus de ce tableau.

L’échelle de gravité utilisée pour évaluer les impacts est la suivante :

ECHELLE	CONSÉQUENCES
G4 CRITIQUE	Incapacité pour la société d’assurer tout ou partie de son activité, avec d’éventuels impacts graves sur la sécurité des personnes et des biens. La société ne surmontera vraisemblablement pas la situation (sa survie est menacée).
G3 GRAVE	Forte dégradation des performances de l’activité, avec d’éventuels impacts significatifs sur la sécurité des personnes et des biens. La société surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé).
G2 SIGNIFICATIVE	Dégradation des performances de l’activité sans impact sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé).
G1 MINEURE	Aucun impact opérationnel ni sur les performances de l’activité ni sur la sécurité des personnes et des biens. La société surmontera la situation sans trop de difficultés (consommation des marges).

Maintenant que l'échelle de gravité est définie nous avons tous les éléments pour définir et évaluer nos évènements redoutés pour chacune des valeurs métiers définies.

VALEUR MÉTIER	EVÉNEMENT REDOUTÉ	IMPACTS	GRAVITÉ
Location	Altération de la génération de devis	* Impacts financiers * Impacts juridiques (faux devis)	2
Vente	Altération de la génération de devis	* Impacts financiers * Impacts juridiques (faux devis)	4
Gestion e-commerce	Fuite des informations clients	* Impacts sur l'image et la confiance * Impacts financiers * Impacts juridiques	3
	Interruption de la disponibilité du site pendant plus de douze heures	* Impacts sur l'image et la confiance * Impacts financiers * Impacts sur les missions et services de l'organisme	3
	Altération des transactions financières	* Impacts financiers * Impacts juridiques	4
Communication	Altération ou destruction de la communication	* Impacts sur l'image et la confiance	2
Livraison	Altération ou destruction des données	* Impacts sur l'image et la confiance * Impact financiers (faible)	1

Atelier 2 - Source de risque

Dans l'atelier 2 nous allons identifier les SR et leurs OV, en lien avec le contexte particulier de l'étude. Pour identifier les SR et les évaluer nous nous sommes basés sur l'échelle suivantes :

			Ressources			
			Incluant les ressources financières, le niveau de compétences cyber, l'outillage, le temps dont l'attaquant dispose pour réaliser l'attaque, etc.			
			Ressources limitées	Ressources significatives	Ressources importantes	Ressources illimitées
Motivation	Intérêts, éléments qui poussent la source de risque à atteindre son objectif	Fortement motivé	Moyennement pertinent	Plutôt pertinent	Très pertinent	Très pertinent
		Assez motivé	Moyennement pertinent	Plutôt pertinent	Plutôt pertinent	Très pertinent
		Peu motivé	Peu pertinent	Moyennement pertinent	Plutôt pertinent	Plutôt pertinent
		Très peu motivé	Peu pertinent	Peu pertinent	Moyennement pertinent	Moyennement pertinent

Comme vous pouvez le voir dans le tableau ci-dessus, nos échelles pour le classement sont la motivation et les ressources des SR. En fonction des valeurs attribuées nous aurons alors une pertinence associée. Plus la pertinence est élevée plus nous considérons la SR comme dangereuse.

Ci-dessous, veuillez trouver le résultat de notre analyse.

Liste des sources de risque

Sources de risque	Objectifs visés	Motivation	Ressources	Pertinence
Hacktiviste écologique	Passer un message sur l'impact environnemental (faune et flore) de l'utilisation de bateaux à moteur	Fortement motivé	Ressources limitées	Moyennement pertinent
Concurrent	Voler nos informations clients	Fortement motivé	Ressources significatives	Plutôt pertinent
Client	Obtenir des marchandises à prix réduits	Peu motivé	Ressources limitées	Peu pertinent
Script-kiddies	Rendre indisponible le site web	Assez motivé	Ressources significatives	Plutôt pertinent
Concurrent	Nuire à l'image (mauvais commentaires, indisponibilité)	Fortement motivé	Ressources importantes	Très pertinent

Atelier 3 - Scénarios stratégiques

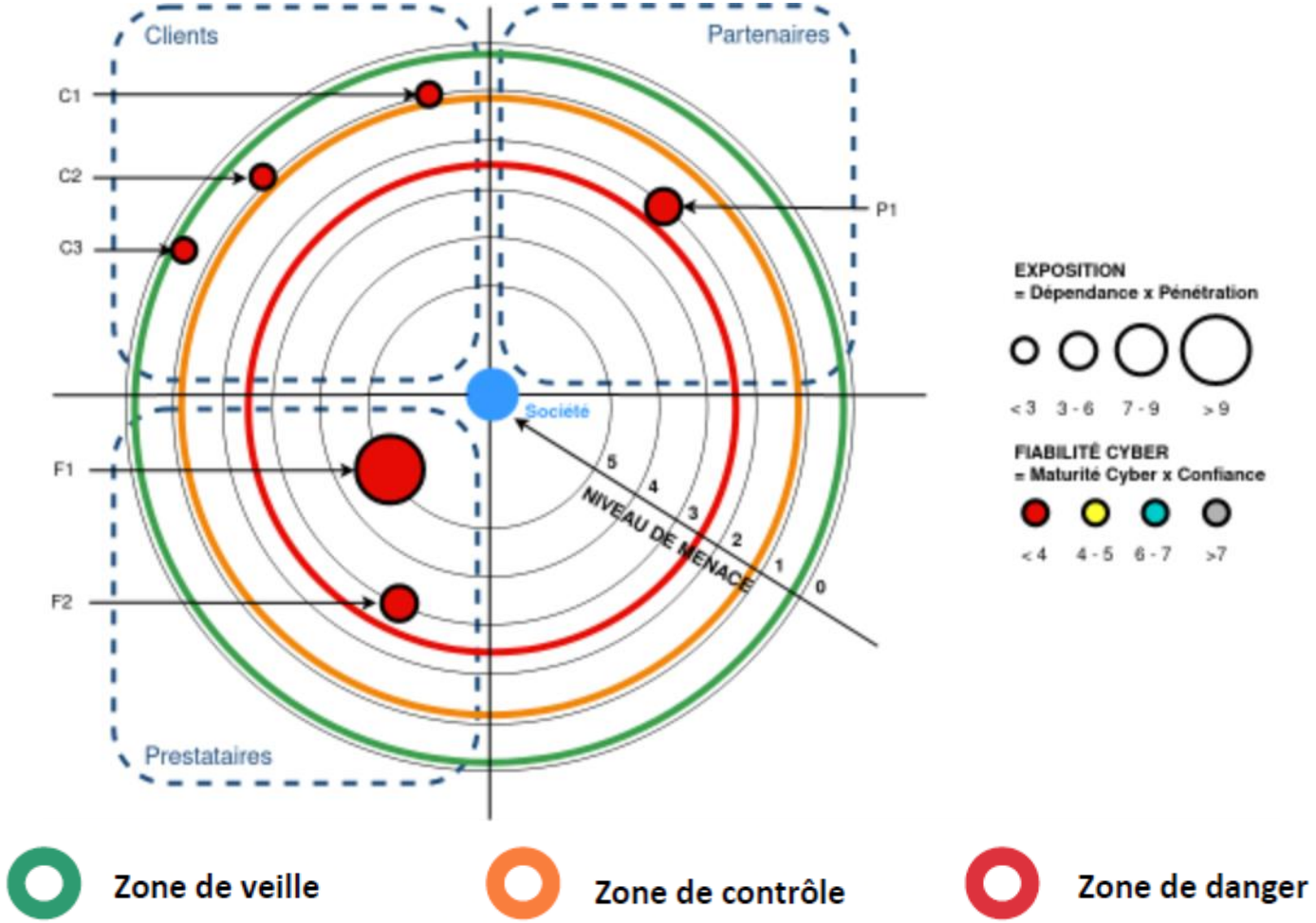
L'objectif de cette partie est d'analyser l'écosystème de l'entreprise. Identifier et mettre en place des mesures de sécurité en fonction de scénarios stratégiques. Cela va nous permettre d'identifier facilement les menaces les plus critiques.

Cartographie de menace numérique de l'écosystème

On identifie ici tous les acteurs de l'entreprise. Le niveau de menace est la division de l'exposition (dépendance * pénétration) par la fiabilité cyber (maturité cyber * confiance).

Catégorie	Nom	Dépendance	Pénétration	Maturité Cyber	Confiance	Niveau de menace
Client	C1 - Particulier	1	1	1	1	1
Client	C2 - Entreprise nautique	1	1	1	1	1
Client	C3 - Association	1	1	1	2	0,5
Partenaire	P1 - Port	2	2	1	2	2
Prestataire	F1 - Prestataire informatique	4	4	1	3	5
Prestataire	F2 - Fournisseur de service de transport	3	1	1	1	3

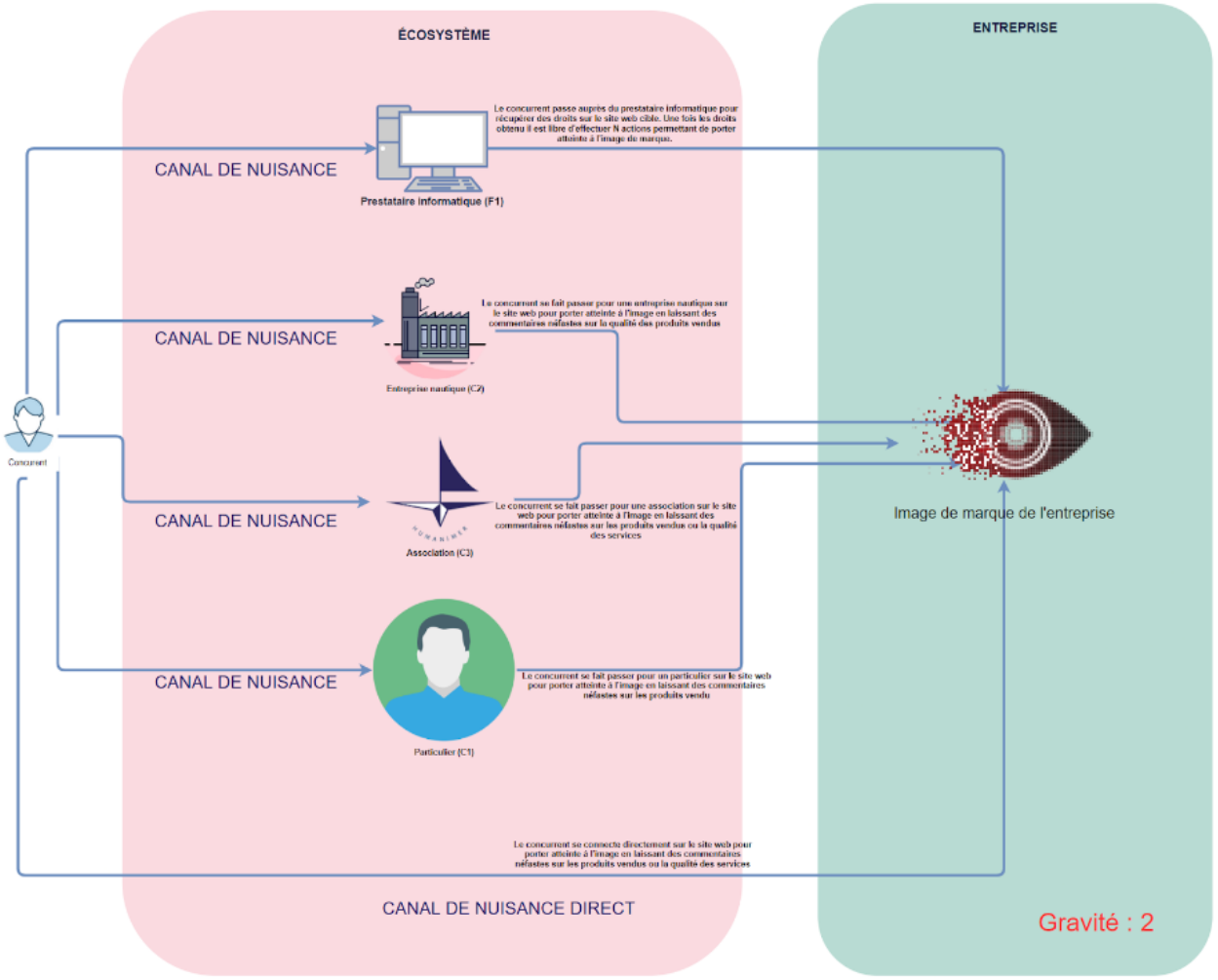
Le schéma reprend le tableau ci-dessus. Plus les points sont proches de la société, plus ils sont dangereux.

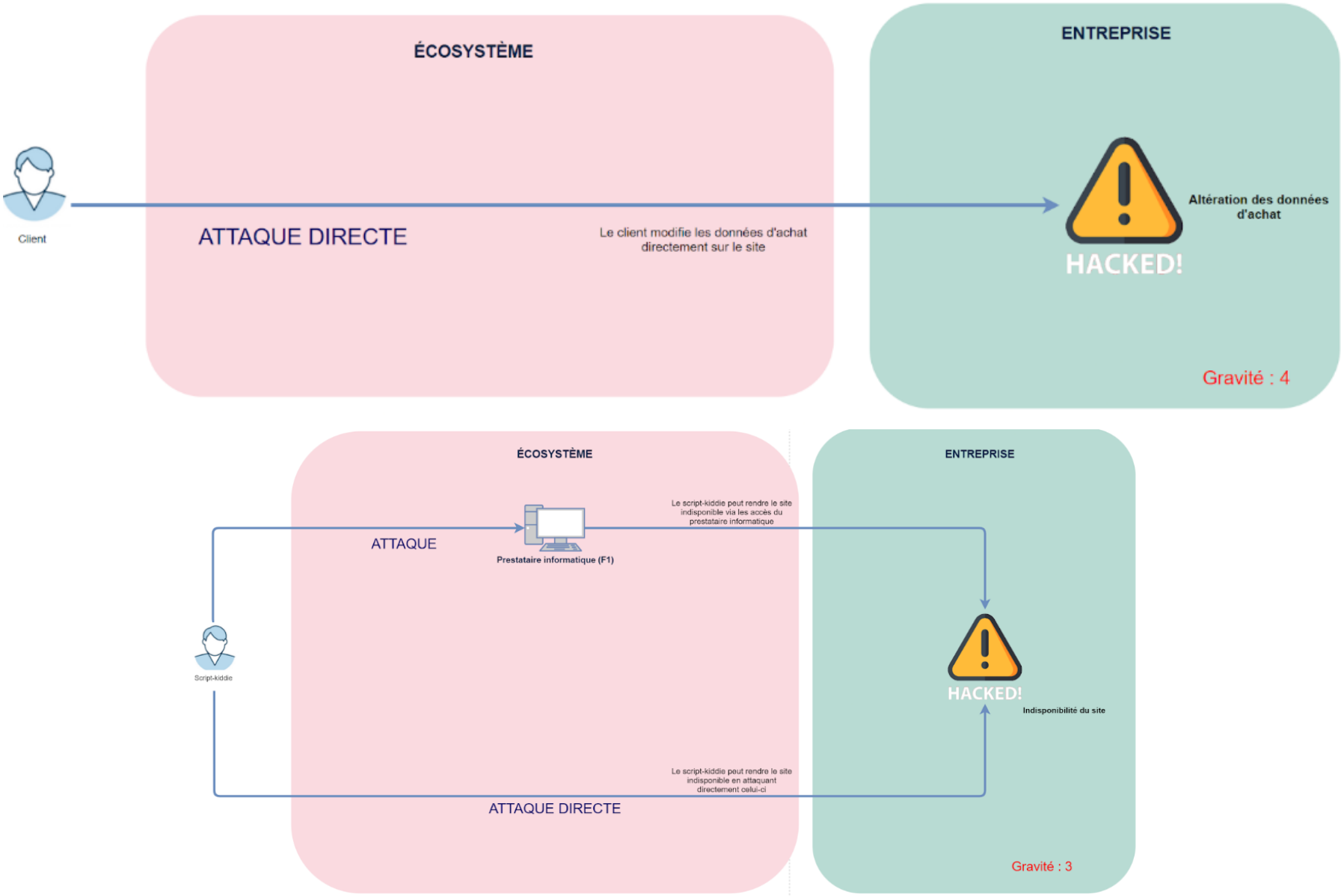


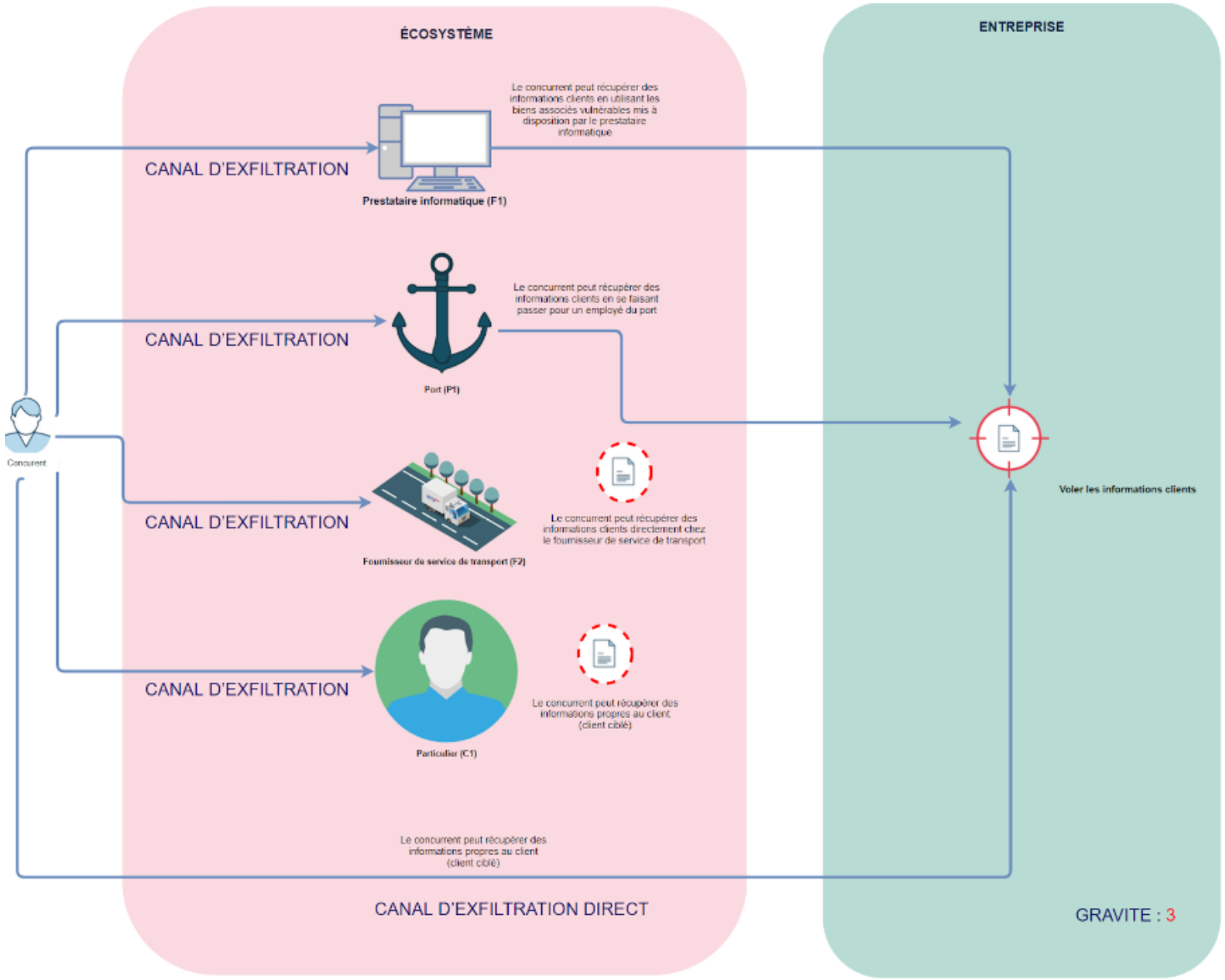
Nous avons retenu C1 - Particulier comme partie prenante critique.
C2 - Entreprise nautique est également retenue comme partie prenante critique.
Les autres parties prenantes n'ont pas été retenues étant donnée que leurs niveaux de menaces sont en deçà de 2.

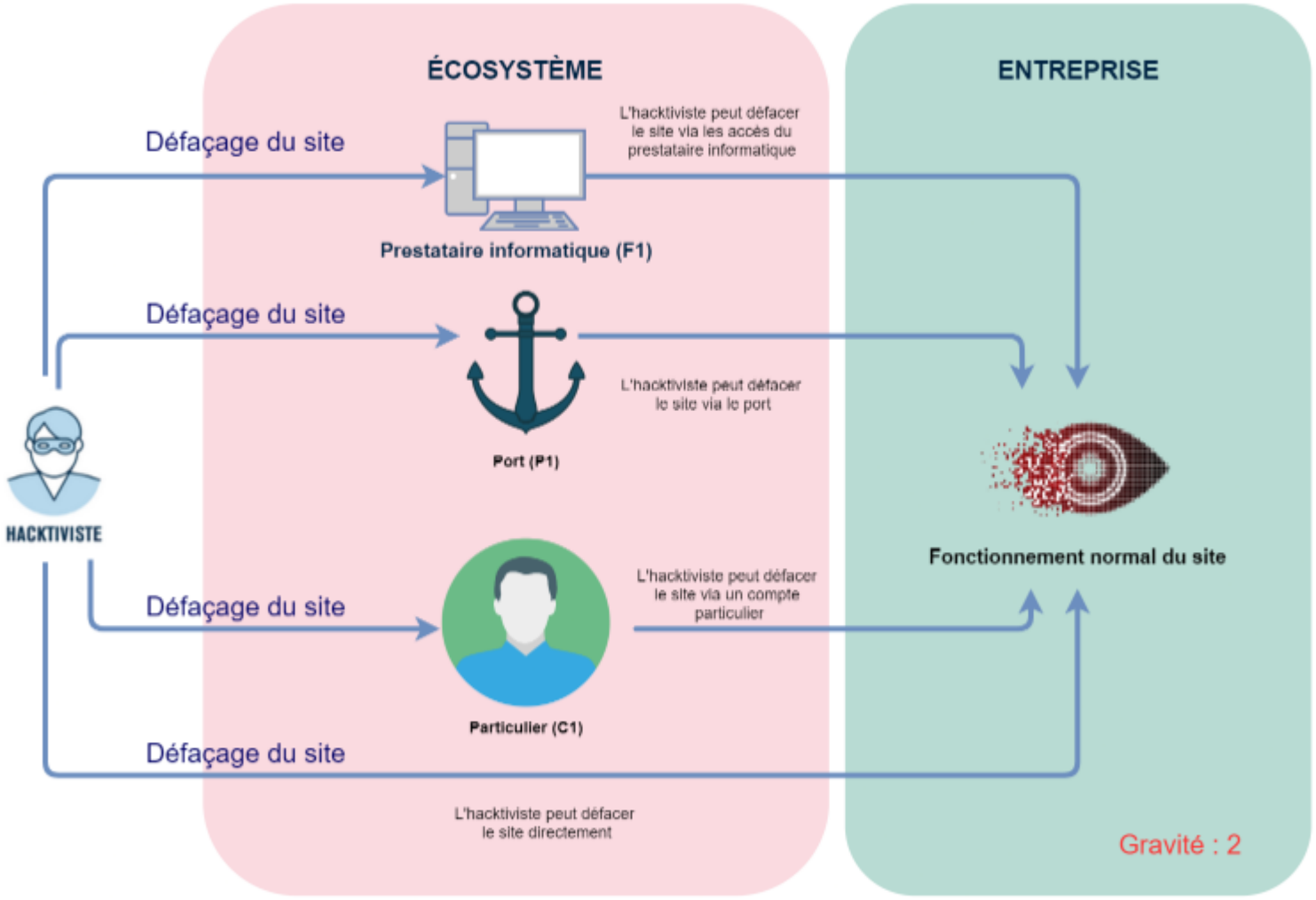
Elaborer des scénarios stratégiques

On imagine ici des scénarios réalistes, pour voir comment un attaquant pourrait procéder pour attaquer notre écosystème.



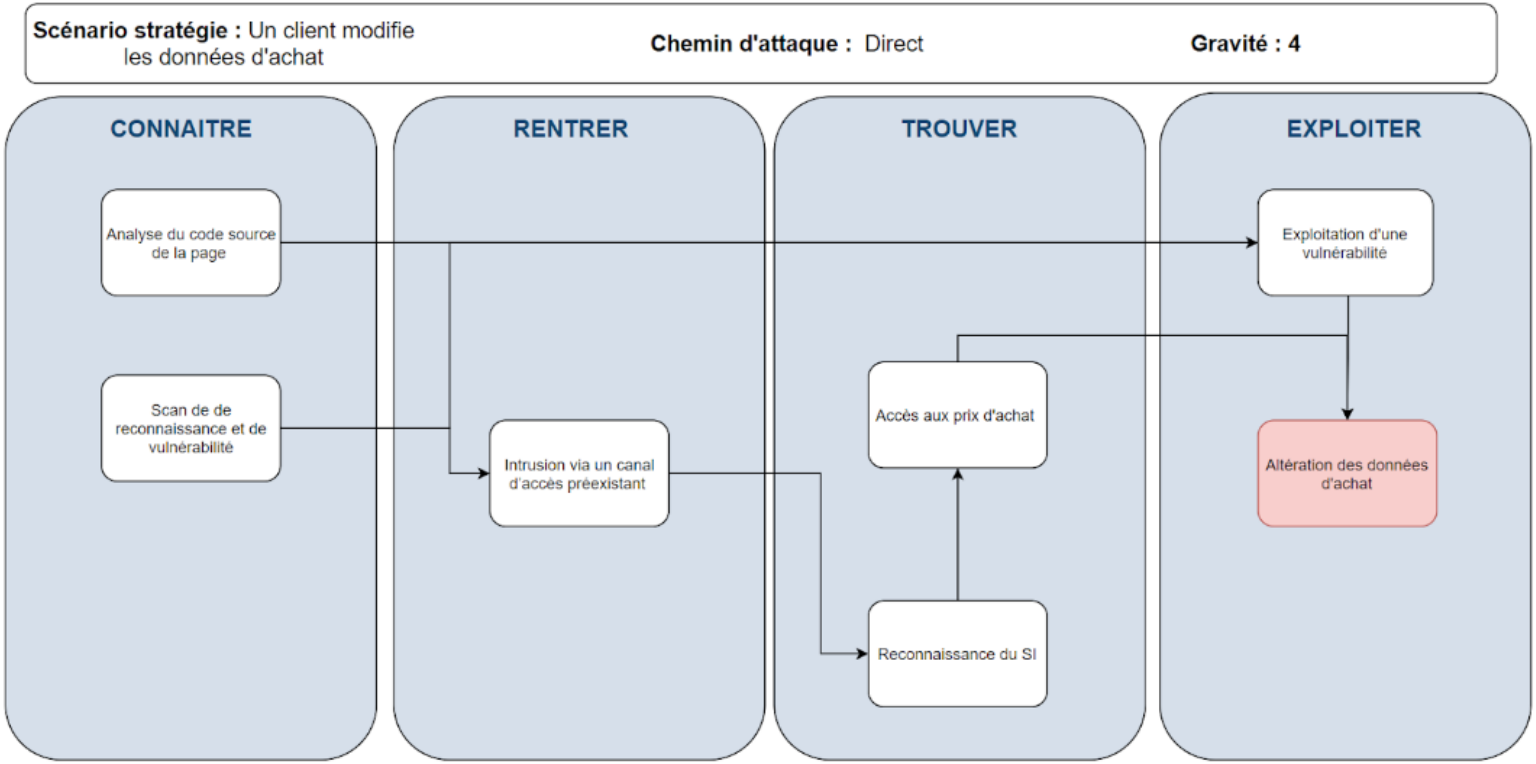

ÉCOSYSTÈME
ENTREPRISE
Client
ATTAQUE DIRECTE
Le client modifie les données d'achat directement sur le site
HACKED!
Altération des données d'achat
Gravité : 4
ÉCOSYSTÈME
ENTREPRISE
ATTAQUE
Prestataire informatique (F1)
Le script-kiddie peut rendre le site indisponible via les accès du prestataire informatique
Script-kiddie
HACKED!
Indisponibilité du site
Le script-kiddie peut rendre le site indisponible en attaquant directement celui-ci
ATTAQUE DIRECTE
Gravité : 3

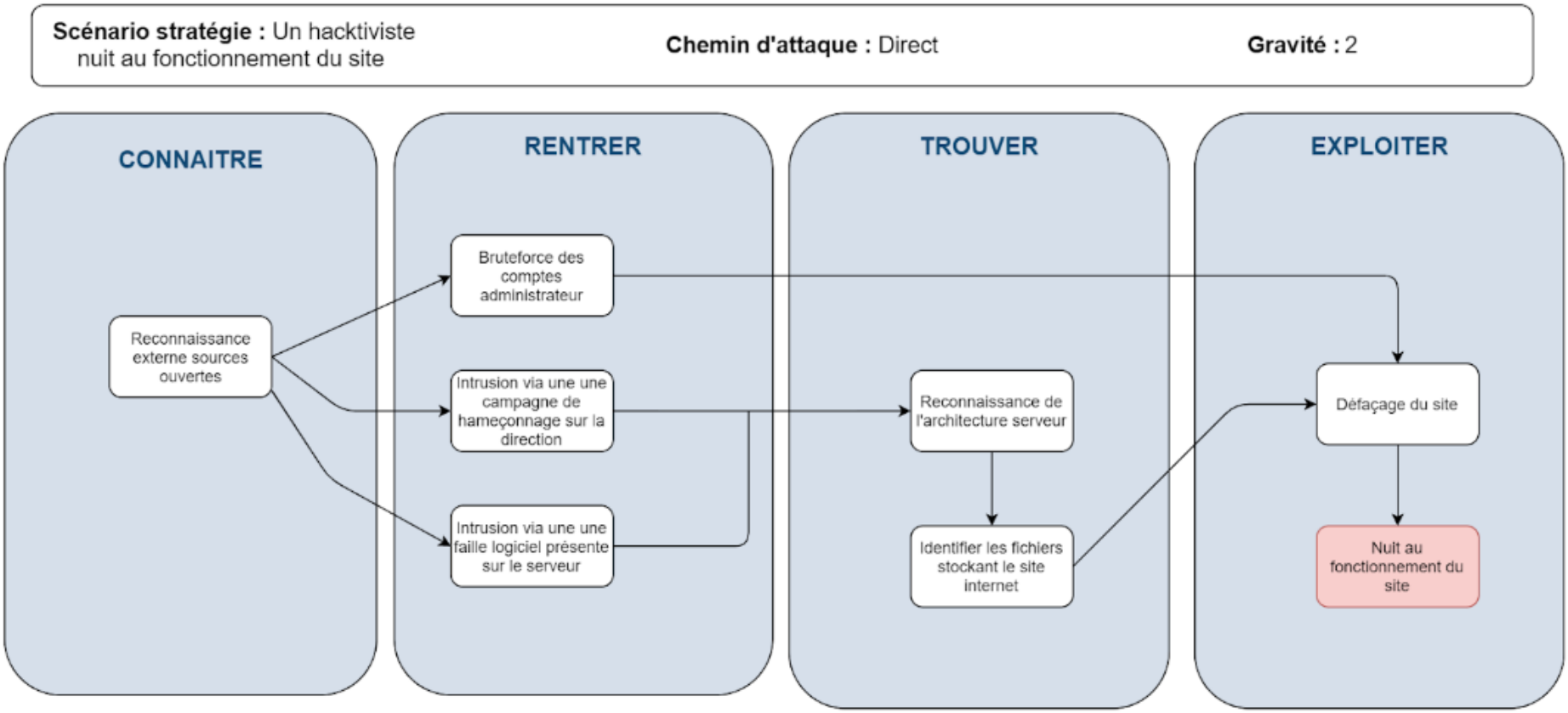

ÉCOSYSTÈME
ENTREPRISE
Le concurrent peut récupérer des informations clients en utilisant les biens associés vulnérables mis à disposition par le prestataire informatique
CANAL D'EXFILTRATION
Prestataire informatique (F1)
Le concurrent peut récupérer des informations clients en se faisant passer pour un employé du port
CANAL D'EXFILTRATION
Port (P1)
Concurrent
CANAL D'EXFILTRATION
Le concurrent peut récupérer des informations clients directement chez le fournisseur de service de transport
Fournisseur de service de transport (F2)
Voler les informations clients
CANAL D'EXFILTRATION
Le concurrent peut récupérer des informations propres au client (client ciblé)
Particulier (C1)
Le concurrent peut récupérer des informations propres au client (client ciblé)
CANAL D'EXFILTRATION DIRECT
GRAVITE : 3

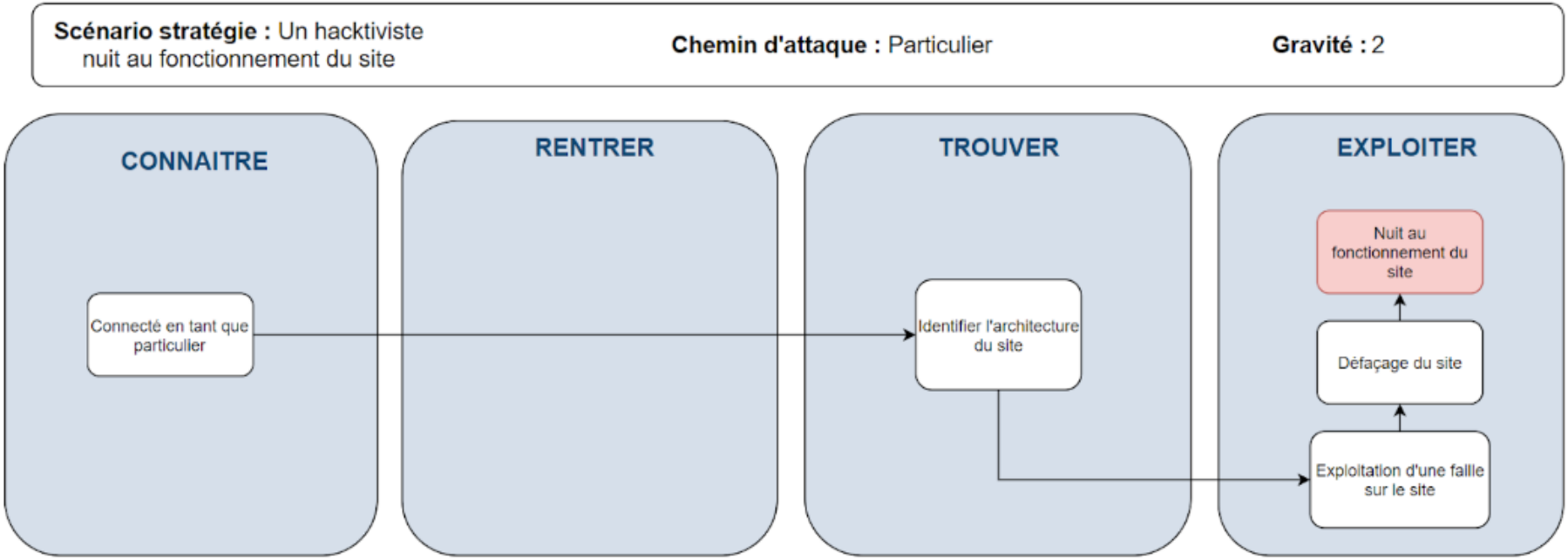

ÉCOSYSTÈME
ENTREPRISE
Défaçage du site
L'hacktiviste peut défacer le site via les accès du prestataire informatique
Prestataire informatique (F1)
Défaçage du site
L'hacktiviste peut défacer le site via le port
Port (P1)
HACKTIVISTE
Fonctionnement normal du site
Défaçage du site
L'hacktiviste peut défacer le site via un compte particulier
Particulier (C1)
Défaçage du site
L'hacktiviste peut défacer le site directement
Gravité : 2

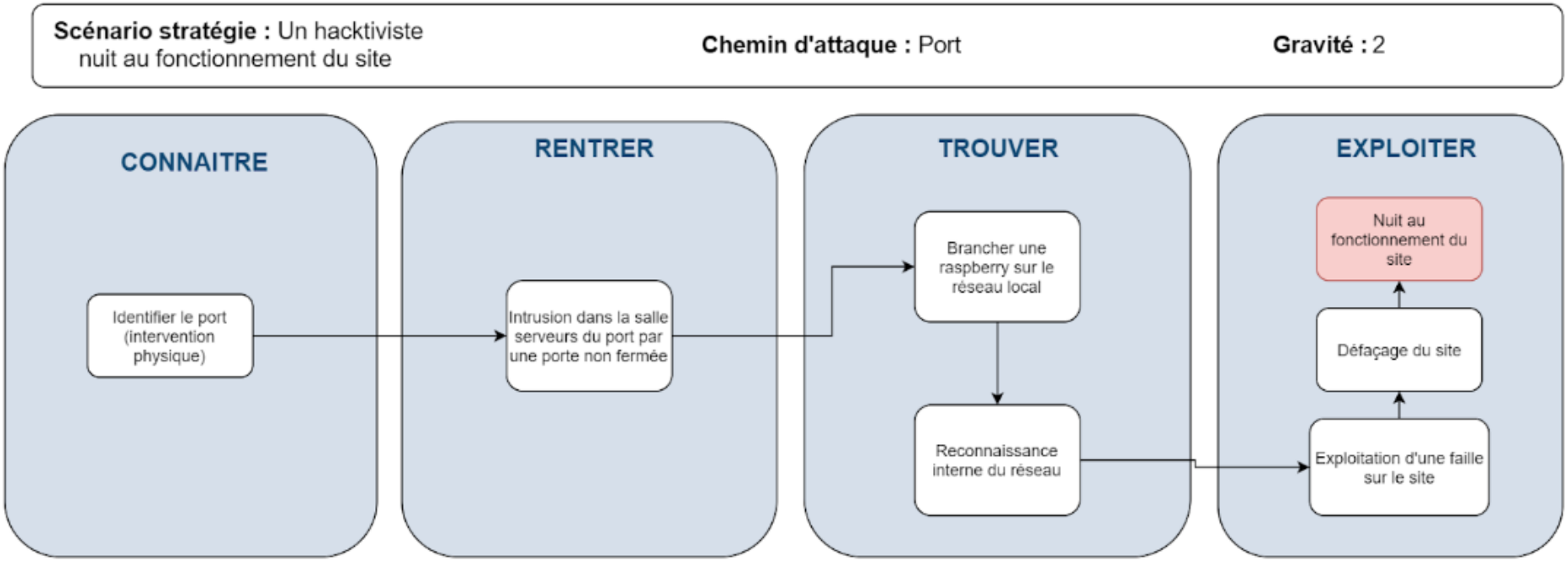
Atelier 4 - Scénarios opérationnels

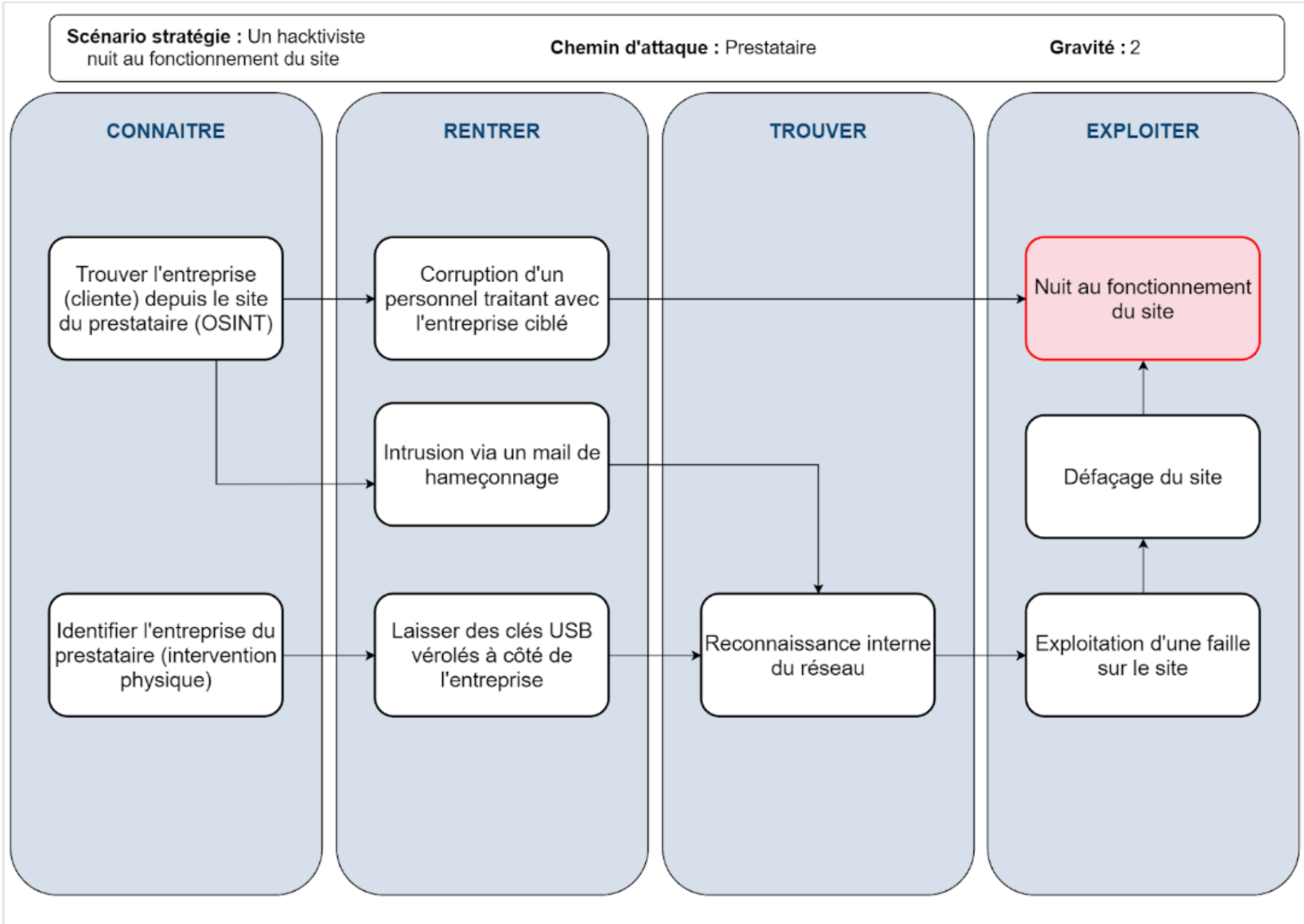
L’objectif de l’atelier 4 est de construire des scénarios opérationnels. Ils schématisent les modes opératoires que pourraient mettre en œuvre les sources de risque pour réaliser les scénarios stratégiques. Cet atelier adopte une démarche similaire à celle de l’atelier précédent mais se concentre sur les biens supports.




Scénario stratégie : Un hacktiviste nuit au fonctionnement du site
Chemin d'attaque : Direct
Gravité : 2
CONNAITRE
RENTRER
TROUVER
EXPLOITER
Reconnaissance externe sources ouvertes
Bruteforce des comptes administrateur
Intrusion via une une campagne de hameçonnage sur la direction
Intrusion via une une faille logiciel présente sur le serveur
Reconnaissance de l'architecture serveur
Identifier les fichiers stockant le site internet
Défaçage du site
Nuit au fonctionnement du site


Scénario stratégie : Un hacktiviste nuit au fonctionnement du site
Chemin d'attaque : Particulier
Gravité : 2
CONNAITRE
RENTRER
TROUVER
EXPLOITER
Connecté en tant que particulier
Identifier l'architecture du site
Nuit au fonctionnement du site
Défaçage du site
Exploitation d'une faille sur le site

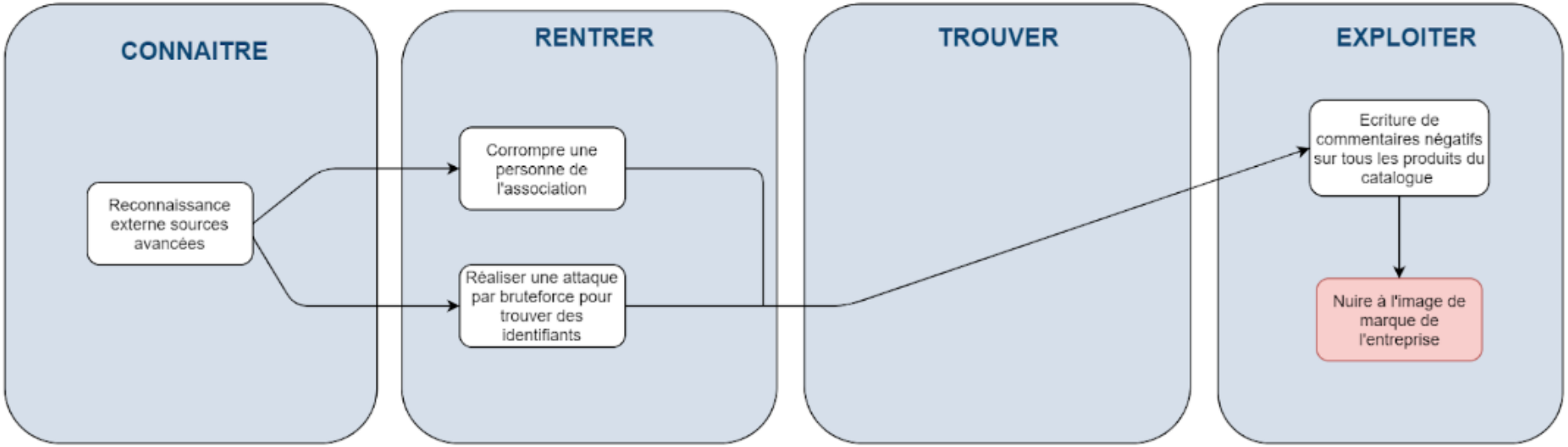

Scénario stratégie : Un hacktiviste nuit au fonctionnement du site
Chemin d'attaque : Port
Gravité : 2
CONNAITRE
Identifier le port (intervention physique)
RENTRER
Intrusion dans la salle serveurs du port par une porte non fermée
TROUVER
Brancher une raspberry sur le réseau local
Reconnaissance interne du réseau
EXPLOITER
Exploitation d'une faille sur le site
Défaçage du site
Nuit au fonctionnement du site

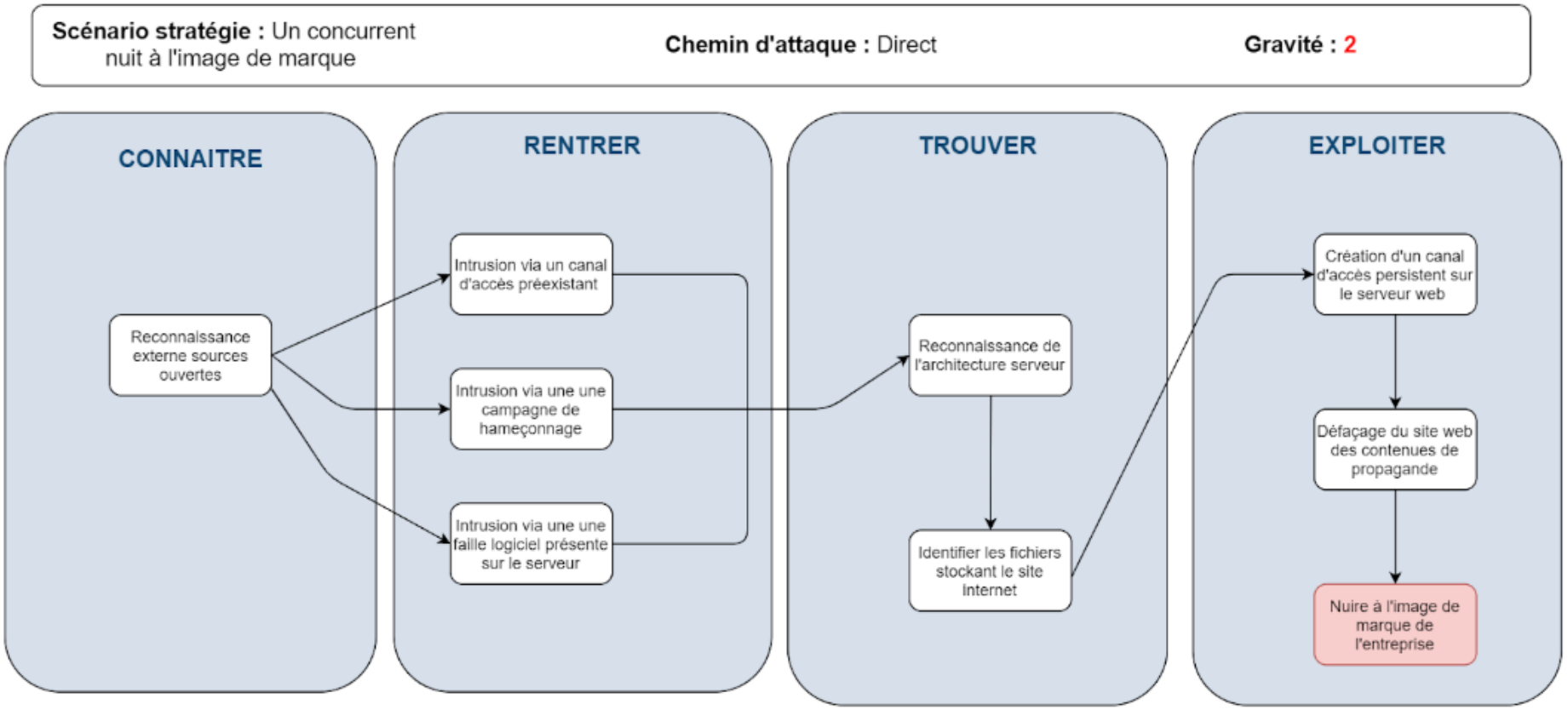

Scénario stratégie : Un hacktiviste nuit au fonctionnement du site
Chemin d'attaque : Prestataire
Gravité : 2
CONNAITRE
RENTRER
TROUVER
EXPLOITER
Trouver l'entreprise (cliente) depuis le site du prestataire (OSINT)
Identifier l'entreprise du prestataire (intervention physique)
Corruption d'un personnel traitant avec l'entreprise ciblé
Intrusion via un mail de hameçonnage
Laisser des clés USB vérolés à côté de l'entreprise
Reconnaissance interne du réseau
Exploitation d'une faille sur le site
Défaçage du site
Nuit au fonctionnement du site

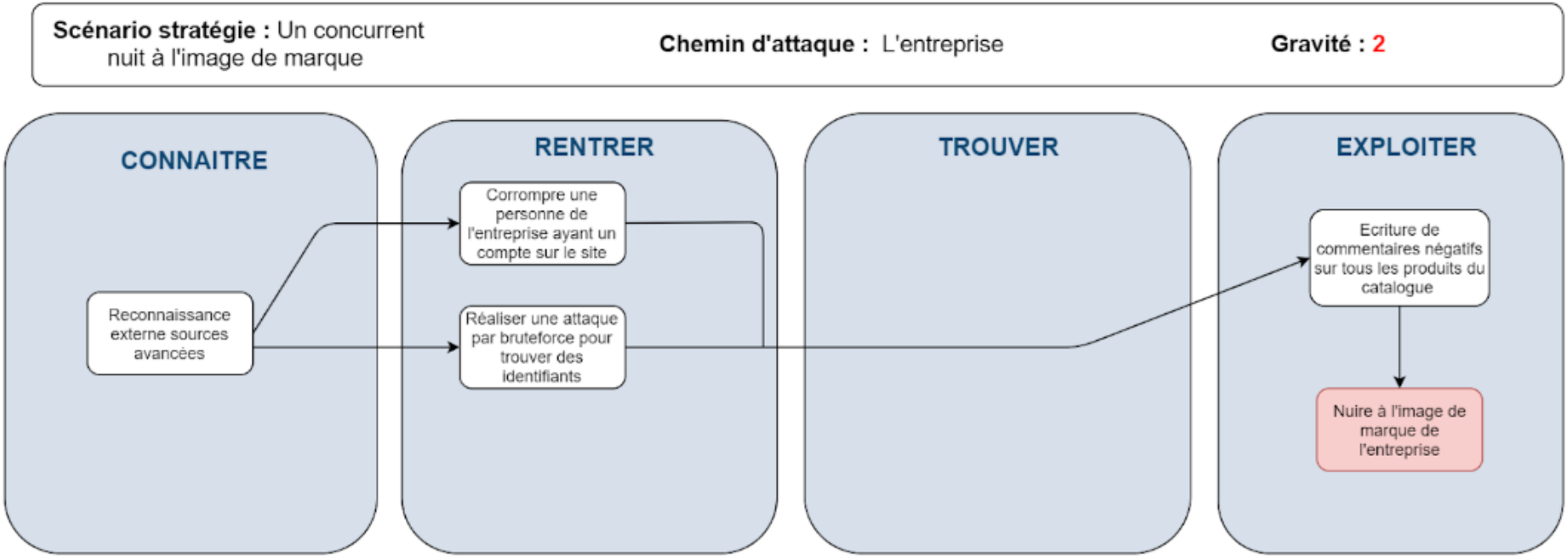
Scénario stratégie : Un concurrent nuit à l'image de marque

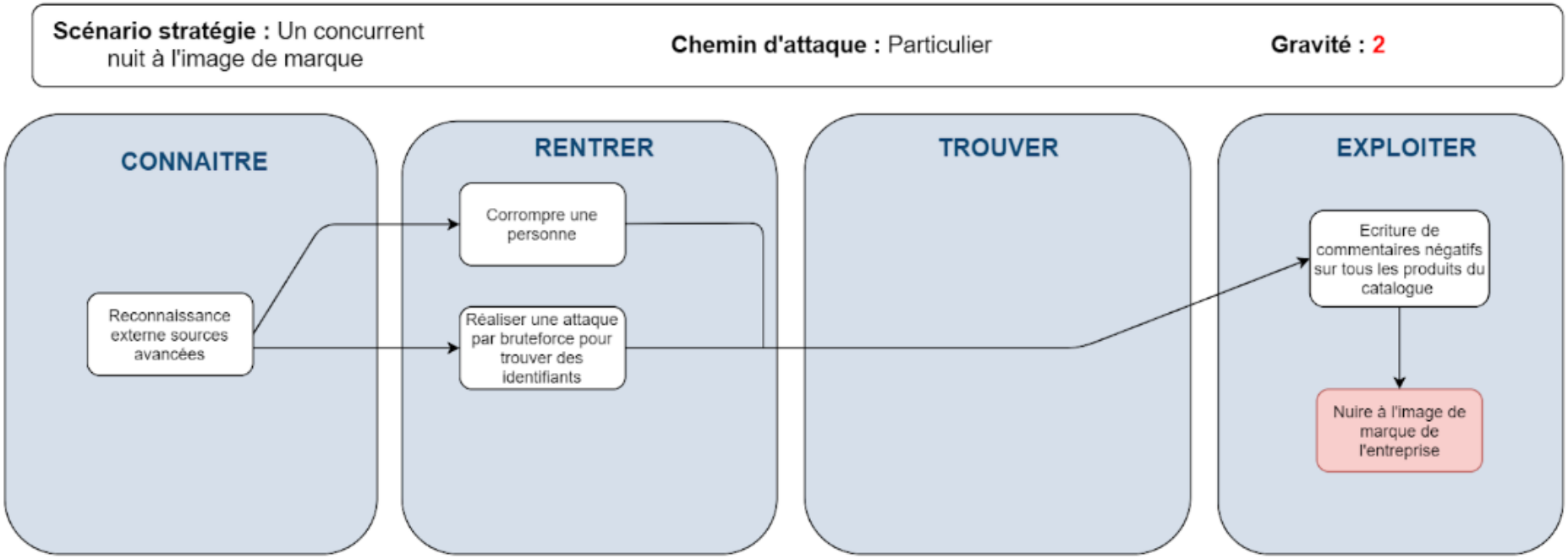
Chemin d'attaque : Association

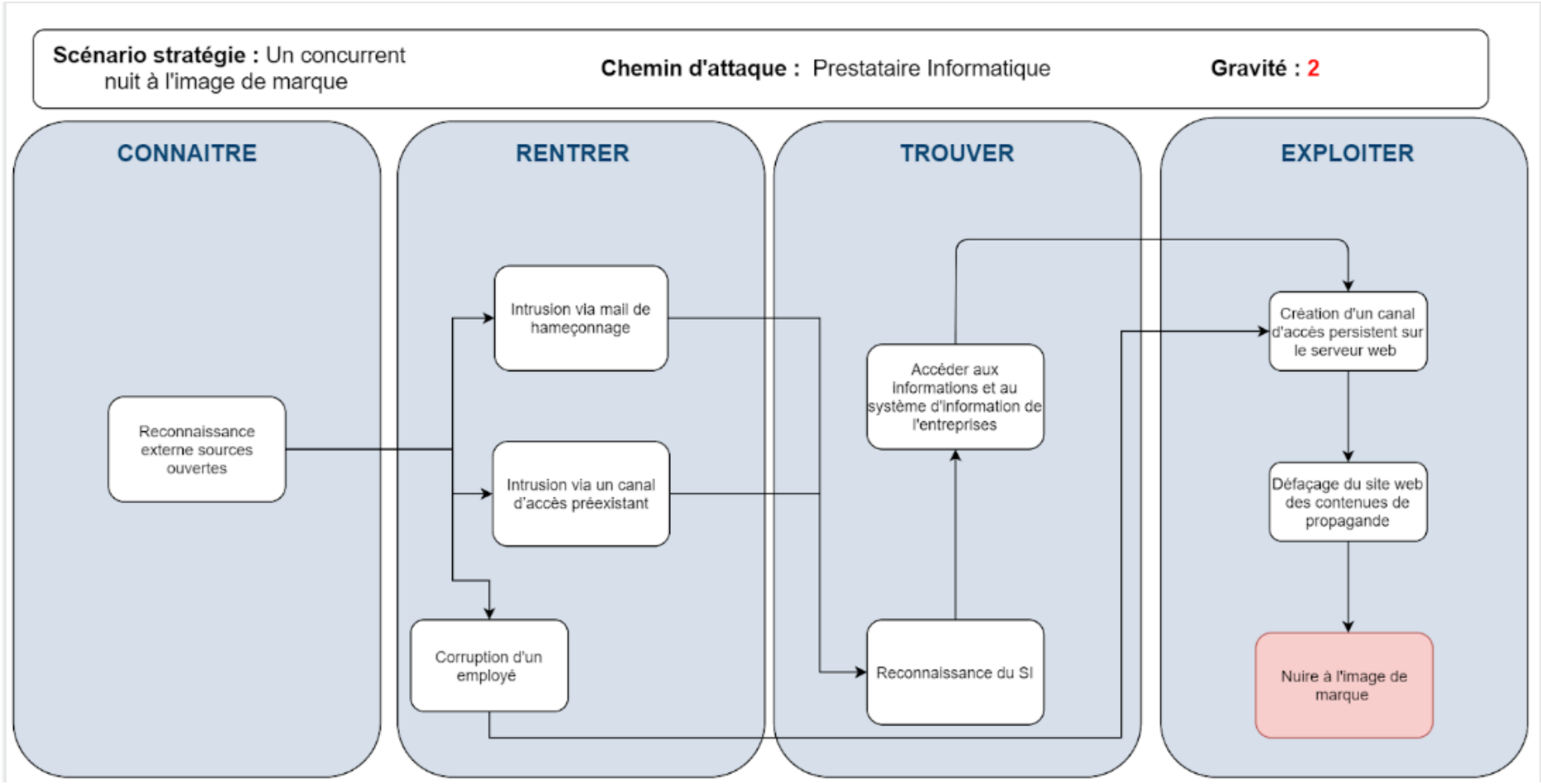
Gravité : 2




Scénario stratégie : Un concurrent nuit à l'image de marque
Chemin d'attaque : Direct
Gravité : 2
CONNAITRE
RENTRER
TROUVER
EXPLOITER
Reconnaissance externe sources ouvertes
Intrusion via un canal d'accès préexistant
Intrusion via une une campagne de hameçonnage
Intrusion via une une faille logiciel présente sur le serveur
Reconnaissance de l'architecture serveur
Identifier les fichiers stockant le site Internet
Création d'un canal d'accès persistent sur le serveur web
Défaçage du site web des contenues de propagande
Nuire à l'image de marque de l'entreprise


Scénario stratégie : Un concurrent nuit à l'image de marque
Chemin d'attaque : L'entreprise
Gravité : 2
CONNAITRE
Reconnaissance externe sources avancées
RENTRER
Corrompre une personne de l'entreprise ayant un compte sur le site
Réaliser une attaque par bruteforce pour trouver des identifiants
TROUVER
EXPLOITER
Ecriture de commentaires négatifs sur tous les produits du catalogue
Nuire à l'image de marque de l'entreprise

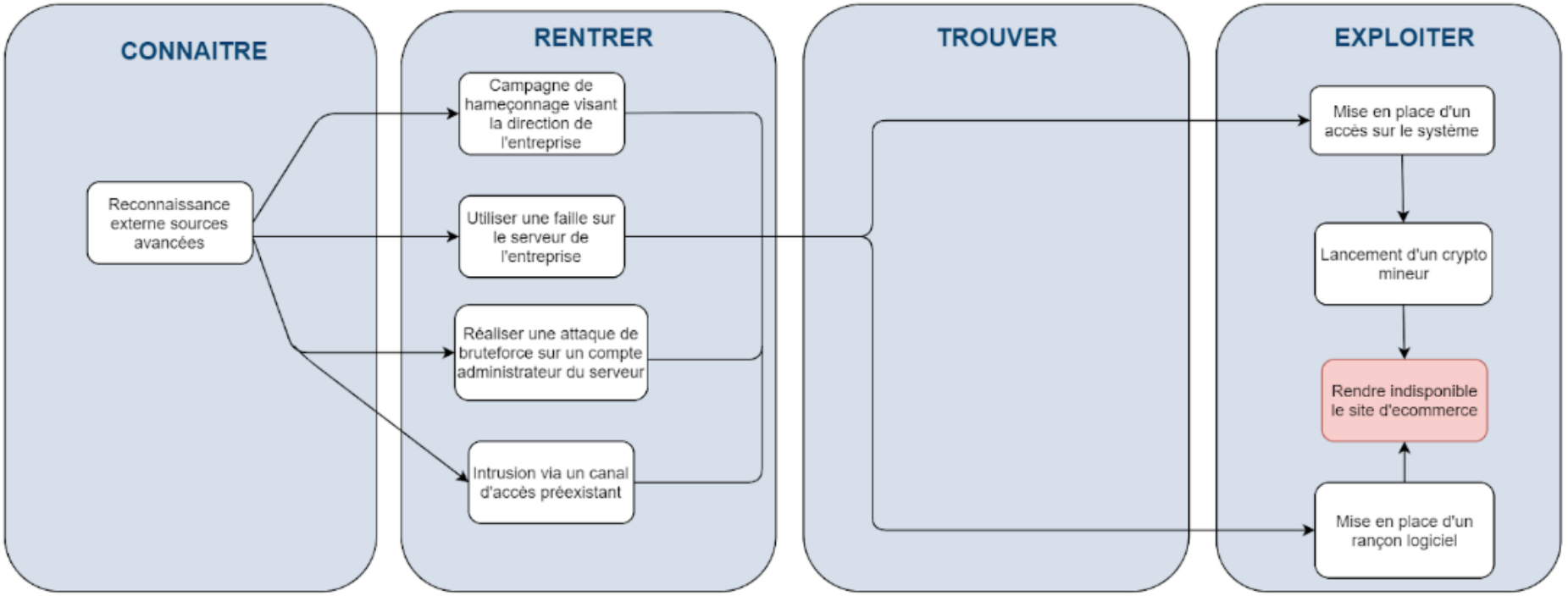

Scénario stratégie : Un concurrent nuit à l'image de marque
Chemin d'attaque : Particulier
Gravité : 2
CONNAITRE
RENTRER
TROUVER
EXPLOITER
Reconnaissance externe sources avancées
Corrompre une personne
Réaliser une attaque par bruteforce pour trouver des identifiants
Ecriture de commentaires négatifs sur tous les produits du catalogue
Nuire à l'image de marque de l'entreprise

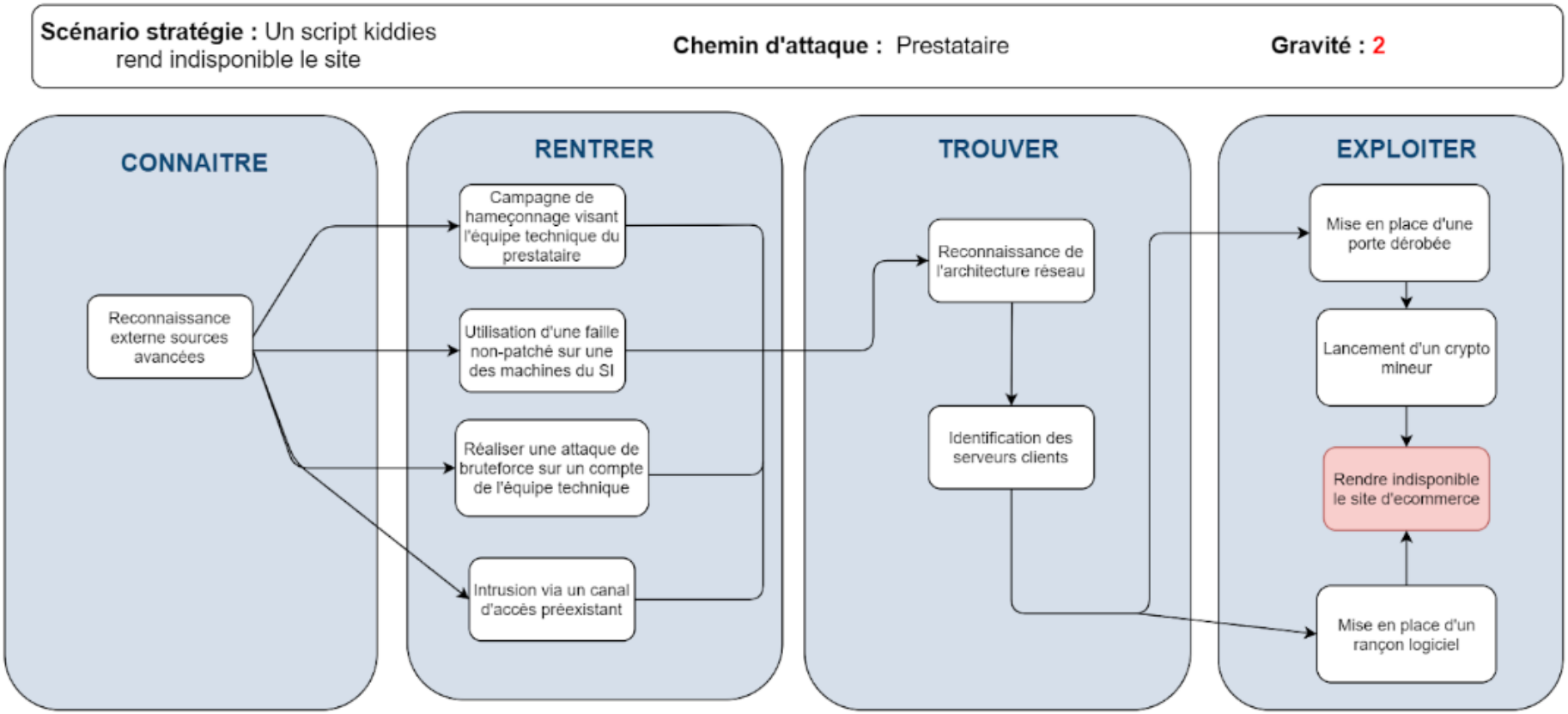

Scénario stratégie : Un concurrent nuit à l'image de marque
Chemin d'attaque : Prestataire Informatique
Gravité : 2
CONNAITRE
RENTRER
TROUVER
EXPLOITER
Reconnaissance externe sources ouvertes
Intrusion via mail de hameçonnage
Intrusion via un canal d'accès préexistant
Corruption d'un employé
Accéder aux informations et au système d'information de l'entreprises
Reconnaissance du SI
Création d'un canal d'accès persistent sur le serveur web
Défaçage du site web des contenues de propagande
Nuire à l'image de marque

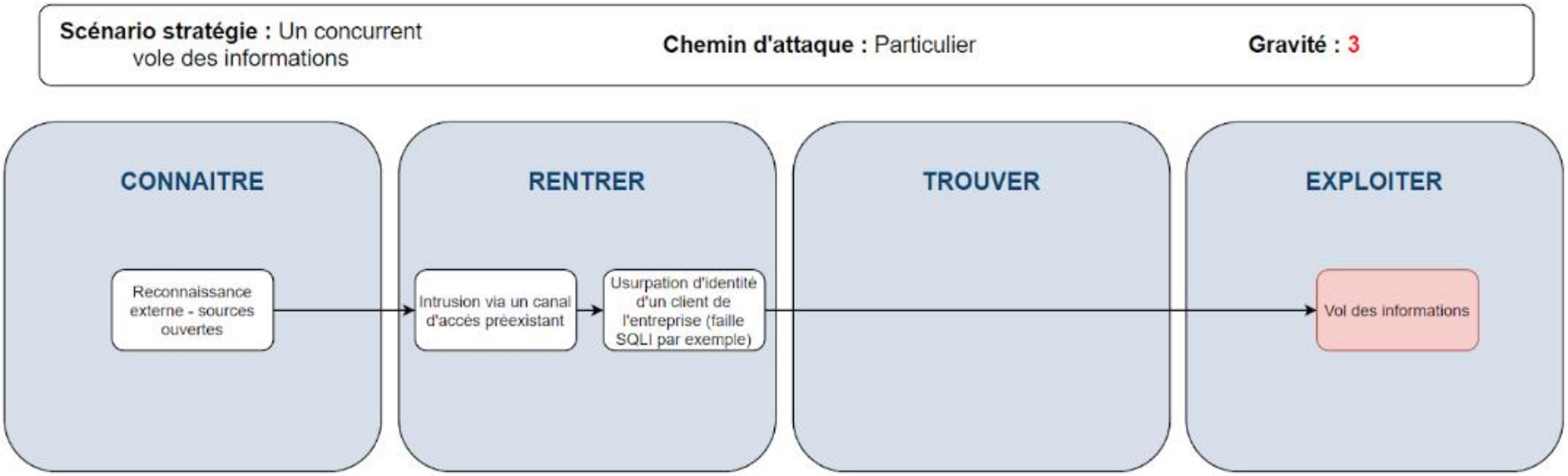
Scénario stratégie : Un script kiddies rend indisponible le site

Chemin d'attaque : Direct

Gravité : 2



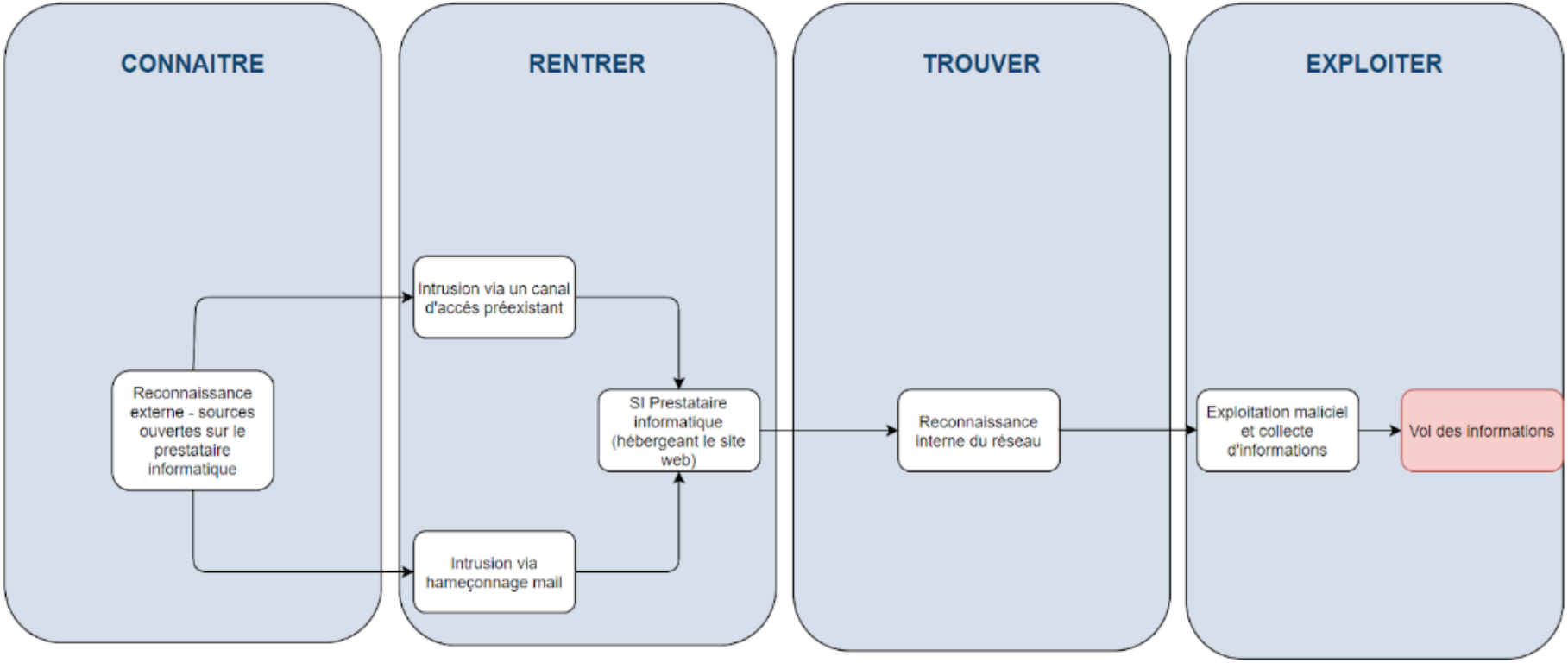

Scénario stratégie : Un script kiddies rend indisponible le site
Chemin d'attaque : Prestataire
Gravité : 2
CONNAITRE
Reconnaissance externe sources avancées
RENTRER
Campagne de hameçonnage visant l'équipe technique du prestataire
Utilisation d'une faille non-patché sur une des machines du SI
Réaliser une attaque de bruteforce sur un compte de l'équipe technique
Intrusion via un canal d'accès préexistant
TROUVER
Reconnaissance de l'architecture réseau
Identification des serveurs clients
EXPLOITER
Mise en place d'une porte dérobée
Lancement d'un crypto mineur
Rendre indisponible le site d'ecommerce
Mise en place d'un rançon logiciel


Scénario stratégie : Un concurrent vole des informations
Chemin d'attaque : Particulier
Gravité : 3
CONNAITRE
RENTRER
TROUVER
EXPLOITER
Reconnaissance externe - sources ouvertes
Intrusion via un canal d'accès préexistant
Usurpation d'identité d'un client de l'entreprise (faille SQLI par exemple)
Vol des informations

Scénario stratégie : Un concurrent vole des informations

Chemin d'attaque : Direct

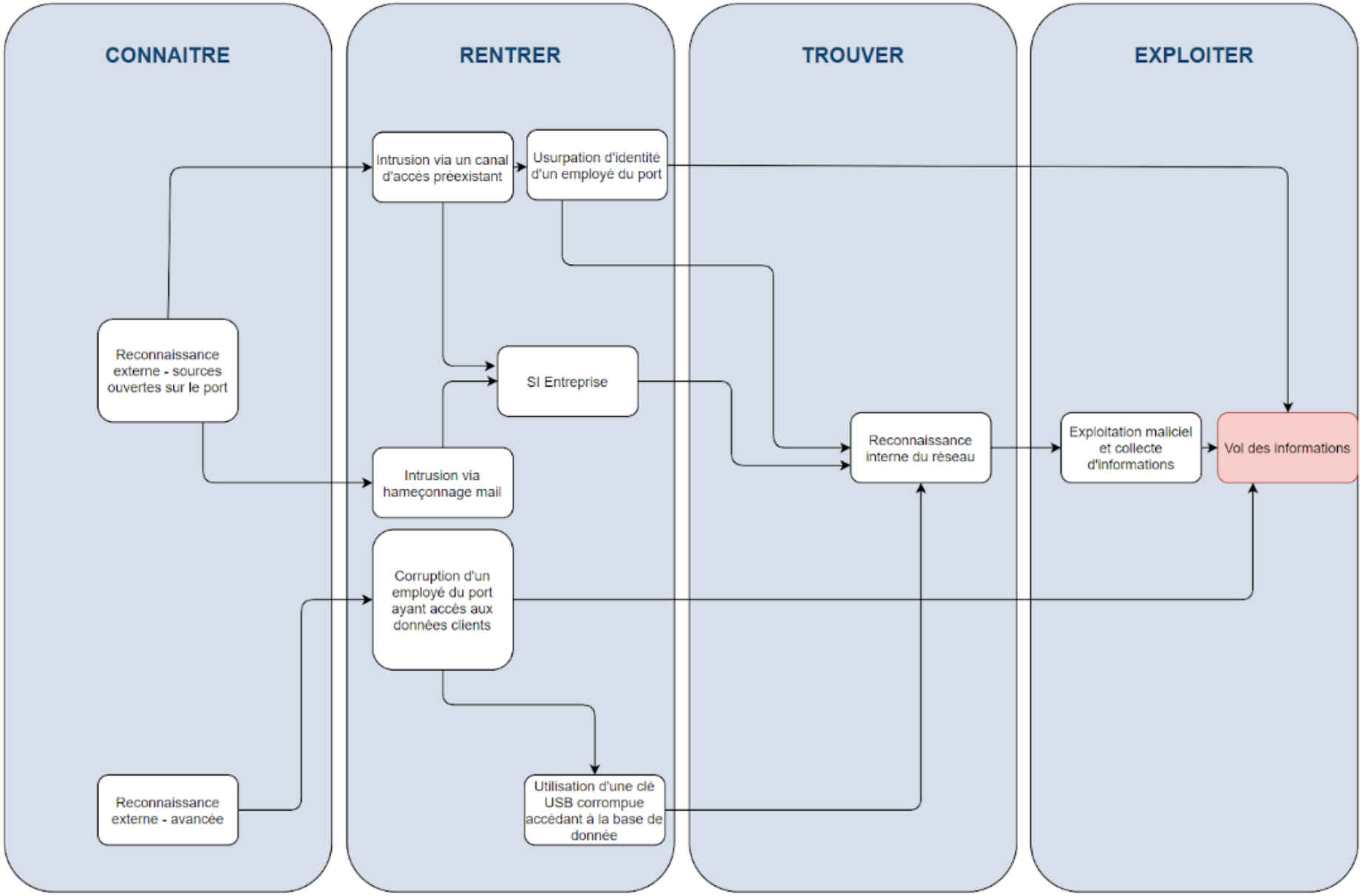
Gravité : 3



Scénario stratégie : Un concurrent vole des informations

Chemin d'attaque : Port

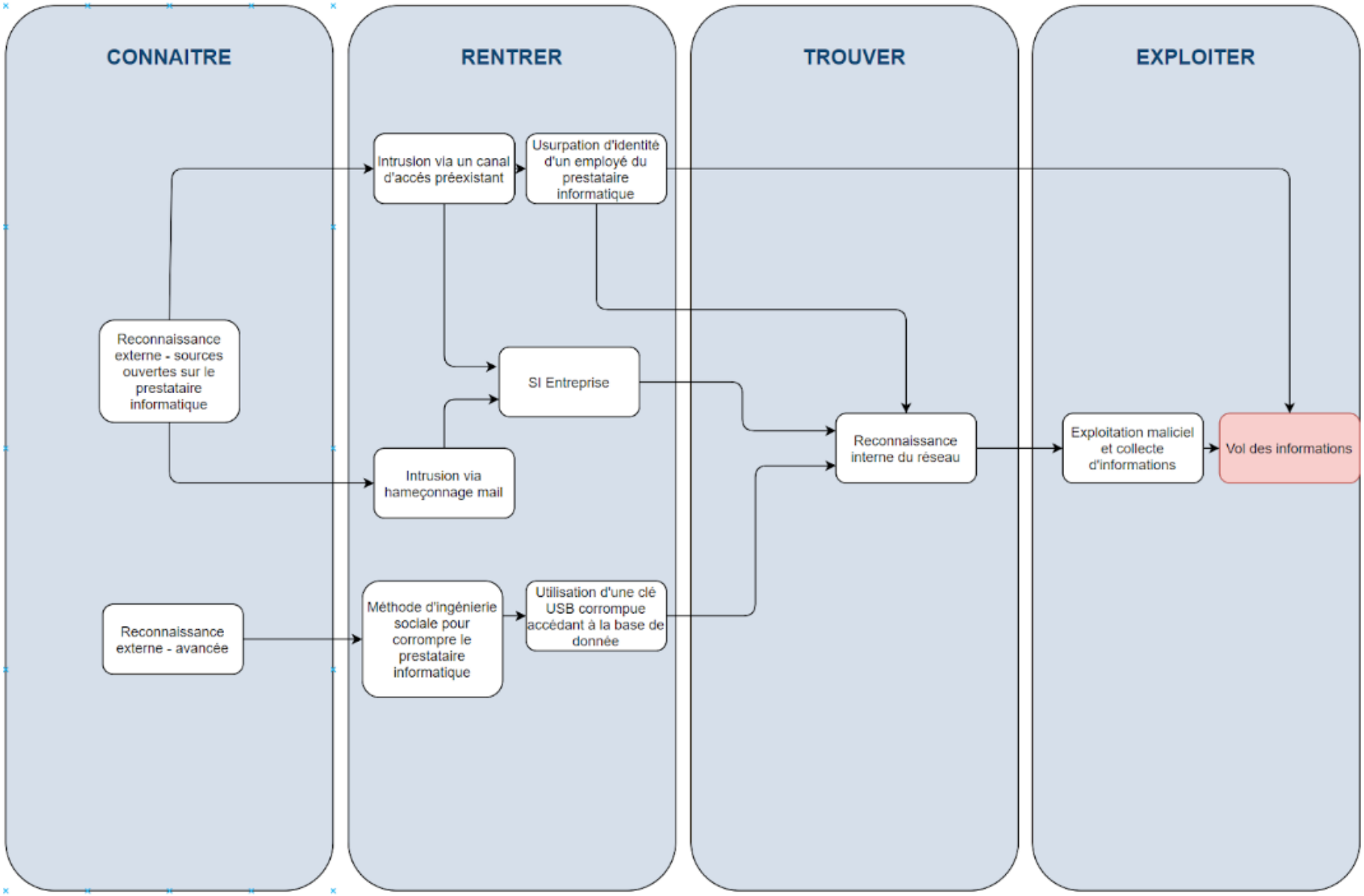
Gravité : 3



Scénario stratégie : Un concurrent vole des informations

Chemin d'attaque : Prestataire informatique

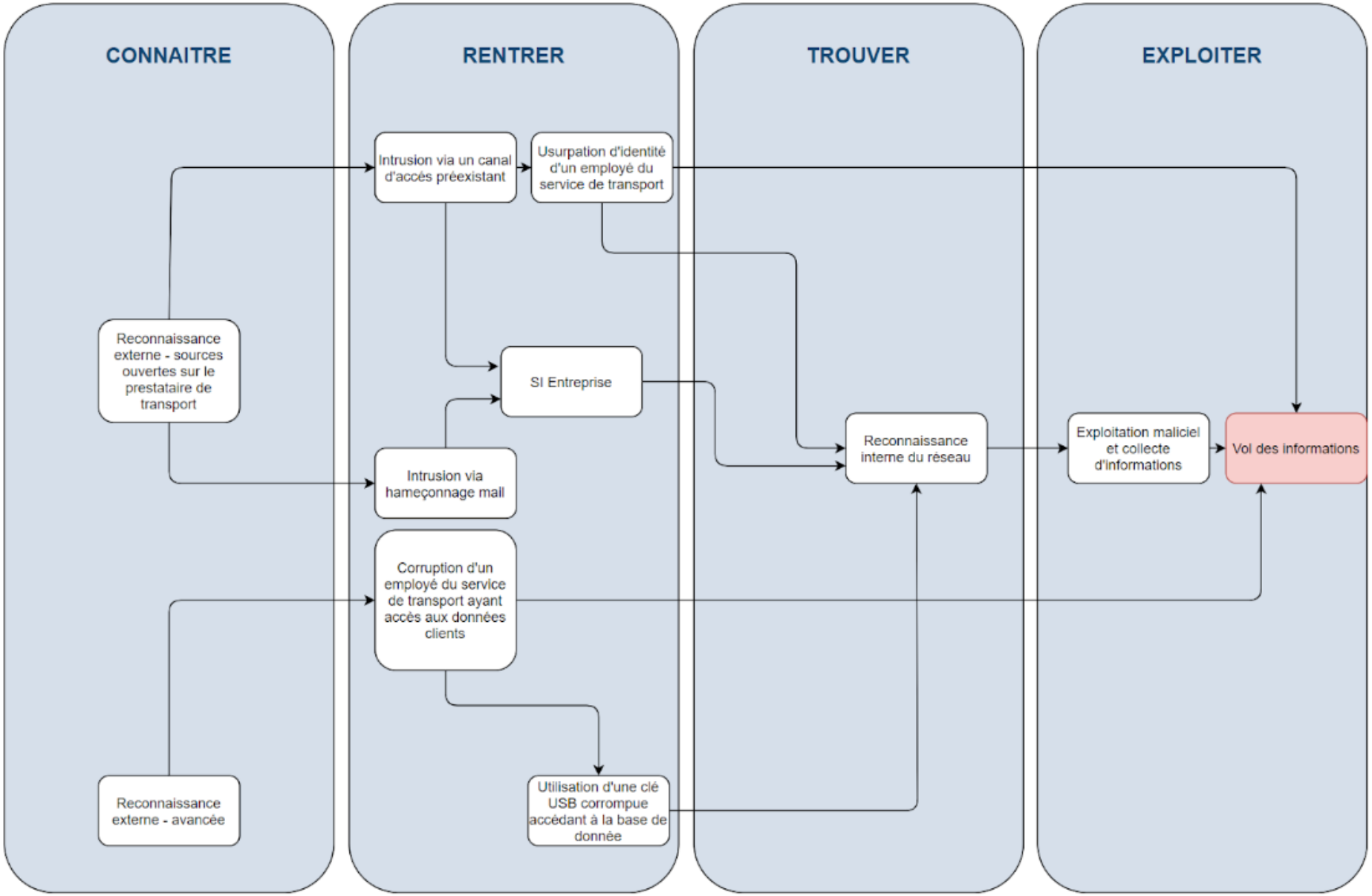
Gravité : 3



Scénario stratégie : Un concurrent vole des informations

Chemin d'attaque : Prestataire de transport

Gravité : 3



Maintenant que nous avons défini nos scénarios opérationnels, nous allons pouvoir évaluer leur vraisemblance. Pour cela nous allons utiliser l'échelle suivante :

ÉCHELLE	DÉFINITION
V4 – CERTAIN OU DÉJÀ PRODUIT	La source de risque va certainement atteindre son objectif visé selon l'un des modes opératoires envisagés OU un tel scénario s'est déjà produit au sein de l'organisation (historique d'incidents)
V3 – TRÈS VRAISEMBLABLE	La source de risque va probablement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est élevée
V2 – VRAISEMBLABLE	La source de risque est susceptible d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est significative
V1 – PEU VRAISEMBLABLE	La source de risque a peu de chances d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est faible

CHEMINS D'ATTAQUE STRATÉGIQUES (ASSOCIÉS AUX SCÉNARIOS OPÉRATIONNELS)	VRAISEMBLANCE GLOBALE
Un hacktiviste nuit au fonctionnement du site directement sur le site	3
Un hacktiviste nuit au fonctionnement du site via un particulier	3
Un hacktiviste nuit au fonctionnement du site via le port	1
Un hacktiviste nuit au fonctionnement du site via le prestataire informatique	4
Le concurrent passe par notre prestataire informatique avec l'objectif de voler des informations de nos clients	3
Un concurrent vole des informations via le système d'information du port partenaire	3
Partageant le même fournisseur de service de transport que notre concurrent, celui-ci peut récupérer des informations auprès d'eux	3
Un concurrent vole des informations clients en usurpant le compte d'un particulier	2
Le concurrent vole des informations clients en effectuant des actions directes sur le SI hébergeant le site	3
Un client effectue une opération d'altération des données d'achat directement sur le site	1
Un script-kiddie rend le site indisponible en passant directement par celui-ci	3

Un script-kiddie rend le site de indisponible en passant par le prestataire informatique	4
Le concurrent nuit à l'image de l'entreprise en passant par un particulier	3
Le concurrent nuit à l'image de l'entreprise en passant par une entreprise nautique	1
Le concurrent nuit à l'image de l'entreprise en passant par des associations	1
Le concurrent nuit à l'image directement depuis le système d'information	2
Le concurrent nuit à l'image de l'entreprise à travers du prestataire informatique	3

Atelier 5 - Traitement du risque

Cet atelier a pour but de synthétiser les scénarios de risques identifiés et de définir une stratégie de traitement des risques.
A partir de là, il est possible de définir des mesures de sécurités permettant de traiter les risques. Ces risques sont recensées dans un plan d'amélioration continue de la sécurité (PACS). Enfin, les risques résiduels seront identifiés ainsi que le cadre de suivi de ces risques.

Les différents scénarios de risques sont détaillés ici :
Le tableau ci-dessous permet de classer les différents scénarios de risques en fonction de leur gravité et de leur vraisemblance.

Référence du scénario de risque	Description	Gravité	Vraisemblance	Stratégie de traitement du risque
R1	Un hacktiviste nuit au fonctionnement du site directement sur le site	**G2**	3	Réduction du risque
R2	Un hacktiviste nuit au fonctionnement du site via un particulier	**G2**	3	Réduction du risque
R3	Un hacktiviste nuit au fonctionnement du site via le port	**G2**	1	Refus du risque
R4	Un hacktiviste nuit au fonctionnement du site via le prestataire informatique (Récupération des informations de locations auprès du port de Vannes)	**G2**	4	Partage du risque (Les actions mise en place n'assurent pas une réduction de risque)
R5	Le concurrent passe par notre prestataire informatique avec l'objectif de voler des informations de nos clients	**G3**	3	Partage du risque
R6	Un concurrent vole des informations via le système d'information du port partenaire	**G3**	3	Refus du risque

R7	Partageant le même fournisseur de service de transport que notre concurrent, celui-ci peut récupérer des informations auprès d'eux	**G3**	3	Partage du risque
R8	Un concurrent vole des informations clients en usurpant le compte d'un particulier (Le client n'ayant pas créer son compte, l'accès à l'option d'achat est naturellement bloquée cependant il peut tout de même exploiter une vulnérabilité pour modifier les données d'achats PUIS basculer sur R9 en créant un compte et en utilisant la modification précédemment faite)	**G3**	2	Réduction du risque
R9	Le concurrent vole des informations clients en effectuant des actions directes sur le SI hébergeant le site	**G3**	3	Réduction du risque
R10	Un client effectue une opération d'altération des données d'achat directement sur le site	**G4**	1	Réduction du risque
R11	Un script-kiddie rend le site indisponible en passant directement par celui-ci	**G2**	3	Réduction du risque
R12	Un script-kiddie rend le site de indisponible en passant par le prestataire informatique	**G2**	4	Maintien du risque
R13	Le concurrent nuit à l'image de l'entreprise en passant par un particulier	**G2**	3	Maintien du risque
R14	Le concurrent nuit à l'image de l'entreprise en passant par une entreprise nautique	**G2**	1	Maintien du risque
R15	Le concurrent nuit à l'image de l'entreprise en passant par des associations	**G2**	1	Maintien du risque
R16	Le concurrent nuit à l'image directement depuis le système d'information	**G2**	2	Réduction du risque

R17	Le concurrent nuit à l'image de l'entreprise au travers du prestataire informatique	**G2**	3	Réduction du risque

A partir de là, une classe de niveau de risque apparaît en fonction de ces deux paramètres.
Voici les différentes classes de niveau de risque recommandées :

NIVEAU DE RISQUE	ACCEPTABILITÉ DU RISQUE	INTITULÉ DES DÉCISIONS ET DES ACTIONS
Faible	Acceptable en l'état	Aucune action n'est à entreprendre
Moyen	Tolérable sous contrôle	Un suivi en termes de gestion du risque est à mener et des actions sont à mettre en place dans le cadre d'une amélioration continue sur le moyen et long terme
Elevé	Inacceptable	Des mesures de réduction du risque doivent impérativement être prises à court terme. Dans le cas contraire, tout ou partie de l'activité sera refusé

Chaque niveau de risque correspond à une plage du tableau ci-dessous, en fonction de la gravité et de la vraisemblance. Plus ces dernières sont élevées pour un scénario, plus celui-ci sera aura de chance d'être classé comme niveau de risque élevé.

	Avant application du PACS				
Gravité					
4	R10				
3		R8	R5, R6, R7, R9		

2	R3, R14, R15	R16	R1, R2, R11, R13, R17	R4, R12	
1					
	1	2	3	4	Vraisemblance

Les risques étant classifiés par niveau de risque, la mise en place de mesures de sécurité permettra de réduire le niveau de risque pour les plus critiques. Les niveaux de risques plus faibles ne seront pas traités en priorité. Cependant les mesures de sécurité appliquées sur les risques à niveau de risque important pourront impacter indirectement les risques plus faibles.
Ainsi, le plan d'amélioration continue de la sécurité (PACS) intégrera ces mesures.
Ce plan définie les responsables et les échéances pour chaque mesure de sécurité afin de faciliter leur mise en œuvre.

MESURE DE SÉCURITÉ	SCÉNARIOS DE RISQUES ASSOCIÉS	RESPONSABLE	FREINS ET DIFFICULTÉS DE MISE EN OEUVRE	COÛT / COMPLEXITÉ	ECHÉANCE	PRIORITÉ (max = 4)	STATUS
Pour commenter un article sur le site le client doit l'avoir acheté au moins une fois	R13,R14,R15	Equipe développement	N/A	1	1 mois	1	A lancer
Isolation informatique entre le port et le site : mise en place d'un serveur mail sécurisé pour la communication des informations	R3, R6	RSSI	Négociation des procédures avec le port	2	2 mois	3	A lancer
Sensibilisation sur la cybersécurité	R4, R5, R12, R17	RSSI	Coûts importants, en ressources financières et humaines car sensibilisation dispensée à	3	18 mois	2	A lancer

			l'extérieur de l'entreprise				
Mise en place d'une clause de confidentialité	R5, R6, R7	Equipe juridique ; RSSI	Négociation des contrats pour y intégrer la clause	1	4 mois	4	A lancer
Mise en place d'une procédure de signalement de tout incident de sécurité ayant lieu chez un prestataire	R4, R5, R7, R9, R12, R17	Equipe juridique ; RSSI	Négociation des contrats pour y intégrer la procédure de signalement d'incident	2	12 mois	3	A lancer
Politique de durcissement des mots de passe	R2, R4, R5, R8, R12, R13, R14, R15, R17	RSSI	N/A	1	1 mois	4	A lancer
PROTECTION							
Développement sécurisé (anti XSS, anti SQLI par exemple) + solutions cryptographiques + connexion (HTTPS)	R1, R2, R9, R10, R11, R16	Equipe dev / RSSI	Plan d'action à définir et valider	3	2 mois	4	A lancer
Déploiement d'une solution Anti-DDoS	R1, R11	RSSI	Comparaisons des fournisseurs de solution	3	4 mois	3	A lancer
DÉFENSE							
Surveillance renforcée des flux entrants et sortants (sonde IDS). Analyse des journaux d'événements à l'aide d'un outil	R1, R2, R3, R4, R8, R9, R10, R11, R12, R16, R17	RSSI	Achat d'un outil + licence ; budget à provisionner	2	9 mois	2	A lancer

RÉSILIENCE							
Mise en place d'une solution de backup effectué régulièrement	R1, R2, R3, R4, R10, R16, R17	RSSI	N/A	2	2 mois	4	A lancer

La construction de l’ensemble de ce tableau reprend certains éléments de l’atelier 3. En fonction du rôle de chaque mesure de sécurité, on classe les mesures par stratégie (Gouvernance, Protection, Défense, Résilience). Pour chaque mesure de sécurité est associée un ou plusieurs scénarios de risques.

Ainsi, l’évaluation des risques résiduels intervient après l’application des mesures de traitement définies dans l’étape précédente.
Chaque risque résiduel comporte un libellé basé sur le modèle suivant :
(page 76. https://www.ssi.gouv.fr/uploads/2018/10/guide-methode-ebios-risk-manager.pdf)

Voici l’ensemble des libellés des risques résiduels :

<table>
<tr><th colspan="3">RR01</th></tr>
<tr><td colspan="3">Description et analyse du risque résiduel :
==> Malgré la réduction du risque nous ne pouvons pas affirmer que la vulnérabilité ne pourra jamais être exploitée (négligence du développeur envisageable, framework vulnérable, Etc.)
- Un hacktiviste nuit au fonctionnement du site directement sur le site- Injection SQL et/ou XSS
- Framework vulnérable / erreurs humaines involontaires</td></tr>
<tr><td colspan="3">Événements redoutés concernés :
- Nuit au fonctionnement du site ; impact sur l'image
- Fuite d'informations (Credentials, Données utilisateurs)</td></tr>
<tr><td colspan="3">Mesures de traitement du risque existantes et complémentaires :
- Mise en place d'une solution de backup effectué régulièrement
- Surveillance renforcée des flux entrants et sortants (sonde IDS). Analyse des journaux d’évènements à l’aide d’un outil
- Développement sécurisé (anti XSS, anti SQLI par exemple) + solutions cryptographiques + connexion (HTTPS)</td></tr>
<tr><td colspan="3">Evaluation du risque résiduel :</td></tr>
<tr><td>Gravité initiale : 2</td><td>Vraisemblance initiale : 3</td><td>Niveau de risque initial : Moyen</td></tr>
<tr><td>Gravité résiduelle : 1</td><td>Vraisemblance résiduelle : 1</td><td>Niveau de risque résiduel : Faible</td></tr>
<tr><td colspan="3">Gestion du risque résiduel :
- MCS / MCO
- Vérification d'intégrité régulière
- Suivi des logs</td></tr>
</table>

RR02		
Description et analyse du risque résiduel : - Un hacktiviste nuit au fonctionnement du site directement sur le site via un particulier - Injection SQL et/ou XSS - Framework vulnérable / erreurs humaines involontaires / Social Engineering		
Événements redoutés concernés : - Nuit au fonctionnement dus site ; impact sur l'image - Fuite d'informations (Credentials, Données utilisateurs)		
Mesures de traitement du risque existantes et complémentaires : - Mise en place d'une solution de backup effectué régulièrement - Surveillance renforcée des flux en-trants et sortants (sonde IDS). Analyse des journaux d'évènements à l'aide d'un outil - Développement sécurisé (anti XSS, anti SQLI par exemple) + solutions cryptographiques + connexion (HTTPS) - Politique de durcissement des mots de passe		
Evaluation du risque résiduel :		
Gravité initiale : 2	Vraisemblance initiale : 3	Niveau de risque initial : Moyen
Gravité résiduelle : 1	Vraisemblance résiduelle : 2	Niveau de risque résiduel : Faible
Gestion du risque résiduel : - MCS / MCO - Vérification d'intégrité régulière - Suivi des logs		

RR04		
Description et analyse du risque résiduel : - Un hacktiviste nuit au fonctionnement du site via le prestataire informatique - Phishing , attaque sur boite mail - Social Engineering, Non respect des mesures de sécurité imposées au prestataire (signalement non respecté / non appliqué), erreurs humaines involontaires		
Événements redoutés concernés : - Vol d'informations - Perte de clients		
Mesures de traitement du risque existantes et complémentaires : - Isolation informatique entre le port et le site : mise en place d'un serveur mail sécurisé pour la communication des informations - Sensibilisation sur la cybersécurité - Mise en place d'une clause de confidentialité - Mise en place d'une procédure de signalement de tout incident de sécurité ayant lieu chez un prestataire		
Evaluation du risque résiduel :		
Gravité initiale : 3	Vraisemblance initiale : 3	Niveau de risque initial : Élevé
Gravité résiduelle : 3	Vraisemblance résiduelle : 1	Niveau de risque résiduel : Faible
Gestion du risque résiduel : - Exercice d'intrusion régulier avec le prestataire (test de la procédure de signalement)		

RR05
Description et analyse du risque résiduel : ==> Injection SQL deux cas de figure : - Usurpation d'un compte admin - Attaque direct de la BDD (Select * from user) par exemple   - Le concurrent passe par notre prestataire informatique avec l'objectif de voler des informations de nos clients - Injection SQL et/ou XSS - Non respect des mesures de sécurité imposées au prestataire (signalement non respecté / non appliqué) / Framework vulnérable / erreurs humaines involontaires / Social Engineering
Événements redoutés concernés : ==> Le concurrent connaissant nos clients, il sera en mesure de les démarcher, ce qui provoquerait une perte drastique du nombre de nos clients - Vol d'informations - Perte de clients
Mesures de traitement du risque existantes et complémentaires : - Politique de durcissement des mots de passe - Mise en place d’une procédure de signalement de tout incident de sécurité ayant lieu chez un prestataire - Mise en place d'une clause de confidentialité
Evaluation du risque résiduel :

Gravité initiale : 3	Vraisemblance initiale : 3	Niveau de risque initial : Élevé
Gravité résiduelle : 3	Vraisemblance résiduelle : 2	Niveau de risque résiduel : Moyen
Gestion du risque résiduel : - Exercice d'intrusion régulier avec le prestataire (test de la procédure de signalement)		

RR07		
Description et analyse du risque résiduel : - Partagant le même fournisseur de service de transport que notre concurrent, celui-ci peut récupérer des informations auprès d'eux - Injection SQL - Social Engineering, Non respect des mesures de sécurité imposées au prestataire (signalement non respecté / non appliqué), erreurs humaines involontaires ou volontaire (corruption)		
Événements redoutés concernés : - Vol d'informations - Perte de clients		
Mesures de traitement du risque existantes et complémentaires : - Sensibilisation sur la cybersécurité - Mise en place d'une clause de confidentialité - Mise en place d'une procédure de signalement de tout incident de sécurité ayant lieu chez un prestataire - Déploiement d'une solution Anti-DDoS		
Evaluation du risque résiduel :		
Gravité initiale : 3	Vraisemblance initiale : 3	Niveau de risque initial : Élevé
Gravité résiduelle : 3	Vraisemblance résiduelle : 2	Niveau de risque résiduel : Moyen
Gestion du risque résiduel : - Exercice d'intrusion régulier avec le prestataire (test de la procédure de signalement)		

RR08		
Description et analyse du risque résiduel : - Un concurrent vole des informations clients en usurpant le compte d'un particulier - Injection SQL et/ou XSS		
Événements redoutés concernés : - Vol d'informations - Perte de clients		
Mesures de traitement du risque existantes et complémentaires : - Politique de durcissement des mots de passe - Développement sécurisé (anti XSS, anti SQLI par exemple) + solutions cryptographiques + connexion (HTTPS) - Surveillance renforcée des flux en-trants et sortants (sonde IDS). Analyse des journaux d'évènements à l'aide d'un outil		
Evaluation du risque résiduel :		
Gravité initiale : 3	Vraisemblance initiale : 2	Niveau de risque initial : Moyen
Gravité résiduelle : 3	Vraisemblance résiduelle : 1	Niveau de risque résiduel : Faible
Gestion du risque résiduel : - N/A		

RR09		
Description et analyse du risque résiduel : - Le concurrent vole des informations clients en effectuant des actions directes sur le site - Injection SQL et/ou XSS - Framework vulnérable / erreurs humaines involontaires / Social Engineering		
Événements redoutés concernés : - Vol d'informations - Perte de clients		
Mesures de traitement du risque existantes et complémentaires : - Développement sécurisé (anti XSS, anti SQLI par exemple) + solutions cryptographiques + connexion (HTTPS) - Surveillance renforcée des flux en-trants et sortants (sonde IDS). Analyse des journaux d'évènements à l'aide d'un outil		
Evaluation du risque résiduel :		
Gravité initiale : 3	Vraisemblance initiale : 3	Niveau de risque initial : Elevé
Gravité résiduelle : 2	Vraisemblance résiduelle : 2	Niveau de risque résiduel : Faible
Gestion du risque résiduel : - MCS / MCO		

RR010		
Description et analyse du risque résiduel : - Un client effectue une opération d'altération des données d'achat directement sur le site - Injection SQL / XSS - Framework vulnérable / erreurs humaines involontaires		
Événements redoutés concernés : - Altération des données d'achats - Perte d'argent significative		
Mesures de traitement du risque existantes et complémentaires : - Développement sécurisé (anti XSS, anti SQLI par exemple) + solutions cryptographiques + connexion (HTTPS) - Surveillance renforcée des flux en-trants et sortants (sonde IDS). Analyse des journaux d'évènements à l'aide d'un outil		
Evaluation du risque résiduel :		
Gravité initiale : 4	Vraisemblance initiale : 1	Niveau de risque initial : Moyen
Gravité résiduelle : 3	Vraisemblance résiduelle : 1	Niveau de risque résiduel : Faible

Gestion du risque résiduel : - Vérification d'intégrité de la database (trigger SQL) - MCS / MCO

RR11		
Description et analyse du risque résiduel : - Un script-kiddie rend le site de e-commerce indisponible en passant directement par celui-ci - - Framework vulnérable		
Événements redoutés concernés : - Indisponibilité du site - Perte d'argent proportionnelle au temps d'indisponibilité - Perte de clients		
Mesures de traitement du risque existantes et complémentaires : - Surveillance renforcée des flux entrants et sortants (sonde IDS). Analyse des journaux d'évènements à l'aide d'un outil - Déploiement d'une solution Anti-DDoS -		
Evaluation du risque résiduel :		
Gravité initiale : 2	Vraisemblance initiale : 3	Niveau de risque initial : Moyen

Gravité résiduelle : 2	Vraisemblance résiduelle : 1	Niveau de risque résiduel : Faible
Gestion du risque résiduel : - MCS / MCO		

RR12
Description et analyse du risque résiduel : ==> Au vu des compétences d'un "script-kiddie" le service anti DDoS annule le risque - Un script-kiddie rend le site de indisponible en passant par le prestataire informatique - ExploitDB sur de nouvelles vulnérabilités non patchées - Framework vulnérable / Erreur humaine
Événements redoutés concernés : - Indisponibilité du site - Perte d'argent proportionnelle au temps d'indisponibilité - Perte de clients
Mesures de traitement du risque existantes et complémentaires : - Surveillance renforcée des flux entrants et sortants (sonde IDS). Analyse des journaux d'évènements à l'aide d'un outil - Déploiement d'une solution Anti-DDoS -

Evaluation du risque résiduel :		
Gravité initiale : 2	Vraisemblance initiale : 4	Niveau de risque initial : Elevé
Gravité résiduelle : 2	Vraisemblance résiduelle : 1	Niveau de risque résiduel : Faible
Gestion du risque résiduel : - MCS / MCO		

RR13		
Description et analyse du risque résiduel : - Le concurrent nuit à l'image en laissant des mauvais commentaires via un particulier - N/A - Erreurs humaines involontaires / Social Engineering		
Événements redoutés concernés : - Nuire à l'image - Perte de clients		
Mesures de traitement du risque existantes et complémentaires : - Pour commenter un article sur le site le particulier doit l'avoir acheté au moins une fois		
Evaluation du risque résiduel :		
Gravité initiale : 2	Vraisemblance initiale : 3	Niveau de risque initial : Moyen

Gravité résiduelle : 2	Vraisemblance résiduelle : 1	Niveau de risque résiduel : Faible
Gestion du risque résiduel : ==> Nous avions pensé à de la modération de commentaire, mais cela serait mal vue, et surtout pas éthique - N/A		

RR14		
Description et analyse du risque résiduel : - Le concurrent nuit à l'image de l'entreprise en faisant de la mauvaise pub via des entreprises nautique - N/A - Erreurs humaines involontaires / Social Engineering		
Événements redoutés concernés : - Nuire à l'image - Perte de clients		
Mesures de traitement du risque existantes et complémentaires : - Pour commenter un article sur le site l'entreprise nautique doit l'avoir acheté au moins une fois		
Evaluation du risque résiduel :		
Gravité initiale : 2	Vraisemblance initiale : 1	Niveau de risque initial : Faible

Gravité résiduelle : 2	Vraisemblance résiduelle : 1	Niveau de risque résiduel : Faible
Gestion du risque résiduel : - N/A		

RR15		
Description et analyse du risque résiduel : - Le concurrent nuit à l'image de l'entreprise en faisant de la mauvaise pub via des associations - N/A - Erreurs humaines involontaires / Social Engineering		
Événements redoutés concernés : - Nuire à l'image - Perte de clients		
Mesures de traitement du risque existantes et complémentaires : - Pour commenter un article sur le site l'association doit l'avoir acheté au moins une fois		
Evaluation du risque résiduel :		
Gravité initiale : 2	Vraisemblance initiale : 1	Niveau de risque initial : Faible

Gravité résiduelle : 2	Vraisemblance résiduelle : 1	Niveau de risque résiduel : Faible
Gestion du risque résiduel : - N/A		

RR16
Description et analyse du risque résiduel : - Le concurrent nuit à l'image directement depuis le système d'information - Injection SQL/ Faille XSS - Erreurs humaines involontaires / Social Engineering
Événements redoutés concernés : - Nuire à l'image - Perte de clients
Mesures de traitement du risque existantes et complémentaires : - Développement sécurisé - Surveillance renforcée des flux entrants et sortants (sonde IDS) - Mise en place d'une solution de backup effectué régulièrement
Evaluation du risque résiduel :

Gravité initiale : 2	Vraisemblance initiale : 2	Niveau de risque initial : Faible
Gravité résiduelle : 1	Vraisemblance résiduelle : 1	Niveau de risque résiduel : Faible
Gestion du risque résiduel : - MCO / MCS / Vérification d'intégrité régulière		

RR17
Description et analyse du risque résiduel : - Le concurrent nuit à l'image de l'entreprise au travers du prestataire informatique - Injection SQL/ Faille XSS - Erreurs humaines involontaires / Social Engineering
Événements redoutés concernés : - Nuire à l'image - Perte de clients
Mesures de traitement du risque existantes et complémentaires : - Pour commenter un article sur le site l'association doit l'avoir acheté au moins une fois - Mise en place d'une procédure de signalement de tout incident de sécurité ayant lieu chez un prestataire - Sensibilisation à la cybersécurité
Evaluation du risque résiduel :

Gravité initiale : 2	Vraisemblance initiale : 3	Niveau de risque initial : Moyen
Gravité résiduelle : 2	Vraisemblance résiduelle : 1	Niveau de risque résiduel : Faible
Gestion du risque résiduel : - MCO / MCS / Vérification d'intégrité régulière		

Les risques résiduels sont ensuite classés dans la matrice précédente. Normalement, les mesures de sécurités permettent la diminution de la gravité et de la vraisemblance pour l'ensemble des risques :

	Après application du PACS				
Gravité					
4					
3	R8, R10	R5, R7			
2	R11, R12, R13, R14, R15, R17	R9	R4		
1	R1, R16	R2			

	1	2	3	4	Vraisemblance

Comme nous pouvons le constater, les mesures de sécurité définies dans le PACS permettent de réduire drastiquement le niveau de risque pour les scénarios relevés. On remarque qu'un seul risque reste à un niveau de risque élevé malgré les mesures de sécurités mises en place. Des moyens de surveillance importants doivent être mis en place pour surveiller ce risque résiduel important.

Glossaire

Acronymes

SR	Source de risque
OV	Objectif visé
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information

Références

- « La méthode EBIOS Risk Manager ». *ANSSI*, https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/