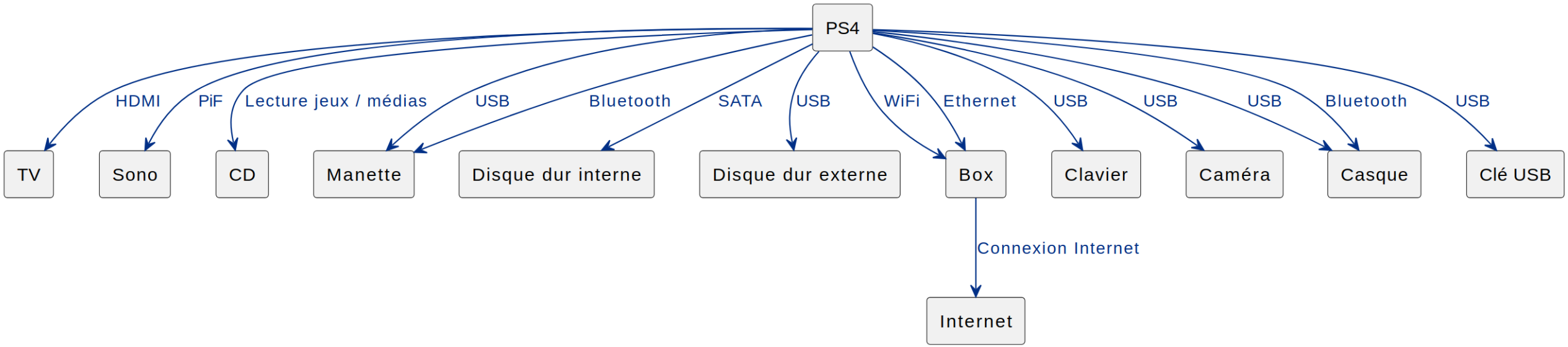
Périmètre métier et technique - Analyse EBIOS PS4 (Sony)



Chapitre 1 : Contexte – Biens et services essentiels

Valeurs Métiers	Services	Gravité	Disponibilité	Accessibilité	Intégrité
VM1	Jouer à des jeux en ligne	3/4	X	X	X
VM2	Jouer à des jeux physiques	1/4	X	X	X
VM3	Regarder des films, musique...	3/4	X	X	X
VM4	Acheter des jeux, des films...	2/4	X	X	X
VM5	Sauvegarde locale des jeux	1/4	X	X	X
VM6	Authentification (comptes, profile utilisateur)	2/4	X	X	X
VM7	Se connecter au PSN (jeu en ligne)	3/4	X	X	X
VM8	Chat vocal pour communiquer	1/4	X	X	X
VM9	Partager ses exploits	1/4	X	X	X
VM10	Accès au web	1/4	X	X	X

Valeurs Métiers	Biens	Gravité	Disponibilité	Accessibilité	Intégrité	Confidentialité
VM1	Binaire des jeux	4/4		X	X	
VM2	Firmware/OS console	4/4		X	X	
VM3	Films, musiques...	1/4		X	X	
VM4	Données bancaires	2/4				X
VM5	Avancement (conf locale)	3/4			X	
VM6	email/mdp + données utilisateurs	2/4				X
VM7	Mdp + données du compte distant	2/4				X
VM8	Liste des participants + voix	2/4		X		X
VM9	Ce que je fais et à quelle heure	2/4				X
VM10	Historique + infos confidentielles	2/4				X

Chapitre 1 : Contexte – Sources de risque/attaquants

Sources de risque	Objectifs visés	Motivation	Ressources	Activité	Pertinence
Joueurs	Jouer à des jeux non authentiques	+++	+	++	Élevée
Concurrents	Cloner la console	+	+++	+	Moyenne
Joueurs	Émuler la console originelle	++	+	+++	Moyenne
Escrocs	Vol de coordonnées bancaires	+++	+++	+++	Élevée
Concurrents	Rendre la console injouable afin de nuire à l'image de marque	+	+++	+	Faible

Chapitre 2 : Événements redoutés

ID ER	Événement redouté (description)	VM / Services concernés	Biens impactés (exemples)	Gravité (1–4)	Types d'impact
ER1	Piratage massif des jeux PS4 (possibilité de jouer à des jeux non authentiques)	VM1 Jouer en ligne, VM2 Jouer à des jeux physiques	Binaire des jeux (4/4), Firmware/OS (4/4)	**4/4**	Financier (perte de ventes), Image (perte de confiance éditeurs/joueurs)
ER2	Altération du firmware / OS rendant la console instable ou injouable	VM2 Jouer à des jeux physiques, VM1/VM7 si la console ne peut plus se connecter	Firmware/OS console (4/4)	**4/4**	Opérationnel (console inutilisable), Image, Support SAV
ER3	Compromission des données bancaires des utilisateurs	VM4 Acheter des jeux/films	Données bancaires (2/4)	**2/4**	Financier, Juridique, Image
ER4	Perte ou corruption des sauvegardes locales de jeux	VM5 Sauvegarde locale	Avancement (conf locale) (3/4)	**3/4**	Satisfaction client, Support, Fidélité
ER5	Compromission des comptes et données utilisateurs (email, mots de passe, historique, profil)	VM6 VM7 VM9 VM10	email/mdp + données utilisateurs (2/4), mdp compte distant (2/4), historique + infos confidentielles (2/4)	**3/4** (cumul des biens à 2/4)	Image, Vie privée, Juridique
ER6	Atteinte à la confidentialité des communications (chat vocal, liste de participants)	VM8 Chat vocal, VM9 Partage exploits	Liste des participants + voix (2/4), ce que je fais et à quelle heure (2/4)	**2/4**	Vie privée, Confiance dans le service
ER7	Indisponibilité significative des services en ligne (PSN, jeu en ligne, achats)	VM1 Jouer en ligne, VM3 Streaming, VM4 Achat, VM7 Connexion PSN	Services PSN, Store (gravité 3/4 côté services)	**3/4**	Financier, Image, Satisfaction client
ER8	Mise en ligne d'un émulateur permettant de se substituer à la console	VM1 Jouer en ligne, VM2 Jouer à des jeux physiques	Binaire des jeux (4/4), Firmware/OS (4/4)	**4/4**	Financier (perte de ventes), Image (perte de confiance éditeurs/joueurs)

Chapitre 3 : Scénarios de menace

ID Scénario	Source de risque	ER ciblé	Description du scénario	Probabilité
SM1	Joueurs – jouer à des jeux non authentiques	ER1 (piratage des jeux)	Un joueur suit un tutoriel (forum / YouTube) pour exploiter une faille du firmware, installer un custom firmware et lancer des jeux non authentiques.	+++ Élevée
SM2	Joueurs – émuler la console originelle	ER1/ER8	Des communautés d'émulation analysent les binaires et le firmware pour développer un émulateur PS4 sur PC, permettant de lancer des jeux sans console.	++ Moyenne
SM3	Escrocs – vol de coordonnées bancaires	ER3 (données bancaires)	Des cybercriminels mettent en place des pages de phishing imitant le PS Store / PSN pour récupérer les identifiants et données CB des joueurs.	+++ Élevée
SM4	Escrocs – vol de comptes PSN / données utilisateur	ER5 (compte et données)	Attaques par phishing, récupération de mots de passe réutilisés, puis accès aux comptes PSN (e-mail/mdp) et historique.	++ Moyenne
SM5	Concurrents – cloner partiellement la console	ER1 / ER2	Un concurrent analyse la console (reverse engineering) pour reproduire certaines fonctions matérielles/logicielles ou contourner des protections.	+ Faible
SM6	Concurrents – rendre la console injouable pour nuire à l'image	ER2 / ER7	Hypothèse de sabotage (exemple théorique) via exploitation de vulnérabilités ou campagnes de désinformation sur la stabilité de la console.	+ Faible

Chapitre 4 : Risques (cotation)

Ici on combine :

Impact (gravité de l'ER) × *Probabilité* (scénario)
et on classe en : Faible / Moyen / Élevé / Critique.

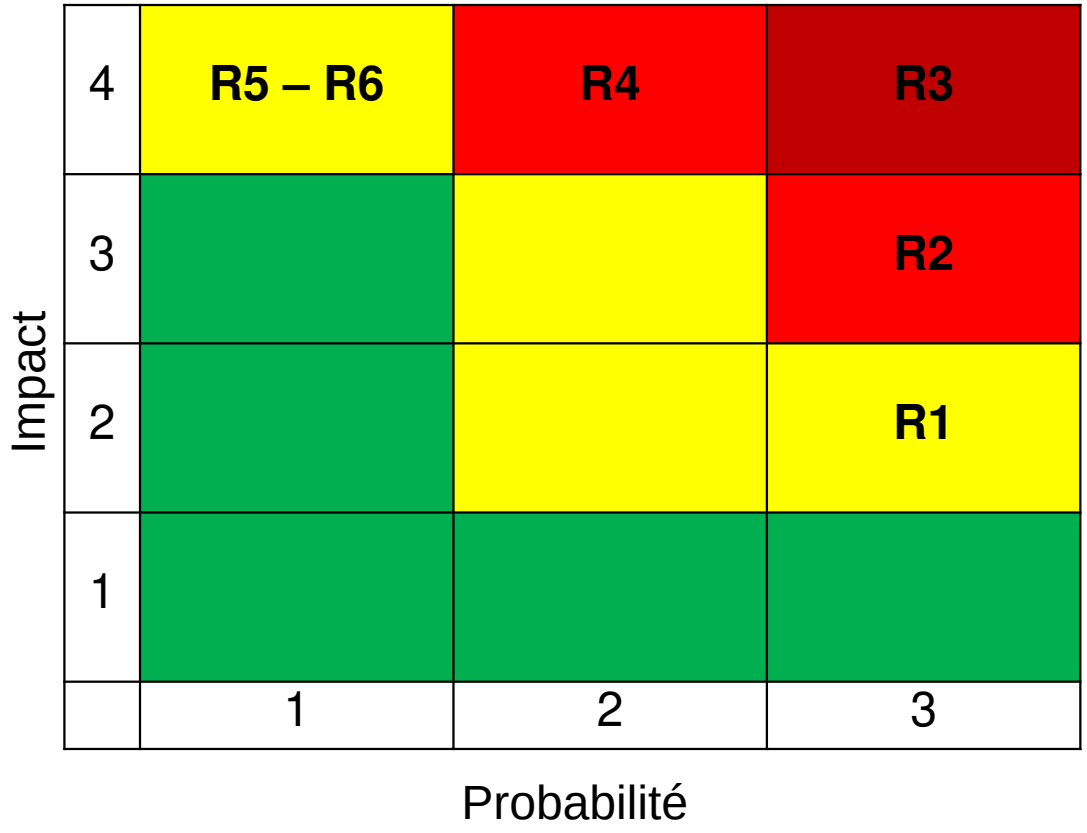
On définit l'échelle suivante :

1–3 : Faible

4–6 : Moyen

7–9 : Élevé

10–12 : Critique



Chapitre 4 : Risques – Cotation des risques

ID Risque	Scénario	ER associé	Impact (1–4)	Probabilité (1–3)	Score (I×P)	Niveau
R1	SM3 – Phishing CB	ER3 – Compromission données bancaires	2	3	6	**Moyen à élevé** (surtout sensible image/juridique)
R2	SM4 – Vol de comptes PSN	ER5 – Compromission comptes et données	3	3	9	**Élevé**
R3	SM1 – Custom firmware / jeux non authentiques	ER1 – Piratage massif des jeux	4	3	12	**Critique** (risque économique majeur)
R4	SM2 – Émulation PS4	ER1 / ER8	4	2	8	**Élevé** (impact fort mais mise en œuvre plus complexe)
R5	SM5 – Clonage par concurrents	ER1 / ER2	4	1	4	**Moyen**
R6	SM6 – Sabotage par concurrents	ER2 / ER7	4	1	4	**Moyen** (scénario peu probable mais impact fort)

Chapitre 5 : Mesures de sécurité

Risque prioritaire	Objectif de sécurité	Mesures de sécurité (exemples)	Type
R3 – Piratage des jeux (custom firmware, jeux non authentiques)	Protéger l'intégrité des jeux et du firmware	Secure boot, signature numérique obligatoire des binaires, vérification d'intégrité du firmware, chiffrement des partitions sensibles, mises à jour régulières pour corriger les failles exploitées	Prévention
		Monitoring des consoles détectées non conformes, mécanisme de bannissement de compte/console, détection d'anomalies côté PSN	Détection / Réaction
R2 – Vol de comptes PSN	Protéger l'authentification et les données utilisateur	Authentification renforcée (2FA), détection de connexions suspectes, limitation des tentatives de login, sensibilisation des joueurs aux risques de phishing	Prévention
		Alertes utilisateur en cas de connexion depuis un nouvel appareil / pays, mécanisme simple de récupération de compte	Détection / Réaction
R4 – Émulation PS4	Limiter le reverse engineering et la facilité d'émulation	Durcissement du firmware, vérification matérielle (présence de composants spécifiques), protocoles propriétaires entre console et PSN	Prévention
R1 – Vol de données bancaires	Protéger la confidentialité des paiements	Paiement via prestataires conformes PCI-DSS, tokenisation des cartes, chiffrement fort des canaux, aucune conservation locale des données CB sur la PS4	Prévention
		Systèmes de détection de fraude, alerte et blocage en cas de comportements anormaux	Détection / Réaction

Chapitre 5 : Mesures de sécurité

VM critique	**Risques couverts**	**Mesures clés**
VM1 Jouer à des jeux en ligne	R3, R4, R7	Intégrité des jeux, disponibilité PSN, mise à jour régulière
VM4 Acheter des jeux/films	R1, R2	Sécurisation des paiements, protection des comptes
VM6/VM7 Authentification & compte distant	R2	2FA, politiques de mots de passe, surveillance des connexions