Analyse de risque – EBIOS RM

Equipe: Quentin Poidevin; Fourgeron Robin; Arrar Rania; Mora Florian

Matrices de Gravité, de Vraisemblance et d'Impact

1. Échelle de Gravité

Niveau	Gravité	Définition
G1	Faible	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).
G2	Significatif	Dégradation des performances de l'activité sans impacts sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé)[3].
G3	Important	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)[4].
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)[5].

2. Échelle de Vraisemblance

Niveau	Vraisemblance	Définition
V1	Peu Probable	Le scénario a peu de chances de se réaliser. Les vul[14]nérabilités sont soit marginales, soit l'attaquant manque de ressources, de temps ou d'informations suffisantes. Ce scénario nécessite un alignement spécifique de circonstances peu fréquentes[15].
V2	Assez Probable	La source de risque a des chances significatives de réussir, mais certains obstacles ou conditions rendent le scénario moins immédiat. La réalisation dépend de facteurs comme la précision des informations de l'attaquant ou la mise en œuvre correcte de l'exploitation[16].
V3	Très Probable	Il y a de fortes chances que la source de risque réussisse à atteindre son objectif. Les modes opératoires identifiés sont réalistes et fréquemment observés dans des contextes similaires. La cible présente une combinaison inquiétante de vulnérabilités et d'attractivité[17].
V4	Pratiquement Certain	La probabilité que la source de risque atteigne son objectif est extrêmement élevée, presque inévitable. Cela peut être dû à une vulnérabilité critique déjà exploitée dans des scénarios similaires ou à une faille majeure bien connue de l'écosystème. La menace est claire et imminente[18].

Equipe: Quentin Poidevin; Fourgeron Robin; Arrar Rania; Mora Florian

Atelier 1 – Cadrage et socle de sécurité

Objectifs de l'étude

- Identifier les risques liés au traitement d'informations classifiées.
- Déterminer les scénarios d'attaque pertinents.
- Établir des mesures de réduction du risque pour atteindre un niveau acceptable compatible avec l'homologation.
- Produire des livrables exploitables pour le dossier d'homologation.

Période considérée

Période stratégique couvrant la **durée du contrat RUE (3ans)** , les échanges d'information et la conservation des données classifiées

A. Périmètre de l'étude

Participants

- **Direction/Décideur :** M. Durand (Dirigeant)
- **Auditeur d'analyse de risque** : M. Poidevin, M. Mora, M. Fougeron, Mme. Arar

Contexte général :

La société Xspace, PME de 30 salariés basée à Paris, est en plein essor et vient de contracter avec le ministère de la défense tchèque. Ce contrat implique la manipulation d'informations classifiées (Diffusion Restreinte / RUE) et nécessite des échanges sécurisés. Le budget alloué à la sécurisation du SI classifié est restreint (< 50 k€).

A.1 Périmètre organisationnel

Entreprise : Xspace, PME française de 30 salariés
Contrat : Ministère de la Défense tchèque – échanges d'informations classifiées RUE
Équipe projet : 10 salariés dédiés au contrat, déplacements possibles en République Tchèque

A.2 Périmètre technique

L'étude porte sur le **SI dédié à la gestion et au traitement d'informations classifiées RUE**, hébergé dans les locaux Xspace, sans interconnexion Internet directe.
Éléments inclus :

- 10 PC utilisateurs dédiés au contrat, interconnecté
- 2 PC de déplacement (durcissement renforcé)
- VLAN utilisateurs séparés, switch L2 isolé
- Services centralisés internes :
    - AD-Admin, AD-Log

    - Serveur de fichiers / VM Files
    - PKI interne pour la gestion des clés
    - Serveur de redondance
- PC de mise à jour isolé
- Pc de chiffrement / déchiffrement isolé
- Station blanche d'analyse amont USB
- Routeur/Firewall (hors Internet sauf usage « mise à jour »)
- Local serveur sécurisé
- Salle Kanal (traitement classifié et renforcé voir DAT)

Exclusions Justifiées

- SI classique non classifié de l'entreprise (pour réduire le périmètre et éviter les connexions non maîtrisées)
- systèmes personnels, BYOD
- accès Internet utilisateurs (incompatible exigences RUE)
- Service de surveillance (Caméras)

Justification
Réduire le périmètre diminue l'exposition, les coûts, et simplifie l'homologation. Inclusion stricte des équipements manipulant ou contenant de l'information classifiée.

B. Définir le périmètre métier et technique

B.1 Objectif général

Permettre à Xspace de **produire, échanger, stocker et transmettre des informations classifiées RUE** avec le Ministère de la Défense tchèque en conformité avec les exigences de sécurité européennes (« crypto UE », matériel qualifié).

Mission et activités concernées

Activités couvertes :

- Production, traitement et stockage d'informations classifiées RUE.
- Rédaction de documents classifiés (Salle Kanal).
- Gestion des identités et habilitations project.
- Transfert sécurisé de mise à jour via Station Blanche.
- Déplacements avec matériels classifiés.

Valeurs métier identifiées

Valeur métier	Type	Description
Informations classifiées RUE	Information	Documents, plans, échanges contractuels classifiés.
Clés cryptographiques (PKI interne)	Information	Clés de chiffrement, signature, authentification.
Produits livrables	Information	Notes, rapports, études, plans
Habilitations et identités	Information	Droits d'accès
Poste mission	Actif support	Poste dédié au projet, utilisé y compris en mobilité.

Justification : Toute atteinte à la confidentialité affecte directement la relation étatique et peut entraîner une perte de contrat ou des sanctions.

Biens supports

Bien support	**Type**	**Rôle**
PC utilisateurs (10)	Poste de travail	Création et consultation d'informations RUE
PC mission	Poste durci	Transport en déplacement
Serveur AD-Admin	Serveur	Contrôle d'accès
Serveur AD-Log	Serveur	Centralisation journaux
Serveur de fichiers + VM	Serveur	Stockage sécurisé
PKI interne	Serveur	Gestion des clés
Switch L2	Réseau	VLAN isolés
Routeur/Firewall	Réseau	Accès unique pour MAJ
PC Mise à jour	Poste isolé	Télécharger les MAJ
Station Blanche	Poste durci	Contrôle média USB
Salle Kanal	Physique	Traitement classifié
Local serveur badge	Physique	Hébergement serveurs

C. Identifier les événements redoutés

Liste des événements redoutés au niveau stratégique

ID	Événement redouté	Description	Disponibilité	Intégrité	Confidentialité	Traçabilité
ER01	Divulgation d'information RUE	Fuite ou accès non autorisé via PC, clé USB, perte ou échange non protégé.	**Significatif** : l'activité peut continuer, mais le contenu divulgué compromet le projet à moyen terme.	**Important** : une fuite peut entraîner une manipulation ultérieure du contenu non détectée.	**Critique** : information classifiée révélée à des personnes non autorisées.	**Important** : traçabilité nécessaire pour identifier la source de la fuite.
ER02	Altération d'un document classifié	Modification non détectée d'un livrable classifié.	**Significatif** : le travail continue, mais sur la base d'informations fausses.	**Important** : l'intégrité est l'enjeu principal car les décisions reposent sur des données exactes.	**Important** : modification pouvant masquer ou divulguer des données sensibles.	**Significatif** : des traces sont utiles pour détecter l'altération, mais pas toujours immédiates.
ER03	Perte des données classifiées	Suppression, corruption ou perte de données stoppant le projet.	**Important** : l'indisponibilité empêche la production des livrables.	**Significatif** : l'intégrité est menacée par la perte, mais elle n'est pas l'objectif principal de l'attaque.	**Important** : perte pouvant aussi entraîner une violation indirecte de confidentialité selon le contexte.	**Significatif** : des logs permettent de comprendre la cause, mais pas toujours de récupérer les données.
ER04	Compromission des clés cryptographiques	Extraction ou usage illégitime des clés de chiffrement PKI.	**Significatif** : l'activité continue, mais les échanges deviennent non fiables.	**Critique** : la falsification de signatures et données rend tout résultat non fiable.	**Critique** : accès complet au chiffrement, permettant la lecture des données classifiées.	**Important** : journaux essentiels pour prouver l'origine et le moment de la compromission.
ER05	Perte ou vol du PC mission	Perte physique du PC en mobilité contenant des données sensibles.	**Significatif** : impact limité si des copies existent sur les serveurs internes.	**Significatif** : l'intégrité des données locales peut être affectée, mais peut être restaurée depuis le serveur.	**Important** : risque élevé de fuite des données locales embarquées sur le PC.	**Significatif** : traces partielles, difficulté à retracer l'usage du PC après le vol.
ER06	Absence de traces exploitables	Logs incomplets ou altérés empêchant les enquêtes et la preuve.	**Faible** : le service continue à fonctionner techniquement.	**Significatif** : l'intégrité du système d'enregistrement peut être compromise.	**Faible** : absence de logs ne provoque pas directement une fuite.	**Critique** : impossibilité de prouver les actions et d'investiguer un incident.
ER07	Incapacité de produire les livrables	Indisponibilité serveurs/outils empêchant la livraison contractuelle.	**Important** : l'arrêt de la production empêche l'exécution contractuelle.	**Significatif** : intégrité des données n'est pas forcément affectée, mais les livrables ne sont pas accessibles.	**Significatif** : pas de fuite directe, mais risque secondaire selon les causes de l'incident.	**Significatif** : traçabilité utile pour comprendre l'origine de l'incident.

Justification stratégique

Les impacts dominants sont liés à la **confidentialité**, puis à la **traçabilité**, et à la **disponibilité**.

D. Déterminer et évaluer le socle de sécurité

Socle de sécurité existant

Thématique	Référentiel / Politique de Sécurité	État d'Application	Écart Constaté (Faiblesse)	Justification / Mesures Compensatoires
1. Réglementaire & Physique	**IGI 1300 / II 901** *(Protection du secret de la défense nationale)*	**Partiel**	La salle "KANAL" est renforcée mais ne dispose pas d'une certification "Zone Protégée" complète (coût infrastructure > budget).	**Compensation Organisationnelle :** • Contrôle d'accès strict (Badge + Code) • Registre papier des entrées/sorties. • Interdiction formelle des smartphones en salle (Casiers à l'entrée).
2. Gestion des Supports (USB)	**PSSI – Politique de Gestion des Supports Amovibles** *(Réf : Note ANSSI Station Blanche)*	**À renforcer**	Le transfert de données (Mises à jour/Livrables) repose entièrement sur des clés USB, vecteur d'attaque majeur pour les réseaux isolés (Air-Gap).	**Mesure Technique & Procédurale :** • Usage obligatoire de la Station Blanche pour décontamination (scan antivirus) avant toute connexion au réseau. • Ports USB des PC utilisateurs bloqués physiquement ou logiquement (sauf clavier/souris). • Utilisation exclusive de clés USB identifiées et chiffrées par l'entreprise.
3. Nomadisme (Missions)	**Guide ANSSI "Partir en mission" / PSSI Nomadisme**	**Non Appliqué**	Les 10 collaborateurs partent en République Tchèque avec des "PC Mission" contenant des données sensibles, sans procédure de retour stricte.	**Mesure de Durcissement :** • Disque dur chiffré intégralement (BitLocker avec TPM). • Filtre écran obligatoire en déplacement. • Procédure de "Quarantaine" au retour : le PC est considéré compromis et doit être formaté/réinstallé avant de toucher le réseau interne.
4. Authentification & Crypto	**RGS (Référentiel Général de Sécurité) / Qualifié UE**	**Appliqué**	Les mots de passe seuls sont insuffisants pour l'accès aux données RUE.	**Mesure Technique :** • Authentification à double facteur (MFA) via clé matérielle (ex: YubiKey/Token qualifié ANSSI/UE) pour l'ouverture de session. • Certificats stockés sur carte à puce/token, pas sur le disque.
5. Cloisonnement Réseau	**Architecture de Défense en Profondeur** *(Ségrégation Admin/Utilisateur)*	**Partiel**	L'architecture repose sur des VLANs (Admin / Utilisateur / Serveur) sur un même commutateur (Switch) physique, faute de budget pour des équipements séparés.	**Mesure Technique :** • Configuration stricte des ACLs (Access Control Lists) sur le switch. • Administration des serveurs uniquement depuis la VM dédiée "Service Admin" (saut de bastion)
6. Maintien en Condition de Sécurité	**Guide d'Hygiène Informatique (ANSSI)** *(Gestion des mises à jour)*	**Difficile**	Absence de connexion Internet directe pour les mises à jour (Windows/Antivirus). Le parc risque de devenir obsolète rapidement.	**Mesure Procédurale :** • Mise en place d'un serveur WSUS Offline (Déconnecté). • Processus mensuel : Téléchargement des patchs sur PC Internet (Zone Jaune) -> Scan Station Blanche -> Import sur Serveur WSUS interne.
7. Gestion des Incidents	**Procédure de Réaction aux Incidents**	**Inexistant**	Aucune chaîne d'alerte définie en cas de perte de PC en mission ou de détection de virus sur une clé USB.	**Mesure Organisationnelle :** • Nomination d'un référent sécurité joignable 24/7. • Fiche réflexe "Perte de matériel" distribuée aux voyageurs (qui appeler, que déclarer).

Atelier 2 – Source de risque

Equipe: Quentin Poidevin; Fourgeron Robin; Arrar Rania; Mora Florian

A. IDENTIFIER LES SOURCES DE RISQUE ET LES OBJECTIFS VISÉS

SR

Catégorie	Exemple objectifs
États hostiles	espionnage, sabotage
Cybercriminels	ransomware, vol de données
Hacktivistes	DDoS, fuite
Employées	sabotage, fuite
Erreurs humaines	mauvaise config
Défaillances techniques	panne, obsolescence
Supply chain	composants compromis
Intrusions physiques	vol, espionnage
Catastrophes naturelles	destruction, arrêt
Perte de PC	Vol de données
Concurrent industriel	Vol de données

OV

Objectifs visés	Description
espionnage, sabotage	Espionnage des plans confidentiel, sabotages du matériel
ransomware, vol de données	Compromission des ordinateurs/serveurs, impossibilité de travailler
DDoS, fuite	Saturation des serveurs, impossibilité de travailler, vol de données confidentiel
sabotage, fuite	Sabotage du matériel
mauvaise config	Faille qui peut potentiellement être exploitées par un attaquant
panne, obsolescence	Matériel qui tombe en panne
composants compromis	Implique de l'espionnage, ou shutdown du matériel
vol, espionnage	Vol de données et autre documents confidentiels
destruction, arrêt	Destruction des matériaux serveurs/ordinateurs, implique perte de données
Vol de données	Vol de données confidentiels

B ÉVALUER LES COUPLES SR/OV

SR	OV	Motivation	Ressource	Pertinence du couple SR/OV	Vraisemblance du couple SR/OV	Retenu	Justification si non retenu
États hostiles	espionnage, sabotage	Avantage technologique	Très élevé	G4 - Critique	V4 – Pratiquement Certain	Oui	
Cybercriminels	ransomware, vol de données	Financier	élevé	G3 - important	V3 – Très probable	Oui	
Hacktivistes	DDoS, fuite	Promouvoir une cause idéologique	faible	G1- Mineur	V2 – Assez probable	Non	Peu probable et pas assez de moyen
Employées	sabotage, fuite	Motivation personnelle	moyen	G2 - Significatif	V2 – Assez probable	Oui	
Erreurs humaines	mauvaise config	Manque de formation ...	moyen	G2 - Significatif	V2 – Assez probable	Oui	
Défaillances techniques	panne, obsolescence	Manque de planification/budget	moyen	G2 - Significatif	V2 – Assez probable	Oui	
Supply chain	composants compromis	Très divers	moyen	G2 - Significatif	V1 – Peu probable	Non	Peu probable, très peu de matériaux
Intrusions physiques	vol, espionnage	faible	faible	G1- Mineur	V1 – Peu probable	Non	Très peu de personnel et environnement sécure
Catastrophes naturelles	destruction, arrêt	Absence de contrôle sur l'événement	faible	G1- Mineur	V1 – Peu probable	Non	Très peu probable
Pertes de PC	Vol de données	Aléatoires	moyen	G2 - Significatif	V2 – Assez probable	Oui	
Concurrent industriel	Espionnage, sabotage	Avantages technologiques	élevé	G3 - important	V3 – Assez probable	Oui	

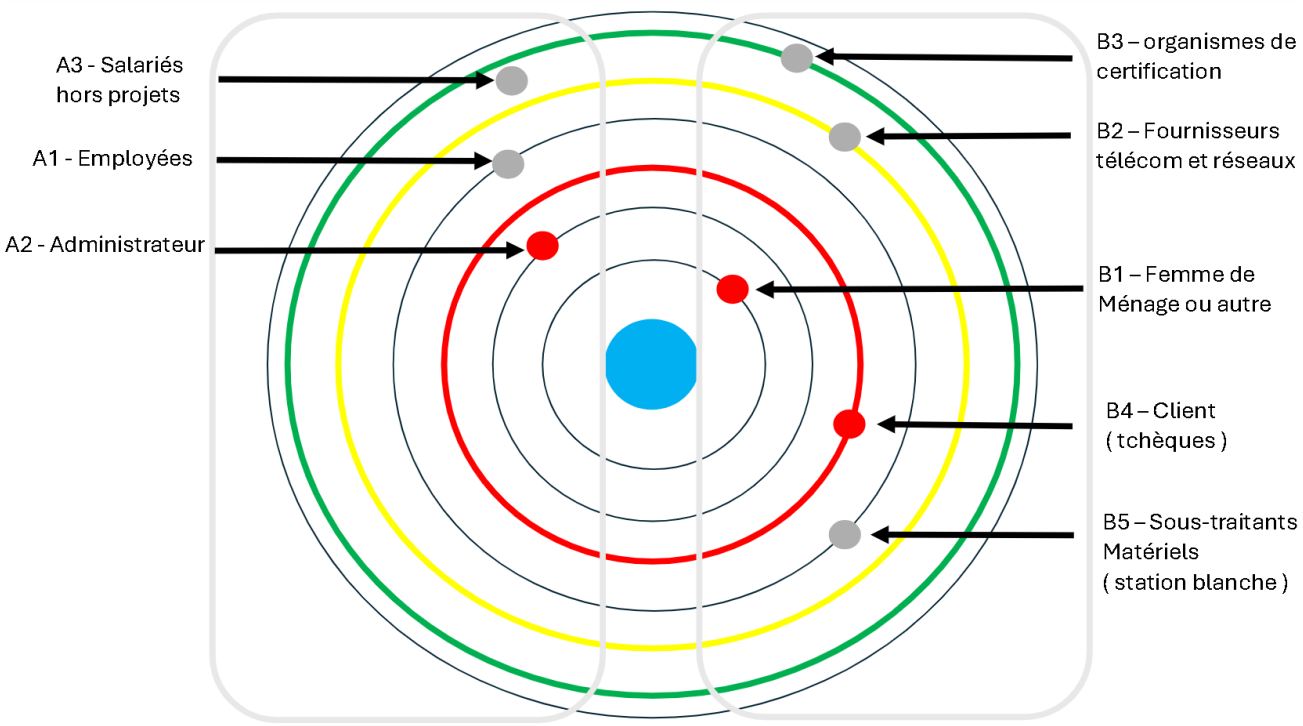
C. Sélectionner les couples SR/OV

SR	OV	Justification de la sélection
États hostiles	espionnage, sabotage	Secteur aérospatiale très sensible et prisé
Cybercriminels	ransomware, vol de données	Secteur très sensible, prisé et avec moyen
Employées	sabotage, fuite	Danger constant
Erreurs humaines	mauvaise config	Danger constant
Défaillances techniques	panne, obsolescence	Toujours présent, à surveiller
Pertes de PC	Vol de données	Déplacement récurent à l'étranger
Concurrent industriel	Espionnage, sabotage	Secteur aérospatiale très sensible et prisé

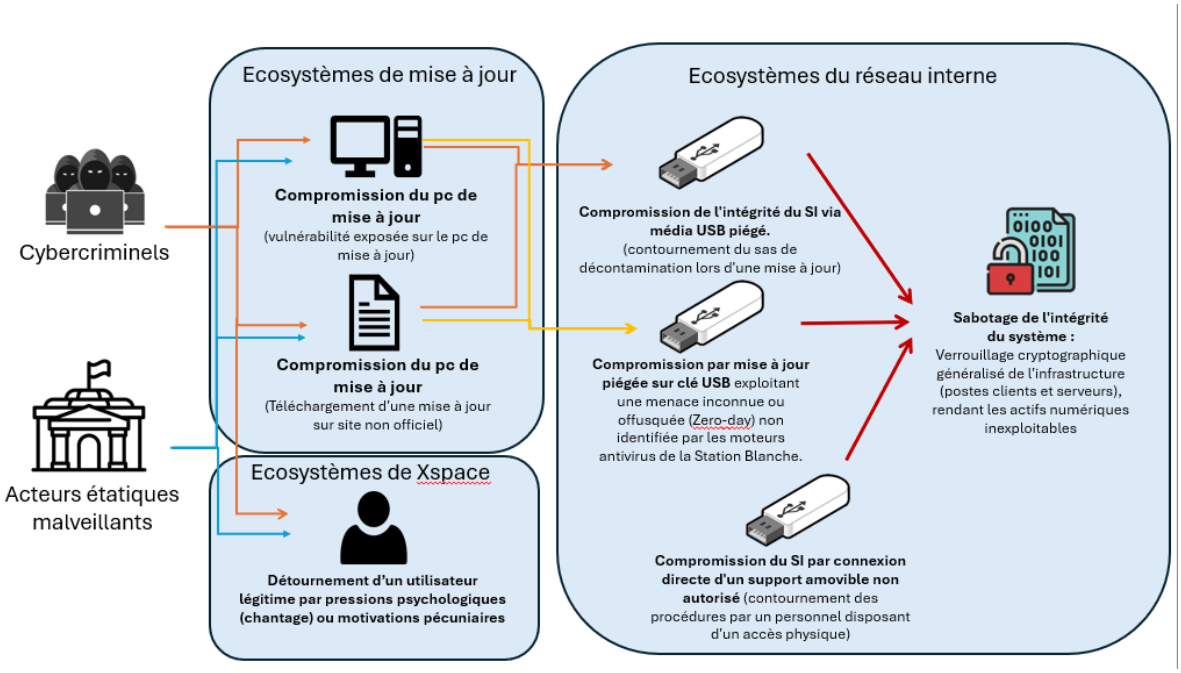
Atelier 3- Scénario stratégiques

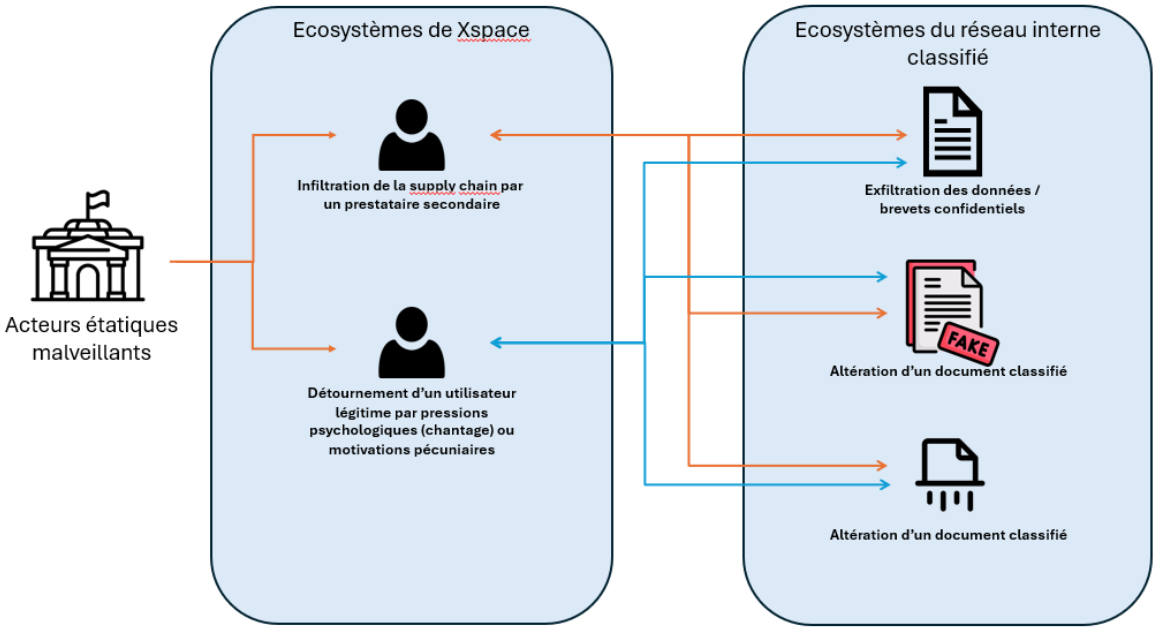
A – Construire la cartographie de dangerosité de l'écosystème et identifier les parties prenantes

CATEGORIE	PARTIE PRENANTE
Partie prenantes internes	A1 - Employées (patron , salariés)
	A2 - Administrateur
	A3 - Salariés hors projets
Partie prenantes externes	B1 - Femme de ménage ou autre
	B2 - Fournisseurs télécom et réseaux
	B3 - Organismes de certification/audit
	B4 - Client (tchèques)
	B5 - Sous-traitants matériels (Station blanche)



B – Elaborer des scénarios stratégiques





C- Définir des mesures de sécurité sur l'écosystème

Totalités des meusure de sécurité sur l'ecosysteme :

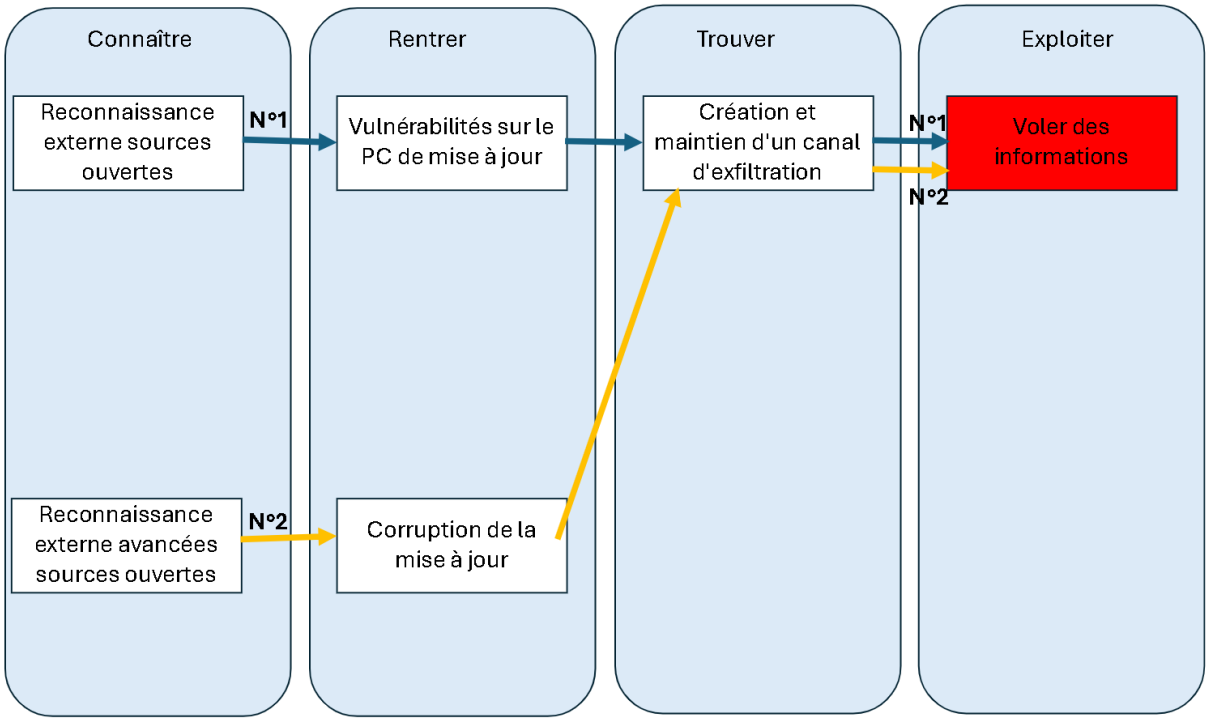
ID	PARTIE PRENANTE	CHEMINS D'ATTAQUE	STRATÉGIQUES	MESURES DE SÉCURITÉ	GRAVITE	VRAISEMBLANCE	MENACE INITIALE	MENACE RÉSIDUELLE
R1	Prestataire secondaire / Supply-chain	Exfiltration via transfert physique	Espionnage ciblé sur le projet (S1)	Qualification prestataires, traçabilité documentaire, double validation, verrouillage physique des supports	4	2	3	1,5
R2	Base documentaire / SI	Introduction de documents modifiés	Sabotage indirect par manipulation de données (S2)	Signature numérique, hashing, workflow figé, double validation	3	1	2	1,2
R3	Employé ciblé / Insider	Copie ou destruction de fichiers sensibles	Recrutement d'un insider (S3)	ACL strictes, séparation comptes admin/user, SIEM interne, rotation tâches, binôme obligatoire	4	1	2,5	1,4
R4	Station blanche / Clé USB	Ransomware via clé USB "oubliée"	Infection via clé USB (S4)	Scan multi-antivirus, sandbox, hashing, contrôle physique USB, double validation	4	2	3	1,3
R5	Station hors ligne / SI	Vol de fichiers sensibles pour rançon	Extorsion sur données volées (S5)	Air-gap, chiffrement, logs immuables, Ubikey, contrôle impression	3	2	2,5	1,2
R6	Prestataire logistique / transport physique	Infection via système du transporteur	Compromission du prestataire logistique (S6)	Qualification prestataire, contrôle supports, hashing, traçabilité	3	1	2	1,4
R7	Sous-traitant / Hacktivistes	Publication de documents sensibles	Dénonciation par fuite externe (S7)	NDA renforcés, contrôle accès, traçabilité, watermark impression	4	2	3	1,3
R8	Systèmes externes (portail RH, emails)	DDoS ou paralysie administrative	Perturbation par attaque sur systèmes externes (S8)	Segmentation réseau, monitoring, plan continuité activité	2	1	1,5	1,2
R9	Employé malveillant	Modification discrète de plans	Sabotage documentaire (S9)	ACL strictes, validation croisée, SIEM, binôme obligatoire	3	2	2,5	1,5
R10	Employé malveillant	Copie sur clé USB personnelle	Extraction de documents sur support physique (S10)	USB chiffrés, contrôle physique, logs transfert, traçabilité	3	2	2,5	1,3
R11	Technicien / sauvegardes	Suppression de sauvegardes incrémentales	Sabotage des sauvegardes (S11)	Sauvegardes immuables hors ligne, air-gap, procédures restauration testées	3	1	2	1,2
R12	Prestataire / serveur isolé	Configuration erronée partage réseau	Mauvaise configuration de serveur isolé (S12)	ACL strictes, revue configuration, tests pré-intégration	1	2	1,5	1,3
R13	Technicien / support USB	Support sensible mal manipulé	Mauvaise manipulation de support sensible (S13)	Support chiffré, scellé, traçabilité, contrôle physique	2	1	1,5	1,2
R14	Poste de mise à jour	Déploiement erroné de mise à jour offline	Déploiement erroné d'une mise à jour (S14)	Sandbox, hash, double validation, test pré-intégration	3	1	2	1,3
R15	Serveur fichiers	Panne majeure	Panne majeure du serveur fichiers (S15)	Redondance, sauvegardes immuables, procédures restauration	2	1	1,5	1,5
R16	Logiciel obsolète / postes isolés	Exploitation faille connue	Obsolescence d'un logiciel sur postes isolés (S16)	Mises à jour testées, limitation interface USB, audit sécurité	2	2	2	1,3
R17	Fournisseur matériel	Composants infectés via firmware	Composants infectés (S17)	Qualification fournisseur, tests firmware, hashing, contrôle transfert	2	1	1,5	1,4
R18	Bureau d'études externe	Documents altérés volontairement	Altération de documents techniques (S18)	Validation croisée, signature interne, double contrôle	2	1	1,5	1,2
R19	Locaux étrangers / supports	Vol physique de clé USB	Vol physique de support (S19)	Contrôle d'accès, verrouillage, traçabilité supports	3	2	2,5	1,2
R20	Poste isolé	Installation de keylogger matériel	Installation de matériel d'écoute (S20)	Surveillance physique, contrôle périodique, scellés	3	1	2	1,2
R21	Site étranger / matériel isolé	Inondation site	Inondation du site à l'étranger (S21)	Plan continuité, sauvegardes hors site, redondance	3	1	2	1,5
R22	Local technique	Incendie	Feu localisé (S22)	Détection incendie, extincteurs, sauvegardes hors site	4	1	2,5	1,3
R23	Laptop hors site	Vol de laptop	Perte d'un laptop avec documentation (S23)	Chiffrement matériel, Ubikey, verrouillage, traçabilité	3	2	2,5	1,2
R24	Transport de support	Perte de clé USB	Support perdu durant transport (S24)	Support chiffré, scellé, journalisation transfert	3	2	2,5	1,2
R25	Salarié approché par concurrent	Vente d'informations	Achats d'informations par concurrent (S25)	NDA, sensibilisation, ACL, suivi SIEM	4	2	3	1,3
R26	Prestataire influencé par concurrent	Retard volontaire / sabotage indirect	Sabotage indirect via sous-traitant (S26)	Qualification prestataire, contrôle livraison, journalisation, audits	3	2	2,5	1,4

Mesure par rapport aux dangerosités de l'écosystème :

ID	PARTIE PRENANTE	CHEMINS D'ATTAQUE	STRATÉGIQUES	MESURES DE SÉCURITÉ	GRAVITE	VRAISEMBLANCE	MENACE INITIALE	MENACE RÉSIDUELLE
R27	Administrateur / opérateur mise à jour	Diffusion involontaire d'une mise à jour compromise ou non sécurisée	Introduction d'un ransomware par mise à jour (involontaire)	Validation automatisée des mises à jour (hash, signature, provenance), station blanche avec sandbox, workflow 4-eyes, monitoring post-déploiement, logs immuables, plan de restauration testé	4	3	3,5	1,3
R28	Prestataire nettoyage (accès opportuniste)	Branche une clé USB si accès ouvert par erreur	Infection par clé USB lors d'un accès furtif	Interdiction totale du nettoyage pendant les heures d'accès, **badge blacklisté sur la salle, sas sécurisé, fermeture automatique des portes, capteurs d'ouverture + alarme immédiate, cache-ports physiquement verrouillés, screensaver instantané + cable lock, patrouilles SSI, traitement des rebuts (aucun poste laissé alimenté)**	4	3	3,5	0,5
R29	Employé mécontent (accès local autorisé)	Branche une clé USB personnelle sur un poste isolé	Infection par malware/ransomware pour bloquer la production	**Blocage matériel des ports USB, station blanche dédiée aux supports, poste scellé (tamper-evident), accès sous supervision (caméra + 4-eyes), audits d'intégrité du BIOS/UEFI, traçabilité forte des actions, suppression des privilèges locaux, contrôle comportemental EDR offline, politique disciplinaire appliquée**	**4**	**3**	3,5	0,5

Atelier 4- Scénario opérationnels

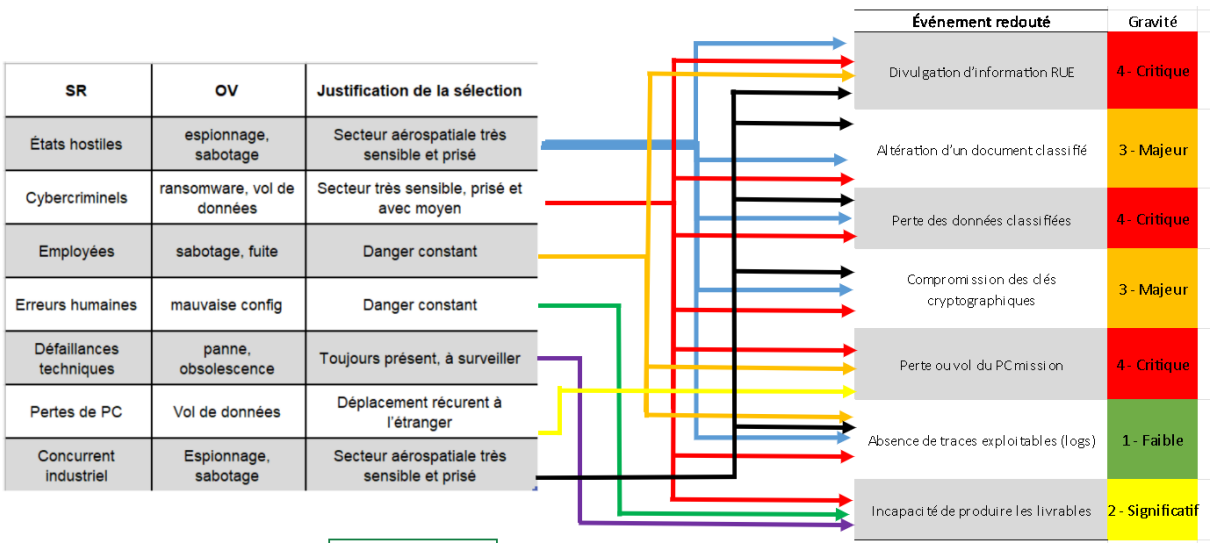
A – Elaborer les scénarios opérationnels



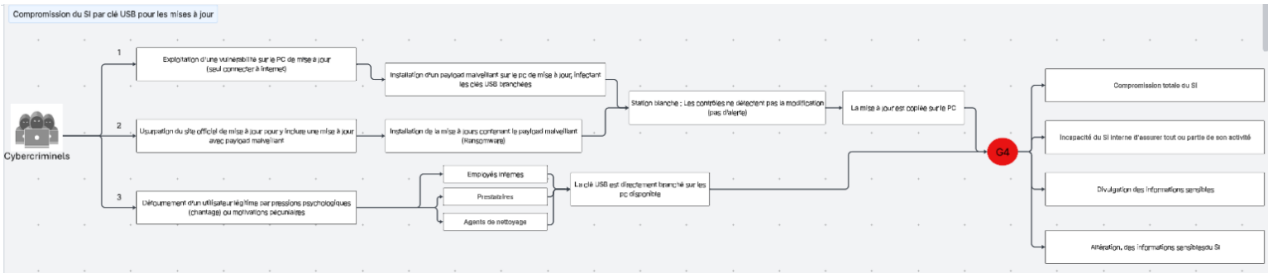
Scénario	Probabilité de succès	Difficulté technique	Vraisemblance (selon la matrice)
Scénario 1	3	3	Elevée (3)
Scénario 2	2	2	Moyenne (2)

B – Evaluer la vraisemblance des scénarios opérationnels

Gravité					
	4 - Critique	R3 - R22	R1 – R4 – R7 - R25	R27 – R28 - R29	
	3 - importance	R2 – R6 – R11 – R14 – R20 – R21	R5 – R9 – R10 – R19 – R23 – R24 - R26		
	2 - Significatif	R8 – R13 – R15 – R17 - R18	R16		
	1 - Faible		R12		
		1 – Peu probable	2 - probable	3 - Très probable	4 - Quasi certain
		Vraisemblance			



Scénarios Opérationnelle (Compromission d'un SI par installation de payload malveillant) :



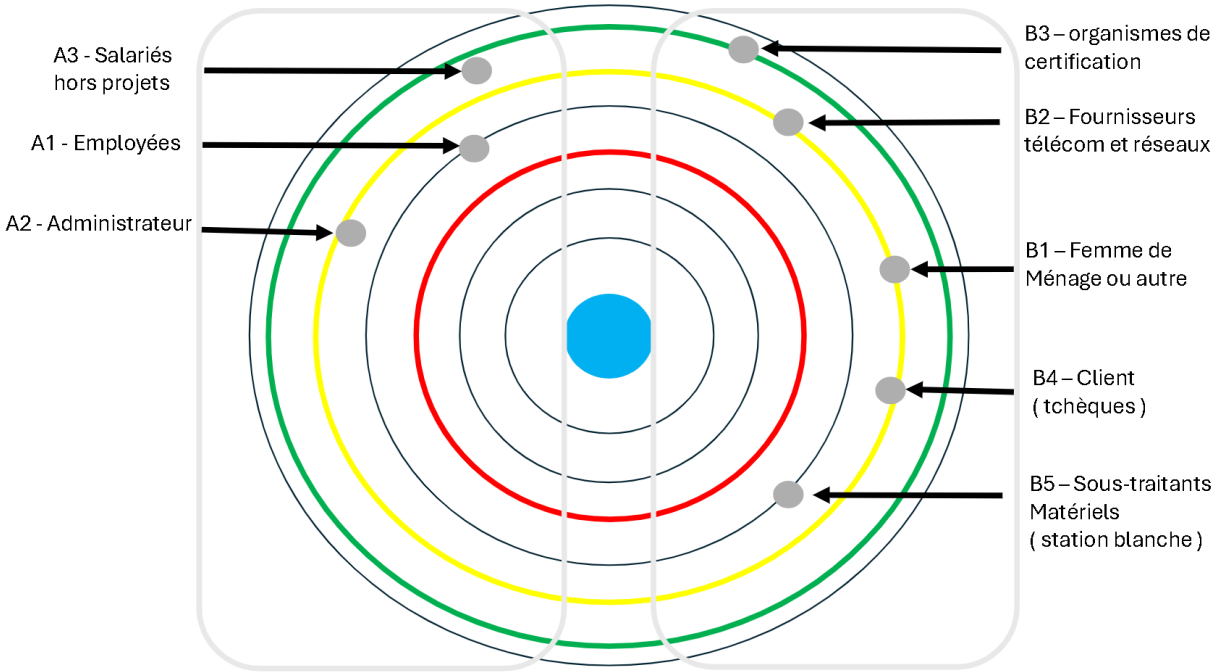
Atelier 5 – Traitement du risque

Définir les mesures de sécurité

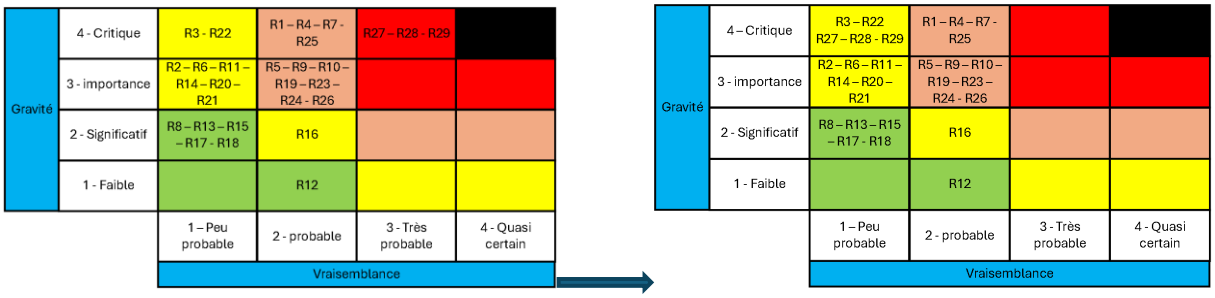
ID	PARTIE PRENANTE	CHEMINS D'ATTAQUE	STRATÉGIQUES	MESURES DE SÉCURITÉ	GRAVITE	VRAISEMBLANCE	MENACE INITIALE	MENACE RÉSIDUELLE
R27	Administrateur / opérateur mise à jour	Diffusion involontaire d'une mise à jour compromise ou non sécurisée	Introduction d'un ransomware par mise à jour (involontaire)	Validation automatisée des mises à jour (hash, signature, provenance), station blanche avec sandbox, workflow 4-eyes, monitoring post-déploiement, logs immuables, plan de restauration testé	4	3	3,5	1,3
R28	Prestataire nettoyage (accès opportuniste)	Branche une clé USB si accès ouvert par erreur	Infection par clé USB lors d'un accès furtif	Interdiction totale du nettoyage pendant les heures d'accès, **badge blacklisté sur la salle, sas sécurisé, fermeture automatique des portes, capteurs d'ouverture + alarme immédiate, cache-ports physiquement verrouillés, screensaver instantané + cable lock, patrouilles SSI, traitement des rebuts (aucun poste laissé alimenté)**	4	3	3,5	0,5
R29	Employé mécontent (accès local autorisé)	Branche une clé USB personnelle sur un poste isolé	Infection par malware/ransomware pour bloquer la production	**Blocage matériel des ports USB, station blanche dédiée aux supports, poste scellé (tamper-evident), accès sous supervision (caméra + 4-eyes), audits d'intégrité du BIOS/UEFI, traçabilité forte des actions, suppression des privilèges locaux, contrôle comportemental EDR offline, politique disciplinaire appliquée**	**4**	**3**	3,5	0,5

La priorité du traitement des menaces à était faite en fonction du score initiale, donc les 3 menace ci-dessus ont été sélectionner car leurs scores de menace sont les plus haut.

Après remédiation :



Gravité	4 – Critique	R3 – R22 R27 – R28 - R29	R1 – R4 – R7 - R25		
	3 - importance	R2 – R6 – R11 – R14 – R20 – R21	R5 – R9 – R10 – R19 – R23 – R24 - R26		
	2 - Significatif	R8 – R13 – R15 – R17 - R18	R16		
	1 - Faible		R12		
		1 – Peu probable	2 - probable	3 - Très probable	4 - Quasi certain
		Vraisemblance			


Gravité
4 - Critique
3 - importance
2 - Significatif
1 - Faible
R3 - R22
R1 – R4 – R7 - R25
R27 – R28 - R29
R2 – R6 – R11 – R14 – R20 – R21
R5 – R9 – R10 – R19 – R23 – R24 - R26
R8 – R13 – R15 – R17 - R18
R16
R12
1 – Peu probable
2 - probable
3 - Très probable
4 - Quasi certain
Vraisemblance
Gravité
4 – Critique
3 - importance
2 - Significatif
1 - Faible
R3 – R22 R27 – R28 - R29
R1 – R4 – R7 - R25
R2 – R6 – R11 – R14 – R20 – R21
R5 – R9 – R10 – R19 – R23 – R24 - R26
R8 – R13 – R15 – R17 - R18
R16
R12
1 – Peu probable
2 - probable
3 - Très probable
4 - Quasi certain
Vraisemblance