

Analyse Des Risques- AgroRAND

CSC_4CS08_TP

2024/2025

Réalisé par :

- EL MEKEDDEM Ikram
- KEBIR Mohammed
- OUERSIGHNI Anis

CADRE DE L'ÉTUDE

L'entreprise AgroRand, composée de 90 employés répartis entre le site de Mâcon et le télétravail, développe des solutions IoT pour la gestion de drones, collecte et traitement de données, tout en gérant des informations sensibles relatives à ses clients et à son administration via un système d'information centralisé.

Titre : AgroRand - Entreprise spécialisée dans la gestion connectée d'exploitations agricoles

* __Mots clés :__ **supervision, segmentation, authentication**

* __ Objectifs de maquettage dans le cadre de l'analyse : __

* __ Contraintes organisationnelles et scénaristiques : __ L'entreprise possède 90 employés, 40 sur le site de Macon et **50 en télétravail partiel**. **Parmi les employés**, nous trouvons (i) les développeurs de logiciels (ils travaillent sur les capteurs IoT, collecte de données et utilisent un backend cloud pour le traitement de ces dernières), (ii) les ingénieurs terrain (qui accèdent aux dashboards IoT, et gèrent la configuration des drones et capteurs), (iii) l'équipe administrative (effectuant la gestion RH, la facturation, le CRM, et l'ERP local), (iv) l'équipe commerciale (qui ont accès aux documents marketing, aux données clients, et aux CRM SaaS), (v) le responsable sécurité IT (qui gère la supervision réseau, les sauvegardes, les mises à jour, et les alertes de sécurité). **Le scénario veut que l'entreprise gère ses propres drones, récupèrent les données de ces derniers et effectue leur traitement dans un backend cloud**. Les résultats de ces traitements sont ensuite renvoyés vers les clients qui les ont demandés.

L'ensemble est automatisé à partir du moment où les drones sont configurés sur le terrain.

Le système d'information de l'entreprise contient à la fois **des données client**, **les données des drones** et capteurs et **les données administratives de l'entreprise**.

* __ Contraintes techniques : __ Déployer le système d'informations sur 6 machines, 1 pour un/une développeur (en remote ou non), 1 représentant un drone (permettant de générer les données de ces derniers), 1 pour les aspects administratifs (sur site et contenant toutes les données RH, facturation, CRM et ERP), 1 pour l'équipe commerciale (en remote, avec toutes les données marketing des clients et des contrats), 1 pour le/la responsable sécurité (sur site) et 1 pour le stockage de l'ensemble des données (RH, clients, marketing, configuration des drones, etc.).

* __ Contraintes sur la menace : **La menace est liée à des attaquants externes** souhaitant **menacer les données** gérées par l'entreprise par **une exfiltration** ou **une demande de rançon**. **Certaines machines (postes et serveurs) sont assez anciennes**.

Il n'y a actuellement **pas d'outil automatique de détection d'activité anormale** et **aucune supervision centralisée des journaux**.

Le réseau local ne possède pas de segmentation entre les services.

Référentiels (base) : sections 14, 17, 22, 23, 36, 37, 40. Rappel : comme deux groupes peuvent traiter le même projet, il est normal que l'on vous laisse une marge de manœuvres sur les sections à couvrir.

1er Atelier : Scope and security baseline

1.1 Contexte organisationnel

Nom de l'entreprise : AgroRAND

- Activité principale : Gestion autonome de drones IoT avec traitement Cloud des données collectées.
- Taille de l'entreprise : 90 employés
 - Macon (sur site) : 40 employés
 - Télétravail partiel : 50 employés

Fonctions clés des départements:

- **Développement logiciel** : capteurs IoT, backend Cloud
- **Ingénierie terrain** : configuration drones, accès dashboards
- **Administration** : RH, facturation, ERP local
- **Commercial** : CRM SaaS, marketing, contrats clients
- **Sécurité IT** : supervision réseau, alertes, sauvegardes

Mission	Gestion autonome de drones IoT avec traitement Cloud des données collectées.		
Dénomination de la valeur Métier	Collecte, traitement et gestion des données IoT	Configuration des drones	Management des Relations Client
Nature de la valeur métier	Processus	Processus	Information

Description	L'entreprise utilise des drones IoT pour collecter des données sur le terrain, qui sont ensuite traitées via un backend Cloud pour fournir des analyses précises à ses clients. Cela permet une gestion automatisée et optimale des drones, avec un traitement sécurisé des données dans le Cloud.	Les ingénieurs terrains sont responsables de vérifier la configuration des drones avant de les faire voler.	L'équipe commerciale et l'équipe administrative sont responsables de la gestion de la communication avec les clients, y compris la facturation, la gestion des CRM, les documents marketing et la gestion des relations. Ces équipes accèdent à des informations sensibles concernant les clients, ce qui nécessite une gestion sécurisée et organisée des données.
Entité ou Personne responsable	Lead Département technique (développeurs, ingénieurs terrain) et Responsable sécurité IT	Lead Ingénieurs Terrain	Responsable équipe commerciale et administrative
Dénomination du/des bien support associés	Serveurs Cloud, drones IoT, systèmes de stockage de données.	Drones, logiciels de configuration IoT (dashboard)	CRM SaaS, systèmes de facturation, outils de communication (email, messagerie)
Description	Le système repose sur une infrastructure matérielle et logicielle comprenant des drones IoT pour la collecte des données, un backend Cloud pour le traitement et le stockage des informations, ainsi que des serveurs et des systèmes de stockage dédiés à la gestion des données sensibles.	Les drones utilisés sur le terrain sont équipés de capteurs et de logiciels pour la collecte de données. Les ingénieurs utilisent des outils logiciels spécialisés pour configurer et ajuster les paramètres des drones avant chaque mission.	La communication avec les clients repose sur des systèmes CRM (pour la gestion des contacts et des interactions) et des outils de communication (emails, messagerie, etc.). Ces systèmes contiennent des données sensibles et sont essentiels pour maintenir une relation continue avec les clients et gérer les transactions.

1.2 Feared Events (Événements Redoutés) Classifiés selon la Sévérité

Valeur Métier	Événement redoutés	Description	Impact	Gravité
Configuration Des drones	Perte de disponibilité des données	Une machine clé (serveur central, drone, etc.) tombe en panne <u>sans sauvegarde adéquate</u> , entraînant une perte partielle ou totale des données.	<ul style="list-style-type: none"> • Perte de données importantes • Arrêt temporaire des opérations • Retard dans la fourniture des services 	G4 - Critique
	Divulgateion ou altération des données échangées sur les accès distants	Un attaquant intercepte les communications entre les employés en télétravail et les systèmes internes, permettant de capturer des identifiants d'accès ou de modifier les données échangées. Ou bien un attaquant qui intercepte les communications entre les drones et les endpoints capteurs IoT.	<ul style="list-style-type: none"> • Compromission des comptes utilisateur • Interception de données sensibles lors des échanges • Risque de diffusion de malwares via les connexions distantes • Risque de falsification des résultats échangés. 	G2 – SIGNIFICATIVE
Collecte, traitement et gestion des données IoT	Indisponibilité du stockage central entraînant l'arrêt des opérations	Un ransomware infecte le serveur central contenant toutes les données (clients, RH, marketing, configuration des drones).	<ul style="list-style-type: none"> • Chiffrement total des données critiques • Arrêt complet des opérations • Coût financier important pour payer la rançon ou restaurer les données 	G4 – CRITIQUE

			<ul style="list-style-type: none"> Retard dans la fourniture des services aux clients. 	
	Altération et fuite furtive des données IoT	Un attaquant obtient un accès non autorisé au backend Cloud utilisé pour traiter les données IoT collectées par les drones. <u>En raison de l'absence de supervision centralisée</u> et d'outils de détection d'anomalie, une intrusion reste détectée trop tardivement, permettant à un attaquant de compromettre plusieurs systèmes avant d'être repéré	<ul style="list-style-type: none"> impacte Confidentialité des données IoT / Clients Manipulation ou destruction des données en temps réel Interruption du traitement des données pour les clients Corruption des analyses fournies aux clients 	G3 – GRAVE
	Altération ou indisponibilité des données métier	Les machines anciennes utilisées par certains employés (développeurs, ingénieurs terrain) peuvent être exploitées par un attaquant grâce à des failles logicielles / kernel surtout avec l'absence d'un EDR.	<ul style="list-style-type: none"> Perte de contrôle sur les postes de travail Utilisation des postes comme point d'entrée vers le réseau interne (AD) Risque de propagation de malware 	G3 – GRAVE
Management des Relations Client	Fuite de données clients	Un attaquant réussit à exfiltrer des données critiques, telles que les informations clients, les configurations des drones, ou les données RH.	<p>valeur métier impactée : Confidentialité des données IoT, Fichiers Configurations Drones, Documents Clients</p> <ul style="list-style-type: none"> Perte de confiance client 	G4 – CRITIQUE

			<ul style="list-style-type: none"> • Risque de sanctions réglementaires (RGPD) • Dommages réputationnels importants • Perturbation des opérations commerciales et administratives 	
	Divulgateion publique des données IoT	Une erreur de configuration dans le backend Cloud expose accidentellement les données client dans le CRM.	<ul style="list-style-type: none"> • Fuite de données sensibles • Violation de la confidentialité des clients • Risque de sanctions légales 	G2 – SIGNIFICATIVE

2eme Atelier : Analyse des risques

Contexte

L'objectif principal est de lier les sources de risque (RS) aux objectifs visés (TO) en fonction des motivations et des ressources des attaquants. Cette analyse permettra d'évaluer la pertinence des couples (RS, TO) et de comprendre comment ces couples sont liés aux événements redoutés (ER) identifiés dans le cadre de l'étude.

2.1 Identification des Sources de Risque

Sources De Risque	Description
Attaquant externe (cybercriminel)	Motivation : Gagner de l'argent via rançons ou exfiltration de données sensibles. Ressources : Techniques sophistiquées d'attaque (phishing, ransomware).
Hacktiviste	Motivation : Saboter ou divulguer des informations pour faire pression sur l'entreprise (ex. pratiques environnementales ou éthiques). Ressources : Compétences techniques limitées mais motivation élevée.
Employé malveillant	Motivation : Accès non autorisé à des données sensibles pour vendre ou nuire. Ressources : Connaissance interne du système.
Concurrent	Motivation : Voler des données sensibles de configurations de nos drones intelligents, les algorithmes de nos systèmes de traitement, ou bien exfiltrer les données pour nuire à notre réputation. Ressources : motivation élevée avec des ressources élevée

2.2 Identification des Objectifs Visés (TO) pour AgroRAND

Les objectifs visés par les attaquants doivent être alignés avec les valeurs métier critiques et les services essentiels de l'entreprise. Voici les principaux objectifs visés par AgroRAND (qui seront visé à compromettre par les malveillants) :

Objectifs Visés par L'entreprise	Description
Confidentialité des données clients	Protection des informations personnelles, contrats, RH.

Intégrité des données traitées par le backend Cloud	Garantie que les analyses fournies aux clients sont exactes et non altérées.
Disponibilité du système de stockage central	Maintien de l'accès permanent aux données critiques (clients, drones, RH).
Sécurité des accès distants aux machines	Protection des connexions des employés en télétravail contre l'interception ou le piratage.
Continuité opérationnelle	Garantir la poursuite des activités métier malgré un incident.
Traçabilité des actions dans le SI	Permettre de surveiller, journaliser et analyser les comportements dans le réseau.
Authentification forte des utilisateurs	Empêcher l'utilisation non autorisée des comptes (via mots de passe simples, absence de 2FA).

2.3 . Lien entre Couples (RS, TO) et Événements Redoutés (ER)

Sources de Risque (RS)	Objectifs Visés (TO)	Motivation	Ressources	Pertinence	Événements Redoutés (ER) Liés
Attaquant externe (cybercriminel)	Confidentialité des données clients	Fortement motivé	Ressources importantes	Très pertinent	Exfiltration massive de données sensibles
Attaquant externe (cybercriminel)	Disponibilité du système de stockage central	Fortement motivé	Ressources importantes	Très pertinent	Ransomware infectant le serveur central de stockage

Attaquant externe (cybercriminel)	Intégrité des données traitées par le backend Cloud	Assez motivé	Ressources significatives	Plutôt pertinent	Accès non autorisé au backend (à travers phishing, vpn compromis ..) et Altération / Exfiltration des données <u>sans être repéré.</u>
Attaquant externe (cybercriminel)	Disponibilité du système de stockage central	Fortement motivé	Ressources importantes	Très Pertinent	Accès non autorisé au backend (à travers phishing, vpn compromis ..) et Altération / Exfiltration des données <u>sans être repéré.</u>
Attaquant externe (cybercriminel)	Compromettre Authentification forte des utilisateurs	Fortement motivé	Ressources limitées	Plutôt pertinent	Exfiltration massive de données sensibles
Attaquant MITM (cybercriminel)	Sécurité des accès distants	Fortement motivé	Ressources significatives	Très pertinent	Interception des communications distantes
Cybercriminel	Continuité opérationnelle	Fortement motivé	Ressources importantes	Très pertinent	Indisponibilité prolongée du SI
Concurrent commercial	Confidentialité des données clients	Fortement motivé	Ressources importantes	Très pertinent	Exfiltration massive de données sensibles
Concurrent commercial	Disponibilité du système de stockage central	Fortement motivé	Ressources importantes	Très pertinent	Exploitation de vulnérabilités sur les machines anciennes qui ne peuvent pas être patchés.
Hacktiviste	Intégrité des données traitées par le backend Cloud	Peu motivé	Ressources limitées	Peu pertinent	Attaque man-in-the-middle (MITM) sur les connexions distantes

Employé malveillant	Confidentialité des données clients	Assez motivé	Ressources limitées	Plutôt pertinent	Exfiltration massive de données sensibles
Employé malveillant	Traçabilité des actions	Assez motivé	Ressources limitées	Plutôt pertinent	Intrusion non détectée

Notice:

En utilisant la matrice fournie, nous pouvons évaluer la pertinence des couples (RS, TO) en fonction de la motivation et des ressources des attaquants.

Motivation	Ressources limitées	Ressources significatives	Ressources importantes	Ressources illimitées
Très peu motivé	Peu pertinent	Moyennement pertinent	Plutôt pertinent	Plutôt pertinent
Peu motivé	Peu pertinent	Moyennement pertinent	Plutôt pertinent	Très pertinent
Assez motivé	Plutôt pertinent	Plutôt pertinent	Très pertinent	Très pertinent
Fortement motivé	Plutôt pertinent	Très pertinent	Très pertinent	Très pertinent

3ème Atelier : Strategic Scenarios

Contexte

L'objectif de cet atelier est d'identifier les parties prenantes critiques dans l'écosystème d'AgroRAND et de construire des scénarios de risques stratégiques. Ces scénarios permettront de comprendre comment un attaquant pourrait exploiter ces parties prenantes pour atteindre les systèmes clés de l'entreprise.

Les entrées nécessaires pour ce atelier proviennent des deux ateliers précédents :

Atelier 1 : Scope and Security Baseline

- Contexte organisationnel
- Événements redoutés classifiés selon leur gravité

Atelier 2 : Analyse des Risques

- Sources de risque identifiées
- Objectifs visés
- Couples RS-TO pertinents

À la fin de cet atelier, nous devrions obtenir :

Ecosystem Threat Mapping : Cartographie des menaces dans l'écosystème.

Strategic Scenarios : Scénarios stratégiques détaillés montrant comment les attaquants peuvent exploiter les parties prenantes.

Security Measures Adopted for the Ecosystem : Mesures de sécurité à adopter pour protéger l'écosystème.

3.1 Parties prenantes critiques

Partie Prenante	Type	Rôle clé dans le SI	Valeurs Métier Associées
Développeurs	Interne	Création/maintenance backend Cloud et capteurs IoT	Collecte, traitement et gestion des données IoT
Ingénieurs terrain	Interne	Configuration des drones, accès aux dashboards	Configuration des drones
Équipe commerciale	Interne	Gestion clients, contrats, CRM SaaS	Communication client
Administration	Interne	RH, facturation, ERP local	Communication client
Sécurité IT	Interne	Supervision réseau, alertes, sauvegardes	Toutes les valeurs métier
Fournisseurs Cloud	Externe	Hébergement infrastructure Cloud	Serveur Cloud, stockage de données
Clients	Externe	Utilisateurs finaux des analyses drone	Données sensibles
Partenaires technologiques	Externe	Intégration matérielle/logicielle des drones	Accès technique temporaire
Télétravailleurs externes	Externe	Collaborateurs distants	Accès au SI via connexions distantes

3.2 Menaces stratégiques liées aux parties prenantes

Partie Prenante	Source de Risque	Menace potentielle	Objectif visé (TO)	Chemin d'attaque possible
Employés internes (développeurs, ingénieurs, administratifs)	Employé malveillant	Vol ou exfiltration de données clients	Confidentialité des données clients	L'employé utilise ses droits d'accès légitimes pour exporter des données vers un service externe non autorisé. lancer un ransomware qui encrypt le serveur de sauvegarde ...
Équipe administrative/commerciale	Phishing ciblé	Obtention d'identifiants valides via mail malicieux	Authentification forte des utilisateurs	Un membre reçoit un email de phishing bien imité, saisit ses identifiants dans un faux portail de connexion. Ces credentials peuvent être utilisé pour tester contre Password-Reuse dans l'une des applications de l'entreprise . une fois compromis, il peut exploiter l'application/privilege pour recevoir un shell et accéder à l'infrastructure.

Télétravailleurs	Attaque MITM	Interception des communications entre télétravailleur et SI	Sécurité des accès distants	Une attaque man-in-the-middle intercepte les échanges via un réseau Wi-Fi public non sécurisé.
Fournisseurs Cloud	Faible de configuration	Exposition accidentelle de données sensibles	Confidentialité des données clients	Erreur de configuration IAM ou de bucket Cloud → données accessibles publiquement.
Clients	Attaquant externe (cybercriminel)	Utilisation du CRM comme vecteur d'attaque	Disponibilité du système de stockage central	Injection SQL via portail client → compromission du serveur backend et accès à l'infrastructure de l'entreprise. Une fois dedans, il peut abuser des serveurs anciens, intercepter les trafics, altérer les informations, Spoofer des personnels.
Partenaires technologiques	Hacktiviste	Sabotage de systèmes via accès temporaire	Intégrité des données traitées par le backend Cloud	Le partenaire a laissé une porte dérobée logicielle lors d'une mise à jour.

Machines anciennes (postes développeurs ou terrain)	Cyber-criminel	Exploitation de vulnérabilités non corrigées	Intégrité des données traitées par le backend Cloud	Logiciel obsolète → CVE-Connue / faille zero-day exploitée → pivot vers AD.
Employés	Réseau non segmenté	Propagation rapide d'un malware après intrusion initiale	Disponibilité du système de stockage central	Un poste infecté → propagation automatique vers serveur central.
Employés	Absence de supervision centralisée	Intrusion non détectée pendant plusieurs jours	Traçabilité des actions dans le SI	Pas de journalisation centralisée ni d'EDR → attaquant reste indétecté.

4ème Atelier : Scénarios Opérationnel

Objectif :

Construire des scénarios opérationnels détaillant les procédures techniques que les sources de risque (RS) pourraient mettre en œuvre pour atteindre leurs objectifs. Ces scénarios doivent être basés sur les scénarios stratégiques identifiés dans l'Atelier 3 et doivent fournir une vision claire des étapes techniques que les attaquants pourraient suivre.

Entrées (Inputs) :

Missions, valeurs métier et actifs support (Atelier 1) :

- Missions clés : Gestion autonome de drones IoT, traitement des données, communication client.
- Valeurs métier : Collecte, traitement et gestion des données IoT, configuration des drones, communication client.
- Actifs support : Serveurs Cloud, drones IoT, CRM SaaS, ERP local, systèmes de stockage.

Base de sécurité (Atelier 1) :

- Absence de supervision centralisée.
- Réseau non segmenté.
- Absence de MFA.
- Machines anciennes non patchées.
- Absence d'EDR.

Sources de risque et objectifs visés (Atelier 2) :



- **Sources de risque** : Attaquant externe (cybercriminel), employé malveillant, phishing ciblé, machines anciennes, réseau non segmenté.
- **Objectifs visés** : Confidentialité des données clients, intégrité des données traitées, disponibilité du système de stockage central, sécurité des accès distants.

Scénarios stratégiques sélectionnés (Atelier 3) :

- **[Disponibilité]** Ransomware infectant le serveur central.
- **[Confidentialité]** Exfiltration massive de données sensibles par un employé malveillant.
- **[Accès distants]** Phishing ciblé contre l'équipe administrative/commerciale.

Sorties (Outputs) :

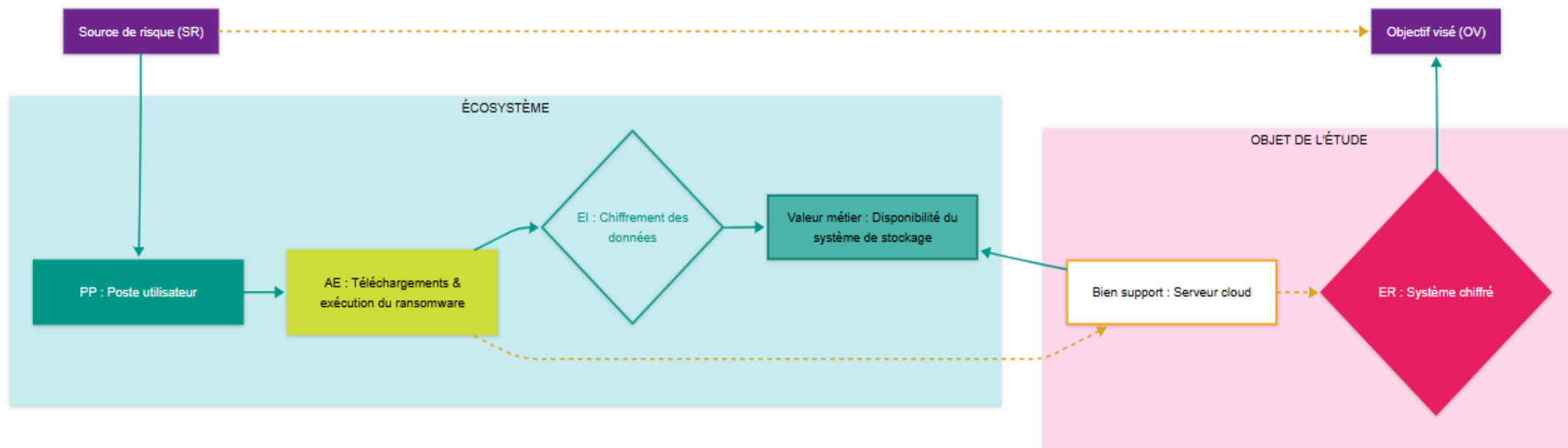
Légende commune aux 3 schémas :

	Chemin d'attaque d'un scénario stratégique
	Mode opératoire d'un scénario opérationnel
AE	Action élémentaire sur un bien support
EI	Événement intermédiaire associé à une valeur métier de l'écosystème
ER	Événement redouté relatif à une valeur métier de l'objet de l'étude
PP	Partie prenante de l'écosystème

Description des scénarios

• Scénario 1 – Indisponibilité du SI RH après ransomware

Un cybercriminel exploite un poste utilisateur RH pour faire exécuter un ransomware. Le chiffrement automatique des fichiers affecte le serveur ERP, rendant indisponibles toutes les données RH et de gestion. Le schéma illustre l'impact direct sur la valeur métier "disponibilité du système de stockage", jusqu'à l'atteinte de l'objectif visé.

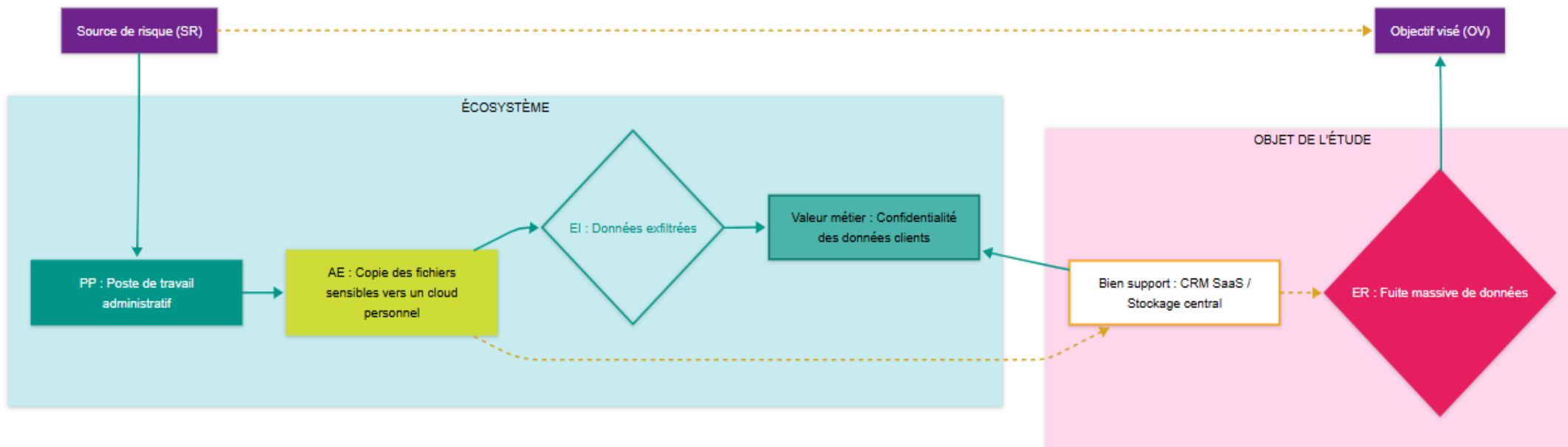


Probabilité estimée : V3 – Très vraisemblable

Criticité : Élevée

- **Scénario 2 – Fuite de données clients par un employé**

Un employé administratif copie des fichiers sensibles clients vers un Cloud personnel depuis son poste. Cette fuite compromet la confidentialité des données dans le CRM. Le schéma représente la chaîne d'attaque et ses conséquences sur la valeur métier et les biens support.

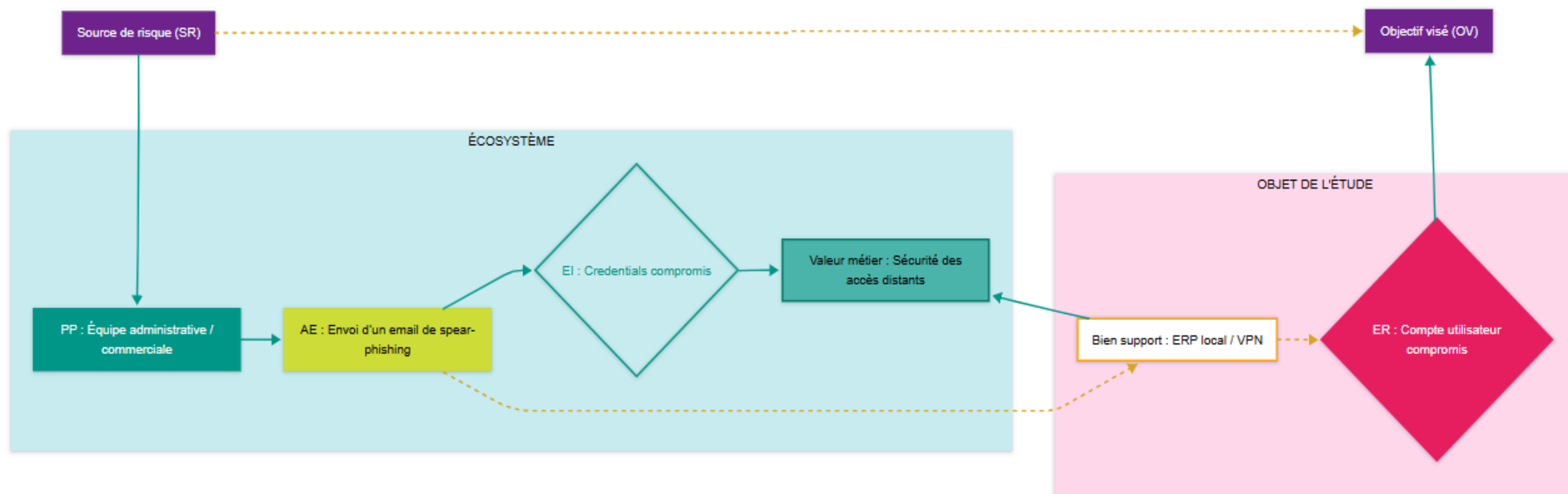


Probabilité estimée : V3 – Très vraisemblable

Criticité : Élevée

Scénario 3 – Compromission des accès distants après phishing

Un courriel de spear-phishing piège un utilisateur de l'équipe administrative. Le mot de passe récupéré permet un accès non autorisé au système ERP ou au VPN, compromettant la sécurité des accès distants. Le schéma met en lumière le chemin d'attaque du phishing jusqu'à la compromission du compte utilisateur.



Probabilité estimée : V2 – Vraisemblable

Criticité : Moyenne

Conclusion :

Cette étape a permis d'illustrer concrètement les chemins d'attaque qui exploitent les failles techniques et organisationnelles d'AgroRAND. Les scénarios montrent des menaces claires sur la continuité des services et la confidentialité des données. Ces scénarios serviront de base à l'Atelier 5, dans lequel seront proposées des mesures correctives pour réduire le niveau de risque.

5ème Atelier : Traitement du risque

Objectif :

Réduire les niveaux de risque inacceptables ou trop élevés identifiés dans l'atelier 4, en mettant en œuvre des mesures de sécurité (organisationnelles ou techniques).

Le but est d'agir sur la vraisemblance (V), la gravité (G), ou les deux, pour ramener le risque à un niveau acceptable.

Leur efficacité est ensuite visualisée sur une matrice gravité/vraisemblance (type EBIOS).

Méthodologie :

- Pour chaque scénario opérationnel (S1, S2, S3), les risques initiaux ont été qualifiés selon une gravité et une vraisemblance.
- Des mesures de sécurité spécifiques ont été définies.
- Un impact attendu sur le risque a été évalué après traitement.

Récapitulatif des traitements des scénarios :

Scénario	Gravité (G)	Vraisemblance (V)	Niveau de risque (G×V)	Criticité	Mesures correctives proposées	Impact attendu
1 – Ransomware sur serveur ERP	4	3	12	Élevée	<ul style="list-style-type: none"> - EDR sur les postes - Segmentation réseau - Sauvegardes régulières automatisées 	↘ V à 2 → Criticité moyenne
2 – Exfiltration par employé malveillant	4	3	12	Élevée	<ul style="list-style-type: none"> - DLP (Data Loss Prevention) - Restriction de l'usage des Clouds externes - Journalisation renforcée des accès 	↘ V à 2 → Criticité moyenne

3 – Phishing ciblé contre équipe admin.	3	2	6	Moyenne	<ul style="list-style-type: none"> - Formation anti-phishing - Double authentification (MFA) - Blocage pièces jointes inconnues 	↘ V à 1 → Criticité faible
------------------------------------------------	---	---	---	---------	------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------

Conclusion :

L'atelier 5 montre que des mesures simples mais ciblées permettent de réduire significativement l'exposition au risque :

- Certaines mesures sont techniques (EDR, segmentation, MFA)
- D'autres organisationnelles (sensibilisation, politique d'usage, journalisation)

Objectif atteint : aucun des scénarios n'est resté dans la zone rouge de la matrice après application des contre-mesures.
Les décisions de traitement peuvent maintenant être validées par la direction sécurité.