Durée : 1h45
Ce contrôle contient : 12 pages

Cas d'étude : société Qualitech

La société Qualitech est une start-up innovante qui développe et maintient une solution destinée à l'industrie. Cette solution est basée sur une application nommée aussi Qualitech et un serveur de traitement. Cette solution permet de définir et dérouler des plans des contrôle/qualité, avec un suivi des actions/indicateurs en temps réel.

Contexte :

Créée en mai 2021 par deux associés : un expert en ventes des solutions industriels et une jeune diplômée d'une école d'ingénierie en systèmes d'information. La société a obtenu un prix à l'innovation, mais elle n'est pas rentable (investissement en R&D pour 3 années). Toutefois l'application Qualitech est en phase pilote avec 3 industriels du monde automobile, les résultats sont prometteurs. Deux de ces industriels sont satisfaits de la réactivité des équipes Qualitech et de la valeur (gains temps/couts) qu'apporte la solution. Ces industriels (deux en France et l'autre aux Etats-Unis) envisagent de signer un contrat au cours de l'année, ce qui permettra à la société d'être rentable.

Les industriels exigent la certification ISO 9001 à la société Qualitech ainsi que des garanties sur les protections de données récoltés.

A savoir que la société Qualitech n'a aucun politique de sécurité des systèmes d'information à ce jour.

L'application Qualitech :

L'application Qualitech est une application mobile pour iOS (.ipa), compatible seulement avec les iPads. Cette application est distribuée via un « store » privé dont le propriétaire est la société Qualitech.

L'application iOS est signée avec un certificat acheté par le client (industriel). En conséquence, il y a une application Qualitech par client.

Cette application permet de collecter des données qualité (saisis manuellement par un operateur), puis de les envoyer au serveur de traitement distant (via des interfaces API).
L'application Qualitech utilise la connectivité de l'iPad (4G ou Wifi) pour se connecter à Internet.
L'opérateur de l'application s'authentifie sous l'application Qualitech avec un login + un mot de passe, ce qui permet à l'application Qualitech d'accéder au serveur de traitement. L'application Qualitech récupère du serveur de traitement le plan des contrôle/qualité personnalisé pour l'opérateur authentifié.

L'application ne sauvegarde rien en local, toutes les informations sont transmises au serveur de traitement et les rapports sont téléchargés à la demande.

Le serveur de traitement a une interface web accessible via HTTPS pour permettre aux utilisateurs de s'authentifier (login + un mot de passe) et de consulter les rapports depuis d'un ordinateur quelconque.

Contraintes :

Les réglementations relatives aux données personnelles doivent êtes prises en compte (GDPR, ou les lois locales, par exemple Discovery aux Etats-Unis, …).
Les données collectées par l'application ont un niveau de classification confidentiel, des mesures de sécurité doivent être mises en place pour les protéger.

Sites : Qualitech est implantée à Paris (Siège social) et à Barcelone (R&D).

Paris :

Environ 5 personnes travaillent au siège social. On y trouve toute l'administration et les directeurs commerciaux, direction des ressources humaines et la direction générale.

Le service commercial :
Trois commerciaux dont seul 1 est sédentaire. Tous les échanges sont réalisés via e-mail ou GoogleDoc.

Le service informatique :
La politique des dirigeants est que le personnel peut utiliser son propre ordinateur (BYOD), ou un ordinateur portable Mac fourni par la société (mais il n'est pas géré, sans mises à jour, durcissement, antivirus, …).
Internet est accessible via une BoxADSL (connexion via WiFi avec un mot de passe unique WAP pour tout le monde).

L'utilisation des services SaaS est obligatoire :

- Le site web de la société est sous-traité à une agence de communication. Ce site est hébergé chez un hébergeur français (OVH).
- Pour la messagerie, la société utilise Office365.
- Pour les échanges de documents et le travail en équipe, la société utilise GoogleDoc, WhatsApp.

Barcelone :

Ce site emploie 15 personnes :

- 1 responsable de site (DSI)
- 2 chercheurs
- 1 expert Datalake
- 1 personne pour le support N1
- 10 développeurs

Le service R&D a par mission : concevoir les algorithmes de traitement des données et ainsi améliorer ou proposer des nouvelles fonctionnalités à l'application.

Le service Développement a pour mission le développement de l'application Qualitech et du serveur de traitement. Tous les développeurs ont les privilèges administrateur de leurs postes de travail.

Le service support : 1 personne dédiée au support N1, puis ce sont les développeurs qui assurent le support niveau 2 et niveau 3. Cette personne est aussi responsable du monitoring des solutions Cloud.

La politique des dirigeants est aussi appliquée au site de Barcelone : utilisation des ordinateurs personnels (BYOD) ou portables Mac fournis par la société, chaque employée est responsable du maintien en conditions opérationnel et de sécurité de son ordinateur.

L'utilisation des services Cloud (SaaS, IaaS…) :

- GitHub privé pour le stockage et versionnage du code source de l'application Qualitech et su serveur de traitement. Authentification login + mot de passe.
- Environnement de tests, démonstrateurs et production hébergés sous AWS. Authentification login + mot de passe.
- Pour la messagerie : Office365. Authentification login + mot de passe.
- Pour les échanges de documents : GoogleDoc. Authentification login + mot de passe.
- Pour les échanges : WhatsApp.
- Pour le suivi des changements, support et demandes clients : JIRA.
- Le serveur de traitement est sur environnement Docker, et les développeurs utilisent des outils comme « Jenkins » pour l'intégration continue sous AWS. La plateforme de production est sur AWS.

Les tiers :

Principaux clients :

- 3 grands industriels automobiles

Principaux fournisseurs :

- OVH
- AWS
- Atlassian
- Microsoft (Office 365)
- Google

Sous-traitants :

- Société de services de développement DEVELOP (5 personnes)
- IT provider IT4ALL (fourniture des ordinateurs MAC, gestion des équipes réseau/boxAdsl pour l'accès à internet)

Principales activités :

Administration : Ce processus comprend la gestion du personnel, la comptabilité, la trésorerie, les finances, les services commerciaux.
Recherche : Ce processus comprend toutes les activités de l'équipe de chercheurs : Etude de nouvelles techniques, Conception de nouveaux produits, conception de maquettes.
Développement des applications : Cette activité prend en charge le développement des interfaces utilisateur, des interfaces de communication, de traitement des données et de mise en forme (reporting).
Commercial : Ce processus a la charge de la gestion des clients. Ce service fournit les éléments de facturation et les éléments contractuels aux services comptabilité et financier de l'entreprise.
Support : Les demandes d'amélioration ou le signalement de bugs sont effectuées par les commerciaux/les clients finaux/les développeurs via le service JIRA. Les demandes sont prises en compte par l'équipe de développement en temps réel.

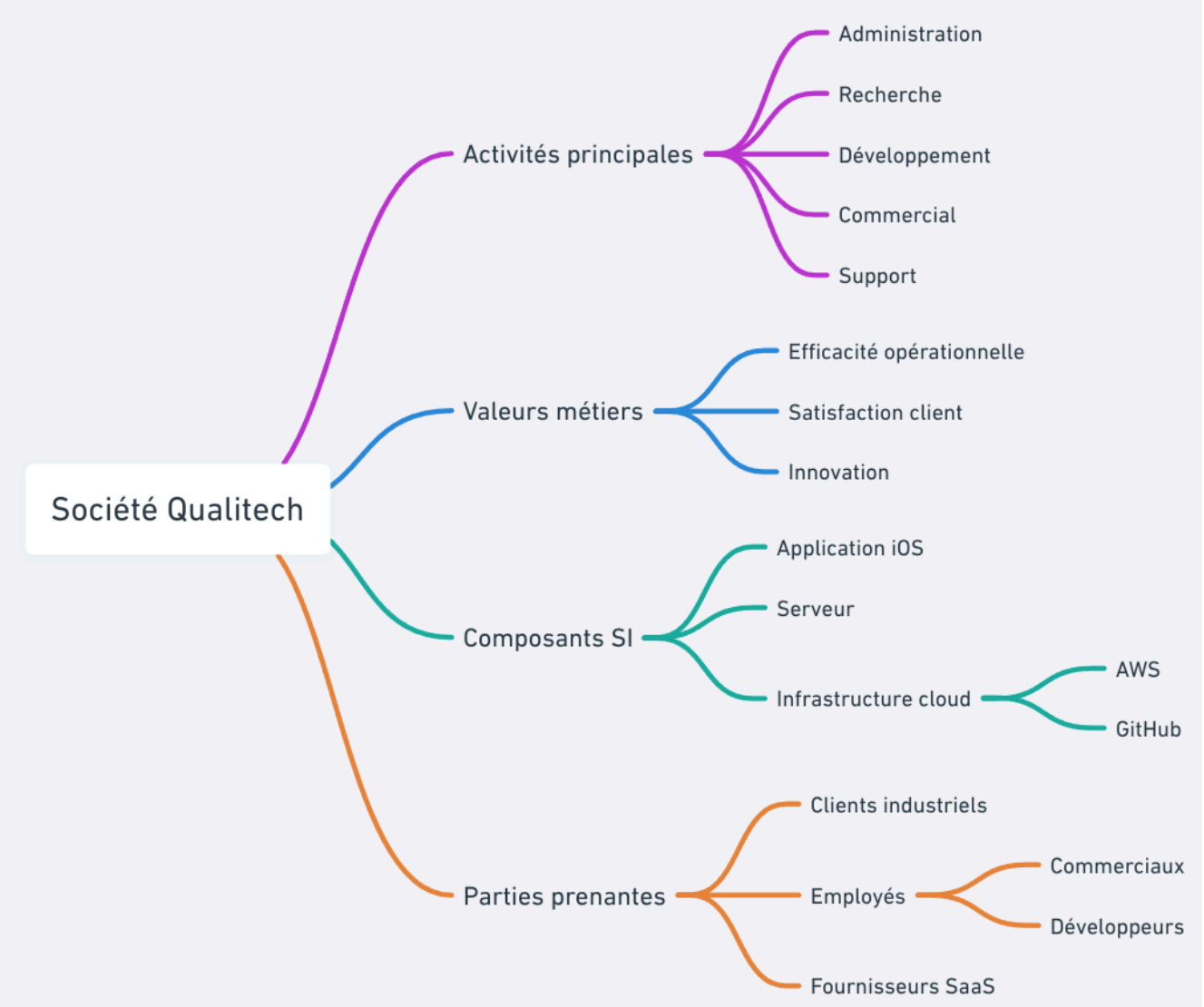
Contrôle continue en équipe

Indiquer le nom et prénom de membres de l'équipe (max 3 personnes)

CHAKIR Mohammed Amine - ABDELMONAIM Mouhalhal - SADIQI Rim

Activité 1 : Schématiser le cas d'étude de la société Qualitech

Croquis avec principales activités, principaux valeur métier, principaux bien support, composant SI, parties prenantes ….



Activité 2 : Au vu du cas d'étude, quel serait le référentiel Cybersécurité à considérer, justifié ?

Référentiel	Justification
ISO/IEC 27001	La norme ISO/IEC 27001 fournit un cadre pour établir, mettre en œuvre, maintenir et améliorer un système de management de la sécurité de l'information (SMSI). Pour une start-up comme Qualitech, visant la certification ISO 9001 et traitant des données confidentielles, l'adoption de l'ISO/IEC 27001 permettrait de structurer et renforcer sa politique de sécurité de l'information, assurant ainsi la protection des données sensibles des clients et la conformité aux exigences réglementaires.

Activité 3 : Identifier les 3 principaux valeurs métier - Indiqué le bien support pour chaque valeur métier

VALAUERS METIERS Quels processus ou informations la société doit-elle absolutement protéger ?	BIEN SUPPORT Sur quoi reposent-elles ?
Développement et maintenance de l'application Qualitech	Code source de l'application (hébergé sur GitHub privé)
Gestion sécurisée des données qualité des clients	Serveur de traitement (hébergé s AWS)
Satisfaction et support client	Plateforme JIRA et services de communication (Office365, Google Docs, WhatsApp)

Activité 4 : Déterminez les événements redoutés, impacts et leur gravité pour les 3 valeur métier identifiés. Utilisez l'échelle suivante pour la gravité, référez-vous au livret stagiaire pour les impacts.

ÉCHELLE	DÉFINITION
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 su 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 impacts 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)

Valeur métier	Evénement redouté	Impacts	Gravité
Développement et maintenance de l'application Qualitech	Compromission du code source (GitHub piraté)	Risque d'intégration de code malveillant, perte de propriété intellectuelle, atteinte à la réputation	G2 - Significatif
Gestion sécurisée des données qualité des clients	Fuite de données clients (violation GDPR)	Amendes, perte de confiance des clients, dommages financiers	G3 - Grave
Satisfaction et support client	Indisponibilité du serveur de traitement	Impact sur les opérations des clients, insatisfaction, perte de contrats potentiels	G4 - Critique

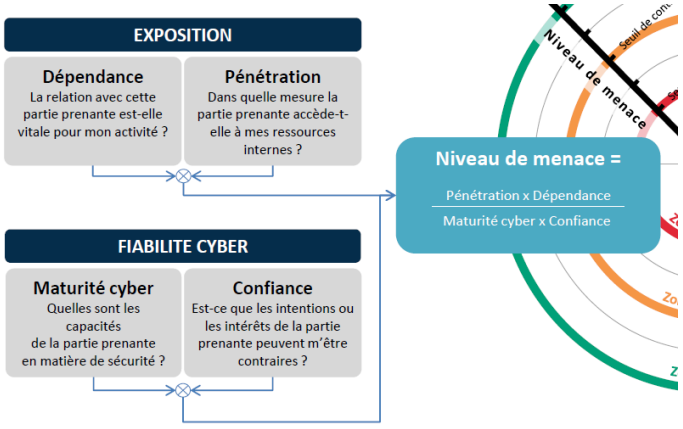
Activité 5 : Déterminez les principaux couples SR/OV (au moins 4) et estimez leur pertinence

			RESSOURCES			
			Incluant les ressources financières, le niveau de compétences cyber, l'ouillage, 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

Sources de risque	Objectifs visés	Motivation	Ressources	Pertinence
Cybercriminels	Lucratif	Peu motivé	Ressources limités	Peu pertinent
Concurrent	Espionnage	Fortement motivé	Ressources importantes	Très pertinent
Activiste	Divulgation des informations	Assez motivé	Ressources significatifs	Plutôt pertinent
Amateur	Amusement	Peu motivé	Ressources limitées	Peu pertinent

Activité 6 : Identifier au moins 3 parties prenantes de l'écosystème et évaluer leurs niveaux de menace. Utilisez l'échelle suivante pour l'évaluation :

	DÉPENDANCE	PÉNÉTRATION	MATURITÉ CYBER	CONFIANCE
1	Pas de lien avec le SI de la partie prenante pour réaliser la mission	Pas d'accès ou accès avec des privilèges de type utilisateur à des terminaux utilisateurs (poste de travail, ordiphone, *etc.*).	Des règles d'hygiène sont appliquées ponctuellement et non formalisées. La capacité de réaction sur incident est incertaine.	Les intentions de la partie prenante ne sont pas connues.
2	Lien avec le SI de la partie prenante utile à la réalisation de la mission	Accès avec privilèges de type administrateur à des terminaux utilisateurs (parc informatique, flotte de terminaux mobiles, etc.)ou accès physique aux bureaux de l'organisme.	Les règles d'hygiène et la réglementation sont prises en compte, sans intégration dans une politique globale. La sécurité numérique est assurée selon un mode réactif.	Les intentions de la partie prenante sont considérées comme neutres.
3	Lien avec le SI de la partie prenante indispensable mais non exclusif (possible substitution)	Accès avec privilèges de type administrateur à des serveurs « métier » (serveur de fichiers, bases de données, serveur web, serveur d'application, *etc.*).	Une politique globale est appliquée en matière de sécurité numérique. Celle-ci est assurée selon un mode réactif, avec une recherche de centralisation et d'anticipation sur certains risques.	Les intentions de la partie prenante sont connues et probablement positives.
4	Lien avec le SI de la partie prenante indispensable et unique (pas de substitution possible)	Accès avec privilèges de type administrateur à des équipements d'infrastructure (annuaires d'entreprise, DNS, DHCP, *switchs*, pare-feu, hyperviseurs, baies de stockage, *etc.*) ou accès physique aux salles serveurs de l'organisme.	La partie prenante met en œuvre une politique de management du risque. La politique est intégrée et prend pleinement en compte une dimension proactive.	Les intentions de la partie prenante sont parfaitement connues et pleinement compatibles avec celles de l'organisation étudiée.



Catégorie	Partie prenante	Dépendance	Pénétration	Maturité	Confiance	Niveau de menace
Client	Administration	4	4	3	3	1.7
Fournisseur SaaS	OVH, AWS, Google, …	4	4	4	2	2

Sous-traitant	It provider	3	3	2	2	2.2
Equipe interne	Devs, commerciaux	3	3	2	3	1.5

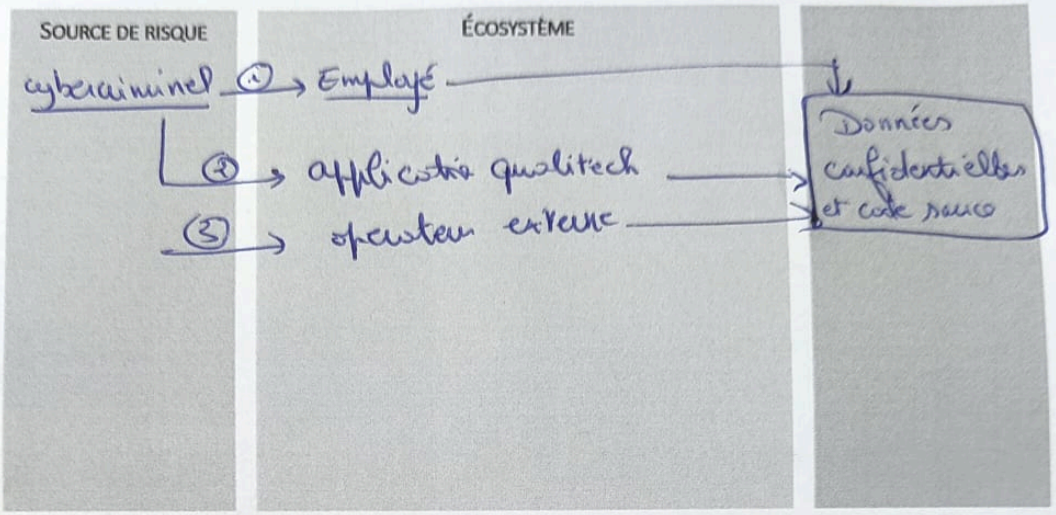
Activité 7 : Élaborez au moins 2 scénarios stratégiques : identifiez et représentez les chemins d'attaques possibles.

ISIMA – 2024/2025 Contrôle continu Politique de sécurité – EBIOS RM

Activité 7 : Élaborez au moins 2 scénarios stratégiques : identifiez et représentez les chemins d'attaques possibles.

Élaborez des scénarios stratégiques

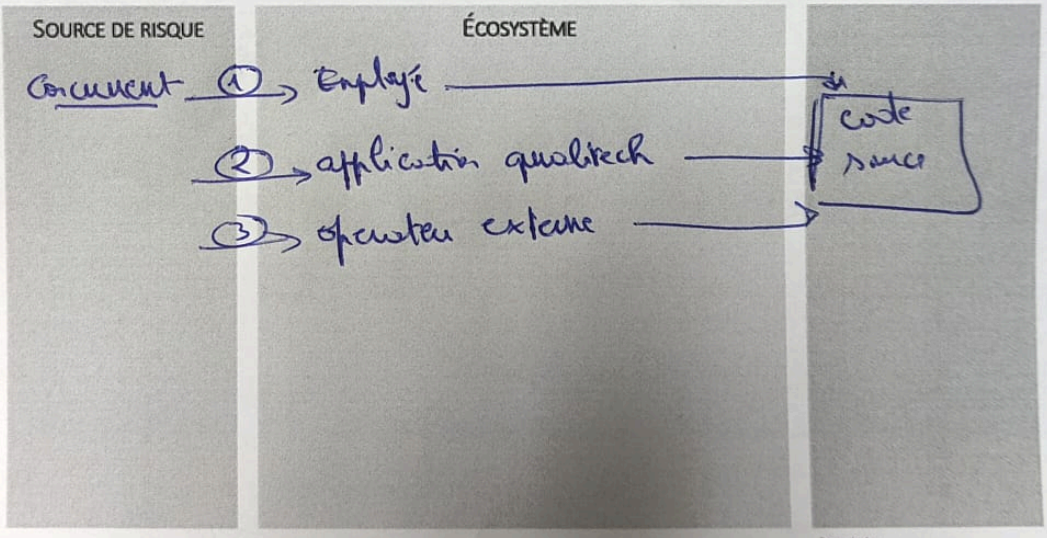
A2 Source de risque : cybercriminel Objectif visé : voler les données confidentielles et le code source



Gravité :

Élaborez des scénarios stratégiques

A2 Source de risque : Concurrent Objectif visé : voler le code source.

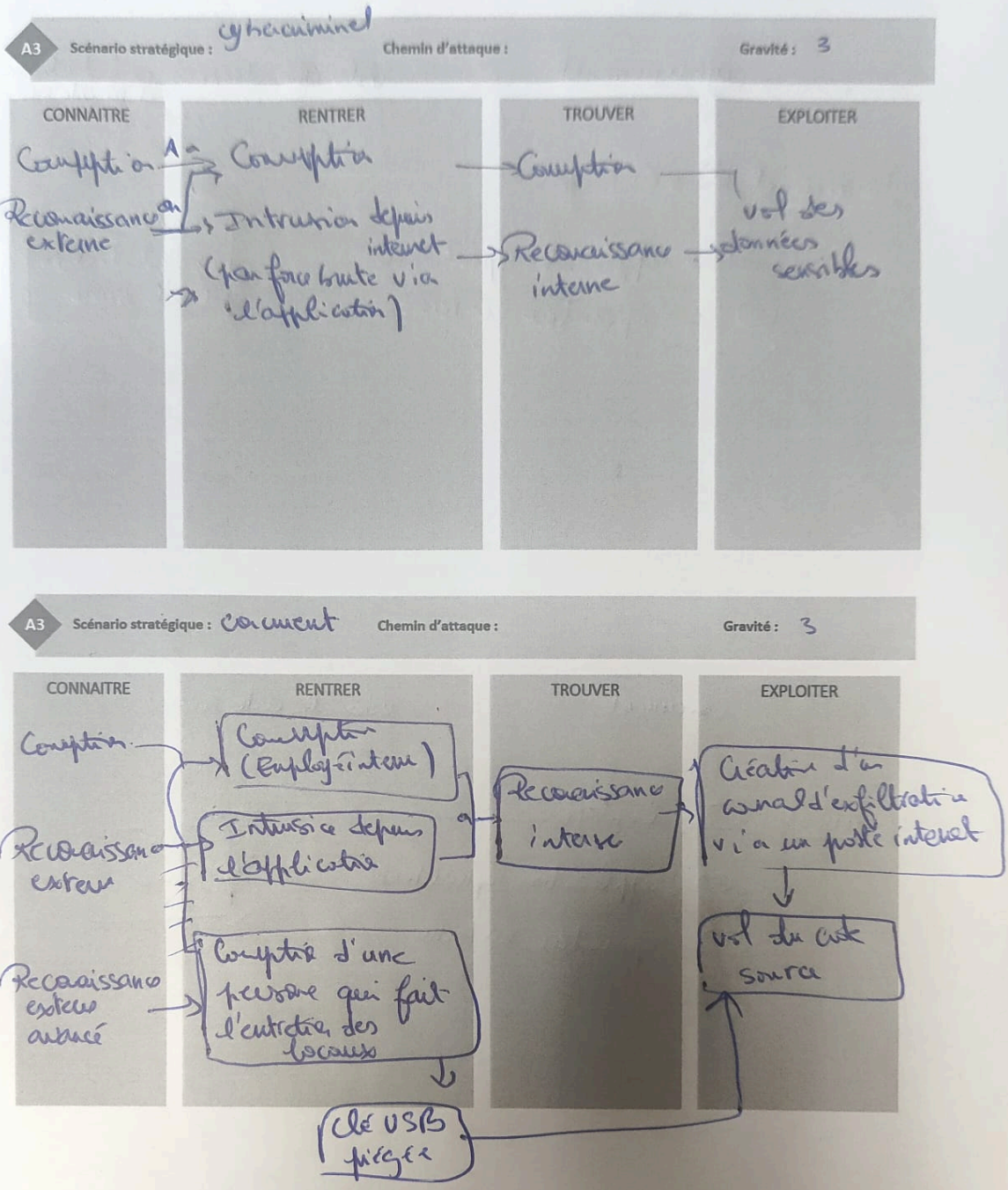


Gravité :

Activité 8 : Élaborez au moins 2 scénarios opérationnels et <u>indiquer la vraisemblance des scenarios</u>

ISIMA – 2024/2025 Contrôle continu Politique de sécurité – EBIOS RM

Activité 8 : Élaborez au moins 2 scénarios opérationnels et indiquer la vraisemblance des scenarios



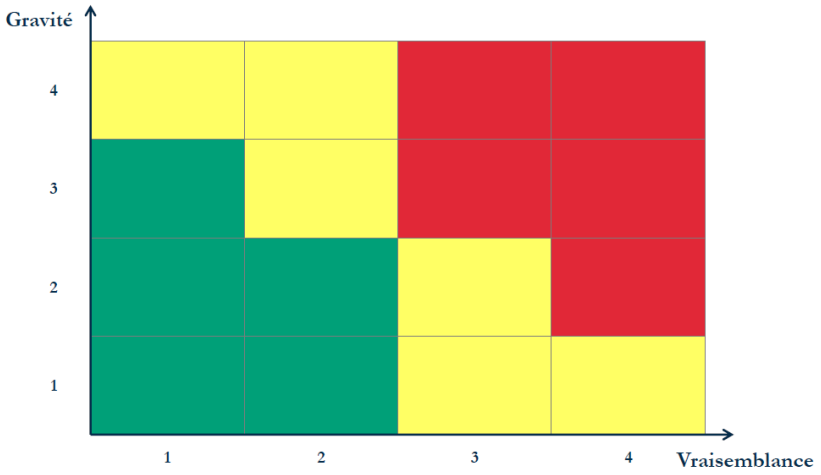
Echelle de vraisemblance à utiliser :

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

Activité 9 : indiquer au moins 2 risques et positionnez-les sur la matrix

- R1 : Fuite de données clients **(Gravité : G3, Vraisemblance : V2)**

- R2 : Indisponibilité de l'application **(Gravité: G4, Vraisemblance : V2)**



Activité 10 : Déterminez les 3 mesures de sécurité les plus pertinentes et proposez une priorisation

Mesure de sécurité	Scénarios de risques associés	Responsable	Freins et difficultés de mise en œuvre	Coût / Complexité	Priorité
Implémentation de MFA sur AWS et GitHub	Compromission des comptes admin	DSI	Adoption des employés	Faible	Haute
Audit de sécurité des API et tests d'intrusion	Exploitation d'une vulnérabilité API	RSSI	Nécessite des ressources externes	Moyenne	Haute
Renforcement du BYOD (MDM, mises à jour forcées)	Infection par malware	Responsable IT	Impact sur la flexibilité des employés	Moyenne	Moyenne