EBIOS Risk Manager

Etude de cas fictive « *Analytics for Talent Management* »

Présentation synthétique

Thierry PERTUS - Consultant Senior (Enterprise Risk Manager - CEFAR, ISO 31000 RM, ISO/IEC 27005 RM, ISO/IEC 27001 LI, CISM)

Afaf FAFI - Consultante Cyber Security & Data Protection (EBIOS RM, ISO/IEC 25005 RM, ISO/IEC 27001 LA, DPO / Privacy Implementer, CISA)

Classification du document : **Public** (éligible à publication)

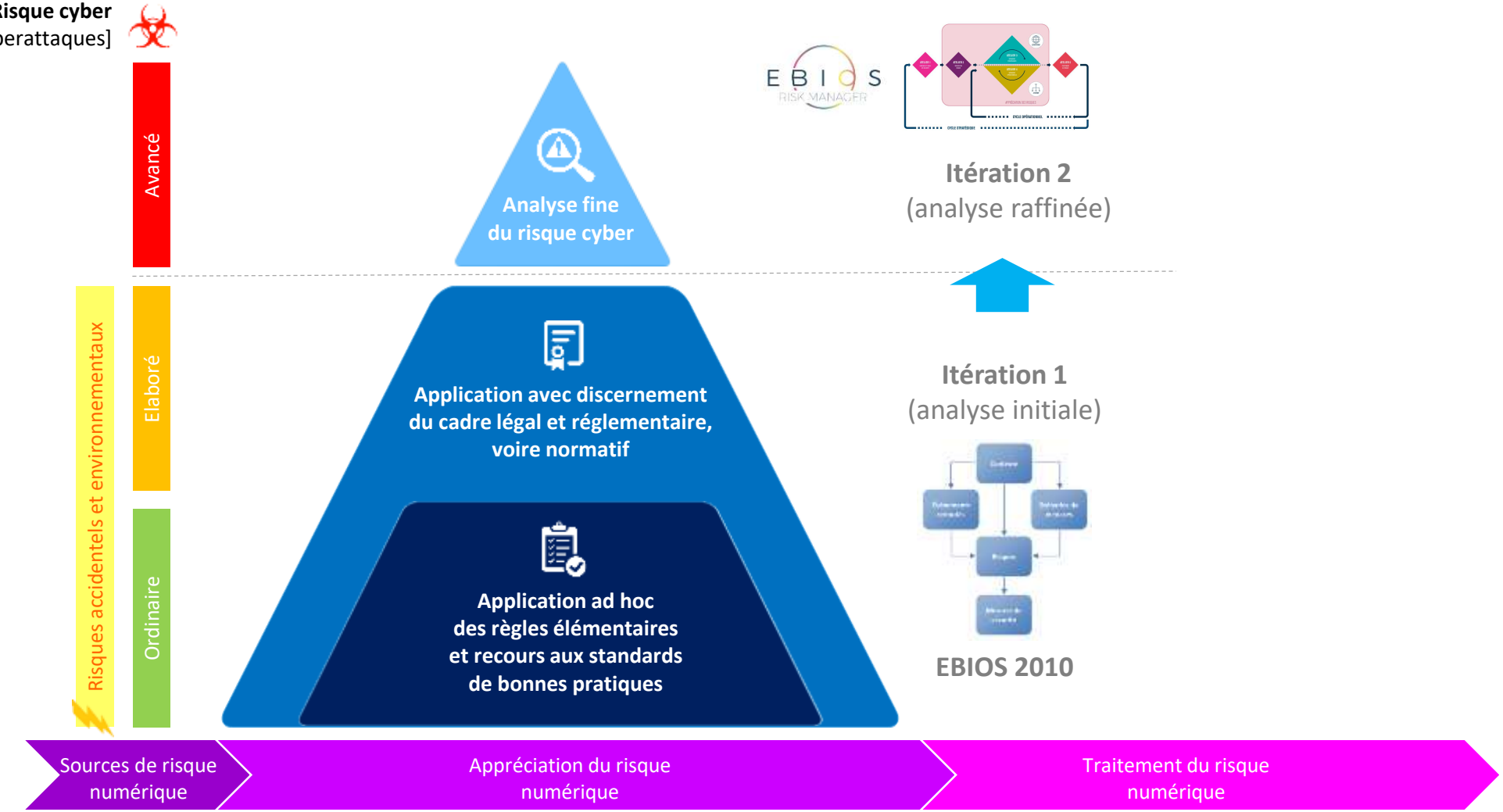
Groupe de travail au sein du Club EBIOS : **Action 55 - « Outils & Pratiques »**

Lien sur le Forum des membres : https://club-ebios.org/forum/viewforum.php?f=55

17/02/2020 - v1.2

Proof of Concept (PoC) : Démarche évolutive et complémentaire EBIOS 2010 > EBIOS Risk Manager

Niveau de cybermenace potentiel > Risque cyber
[capacité, ciblage, sophistication des cyberattaques]



Adhérence normative avec l'ISO 31000:2018

CLUBEBIOS

Descripteurs de l’étude de cas

Trame narrative de l'étude de cas *(storyline)*

Cyber-attaque

DigiTalents NextGen

WeTalents

Sécurité & cadre privé nativement intégrés
(Security & Privacy by Design)

Mise en production
(Roll-out)

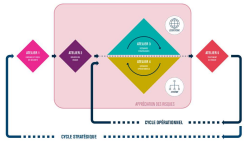
Sécurité orientée scénarios d'attaque
(Attack scenarios-based Security)

Cession
(Due diligence)

Chronologie
(Timeline)

EBIOS 2010

Plateforme S.A.B.E en SaaS
(Smart Analytics for Business Enabling)



EBIOS RISK MANAGER

Jalon stratégique
(Strategic milestone)

CLUBEBIOS

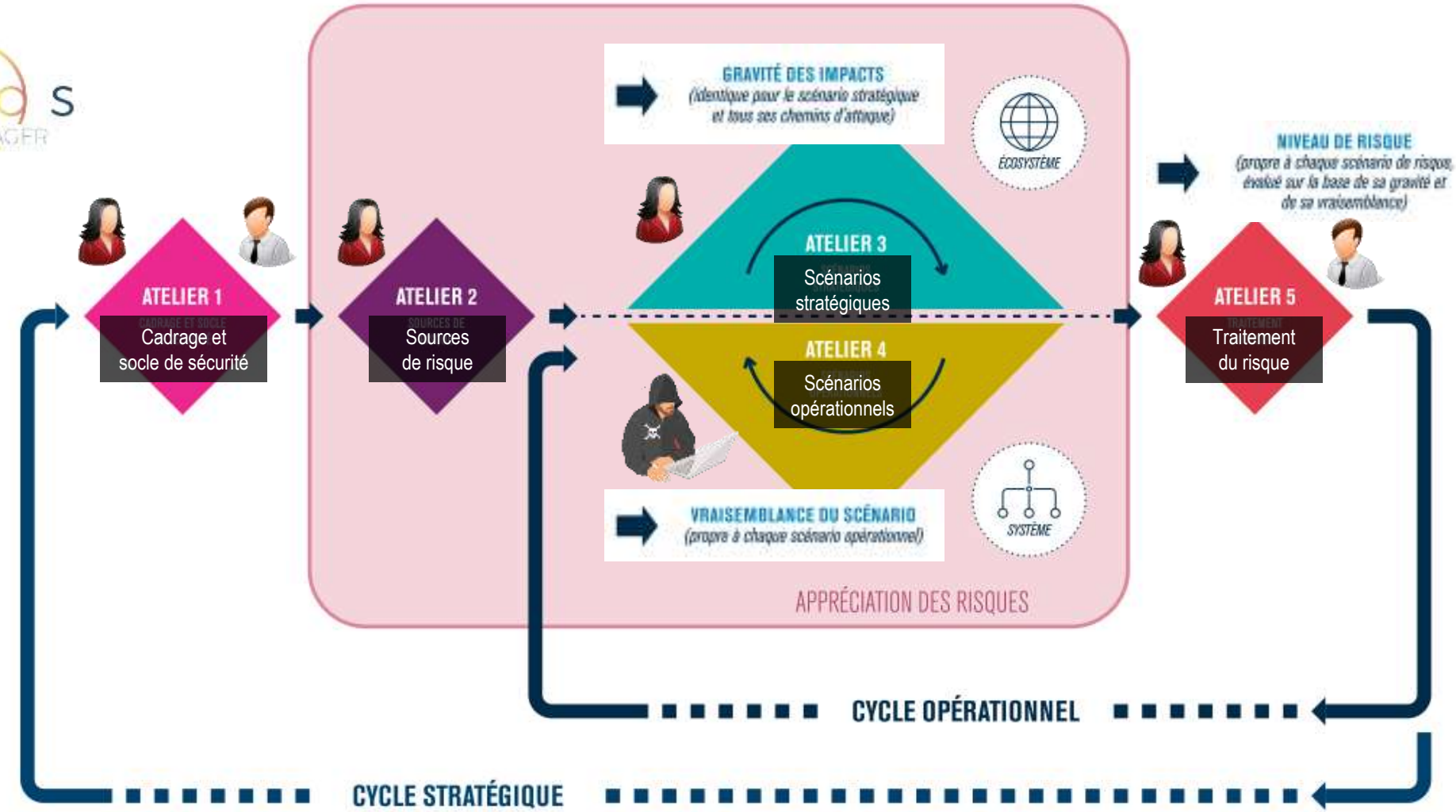
Interlocuteurs clés sollicités lors des 5 ateliers

RACI

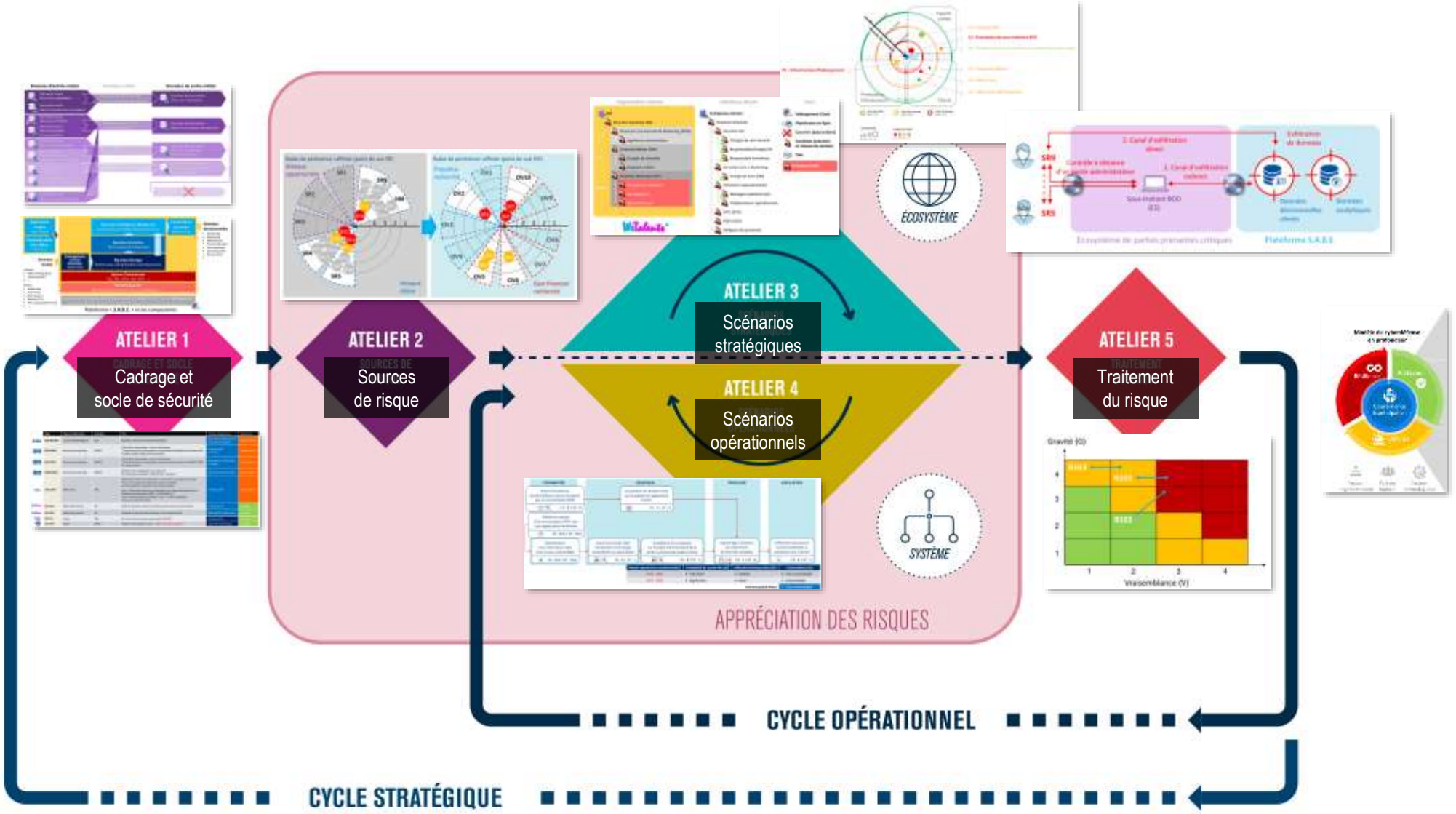
A
Responsable SSI

R
Analyste en risque cyber

C
Responsable métier
Référent technique
Hacker éthique



Déroulement de l'étude de cas selon EBIOS Risk Manager *(screenshots)*



5b. définir la stratégie de traitement du risque et les mesures de sécurité

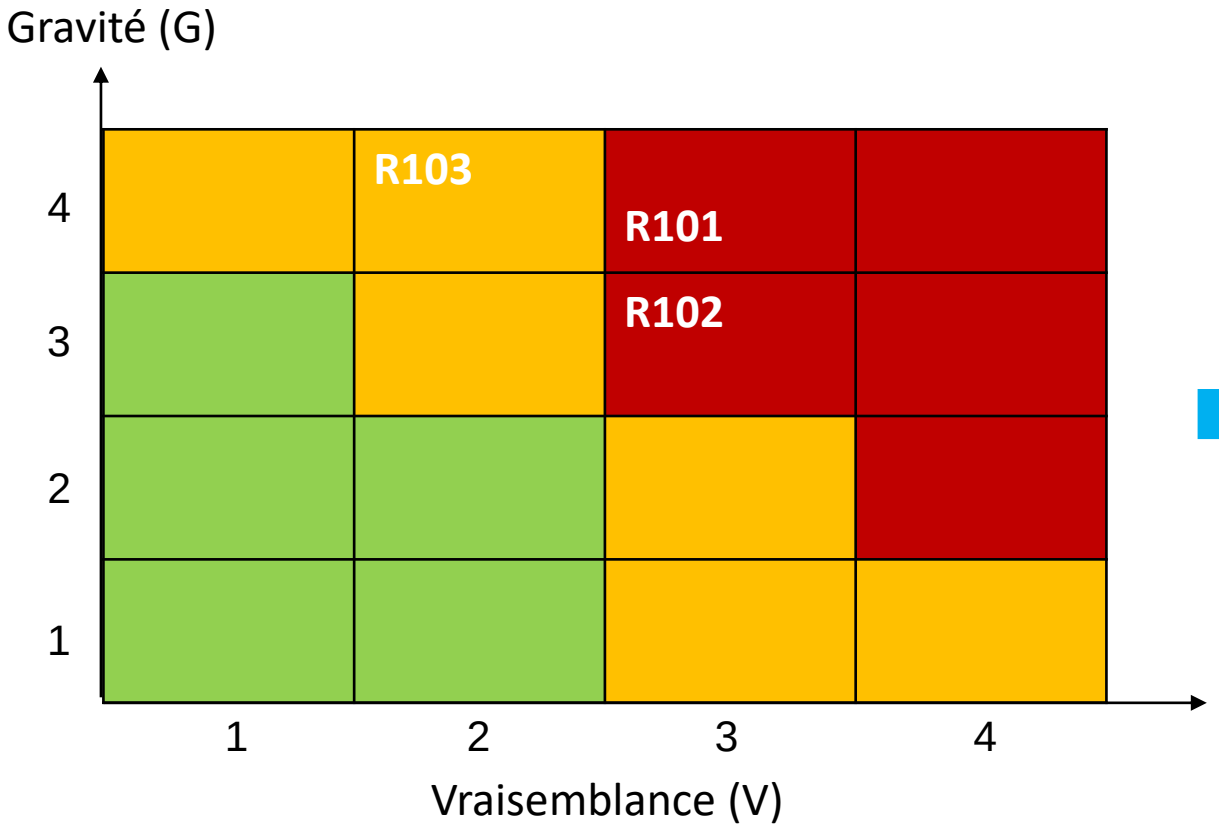
Index	Mesure de sécurité	Scénarios de risques associés	Responsable	Freins / difficultés de mise en œuvre	Coût / Complexité	Échéance	Statut
Gouvernance							
MSG1	Choisir un contrat de service pour la sous-traitance BOD auprès d'une société localisée en zone UE. Formaliser un plan assurance sécurité précisant les règles de sécurité organisationnelles et techniques appliquées	R101, R103	DM, DPO, RSSI	Anticiper la fin de contrat avec le prestataire actuel	++	12 mois	A lancer
MSG2	Pour le choix de l'hébergeur Cloud, exiger la certification ISO/IEC 27001, voire CSA STAR et que les données traitées soient toujours localisées en zone UE	R101, R103	DT, RSSI, DPO	Anticiper la fin de contrat avec la société actuelle	++	9 mois	En cours
MSG3	Intégrer des clauses de sécurité dans les contrats avec l'ensemble des prestataires (auditabilité, confidentialité, incidents de sécurité, etc.)	R101, R102, R103	DM, DT, RSSI	Effectué au fil de l'eau à la renégociation des contrats	++	12 mois	A lancer
MSG4	Souscrire à un contrat de cyberassurance en cas de cyber-attaque impactant les données clients	R101, R102, R103	DG, RSSI	Faire une étude de marché pour évaluer les différentes solutions	++	6 mois	En cours
MSG5	Mise en place de CGU (Conditions Générales d'Utilisation) applicables aux utilisateurs clients et d'une charte administrateur opposables	R101, R103	DM, DT, RSSI, DPO	Faire valider la licéité du contenu auprès d'un cabinet d'avocat spécialisé	+	6 mois	En cours
MSG6	Mise en place d'une procédure de notification d'incident de sécurité vers les entreprises clientes	R101, R102, R103	DPO, RSSI	A intégrer dans la gestion des incidents de sécurité (MSG3)	++	6 mois	En cours
MSG7	Audit de sécurité organisationnel des prestataires assurant l'hébergement cloud et le BOD. Mise en place et suivi des plans d'action correctifs	R101, R102, R103	RSSI	Acceptation de la démarche par les prestataires (MSG1, MSG2 et MSG3)	+++	18 mois	A lancer

5b. définir la stratégie de traitement du risque et les mesures de sécurité

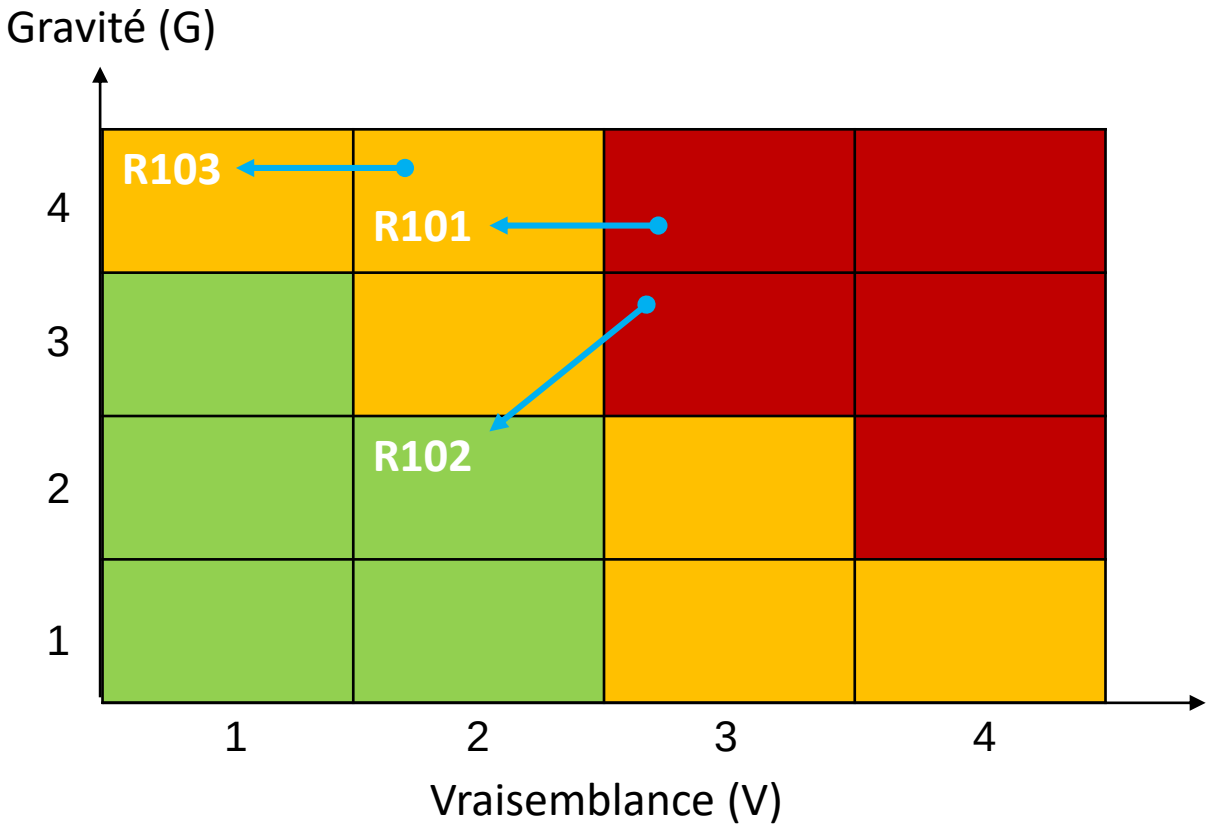
Index	Mesure de sécurité	Scénarios de risques associés	Responsable	Freins / difficultés de mise en œuvre	Coût / Complexité	Échéance	Statut
Protection							
MSP1	Chiffrer en natif les mots de passe clients stockés et lors de l'authentification	R103	DT	Gestion des clés de chiffrement	++	3 mois	Terminé
MSP2	Définir une politique de gestion des mots de passe utilisateurs (complexité, renouvellement, …)	R102, R103	DM, DT, RSSI	Réticence des clients	+	6 mois	A lancer
MSP3	Mettre en place une notification d'alerte (email) vers l'utilisateur légitime si une connexion est faite avec son compte depuis une nouvelle IP	R102	DM	Mettre en place un système de gestion des évènements de sécurité (MSD2)	++	9 mois	En cours
MSP4	Mettre en place une solution de Sandbox pour analyser préventivement les emails entrants et PJ	R101	DT	Etude de faisabilité à diligenter auprès de l'hébergeur cloud	++	6 mois	En cours
Défense							
MSD1	Souscrire à un service SOC pour la surveillance des flux par un NIDS, l'analyse et la corrélation des journaux d'évènements par un SIEM	R101, R102, R103	DM, DT, RSSI	Etude de faisabilité à diligenter auprès de l'hébergeur cloud	+++	18 mois	A lancer
MSD2	Mettre en place un bastion d'administration avec authentification forte pour sécuriser les accès à distance	R102, R103	DT	Réticence des administrateurs	++	9 mois	A lancer
Résilience							
MSR1	Mettre en place un dispositif de sauvegarde non accessible par le réseau principal avec test de restauration régulier	R102	DT	A intégrer dans le contrat d'hébergement (MSG2)	++	9 mois	En cours

5c. Évaluer et documenter les risques résiduels

Cartographie des risques nets
(avant traitement)



Cartographie des risques résiduels
(après traitement)



CLUBEBIOS

CLUBEBIOS

CLUBEBIOS

Site : https://club-ebios.org
Twitter : @club_ebios
LinkedIn : https://fr.linkedin.com/company/club-ebios