EBIOS-RM example

Atelier 1 - Cadrage et socle de sécurité

1. Identification des valeurs métier

Mission : Développer et exploiter des applications mobiles

Dénomination de la valeur métier	Nature de la valeur métier	Description	Propriétaire
Développement d'applications	Processus	Activité de conception et développement d'applications mobiles comprenant : • L'analyse des besoins • La conception de l'architecture • Le développement du code • Les tests et la validation • Le déploiement sur les stores	CTO
Plateforme de gestion des utilisateurs	Processus	Système permettant de gérer les comptes utilisateurs, les authentifications et les autorisations pour l'ensemble des applications	DSI
Données des utilisateurs	Information	Ensemble des données personnelles et d'utilisation collectées via les applications mobiles	DPO
Infrastructure cloud	Processus	Ensemble des ressources cloud (serveurs, stockage, réseau) hébergeant les applications et les données	DSI

Dénomination du/ des biens supports associés	Description	Propriétaire (interne/ externe)
Environnement de développement	Ensemble des outils et plateformes utilisés pour le développement (IDE, gestionnaires de versions, etc.)	Interne (DSI)
Serveurs d'applications	Serveurs hébergeant les applications en production	Externe (Fournisseur cloud)

Dénomination du/ des biens supports associés	Description	Propriétaire (interne/ externe)
Base de données utilisateurs	Système de gestion de base de données stockant les informations des utilisateurs	Externe (Fournisseur cloud)
Plateforme d'authentification	Service gérant l'authentification et les autorisations des utilisateurs	Interne (DSI)
Serveurs de stockage	Infrastructure de stockage des données utilisateurs et des logs applicatifs	Externe (Fournisseur cloud)

Ce tableau présente les principales valeurs métier et biens supports de MobiTech, en se concentrant sur les éléments essentiels liés au développement et à l'exploitation d'applications mobiles, ainsi qu'à la gestion des utilisateurs et de leurs données.

2. Événements redoutés et analyses

Valeur métier	Événement redouté	Impacts	Gravité
Développement d'applications	Fuite du code source d'une application en développement	• Missions et services de l'entreprise • Avantage concurrentiel • Image et confiance • Financiers	3
Plateforme de gestion des utilisateurs	Indisponibilité de la plateforme pendant plus de 4 heures	• Missions et services de l'entreprise • Financiers • Image et confiance • Satisfaction des utilisateurs	4
Données des utilisateurs	Vol massif de données personnelles des utilisateurs	• Juridiques • Image et confiance • Financiers • Satisfaction des utilisateurs	4
Infrastructure cloud	Compromission de l'infrastructure cloud	• Missions et services de l'entreprise • Confidentialité des données • Intégrité des systèmes • Financiers	3

Ce tableau présente les principaux événements redoutés pour MobiTech, associés à chaque valeur métier identifiée précédemment. La gravité est évaluée sur une échelle de 1 à 4, où 4 représente le niveau le plus critique.

Type de référentiel	Nom du référentiel	État d'application	Écarts	Justification des écarts
Règles d'hygiène informatique et bonnes pratiques	Guide d'hygiène informatique de l'ANSSI	Appliqué avec restrictions	Règle 12 : Cloisonner le réseau en zones de confiance	L'architecture réseau actuelle ne permet pas un cloisonnement complet entre les environnements de développement et de production
Règles de sécurité internes	Politique de Sécurité des Systèmes d'Information (PSSI) de MobiTech	Appliqué avec restrictions	Politique de gestion des mots de passe	La complexité des mots de passe n'est pas appliquée sur tous les systèmes hérités
Exigences réglementaires	RGPD	Appliqué avec restrictions	Droit à l'effacement des données personnelles	Le processus d'effacement des données n'est pas entièrement automatisé sur toutes les applications
Normes	ISO 27001	Non appliqué	Ensemble des exigences de la norme	La certification ISO 27001 est un objectif à moyen terme pour l'entreprise

Ce tableau présente une vue d'ensemble du socle de sécurité de MobiTech, mettant en évidence les principaux référentiels applicables, leur état d'application, ainsi que les écarts identifiés et leurs justifications. Il permet d'avoir une vision claire des domaines où des améliorations sont nécessaires pour renforcer la sécurité de l'entreprise.

Atelier 2 - Sources de risque

1. Identification des SR/OV

Sources de risque	Objectifs visés
Concurrent	

Sources de risque	Objectifs visés
	Voler le code source d'applications en développement pour copier des fonctionnalités innovantes et obtenir un avantage concurrentiel
Cybercriminel	Exfiltrer les données personnelles des utilisateurs pour les revendre sur le dark web
Hacktiviste	Perturber les services de MobiTech pour nuire à son image et dénoncer la collecte excessive de données personnelles
Employé mécontent	Saboter le développement d'une application majeure pour se venger d'un licenciement
État étranger	Implanter une porte dérobée dans une application populaire pour surveiller les communications des utilisateurs

Ce tableau présente une sélection de couples sources de risque / objectifs visés (SR/OV) pertinents pour MobiTech. Il couvre différents types d'attaquants potentiels et leurs motivations possibles, en lien avec les activités spécifiques de l'entreprise.

2. Évaluation de la pertinence

Sources de risque	Objectifs visés	Motivation	Activité	Ressources	Pertinence
Concurrent	Voler le code source d'applications en développement pour copier des fonctionnalités innovantes	Élevée	Modérée	Importantes	Élevée
Cybercriminel	Exfiltrer les données personnelles des utilisateurs pour les revendre sur le dark web	Élevée	Importante	Significatives	Élevée
Hacktiviste	Perturber les services de MobiTech pour nuire à son image et dénoncer la collecte	Modérée	Faible	Modérées	Moyenne

Sources de risque	Objectifs visés	Motivation	Activité	Ressources	Pertinence
	excessive de données personnelles				
Employé mécontent	Saboter le développement d'une application majeure pour se venger d'un licenciement	Élevée	Faible	Limitées	Moyenne
État étranger	Implanter une porte dérobée dans une application populaire pour surveiller les communications des utilisateurs	Modérée	Faible	Importantes	Faible

Ce tableau présente une évaluation de la pertinence des couples sources de risque / objectifs visés (SR/OV) pour MobiTech. La pertinence est évaluée en fonction de la motivation de la source de risque, de son niveau d'activité dans le secteur, et des ressources dont elle dispose pour mener à bien son objectif.

Voici un exemple d'évaluation de la pertinence des sources de risque pour MobiTech :

- **Concurrent / Voler le code source d'applications en développementa**

"Le dernier rapport trimestriel de MobiTech mentionne le développement d'une fonctionnalité innovante de réalité augmentée pour leur application phare, ce qui a suscité beaucoup d'intérêt dans l'industrie."

- **Cybercriminel / Exfiltrer les données personnelles des utilisateurs**

"Le rapport annuel de l'ANSSI indique une augmentation de 30% des attaques visant le vol de données personnelles dans le secteur des applications mobiles au cours de l'année écoulée."

- **Hacktiviste / Perturber les services de MobiTech**

"Un groupe hacktiviste connu a récemment publié un manifeste critiquant les pratiques de collecte de données des entreprises technologiques et a menacé de cibler plusieurs startups, dont potentiellement MobiTech."

- **Employé mécontent / Saboter le développement d'une application majeure**

"MobiTech a récemment procédé à une restructuration de son équipe de développement, ce qui a entraîné le licenciement de plusieurs employés seniors."

Les couples SR/OV jugés les plus pertinents (pertinence "Élevée") seront probablement retenus en priorité pour la suite de l'analyse de risque, tandis que ceux de pertinence "Moyenne" pourront être considérés dans un second temps. Le couple de pertinence "Faible" pourrait être écarté dans un premier temps, mais pourrait faire l'objet d'une surveillance.

Atelier 3 - Scénarios stratégiques

1. Cartographie de dangerosité des parties prenantes

Partie prenante	Catégorie
Clients	Utilisateurs finaux des applications mobiles
Partenaires technologiques	Fournisseurs de services cloud et API externes
Prestataires	Entreprises sous-traitantes pour le développement ou la maintenance des applications
Régulateurs	Autorités de régulation en matière de protection des données (ex. CNIL pour le RGPD)
Fournisseurs tiers	Développeurs d'outils ou bibliothèques intégrés aux applications

Partie prenante	Exposition	Fiabilité cyber	Niveau de dangerosité
Clients	Faible	Modérée	Faible
Partenaires technologiques	Élevée	Modérée	Élevée
Prestataires	Moyenne	Faible	Moyenne
Régulateurs	Faible	Élevée	Faible
Fournisseurs tiers	Moyenne	Faible	Moyenne

Cette analyse met en évidence les parties prenantes critiques qui nécessitent une attention particulière dans l'élaboration des scénarios stratégiques et la mise en place de mesures de sécurité adaptées.

Le diagramme suivant représente la cartographie de dangerosité des parties prenantes de MobiTech. Les parties prenantes sont positionnées selon leur **niveau d'exposition** (axe vertical) et leur **fiabilité cyber** (axe horizontal).

Les parties prenantes représentées sont (à titre d'exemple) :

- F3 : Fournisseur de services cloud
- C1 : Clients principaux
- P2 : Partenaires technologiques
- F1 : Fournisseurs d'outils de développement
- P1 : Prestataires de développement externe

- F2 : Fournisseur de services de paiement

Dans ce diagramme :

- La zone de danger (quadrant supérieur gauche) contient F2 et F3, qui sont les parties prenantes les plus critiques pour MobiTech.
- La zone de contrôle (quadrant supérieur droit) contient P1 et F1, qui nécessitent une attention particulière.
- La zone de veille (quadrant inférieur gauche) contient C1 et P2, qui présentent un risque moindre mais doivent être surveillées.

Cette représentation permet à MobiTech d'identifier rapidement les parties prenantes qui nécessitent une attention particulière dans sa stratégie de gestion des risques.

PPC
PPC

2. Scénarios stratégiques

L'équipe projet a décidé de représenter les scénarios opérationnels sous la forme de graphes d'attaque. Elle a choisi de se concentrer sur la réalisation d'un premier scénario opérationnel correspondant à un chemin d'attaque stratégique identifié dans l'atelier 2.

Scénario opérationnel relatif au chemin d'attaque "Un cybercriminel exfiltre les données des utilisateurs en exploitant une vulnérabilité dans la plateforme de gestion des utilisateurs".

L'équipe projet a étudié plusieurs techniques d'accès, parmi lesquelles des actions d'ingénierie sociale, permettant à l'attaquant de rentrer dans le système d'information. L'exploitation d'une éventuelle faille de sécurité non corrigée a été considérée à la suite du retour d'expérience du RSSI, mais reste à approfondir. Si une telle faille existe, alors elle pourrait également servir de point d'entrée pour d'autres attaques (flèche en pointillé).

3 modes opératoires ont été jugés pertinents.

1. L'attaquant s'introduit dans le système d'information en exploitant une faille de sécurité non corrigée dans le framework web. Il accède ensuite aux données des utilisateurs du fait notamment de l'absence de cloisonnement entre les différentes parties de l'application puis les exfiltre en utilisant un canal caché.
2. L'attaquant corrompt un employé de l'équipe de développement qui récupère ensuite facilement les informations depuis son poste de travail, dans la mesure où aucune action de supervision n'est réalisée sur les accès aux données sensibles.
3. L'attaquant exploite une vulnérabilité zero-day dans le système de gestion de base de données. Cette opération est facilitée par le fait que les mises à jour de sécurité ne sont pas appliquées régulièrement et que les accès à la base de données ne sont pas suffisamment restreints.

Lors de l'atelier, il a été noté à maintes reprises que le manque de rigueur actuel dans l'application des correctifs de sécurité facilitait considérablement l'exploitation de vulnérabilités.

L’exfiltration des données des utilisateurs par l’exploitation d’une vulnérabilité dans la plateforme de gestion est considérée comme quasi certaine. D’une part, la plateforme utilise des composants logiciels obsolètes et d’autre part, les contrôles d’accès aux données sensibles sont insuffisants. La combinaison de ces facteurs aggravants rend ce scénario particulièrement critique pour MobiTech.

Voici un autre exemple de scénario opérationnel pour MobiTech :

Scénario opérationnel relatif au chemin d’attaque “Un hacktiviste perturbe les services de MobiTech pour nuire à son image et dénoncer la collecte excessive de données personnelles”.

L’équipe projet a étudié plusieurs techniques d’accès, parmi lesquelles des actions d’ingénierie sociale, permettant à l’attaquant de rentrer dans le système d’information. L’exploitation d’une éventuelle faille de sécurité non corrigée a été considérée à la suite du retour d’expérience du RSSI, mais reste à approfondir. Si une telle faille existe, alors elle pourrait également servir de point d’entrée pour d’autres attaques (flèche en pointillé).

3 modes opératoires ont été jugés pertinents.

1. L’attaquant s’introduit dans le système d’information en exploitant une faille de sécurité non corrigée dans le framework web utilisé pour la plateforme de gestion des utilisateurs. Il accède ensuite aux données des utilisateurs du fait notamment de l’absence de cloisonnement entre les différentes parties de l’application puis les exfiltre en utilisant un canal caché.
2. L’attaquant corrompt un employé de l’équipe de développement qui récupère ensuite facilement les informations depuis son poste de travail, dans la mesure où aucune action de supervision n’est réalisée sur les accès aux données sensibles.
3. L’attaquant lance une attaque DDoS massive sur l’infrastructure cloud de MobiTech, exploitant le fait que les mesures de protection contre ce type d’attaque sont insuffisantes. Cette opération est facilitée par le fait que les capacités de mitigation n’ont pas été correctement dimensionnées et que les procédures de réponse à incident ne sont pas régulièrement testées.

Lors de l’atelier, il a été noté à maintes reprises que le manque de rigueur actuel dans l’application des correctifs de sécurité facilitait considérablement l’exploitation de vulnérabilités.

La perturbation des services de MobiTech par une attaque DDoS sur l’infrastructure cloud est considérée comme très vraisemblable. D’une part, les mesures de protection contre les attaques DDoS sont insuffisantes et d’autre part, les procédures de réponse à incident ne sont pas régulièrement testées. La combinaison de ces facteurs aggravants rend ce scénario particulièrement critique pour MobiTech.

Voici en résumé les principaux éléments scénarios stratégiques pour MobiTech avec leur niveau de gravité associé :

Sources de risque	Objectifs Visés	Chemins d'attaque stratégiques	Gravité
Cybercriminel	Exfiltrer les données des utilisateurs pour les revendre	Trois chemins d'attaque à investiguer. Un cybercriminel exfiltre les données des utilisateurs : 1. en compromettant un fournisseur de services cloud ; 2. en exploitant une vulnérabilité dans la plateforme de gestion des utilisateurs ; 3. en attaquant directement l'infrastructure de stockage des données.	4 Critique
Hacktiviste	Perturber les services de MobiTech pour nuire à son image et dénoncer la collecte excessive de données personnelles	Deux chemins d'attaque à investiguer. Un hacktiviste perturbe les services de MobiTech : 1. en provoquant une interruption du service par une attaque DDoS massive sur l'infrastructure cloud ; 2. en exploitant une faille de sécurité dans la plateforme de gestion des utilisateurs pour accéder et divulguer des données personnelles.	4 Critique

3. Définition des mesures de sécurité sur l'écosystème

Partie prenante	Chemins d'attaque stratégiques	Mesures de sécurité	Menace initiale	Menace résiduelle
Plateforme de gestion des utilisateurs	Exploiter une vulnérabilité dans la plateforme pour accéder aux données des utilisateurs.	- Mettre en place une politique stricte de mise à jour des frameworks et bibliothèques. - Renforcer les mécanismes d'authentification (authentification multi-facteurs). - Cloisonner les données sensibles pour limiter l'accès.	3,5	2
Infrastructure cloud	Lancer une attaque DDoS massive sur l'infrastructure cloud pour perturber les services.	- Augmenter la capacité de mitigation des attaques DDoS via un fournisseur spécialisé. - Tester régulièrement les procédures de réponse à incident. - Mettre en place une surveillance proactive des flux réseau.	4	2,5

Ce tableau synthétise les chemins d'attaque stratégiques identifiés, les mesures de sécurité proposées pour réduire le risque, et l'évolution estimée des niveaux de menace après mise en œuvre des mesures.

Atelier 4 - Scénarios opérationnels

1. Élaborer les scénarios opérationnels

L'équipe projet a décidé de représenter les scénarios opérationnels sous la forme de graphes d'attaque. Elle a choisi de se concentrer sur la réalisation d'un premier scénario opérationnel correspondant à un chemin d'attaque stratégique identifié dans l'atelier 3.

Scénario opérationnel relatif au chemin d'attaque "Un cybercriminel exfiltre les données des utilisateurs en exploitant une vulnérabilité dans la plateforme de gestion des utilisateurs" :

Connaître	Rentrer	Trouver	Exploiter
Reconnaissance externe sources ouvertes	Exploitation d'une faille de sécurité dans le framework web	Latéralisation vers la base de données utilisateurs	Vol et exfiltration des données utilisateurs
Reconnaissance externe avancée	Instruction via mail de hameçonnage ciblé sur un développeur	Reconnaissance interne du réseau	Création et maintien d'un canal d'exfiltration via un serveur compromis
Corruption d'un employé de l'équipe de développement	Élévation de privilèges	Exploitation d'un maliciel de collecte et d'exfiltration	
Exploitation d'une vulnérabilité zero-day dans le système de gestion de base de données			

L'équipe projet a étudié plusieurs techniques d'accès, parmi lesquelles des actions d'ingénierie sociale, permettant à l'attaquant de rentrer dans le système d'information. L'exploitation d'une éventuelle faille de sécurité non corrigée a été considérée à la suite du retour d'expérience du RSSI, mais reste à approfondir. Si une telle faille existe, alors elle pourrait également servir de point d'entrée pour d'autres attaques (flèche en pointillé).

3 modes opératoires ont été jugés pertinents.

1. L'attaquant s'introduit dans le système d'information en exploitant une faille de sécurité non corrigée dans le framework web. Il accède ensuite aux données des utilisateurs du fait

notamment de l’absence de cloisonnement entre les différentes parties de l’application puis les exfiltre en utilisant un canal caché.

2. L’attaquant corrompt un employé de l’équipe de développement qui récupère ensuite facilement les informations depuis son poste de travail, dans la mesure où aucune action de supervision n’est réalisée sur les accès aux données sensibles.
3. L’attaquant exploite une vulnérabilité zero-day dans le système de gestion de base de données. Cette opération est facilitée par le fait que les mises à jour de sécurité ne sont pas appliquées régulièrement et que les accès à la base de données ne sont pas suffisamment restreints.

Schéma d’attaque
Schéma d’attaque

2. Évaluation de la vraisemblance des scénarios opérationnels

Chemins d’attaque stratégiques (associés aux scénarios opérationnels)	Vraisemblance globale
Un cybercriminel exfiltre les données des utilisateurs en exploitant une faille de sécurité dans le framework web	V4 Quasi-certain
Un cybercriminel exfiltre les données des utilisateurs en corrompant un employé de l’équipe de développement	V2 Vraisemblable
Un cybercriminel exfiltre les données des utilisateurs en exploitant une vulnérabilité zero-day dans le système de gestion de base de données	V3 Très vraisemblable
Un hacktiviste perturbe les services en lançant une attaque DDoS massive sur l’infrastructure cloud	V3 Très vraisemblable
Un hacktiviste perturbe les services en exploitant une faille de sécurité dans la plateforme de gestion des utilisateurs pour accéder et divulguer des données personnelles	V2 Vraisemblable

L’exfiltration des données des utilisateurs par l’exploitation d’une faille de sécurité dans le framework web est considérée comme quasi certaine. D’une part, le framework utilisé comporte des composants logiciels obsolètes et d’autre part, les mises à jour de sécurité ne sont pas appliquées régulièrement. La combinaison de ces facteurs aggravants rend ce scénario particulièrement critique pour MobiTech.

Atelier 5 - Traitement du risque

1. Réaliser une synthèse des scénarios de risque

Scénario stratégique	Gravité	Vraisemblance	Niveau de risque
Un cybercriminel exfiltre les données des utilisateurs en exploitant une faille de sécurité dans le framework web	4	4	Critique
Un cybercriminel exfiltre les données des utilisateurs en corrompant un employé de l'équipe de développement	4	2	Majeur
Un cybercriminel exfiltre les données des utilisateurs en exploitant une vulnérabilité zero-day dans le système de gestion de base de données	4	3	Critique
Un hacktiviste perturbe les services en lançant une attaque DDoS massive sur l'infrastructure cloud	4	3	Critique
Un hacktiviste perturbe les services en exploitant une faille de sécurité dans la plateforme de gestion des utilisateurs pour accéder et divulguer des données personnelles	4	2	Majeur

Ce tableau synthétise les scénarios stratégiques identifiés pour MobiTech, en indiquant leur gravité, leur vraisemblance, et le niveau de risque résultant. Les niveaux de risque sont déterminés en combinant la gravité et la vraisemblance de chaque scénario.

L'exfiltration des données des utilisateurs par l'exploitation d'une faille de sécurité dans le framework web est considérée comme le risque le plus critique, avec une gravité et une vraisemblance maximales. Cela s'explique par l'utilisation de composants logiciels obsolètes et le manque de rigueur dans l'application des mises à jour de sécurité.

Les attaques DDoS et l'exploitation de vulnérabilités zero-day sont également considérées comme des risques critiques, en raison de leur impact potentiel élevé et de leur vraisemblance importante.

Les scénarios impliquant la corruption d'un employé ou l'exploitation d'une faille pour divulguer des données personnelles sont jugés comme des risques majeurs, principalement en raison de leur vraisemblance plus faible.

2. Décider de la stratégie de traitement du risque et définir les mesures de sécurité

Scénario stratégique	Gravité	Vraisemblance	Niveau de risque	Traitement	Mesures de sécurité
Un cybercriminel exfiltre les données des utilisateurs en exploitant une faille de sécurité dans le framework web	4	4	Critique	Réduire	- Mettre en place une politique stricte de mise à jour des frameworks et bibliothèques - Renforcer les mécanismes d'authentification (authentification multi-facteurs) - Cloisonner les données sensibles pour limiter l'accès
Un cybercriminel exfiltre les données des utilisateurs en corrompant un employé de l'équipe de développement	4	2	Majeur	Réduire	- Sensibiliser et former régulièrement les employés à la sécurité - Mettre en place une politique de contrôle d'accès stricte - Implémenter un système de détection des comportements suspects
Un cybercriminel exfiltre les données des utilisateurs en exploitant une vulnérabilité zero-day dans le système de gestion de base de données	4	3	Critique	Réduire	- Mettre en place une surveillance proactive des vulnérabilités - Renforcer la segmentation du réseau - Implémenter un système de détection d'intrusion (IDS)

Scénario stratégique	Gravité	Vraisemblance	Niveau de risque	Traitement	Mesures de sécurité
Un hacktiviste perturbe les services en lançant une attaque DDoS massive sur l'infrastructure cloud	4	3	Critique	Réduire	- Augmenter la capacité de mitigation des attaques DDoS - Mettre en place une surveillance proactive des flux réseau - Élaborer et tester régulièrement un plan de continuité d'activité
Un hacktiviste perturbe les services en exploitant une faille de sécurité dans la plateforme de gestion des utilisateurs pour accéder et divulguer des données personnelles	4	2	Majeur	Réduire	- Effectuer des audits de sécurité réguliers de la plateforme - Renforcer le chiffrement des données personnelles - Mettre en place un système de gestion des accès privilégiés

Ce tableau synthétise les scénarios stratégiques identifiés pour MobiTech en ajoutant la stratégie de traitement choisie et les mesures de sécurité proposées pour réduire chaque risque.

Pour tous les scénarios, la stratégie de traitement choisie est de réduire le risque, étant donné leur impact potentiel significatif sur l'entreprise. Les mesures de sécurité proposées visent à renforcer la protection des données, améliorer la détection des menaces et renforcer la résilience de l'infrastructure de MobiTech.