Application mobile d'analyse des risques

Nom de l'entreprise

Épreuve E5 - PRODUCTION ET FOURNITURE DE SERVICES INFORMATIQUES

DATE	PRESTATIONS REALISEES PAR :	PRESTATIONS REALISEES POUR :
09/11/2023		Épreuve E5 - PRODUCTION ET FOURNITURE DE SERVICES INFORMATIQUES

Contexte de l'Entreprise :

CyberGuard Solutions est une entreprise spécialisée dans la sécurité informatique et la gestion des risques cyber. L'entreprise offre des services de consultation en sécurité informatique aux entreprises de toutes tailles, les aidant à identifier, évaluer et atténuer les risques liés à la sécurité de leurs systèmes d'information. Avec une équipe d'experts en sécurité informatique, CyberGuard Solutions a acquis une solide réputation en fournissant des solutions personnalisées pour renforcer la sécurité de ses clients.

Objectifs de l'Entreprise :

CyberGuard Solutions vise à répondre aux besoins croissants de ses clients en matière de sécurité informatique. L'entreprise cherche à améliorer la qualité de ses services d'audit en fournissant une application mobile dédiée à ses consultants. Cette application permettra aux consultants de mener des évaluations de risques plus efficaces et de fournir des rapports d'audit de haute qualité à leurs clients.

Rôle de l'Application Mobile :

L'application mobile à développer sera un outil essentiel pour les consultants de CyberGuard Solutions lors de leurs missions d'audit en entreprise. Elle leur permettra de collecter des données sur les actifs informatiques, de gérer les menaces et vulnérabilités, d'estimer les risques, et de générer des rapports d'audit détaillés. L'application vise à automatiser une partie du processus d'audit tout en offrant la flexibilité nécessaire pour personnaliser les évaluations de risques en fonction des besoins spécifiques de chaque client.

Avantages de l'Application :

L'application mobile apportera plusieurs avantages à CyberGuard Solutions :

- Amélioration de l'efficacité des consultants en automatisant certaines tâches répétitives.
- Standardisation des processus d'audit pour garantir la cohérence dans les évaluations de risques.
- Génération de rapports d'audit plus rapidement, améliorant la réactivité envers les clients.
- Possibilité de fournir des recommandations de sécurité spécifiques pour atténuer les risques.

Concurrents et Différenciation :

Bien que de nombreuses entreprises proposent des services de sécurité informatique, CyberGuard Solutions se distingue par son engagement envers l'innovation technologique. L'application mobile prévue offre un avantage concurrentiel en termes de qualité et d'efficacité des services fournis par l'entreprise.

Enjeux et Contraintes :

Le projet doit respecter des contraintes budgétaires et de délais, et doit garantir la sécurité des données collectées par l'application. De plus, l'application doit être conviviale pour les consultants, même pour ceux ayant peu d'expérience en technologie mobile.

Ce contexte d'entreprise illustre comment l'application mobile d'analyse des risques cyber en entreprise s'inscrit dans la stratégie globale de CyberGuard Solutions en matière de sécurité informatique, en améliorant ses services de consultation pour répondre aux besoins de ses clients de manière plus efficace et réactive.

Objectif :

L'objectif de cette application mobile est de fournir aux consultants un outil efficace pour l'analyse des risques cyber lors des audits en entreprise. L'application doit être conviviale, intuitive et offrir des fonctionnalités avancées pour faciliter le processus d'analyse des risques. Elle doit prendre en compte les besoins spécifiques des consultants en matière de gestion des actifs, de gestion des menaces et des vulnérabilités, ainsi que d'estimation des risques automatique et manuelle avec évaluation de la gravité.

Fonctionnalités requises :

- Inventaire des actifs : Permettre aux consultants de recenser et de gérer les actifs numériques et matériels de l'entreprise, tels que les serveurs, les bases de données, les ordinateurs, etc.
- Gestion des menaces et des vulnérabilités : Fournir une fonctionnalité permettant d'identifier, d'évaluer et de gérer les menaces et les vulnérabilités liées aux actifs de l'entreprise. Cette fonctionnalité devrait inclure des bases de données de référence pour les menaces courantes et les vulnérabilités connues.
- Estimation des risques : Offrir la possibilité de réaliser des évaluations de risques automatiques et manuelles en utilisant des modèles prédéfinis ou en permettant aux consultants de créer leurs propres modèles personnalisés. L'application doit également permettre d'évaluer la gravité des risques identifiés.
- Rapports et recommandations : Générer des rapports détaillés sur les résultats des analyses de risques, ainsi que des recommandations pour atténuer les risques identifiés. Les rapports doivent être personnalisables et exportables dans différents formats, tels que PDF, CSV, etc.
- Sécurité des données : Assurer la confidentialité et l'intégrité des données collectées et stockées par l'application. Mettre en place des mesures de sécurité robustes, telles que le chiffrement des données et l'authentification des utilisateurs.

Intégration avec d'autres outils : Permettre l'intégration de l'application avec d'autres outils et systèmes pertinents pour faciliter le processus d'audit et d'analyse des risques, tels que les outils de gestion des incidents, les systèmes de gestion des vulnérabilités, etc.

Période d'exécution

Les services commenceront le 8 novembre 2023, et se poursuivront jusqu'au 30 mars 2024.

Ressources de participation

Equipe de 3 personnes

Ordinateur du lycée ou personnel

Machine virtuelle sous windows

Logiciel de developpement Windev mobile

Github

Fonctionnalités

- Saisie de l'Inventaire des Actifs
  - Permettre aux consultants de saisir les informations sur les actifs informatiques de l'entreprise, y compris les serveurs, les applications, les périphériques, etc.
  - Possibilité de décrire chaque actif, d'indiquer sa localisation et son importance pour l'entreprise.
- Gestion des Menaces et Vulnérabilités
  - Intégrer une base de données de menaces et de vulnérabilités.
  - Permettre aux consultants de faire correspondre les menaces aux actifs, et d'indiquer les vulnérabilités associées.
- Estimation des Risques (Automatique)
  - Intégrer un mécanisme automatique d'estimation des risques en fonction des actifs, des menaces, et des vulnérabilités.
  - Générer des évaluations de risques préliminaires.
- Estimation des Risques (Manuelle)
  - Permettre aux consultants d'ajuster manuellement les évaluations de risques.
  - Prendre en compte des facteurs tels que la gravité, la probabilité, et l'impact.

Contraintes Techniques

- Plateformes
  - L'application doit être développée pour les plateformes iOS et Android.
- Sécurité
  - La sécurité des données est une priorité, y compris la protection des informations sensibles concernant les actifs et les évaluations des risques.
- Performance
  - L'application doit être réactive et performante, même avec des volumes importants de données.

Matériaux livrables

Les livrables attendus incluent l'application mobile, la documentation technique, et les rapports d'audit générés.

Évaluation de la Qualité

L'entrepreneur doit avoir rempli ses obligations lorsque l'un des événements suivants se produit pour la première fois :

- L'entrepreneur accomplit les activités de l'entrepreneur décrites dans le présent EDT, y compris la livraison au client des matériaux énumérés dans la section intitulée « Matériaux livrables », et le client accepte ces activités et ces matériaux sans objections déraisonnables. Aucune réponse du client dans les 2 jours ouvrables suivant la livraison des produits livrables par l'entrepreneur est considérée comme une acceptation.
- L'entrepreneur et/ou le client a le droit d'annuler les services ou les livrables non encore fournis avec un préavis écrit de 20 jours ouvrables à l'autre partie.

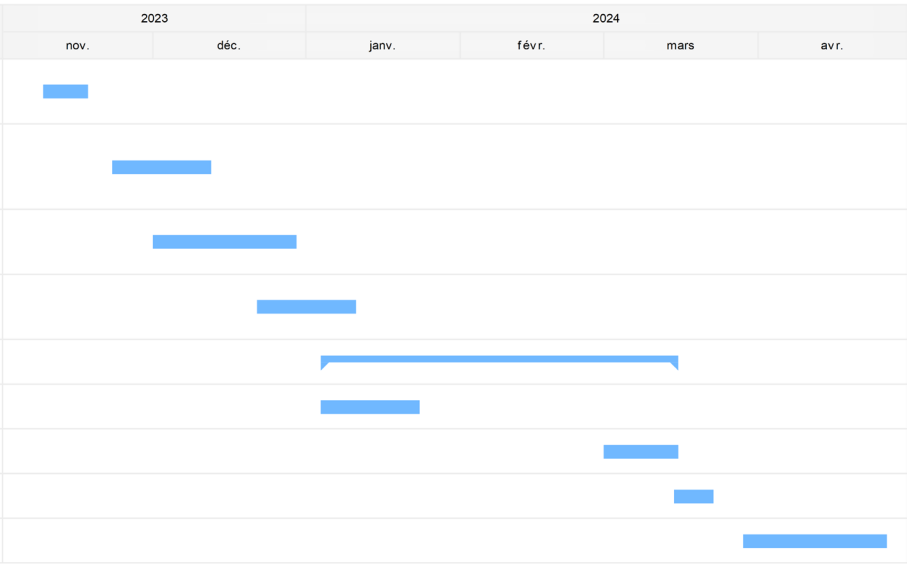
L'application sera évaluée en fonction de la précision de l'estimation des risques, de la fiabilité de l'application, et de la satisfaction des utilisateurs.

Hypothèses répartition des activités

Vous trouverez ci-dessous une idée pour la répartition de votre charge de travail.

réalisation du projet de l'application mobile d'analyse des risques cyber en entreprise

ID	Tache	Durée	Complete
1	Élaboration du cahier des charges	7.0 d.	0.0%
2	Conception de l'app (interface, bases de données, sécurité)	14.0 d.	0.0%
3	Développement de l'app (front-end, back-end)	21.0 d.	0.0%
4	Intégration des fonctionnalités	14.0 d.	0.0%
5	**Tests et débogage**	52.0 d.	0.0%
6	Test P1	14.0 d.	0.0%
7	Test P2	11.0 d.	0.0%
8	Documentation technique	6.0 d.	0.0%
9	Oral	21.0 d.	0.0%



Procédure de travail

- Élaboration du cahier des charges

L'élaboration du cahier des charges est une étape cruciale dans le processus de développement de tout projet informatique, y compris la création de l'application mobile pour l'analyse des risques cyber en entreprise. Voici le détail du travail à effectuer lors de cette phase :

- Collecte d'Informations :
  - Identifier les besoins et les objectifs du projet en consultation avec les parties prenantes, y compris les consultants, les clients, et les équipes de développement.
  - Recueillir des informations sur le contexte du projet, l'environnement organisationnel, et les contraintes spécifiques.
- Définition des Objectifs :
  - Clarifier les objectifs du projet, y compris la création de l'application mobile, les fonctionnalités clés à inclure, les plateformes cibles (iOS, Android), et les résultats attendus.
- Identification des Fonctionnalités:
  - Déterminer les fonctionnalités essentielles de l'application, notamment la saisie de l'inventaire des actifs, la gestion des menaces et vulnérabilités, et l'estimation des risques (automatique et manuelle).
  - Identifier d'autres caractéristiques importantes telles que l'authentification, la sécurité des données, la génération de rapports, etc.
- Sélection des Technologies :
  - Choisir les technologies nécessaires pour le développement de l'application mobile, y compris les langages de programmation, les frameworks, les bases de données, etc.
- Sécurité des Données :
  - Définir les mesures de sécurité nécessaires pour protéger les données sensibles collectées par l'application.
  - Identifier les protocoles de chiffrement, les mécanismes d'authentification, et les stratégies de protection des données.
- Spécifications Techniques :

        - Établir des spécifications techniques pour l'application, y compris les interfaces utilisateur, les bases de données, les flux de données, et les critères de performance (Diagramme du modèle de flux de données, modélisation UML, architecture logiciel, organigramme du programme, structure du programme, MCD, etc...).
    - Contraintes Budgétaires et Calendrier :
        - Définir les contraintes budgétaires, y compris les coûts de développement, les ressources humaines, et les autres dépenses.
        - Établir un calendrier préliminaire pour le projet, y compris la date de début et la date de fin.
    - Gestion des Risques :
        - Identifier les risques potentiels liés au projet, tels que les retards, les changements de portée, et les problèmes techniques.
        - Élaborer un plan de gestion des risques pour atténuer les impacts négatifs.
    - Approbation des Parties Prenantes :
        - Partager le brouillon initial du cahier des charges avec les parties prenantes et recueillir leurs commentaires et suggestions.
        - Réviser et finaliser le cahier des charges en fonction des retours reçus.
    - Validation du Cahier des Charges :
        - Obtenir l'approbation formelle de toutes les parties prenantes, y compris les clients, les consultants, et les équipes de développement, pour le cahier des charges final.

- Conception de l'app (interface, bases de données, sécurité)

La phase de conception de l'application est cruciale pour définir en détail l'architecture de l'application mobile, y compris son interface utilisateur, sa base de données, et ses mesures de sécurité. Voici le détail du travail à effectuer lors de cette phase :

    - Conception de l'Interface Utilisateur (UI) :
        - Élaboration des maquettes et des prototypes de l'interface utilisateur en tenant compte des besoins des utilisateurs.
        - Définition de la structure de l'interface, de l'agencement des éléments, et de la navigation entre les écrans.
        - Création d'une expérience utilisateur (UX) conviviale en utilisant des éléments de conception tels que des icônes, des couleurs et des typographies cohérentes.
    - Conception de la Base de Données :
        - Définition du modèle de données qui stockera les informations liées aux actifs, aux menaces, aux vulnérabilités et aux évaluations des risques.
        - Spécification des tables, des champs et des relations entre les données.
        - Choix du système de gestion de base de données (SGBD) approprié, en prenant en compte la sécurité et les performances.
    - Conception de la Sécurité :
        - Identification des vulnérabilités potentielles et des menaces de sécurité spécifiques à l'application.
        - Définition des mécanismes de sécurité, notamment l'authentification, l'autorisation, le chiffrement des données et la protection contre les attaques.
        - Élaboration d'un plan de gestion des risques de sécurité pour minimiser les vulnérabilités.
    - Choix des Technologies :
        - Sélection des technologies et des frameworks appropriés pour le développement de l'application mobile en fonction des spécifications de sécurité et de performances.
        - Détermination des langages de programmation, des bibliothèques et des outils nécessaires pour la conception.
    - Planification de la Performance :
        - Élaboration d'un plan pour garantir que l'application soit réactive et performante, même avec un grand volume de données.
        - Optimisation de l'application en termes de vitesse d'exécution et d'utilisation de la mémoire.
    - Intégration de la Sécurité :
        - Intégration de mécanismes de sécurité tout au long de l'application, y compris la validation des entrées, la protection contre les injections SQL, et la gestion des identifiants de session.
        - Mise en place de mesures de sécurité pour les communications entre l'application et les serveurs, notamment l'utilisation de protocoles sécurisés.
    - Choix des Outils de Développement :
        - Sélection des outils de développement, de test et de débogage nécessaires pour le projet.
        - Mise en place de l'environnement de développement, y compris les IDE (environnements de développement intégrés) et les systèmes de contrôle de version.
    - Documentation de Conception :

        - Rédaction de la documentation de conception technique qui décrit en détail l'architecture de l'application, les interfaces, la base de données, les éléments de sécurité, et d'autres aspects techniques.
    - Validation de la Conception :
        - Révision et validation de la conception avec les parties prenantes pour s'assurer qu'elle répond aux besoins et aux attentes du projet.

Une fois la conception de l'application complète et validée, l'équipe de développement peut commencer la phase de développement proprement dite en se basant sur cette conception détaillée. Il est essentiel de maintenir la cohérence entre la conception et le développement pour garantir la réussite du projet.

- Développement de l'app (front-end, back-end)

Le développement de l'application mobile comprend deux aspects importants : le développement du front-end et le développement du back-end. Voici le détail du travail à effectuer lors de ces deux phases :

    - Programmation de l'Interface Utilisateur (UI) :
        - Convertir les maquettes et les prototypes de l'interface utilisateur en code.
        - Créer les écrans, les composants d'interface utilisateur et les interactions conformément à la conception.
    - Gestion de la Navigation :
        - Mettre en place la navigation entre les différents écrans de l'application.
        - Assurer une expérience utilisateur fluide et intuitive.
    - Intégration des Données :
        - Intégrer les données collectées dans l'interface utilisateur, en affichant les actifs, les menaces, les vulnérabilités et les évaluations des risques de manière compréhensible.
    - Optimisation de la Performance :
        - Veiller à ce que l'application soit réactive et performante en optimisant les éléments d'interface et en minimisant les temps de chargement.
    - Gestion des Événements :
        - Programmer les interactions utilisateur, telles que la saisie de données, la gestion des actions et les événements.
    - Tests du Front-End :
        - Effectuer des tests d'interface utilisateur pour s'assurer que l'interface fonctionne correctement sur toutes les plateformes cibles (iOS et Android).
        - Identifier et résoudre les bogues et les problèmes d'affichage.

- Développement du Back-End :
    - Création de la Base de Données :
        - Mettre en place la base de données en utilisant le modèle de données conçu précédemment.
        - Créer des tables, des index et des relations nécessaires.
    - Programmation des Services Web :
        - Développer les services web pour la gestion des actifs, des menaces, des vulnérabilités et des évaluations des risques.
        - Assurer la communication sécurisée entre le front-end et le back-end.
    - Logique de l'Application :
        - Mettre en œuvre la logique de l'application, y compris les algorithmes pour l'estimation des risques (automatique et manuelle).
        - Intégrer des mécanismes d'authentification et d'autorisation pour garantir la sécurité.
    - Optimisation de la Performance :
        - S'assurer que le back-end est capable de gérer un grand volume de données de manière efficace.
        - Optimiser les requêtes de base de données et les opérations pour des performances optimales.
    - Sécurité du Back-End :
        - Implémenter des mesures de sécurité, y compris la validation des entrées, la protection contre les injections SQL et la gestion des sessions.
    - Tests du Back-End :
        - Effectuer des tests unitaires et des tests d'intégration pour s'assurer que le back-end fonctionne correctement et communique efficacement avec le front-end.
    - Documentation du Back-End :
        - Rédiger une documentation technique pour le back-end, décrivant les services, les bases de données, et les éléments de sécurité.

Une fois le développement du front-end et du back-end terminé, l'application mobile doit être testée dans son ensemble pour garantir son bon fonctionnement. Les tests d'intégration entre les deux parties (front-end et back-end) sont également essentiels pour identifier et corriger tout problème d'interaction entre les composants.

- Intégration des fonctionnalités

L'intégration des fonctionnalités est une étape clé dans le processus de développement de l'application mobile. Elle consiste à assembler toutes les parties du système, y compris le front-end, le back-end, les services, les bases de données, et les composants de l'interface utilisateur, pour former une application fonctionnelle. Voici le détail du travail à effectuer lors de l'intégration des fonctionnalités :

- Intégration du Front-End et du Back-End :
  - Assurer que le front-end et le back-end sont correctement connectés.
  - Vérifier que les requêtes et les réponses entre les deux parties sont cohérentes et conformes à la documentation.
- Tests d'Intégration :
  - Effectuer des tests d'intégration pour s'assurer que l'application fonctionne de manière globale.
  - Identifier et résoudre les problèmes d'interaction entre le front-end et le back-end.
- Gestion des Données :
  - Assurer la synchronisation des données entre le front-end et le back-end.
  - Valider que les données sont correctement stockées dans la base de données et accessibles depuis l'interface utilisateur.
- Gestion des Sessions et de l'Authentification :
  - Vérifier que les mécanismes d'authentification et de gestion des sessions fonctionnent correctement.
  - S'assurer que les utilisateurs sont correctement identifiés et autorisés à accéder aux fonctionnalités de l'application.
- Tests de Performance :
  - Mesurer les performances de l'application en simulant des charges de travail réalistes.
  - Identifier les éventuels goulets d'étranglement de performance et les optimiser.
- Tests de Sécurité :
  - Effectuer des tests de sécurité pour identifier et corriger les vulnérabilités éventuelles.
  - Vérifier que les mécanismes de sécurité, y compris le chiffrement et la protection contre les attaques, sont en place et fonctionnent correctement.
- Tests d'Utilisation Réelle :
  - Engager des utilisateurs réels ou des bêta-testeurs pour évaluer l'application dans des scénarios d'utilisation réelle.
  - Recueillir des commentaires sur l'expérience utilisateur, les bogues et les problèmes de convivialité.
- Validation de la Conformité aux Exigences (Oral):
  - Comparer l'application aux exigences du cahier des charges initial pour s'assurer qu'elle répond aux besoins et aux attentes des parties prenantes.
- Optimisation (Oral):
  - Identifier les zones d'optimisation possibles en termes de performances, de sécurité, et d'expérience utilisateur.
  - Mettre en œuvre les améliorations nécessaires.
- Documentation de l'Intégration (Oral):
  - Documenter le processus d'intégration, y compris les problèmes rencontrés et les solutions apportées.
  - Mettre à jour la documentation technique au besoin.
- Formation :
  - Prévoir la formation des utilisateurs finaux et des administrateurs système sur l'utilisation de l'application.
- Validation des Parties Prenantes :
  - Impliquer les parties prenantes pour la validation finale de l'application intégrée.
  - Obtenir leur approbation pour le lancement.

Une fois que l'intégration des fonctionnalités est complète et que l'application répond aux exigences et aux normes de qualité, elle est prête à être déployée pour les utilisateurs finaux. Il est essentiel de consacrer du temps à cette phase pour garantir que l'application fonctionne de manière fiable et répond aux besoins des utilisateurs.

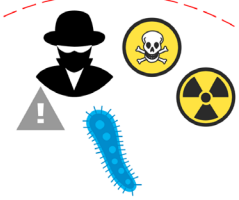
Les différentes étapes de l'analyse des risques cyber

1

Identification des actifs informatiques

La première étape consiste à identifier tous les actifs informatiques de l'entreprise, tels que les systèmes, les logiciels, les données sensibles et les équipements. Il est important de connaître précisément ce qui doit être protégé.

2



Évaluation des vulnérabilités

Une fois les actifs identifiés, il est essentiel d'évaluer les vulnérabilités potentielles de chaque actif. Cela inclut l'examen des systèmes obsolètes, des configurations incorrectes, des mots de passe faibles, des accès non autorisés et d'autres facteurs de risque.

3

Estimation de l'impact des menaces .

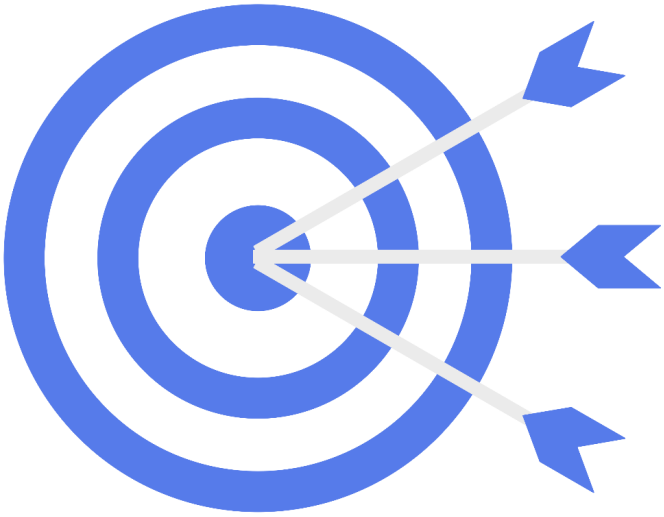
À cette étape, il convient d'évaluer l'impact financier, opérationnel et réputationnel que chaque vulnérabilité peut avoir sur l'entreprise. Il est important de considérer les conséquences d'une éventuelle exploitation de ces vulnérabilités.

4

Priorisation des mesures de protection

Enfin, il est essentiel de hiérarchiser les mesures de protection en fonction de l'impact potentiel et de la probabilité d'occurrence des menaces. Cela permet de définir une stratégie de cybersécurité efficace et de mettre en place les contrôles appropriés.

Identification des actifs



Inventaire visuel des systèmes d'information

01

Parcourir les locaux de l'organisation pour inventorier les actifs du système d'information.

- Matériels (type, Adresse MAC, Adresse IP, configuration, etc.)
- Logiciel (Libelle, version, licence, installation)

Scanner le réseau

02

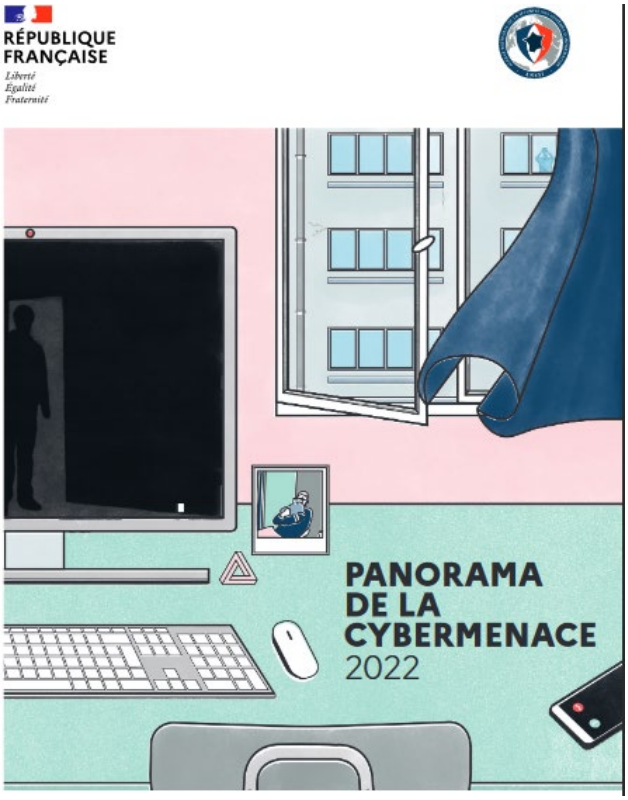
Scanner le réseau pour observer toutes les connexions présentes sur l'environnement de l'organisation

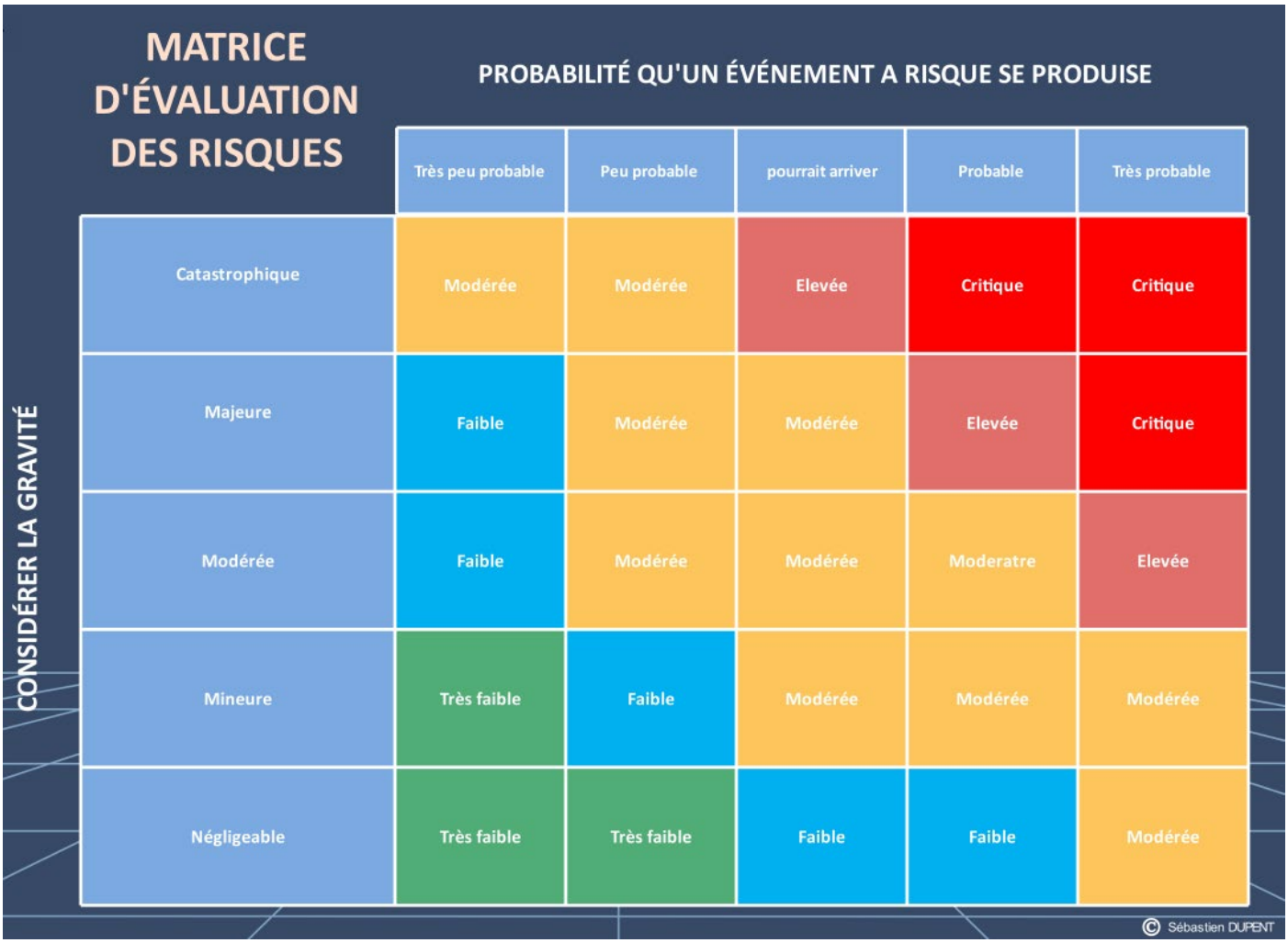
Inventaire précédent

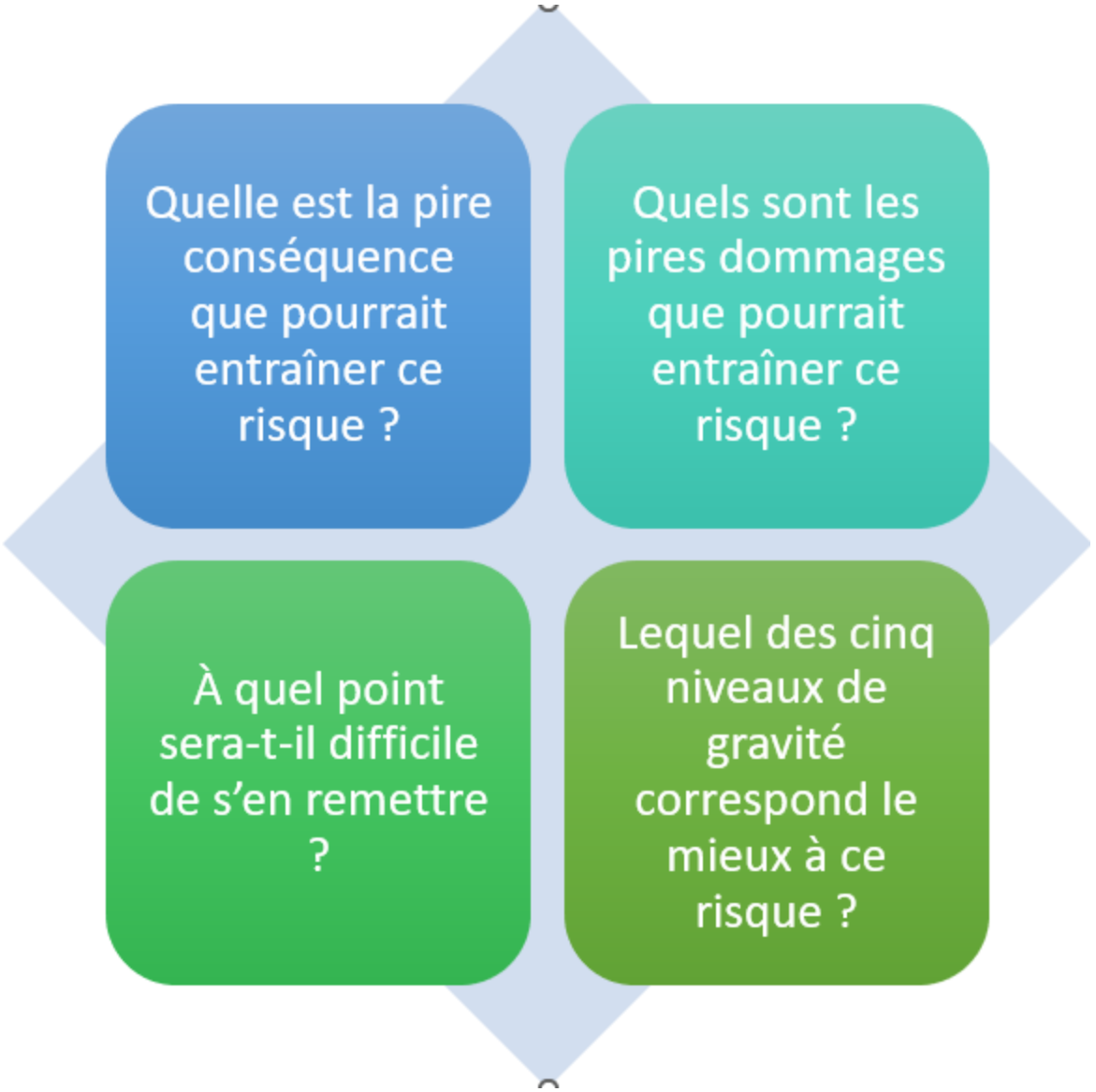
03

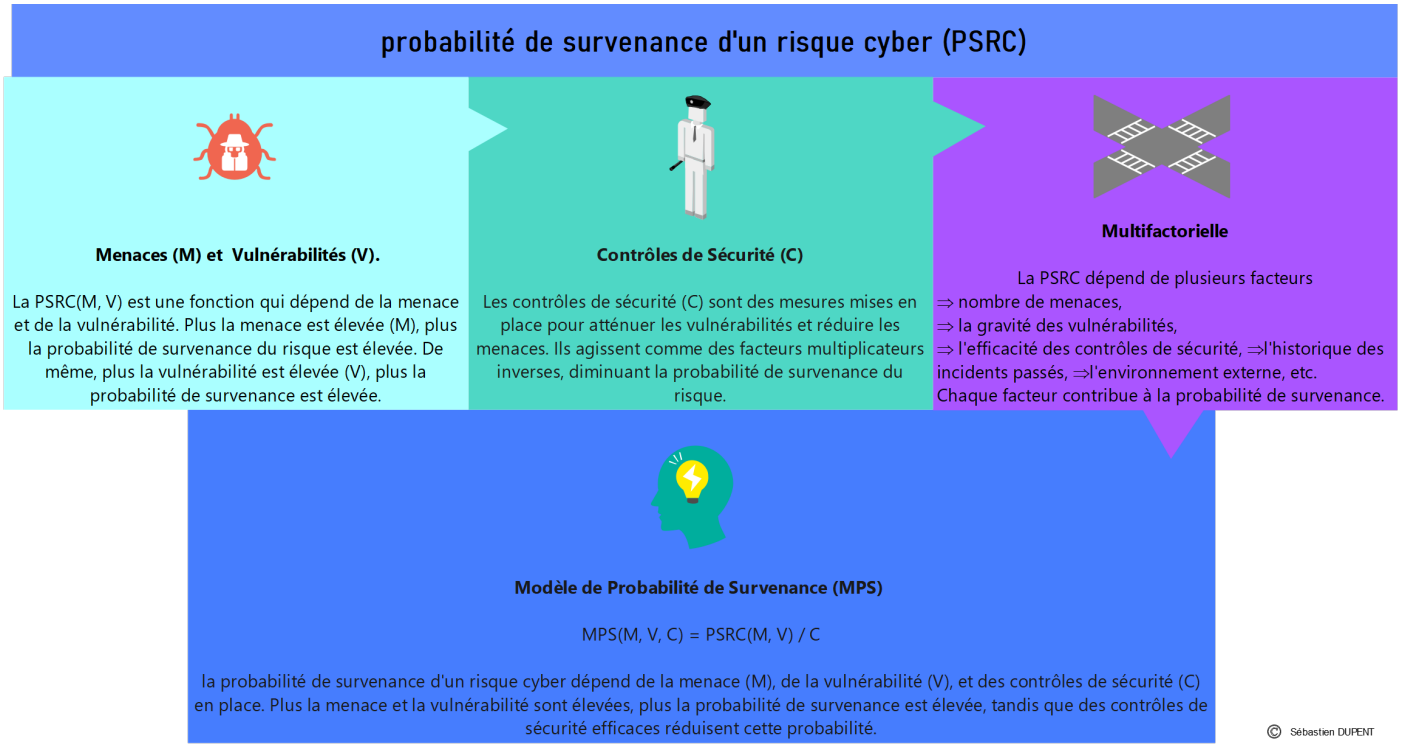
Consulter les inventaires précédents et les achats effectué.

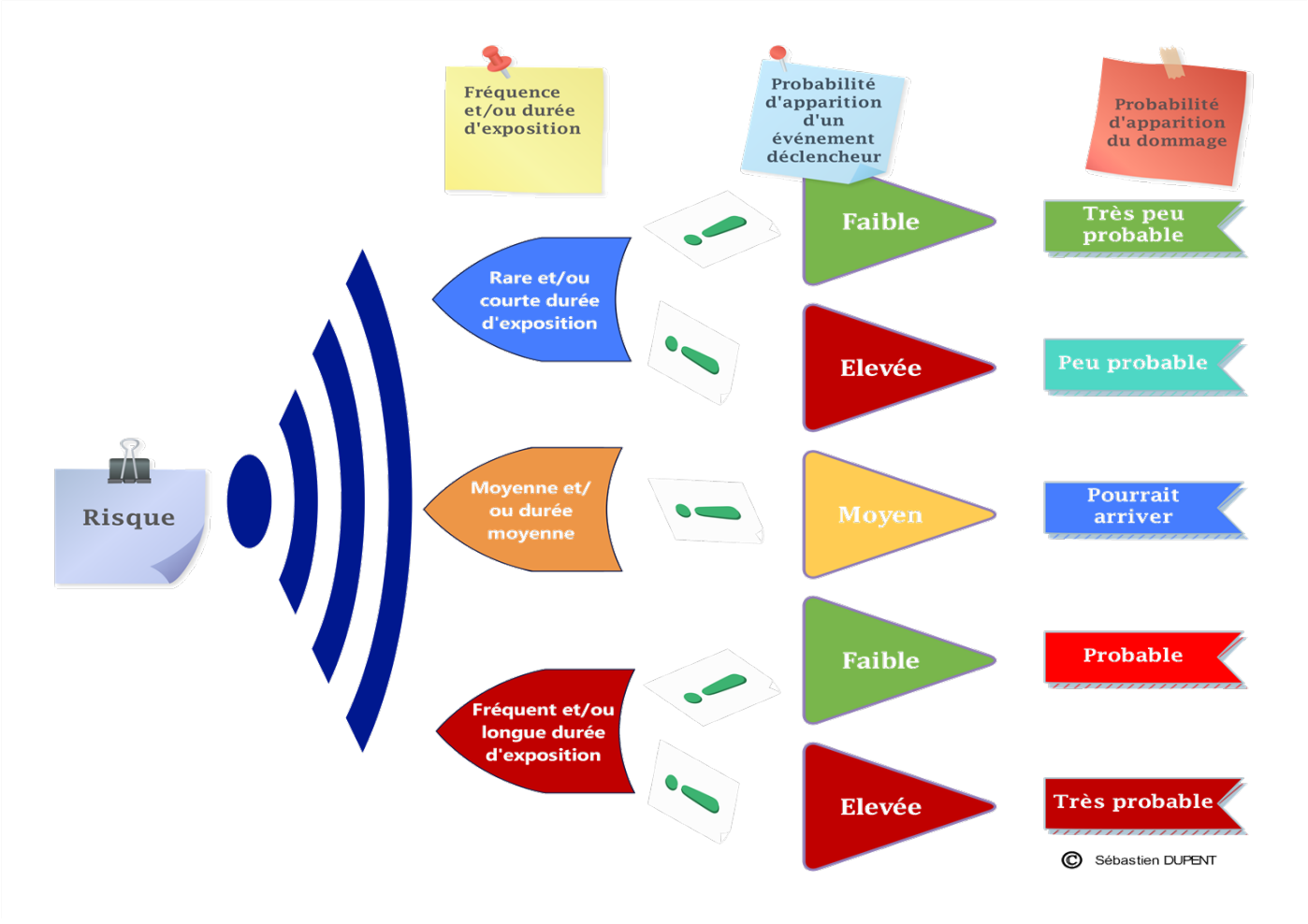
© Sébastien DUPENT

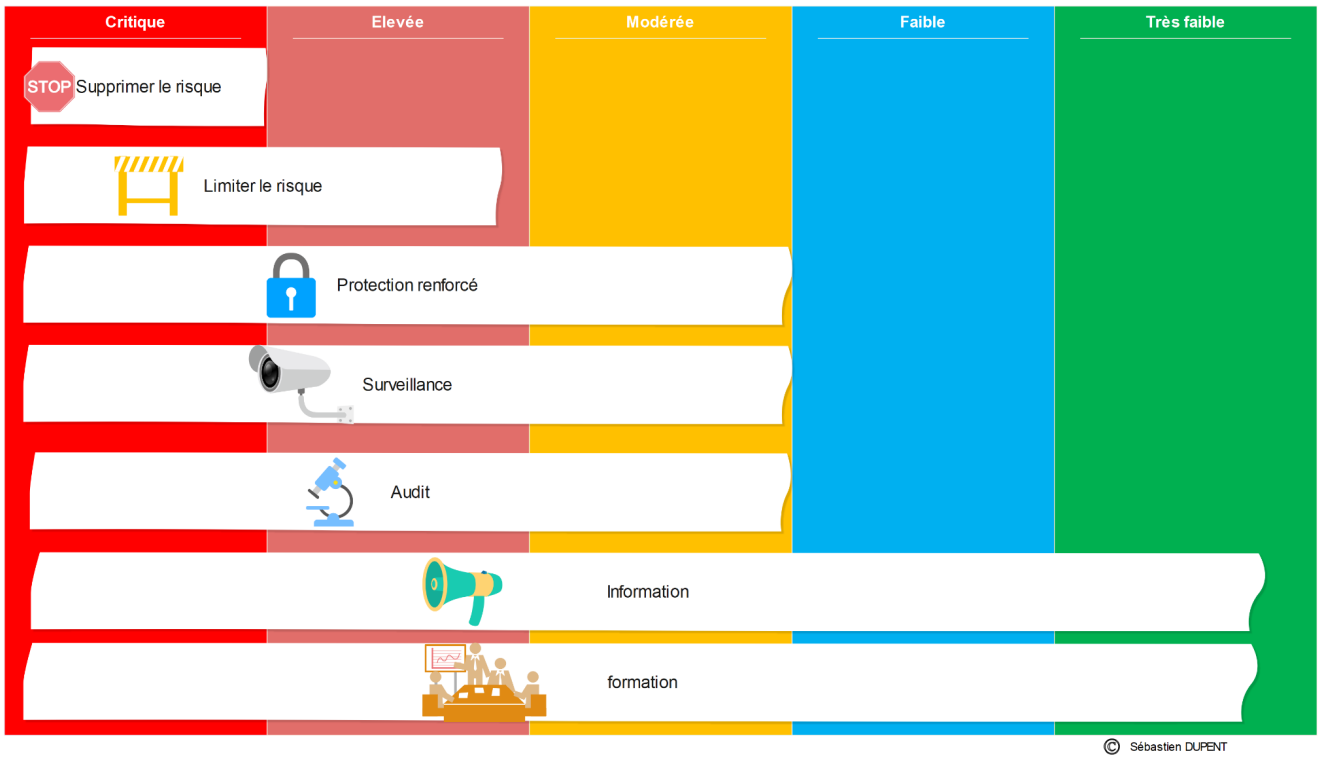



MATRICE D'ÉVALUATION DES RISQUES
PROBABILITÉ QU'UN ÉVÉNEMENT A RISQUE SE PRODUISE
CONSIDÉRER LA GRAVITÉ
Très peu probable
Peu probable
pourrait arriver
Probable
Très probable
Catastrophique
Modérée
Modérée
Elevée
Critique
Critique
Majeure
Faible
Modérée
Modérée
Elevée
Critique
Modérée
Faible
Modérée
Modérée
Moderatre
Elevée
Mineure
Très faible
Faible
Modérée
Modérée
Modérée
Négligeable
Très faible
Très faible
Faible
Faible
Modérée
© Sébastien DUPENT


Quelle est la pire conséquence que pourrait entraîner ce risque ?
Quels sont les pires dommages que pourrait entraîner ce risque ?
À quel point sera-t-il difficile de s'en remettre ?
Lequel des cinq niveaux de gravité correspond le mieux à ce risque ?


probabilité de survenance d'un risque cyber (PSRC)
Menaces (M) et Vulnérabilités (V).
La PSRC(M, V) est une fonction qui dépend de la menace et de la vulnérabilité. Plus la menace est élevée (M), plus la probabilité de survenance du risque est élevée. De même, plus la vulnérabilité est élevée (V), plus la probabilité de survenance est élevée.
Contrôles de Sécurité (C)
Les contrôles de sécurité (C) sont des mesures mises en place pour atténuer les vulnérabilités et réduire les menaces. Ils agissent comme des facteurs multiplicateurs inverses, diminuant la probabilité de survenance du risque.
Multifactorielle
La PSRC dépend de plusieurs facteurs
⇒ nombre de menaces,
⇒ la gravité des vulnérabilités,
⇒ l'efficacité des contrôles de sécurité, ⇒l'historique des incidents passés, ⇒l'environnement externe, etc.
Chaque facteur contribue à la probabilité de survenance.
Modèle de Probabilité de Survenance (MPS)
MPS(M, V, C) = PSRC(M, V) / C
la probabilité de survenance d'un risque cyber dépend de la menace (M), de la vulnérabilité (V), et des contrôles de sécurité (C) en place. Plus la menace et la vulnérabilité sont élevées, plus la probabilité de survenance est élevée, tandis que des contrôles de sécurité efficaces réduisent cette probabilité.
© Sébastien DUPENT


Fréquence et/ou durée d'exposition
Probabilité d'apparition d'un événement déclencheur
Probabilité d'apparition du dommage
Risque
Rare et/ou courte durée d'exposition
Faible
Très peu probable
Elevée
Peu probable
Moyenne et/ ou durée moyenne
Moyen
Pourrait arriver
Faible
Probable
Fréquent et/ou longue durée d'exposition
Elevée
Très probable
© Sébastien DUPENT


Critique
Elevée
Modérée
Faible
Très faible
STOP Supprimer le risque
Limiter le risque
Protection renforcé
Surveillance
Audit
Information
formation
© Sébastien DUPENT