L’analyste d’affaires dans l’ère des cyberattaques

Rhouma Naceur, PhD

Analyste d’affaires

Desjardins

Contexte et cible

- 19 septembre 2023 : *the annual SIBOS conference of the Swift IT messaging financial network*
- *Les cyberattaques contre les institutions financiers à augmenter de 300% (Source : itworldcanada)*
- *Nombreux changements, tactiques et motivations géopolitiques ont changé au cours des 18 derniers mois, provoquant une crise, en particulier dans les services financiers*
- À l'échelle mondiale, les pertes causées par les cyberattaques dépassaient les 6000 milliards $ (groupe d'experts américains Cybersecurity Ventures).
- Durant la seule année 2021, à toutes les 11 secondes une organisation a fait l'objet d'une cyberattaque.
- Le Canada arrive en seconde position, après le Royaume-Uni, dans le classement des pays ayant le plus de victimes déclarées.
- Selon Statistique Canada (2021), 21 % des entreprises canadiennes ont été touchées par une cyberattaque. De ces entreprises, 18 % sont des PME de 10 à 49 employés et 29 % des PME de 50 à 249 employés.

Contexte et cible

❑ Pour la seule période de 2019 à 2020, le nombre de cyberattaques a cru de plus de 485 % (Source: Bitdefender).
❑ Le temps d'arrêt (Dwell time) suite à une cyberattaque, oscille entre 24 et 56 jours (Source: Mandiant).
❑ Environ 34% des entreprises ont mis plus d'une semaine pour retrouver les accès à leurs données (Source: Kaspersky).

Cible

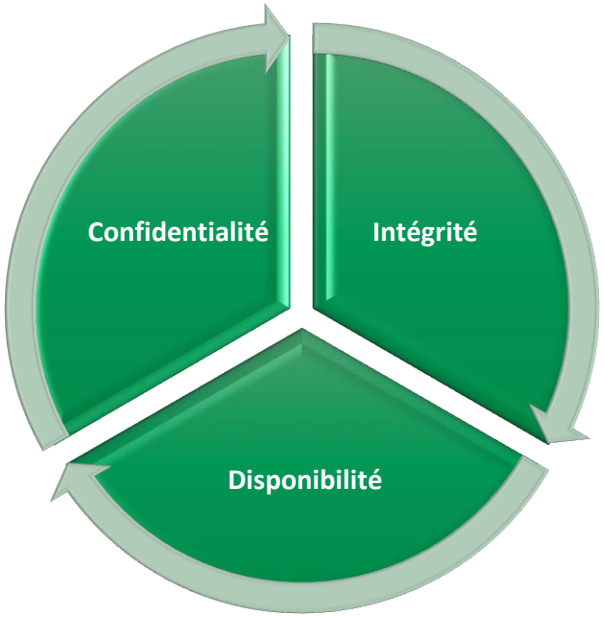
Rehausser la posture de sécurité des services critiques de l'ensemble des domaines d'affaires de l'organisation face à la menace de cyberattaque et la capacité de recouvrement en cas d'attaque.

Vision gestionnaire

Quels sont les défis du rôle de l'analyste d'affaires dans le contexte des projets en sécurité et en cybersécurité?

Quelle est votre vision pour l'évolution du rôle du AA?

Portée du projet



- Analyse de la posture de sécurité et la capacité de recouvrement des services critiques
- Définition des indicateurs de performance pour évaluer la posture de sécurité actuelle et les indicateurs de performance cibles
- Élaboration des plans d'action pour le renforcement de la posture de sécurité
- Définition des métriques pour assurer une vigilance accrue et continue sur les services critiques
- Développement des processus et procédures d'isolation en cas d'attaque cybersécurité
- Développement des processus et procédures de recouvrement suite à une attaque cybersécurité
- Développement de la stratégie de simulation et tests des processus d'isolation et de recouvrement

Activités de l’équipe AA

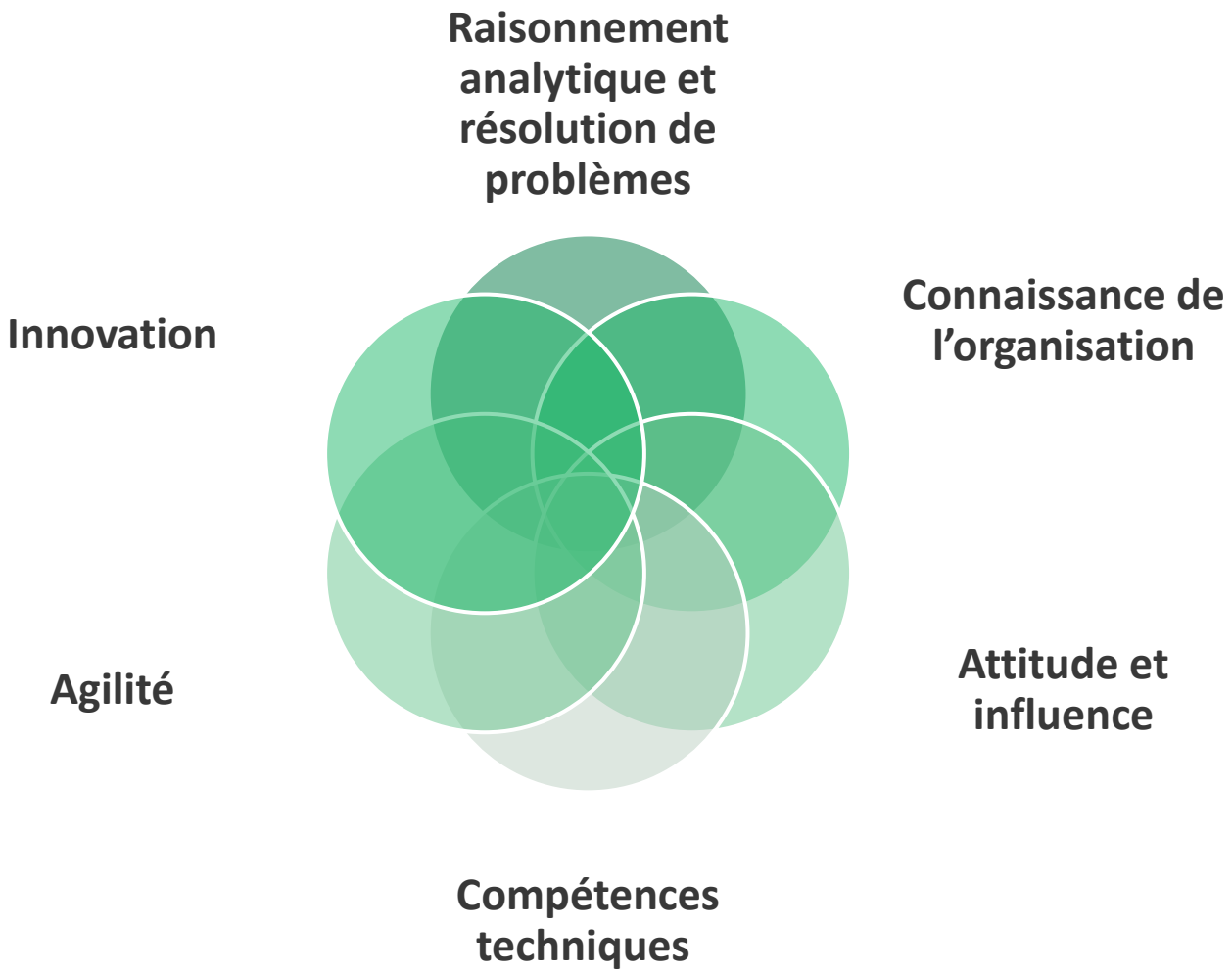
Faits saillants

- **+800 ateliers.**
- **+150 équipes** impliquées.
- **+2000 tickets Jira.**
- **+ 100 Processus de recouvrement** ont été définis.
- TableTop et **tests** de simulation exécutés avec **succès.**
- Meilleure **compréhension** de l'écosystème des services critiques.
- Meilleure **collaboration** entre les **équipes.**
- **Réussir le défi** par l'équipe d'analystes d'affaires dans l'**identification des exigences** transverses et dans l'**encadrement des ateliers.**
- Livraison des **processus dynamiques et évolutifs** dans des **délais très restreints**.
- La **capacité d'adaptation** importante de toutes les **équipes** impliquées.
- **Les livrables des analystes d'affaires ont été évalués par une firme experte en cybersécurité comme étant « les plus complets et les plus détaillés » par rapport à la documentation d'autres organisations auditées « au Canada et ailleurs ».**

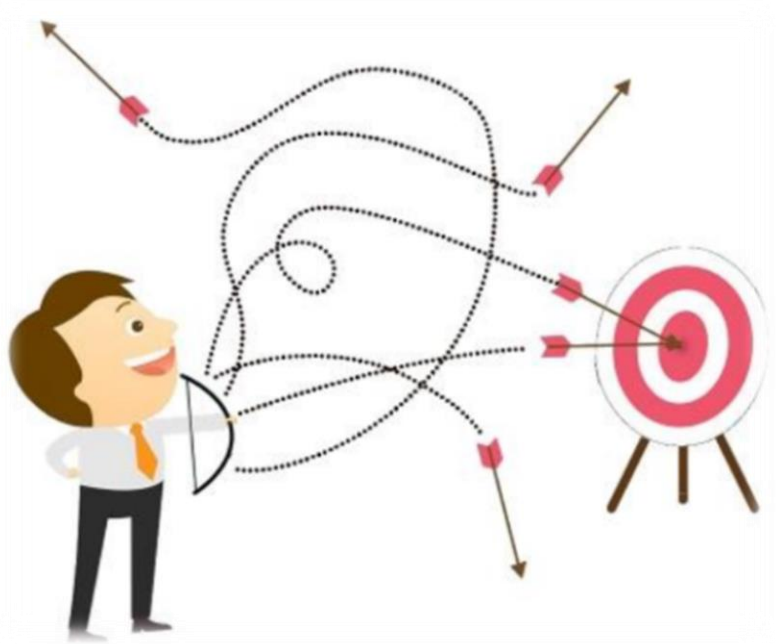
Tracer notre chemin dans l’obscurité

- Incompréhension
- Ambiguïté
- Complexité technique
- Résistance au changement
- Absence d’un modèle à suivre

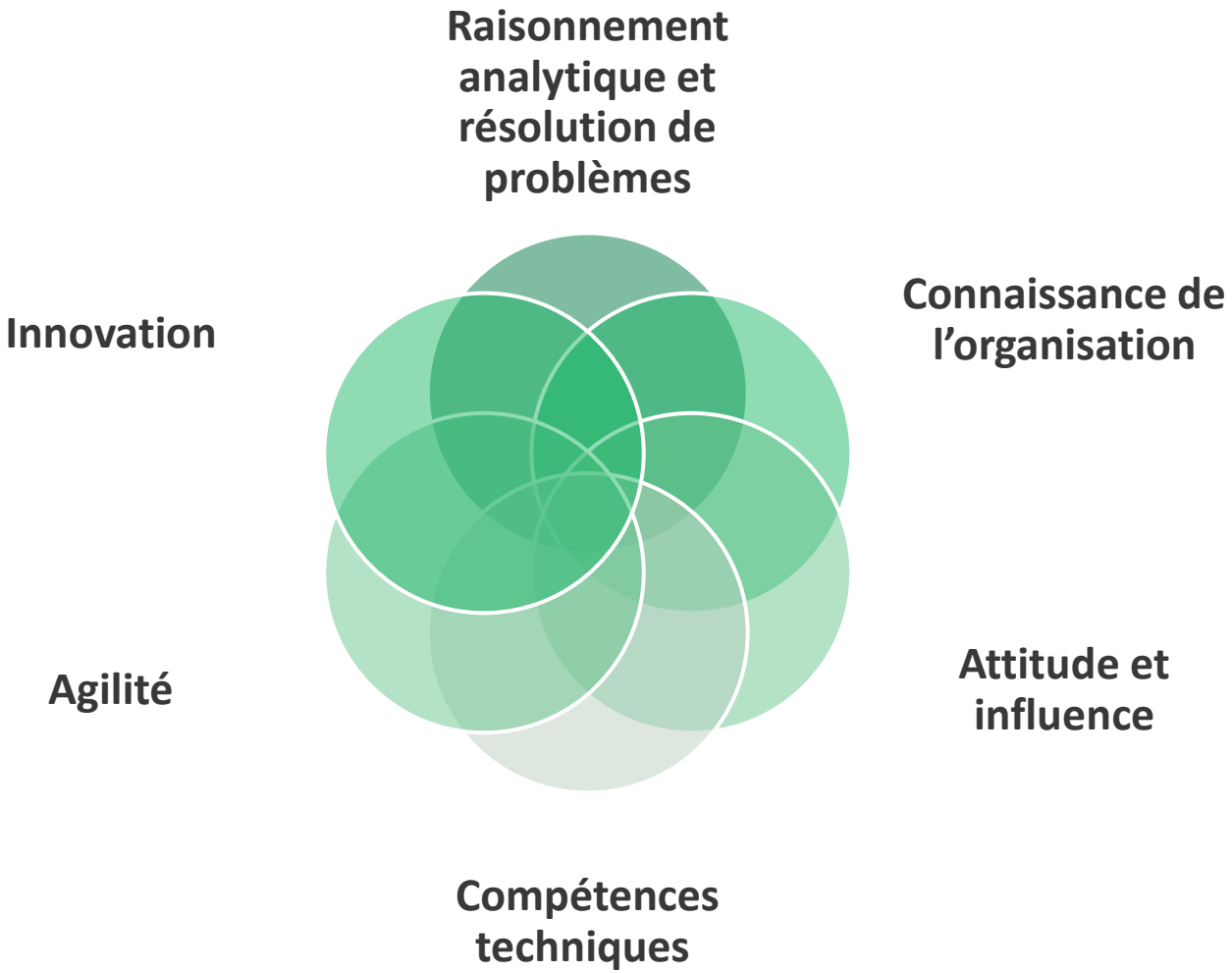
Comment avant nous parvenir à livrer de la valeur?



Comment avant nous parvenir à livrer de la valeur?



- Apprentissage par l’échec
- Droit à l’erreur

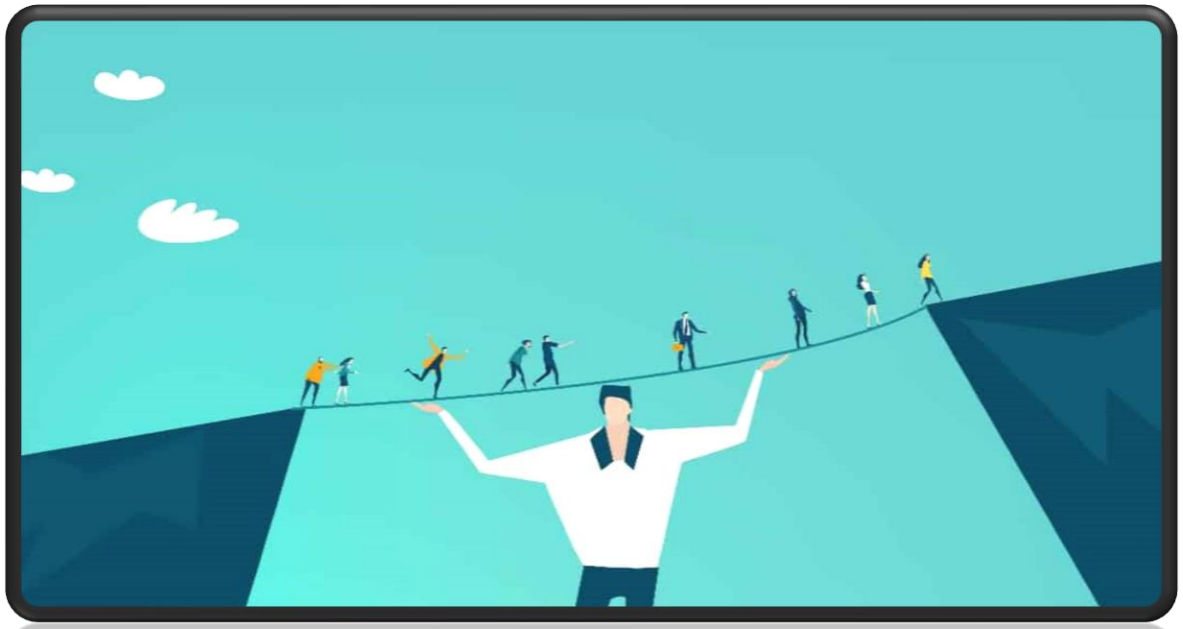


Innovation et apprentissage par l’échec

- Challenger les préjugés et oser proposer des nouvelles idées
  - Adapter le modèle CMMI pour évaluer la posture de sécurité
  - Documenter les processus de recouvrement et leurs recettes techniques
- Adapter le mode agile au contexte du projet
  - Travailler étroitement avec le Coach agile pour trouver la bonne structure du backlog
- Miser sur l’amélioration continue (rétrospective) pour grandir ensemble en tant qu’équipe et raffiner la qualité de nos livrable

  La majorité des premiers ateliers avec les équipes étaient un échec

Facteurs du succès



Équipe du projet

Merci de votre attention

Desjardins