Présentée par :
Amira Chebil,
D.E.S.S , C.C.A

LA CYBERSÉCURITÉ: UNE AFFAIRE D'ANALYSE

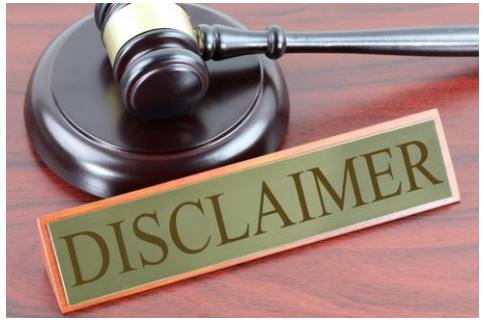
Bref aperçu sur mon profil: Qui suis-je?

- D.E.S.S Conseil en Management et certifiée C.C.A (Certificate in Cybersecurity Analysis) de l'IIBA.

- Associée de Becoming Elsewhere, entreprise dans le développement économique & développement international d'entreprises innovantes en Cyber/IA/Défense. Initiateur/Fondateur du CQTNC (Consortium Québécois en Transformation Numérique et Cybersécurité)

- Analyste d'affaires de carrière. Domaines d'expertise: Municipal, Financier, Télécommunications, Industries, Transport.

- Mandats variés allant de l'architecture d'entreprise à la réalisation en passant par la cartographie des processus.



Je n'ai pas d'interêt au travers de cette présentation sauf partager ce que j'avais appris de ma formation et de mes expériences

Becoming Elsewhere
Entrepreneurs

PRINCIPALES QUESTIONS

1. Qu'est-ce que la sécurité?

2. Qu'est-ce que la Cybersécurité?

3. Pourquoi est-il important de sécuriser les actifs de l'entreprise?

4. Quelle rôle l'analyste d'affaires peut jouer dans le processus de vigilance continuelle de Cybersécurité du point de vue CCA?

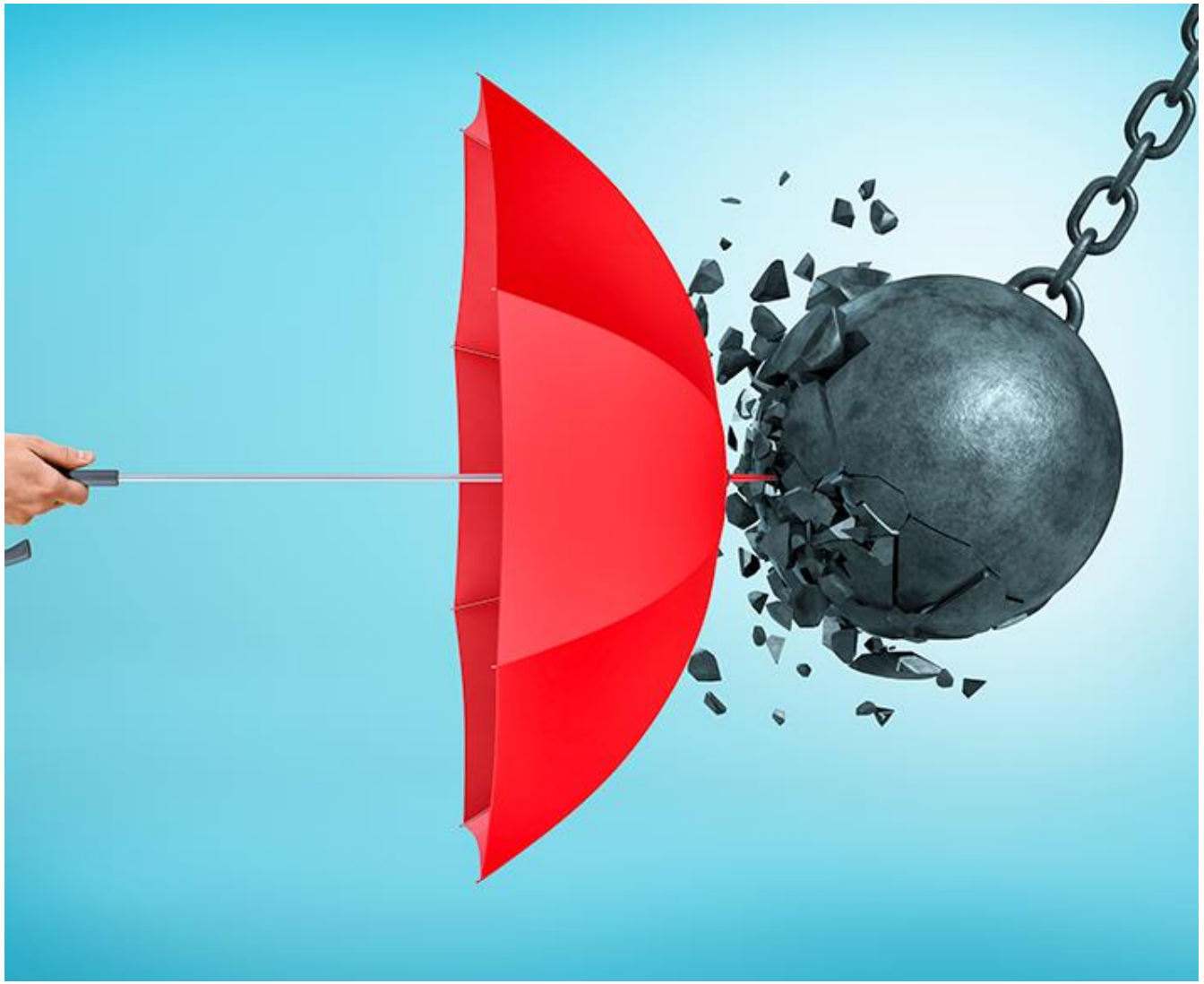
5.Quelle pourrait être la valeur ajoutée dans un domaine très particulier comme la sécurité des TI tout en exploitant les qualités et les techniques d'analyse d'affaires?

6. Comment faire pour créer sa place comme un pont entre les TI et la sécurité? Et entre la sécurité et les affaires?

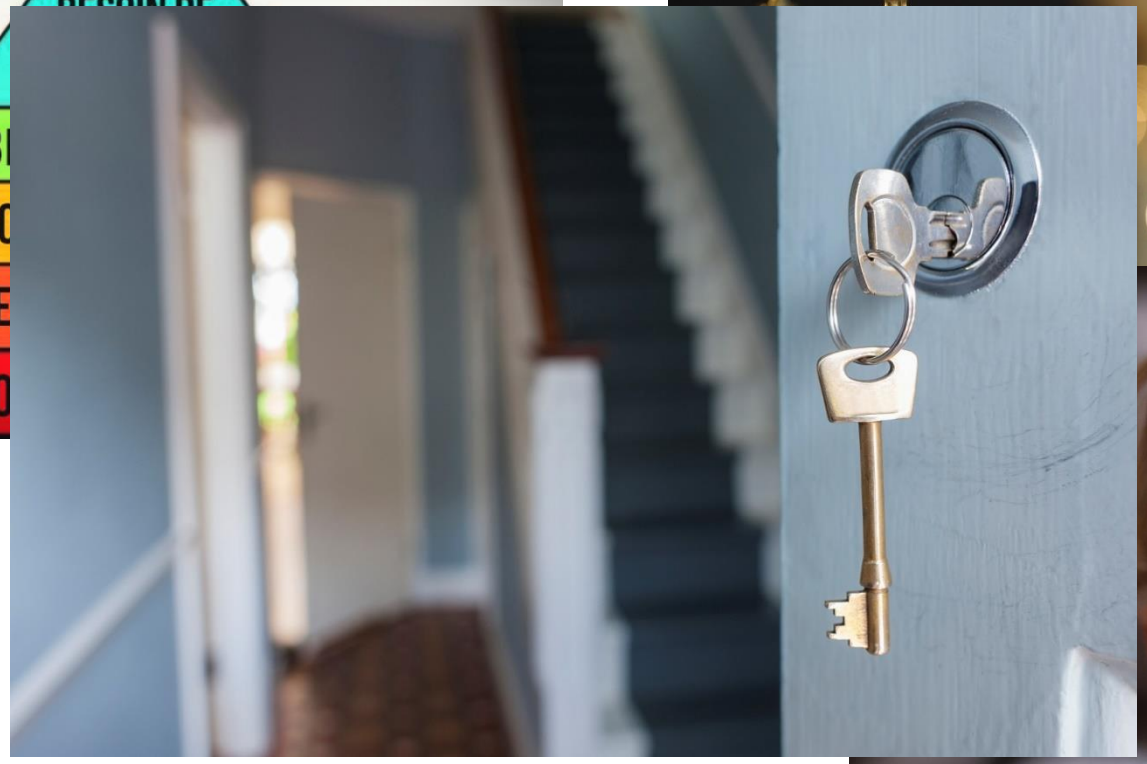
7. Le CCA en bref!

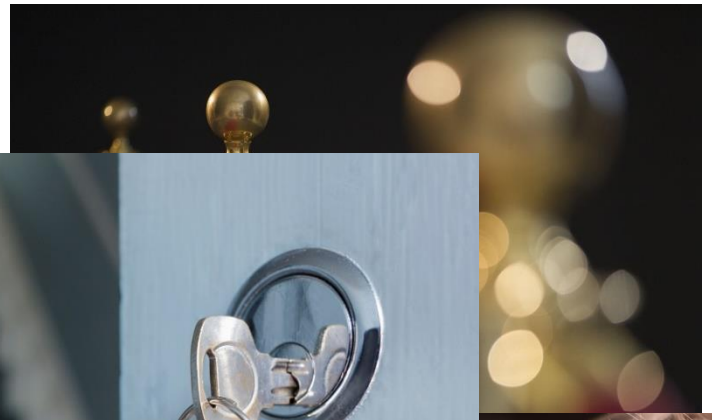
Mot de la fin

1. QU'EST-CE QUE LA SÉCURITÉ?



Situation dans laquelle quelqu'un, quelque chose n'est exposé à aucun **danger**, à aucun **risque**, en particulier d'agression physique, d'accidents, de vol, de détérioration.





2. QU'EST-CE QUE LA CYBERSÉCURITÉ?

« LA CYBERSÉCURITÉ EST LA PRATIQUE CONSISTANT À **PROTÉGER** LES SYSTÈMES, LES RÉSEAUX ET LES PROGRAMMES CONTRE LES ATTAQUES NUMÉRIQUES.
CES CYBER ATTAQUES VISENT GÉNÉRALEMENT À ACCÉDER À DE L'INFORMATION SENSIBLE, À LA MODIFIER OU À LA DÉTRUIRE, À EXTORQUER DE L'ARGENT À D'AUTRES UTILISATEURS, OU À INTERROMPRE LES PROCESSUS D'AFFAIRES. »

Référence : Cisco

3. POURQUOI EST-IL IMPORTANT DE SÉCURISER LES ACTIFS DE L'ENTREPRISE?

Selon l'ISACA (Information Systems Audit and Control Association®), les cyber-attaques se classent comme le type de **crime qui évolue le plus rapidement** aux États-unis causant des arrêts d'activités de très grande envergure voire catastrophiques.

Les dommages causés par les cyber-attaques pourraient atteindre 6 M$ cette année.

Source : Site de l'ISACA

Exemples d’actifs dans une entreprise

Les données (qui sont considérées comme « L’or noir du 21ieme Siècle ») ; notamment légales/financières/opérationnelles

Les systèmes (applications);

Les infrastructures ;

Les secrets commerciaux, industriels;

R&D.

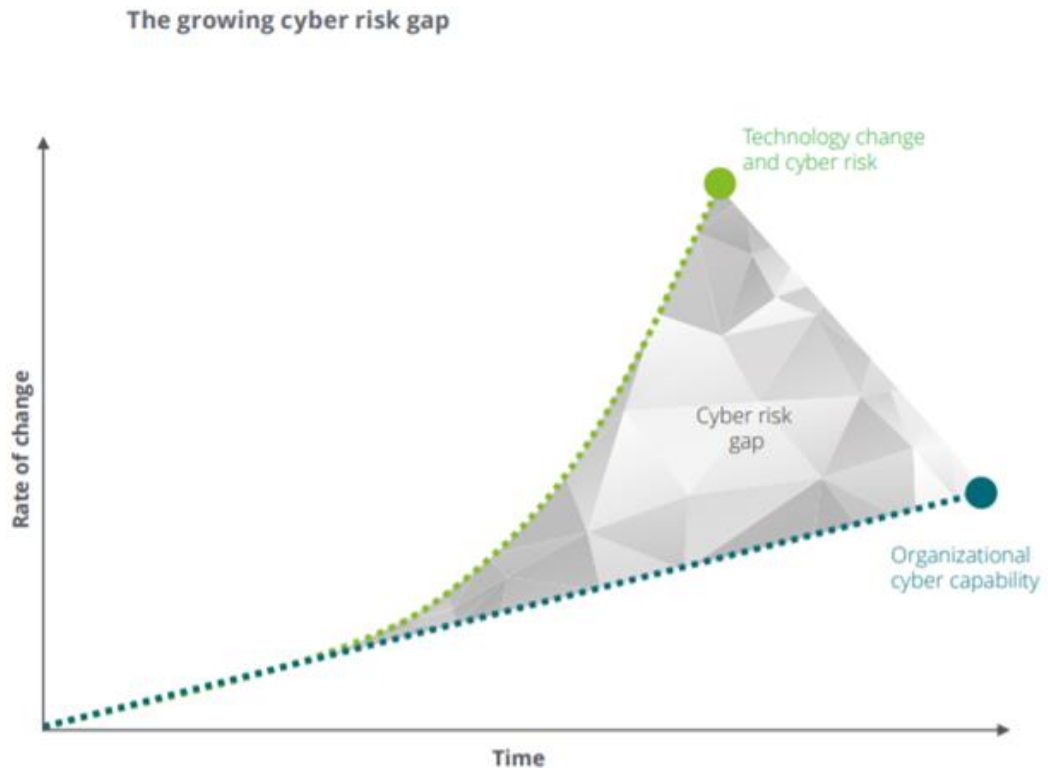
Les coûts de déploiements de technologies de par leur complexité, leur étendues et leurs impacts sur les finances des entreprises peuvent s'avérer élevés en valeur nette.

Dans le cas de la cybersécurité, le coût de ne pas sécuriser les actifs de l'entreprise est nettement supérieur à l'investisssement y est relié.

Une seule fuite de données peut coûter extrêmement cher.

L'investissement en cybersécurité doit être proportionnel à la valeur des actifs

Les « Crown Jewells » **doivent être les actifs les plus sécurisés**



Gartner prévoit que les acquisitions des produits et service de la sécurité informatique dépasserait les 133 M$ en 2022 (Deloitte)

QUELQUES CYBER ATTAQUES MARQUANTES EN 2020

SOLARWINDS (INJECTION DE CODE INFECTÉ)

L'attaque sur le logiciel **SolarWinds** a marqué 2020 puisqu'elle a permis aux cybercriminels de compromettre de multiples systemes gouvernementaux (exemple: Département de la défense américaine) et de compagnies internationales (exemple: Microsoft).

Le problème est qu'un des serveurs qui fournissait les mises à jour de sécurité et les correctifs a été compromis et a permis aux cybercrimiels d'injecter du code dans la mise à jour de logiciels et d'infecter un grand nombre de clients en même temps. Le code infecté permettait de :

- ❑ Permet l'alteration des données (integrité des données);
- ❑ Permet d'exfiltrer des données (Confidentialité);
- ❑ Accès distant à tous les appareils (Endpoints) surlesquels le logiciel a été installé (Gestion des accès).

Vulnérabilité : Système de mise à jour et de correctifs.

TWITTER (INGÉNIERIE SOCIALE)

"All Bitcoin sent to the address below will be sent back double! If you send $1000, I will send back $2000. Only doing this for 30 minutes. [the link]. Enjoy"

- L'attaque consistait à « voler » l'accès aux comptes de célébrités (donc crédibles et hautement suivis) dans TWITTER pour diffuser de fausses informations sur la cryptomonnaie « BITCOIN ».
- Le cyber-criminel a Tweeté que ceux qui enverrait des fonds au lien indiqué recevrait le double du montant .
- L'attaque n'a été que de courte durée mais elle a été chiffrée à + de 100 K$.

Vulnérabilité: Humaine

Becoming Elsewhere
Entrepreneurs

MARRIOTT (ACCÈS NON AUTORISÉ)

- La chaine Marriott est la chaine hotelière la plus importante au monde avec 7300 hôtels et installations touristiques dans 134 pays.
- Elle a subi une attaque tristement célébre en 2018 ayant causé l'accès aux données personnelles de quelques 500 M de clients. (noms, adresses, numéros de téléphones, dates de naissances et les programmes de fidélité)
- En 2020, une autre attaque similaire a causé la fuite des données de 5.2 M de clients.
- Les cyber-criminels ont non seulement accédé aux données personnelles mais ils les ont copiées et les ont cryptées.

4. Quel est le rôle à jouer par l'analyste d'affaires dans le processus de vigilance continuelle de Cybersécurité du point de vue CCA?

VALEUR AJOUTÉE DE L'ANALYSE D'AFFAIRES EN CYBERSÉCURITÉ

- Participer à la gouvernance de données (identifier le Data Custodian, documenter le processus de gestion des données en collaboration avec les parties prenantes, etc.)
- Déterminer la période de rétention selon les règlements et les lois applicables
- Veiller (à) et exiger la protection des renseignements personnels dans le processus d'élicitation des requis business en documentant les requis de sécurité s'y rattachant.
- système) et les intégrer dans les étapes de prise de besoins.

VALEUR AJOUTÉE DE L'ANALYSE D'AFFAIRES EN CYBERSÉCURITÉ

- Prendre les besoins de sécurité en amont (sans traiter des éléments techniques forcément) sous format de Baseline Security Requirements en lien avec les clients du processus ou du système.
- Documentation et mise en place des règles d'archivage, d'encryption d'anonymisation,de pseudonymisation
- Minimiser la collecte des données personnelles

VALEUR AJOUTÉE DE L'ANALYSE D'AFFAIRES EN CYBERSÉCURITÉ

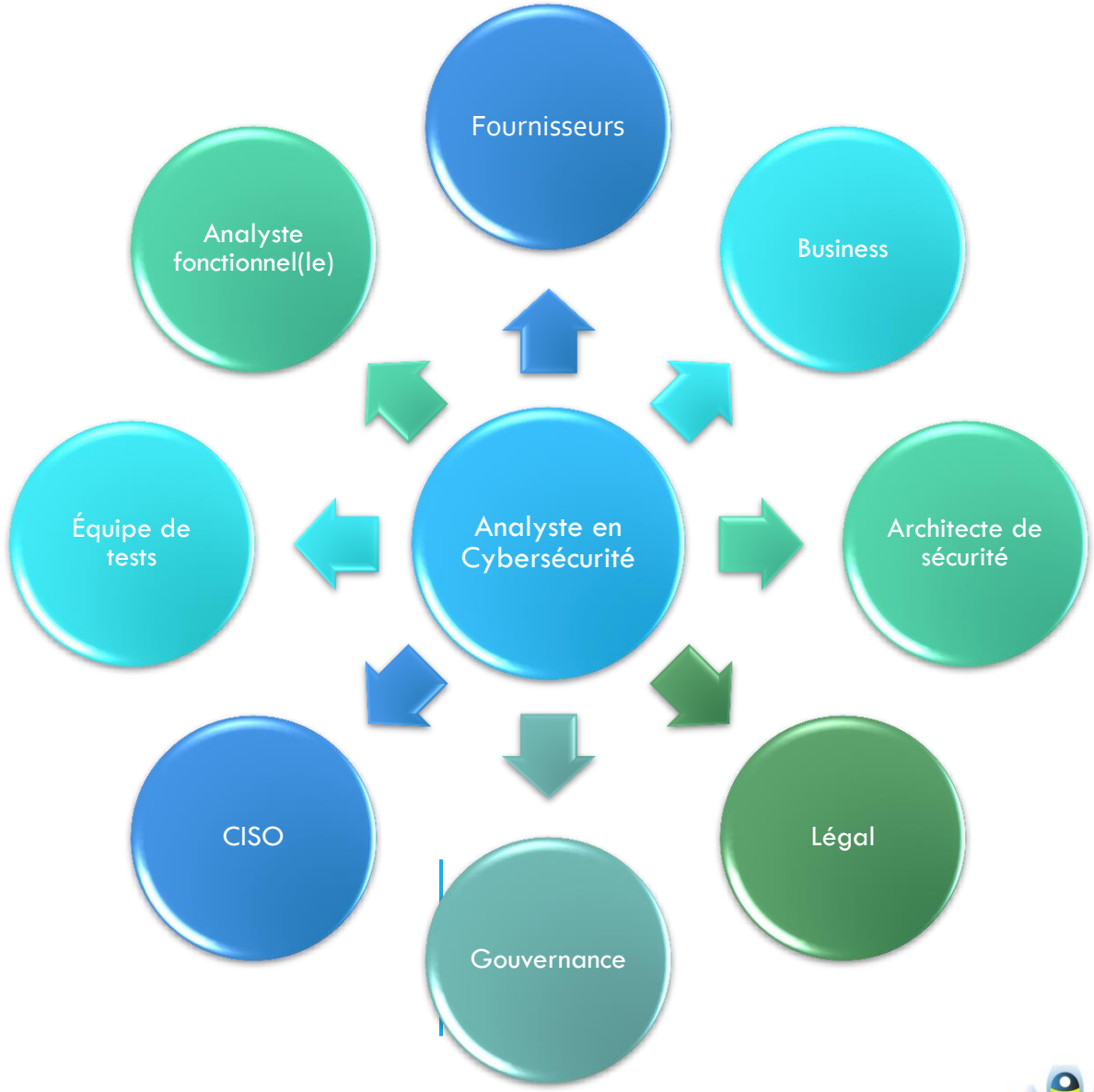
- Faire le suivi des requis de sécurité tout au long du SDLC
- Contribuer à la documentation de la politique de sécurité (les AA ne sont pas responsables de la politique de sécurité)
- Faire la promotion des Systèmes d'Information "Secure by Design" ou sécuritaire de par la conception et du "Privacy by Design"
- Sensibiliser les parties prenantes des exigences de sécurité
- Aider à la vigie des exigences de sécurité
- Aider dans la documentation de la politique de sécurité
- Maintenir ou contribuer dans le maintien du registre des menaces (Threat register)

- Contribuer à la sécurité des couches OSI
- Contribuer à la sécurité physique
- Sécurité des plateformes et des serveurs
- GIA (authentification et autorisations)
- Sécurité des produits (Internet of Things)
- Services infonuagiques
- Modélisation des menaces
- Classification des données
- Gestion des privilèges
- Livraison des solutions de sécurité informatique
- Réponse aux incidents
- Risques opérationnels SIEM
- Gestion des preuves
- Protection des données clients et des fournisseurs

La liste est encore très longue ☺

5.QUELLE POURRAIT ÊTRE LA **VALEUR AJOUTÉE** DANS UN DOMAINE TRÈS PARTICULIER COMME LA SÉCURITÉ DES TI TOUT EN EXPLOITANT LES QUALITÉS ET LES TECHNIQUES D'ANALYSE D'AFFAIRES?

Le CCA dans l'écosystème de l'entreprise



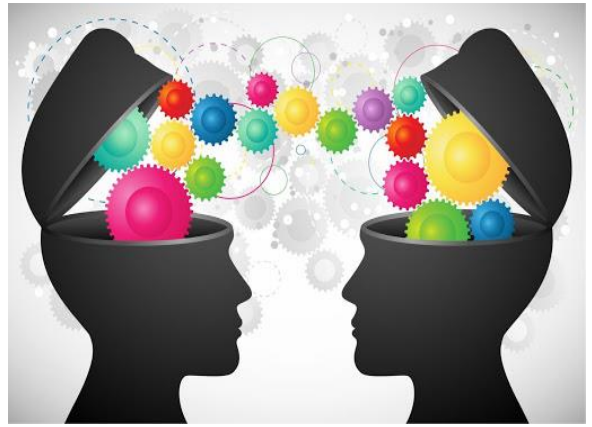
Analyste d'Affaires	Analyste en Cybersécurité
Comprendre le contexte des parties prenantes et documenter les processus d'affaires	Comprendre le contexte d'affaires de la Business et documenter les risques de sécurité en lien avec les processus d'affaires
Faire la liaison entre les Affaires et les TI	Faire le lien entre les Affaires, les TI et la sécurité
Documenter les requis d'affaires	Documenter les exigences de sécurité (requis non fonctionnels)
Assister les équipes de tests afin de s'assurer que les résultats de tests soient conformes aux requis d'affaires	Assister les équipes de tests afin de s'assurer que les résultats de tests soient conformes aux requis de sécurité et/ou d'affaires.
Recommandation des solutions technologiques les plus adaptées aux besoins d'affaires	Recommandation des solutions technologiques les plus adaptées aux besoins de sécurité en concordance avec les objectifs des affaires.
Faire une vigie des dernières technologies et innovations	Faire un vigie des dernières technologies en sécurité

Multi-tâches, multi-compétences

- Analyse , planification et vigie
- Élicitation et collaboration
- Rôle de facilitateur dans les ateliers de prise de besoins en sécurité
- Analyse du contexte
- Validation de la concordance de la solution avec les besoins d'affaires.

6. COMMENT FAIRE POUR CRÉER SA PLACE COMME UN PONT ENTRE LES TI ET LA SÉCURITÉ? ET ENTRE LA SÉCURITÉ ET LES AFFAIRES?

- Être présent auprès des clients et expliquer pourquoi c'est important d'être vigilent avec des mots simples et compréhensibles par tous.



- Les analystes en Cybersécurité sont des catalyseurs et des connecteurs (Dots Connectors) : la réalité business et les TI est **un** ensemble à **protéger.**

- La cybersécurité est une toile de **mécanismes** de sécurité . Elle se veut transversale, aussi bien préventive (architecture, planification, etc.) que curative (équipe d'intervention et de réponse aux incidents). Les compétences pragmatiques et communicationnelles des analystes d'affaires sont **essentielles.**

Communiquer, demeurer **curieux**, rester **à jour**, faire du **réseautage**, et penser sécurité!

Becoming Elsewhere
Entrepreneurs

7.LE CCA EN BREF!

Un certificat co-élaboré par IEEE (Institute Of Electrical and Electronics Engineers) et IIBA

- Formation transverse
- Permet d'avoir les connaissances nécessaires pour comprendre les principes de sécurité TI
- Permet aux analystes d'affaire d'entrer dans le marché de la Cybersécurité en démontrant la complémentarité des deux rôles.


PLAN
INTRODUCTION
RÉSUMÉ
FIN
MERCI
CONCLUSION
BILAN
MOTS-CLÉS
EXPOSÉ
PERSPECTIVES
PROJET IDÉES
PRÉSENTATION
DISCUSSION
QUESTIONS
ANNEXES
PARTIE
SUITE
ANALYSE
RÉSULTATS

La cybersécurité nous concerne spécifiquement car nous sommes :

- Des professionnels en TI qui participons à la conception des systèmes d'information.
- Des clients chez des compagnies et nos informations personnelles sont gérées par ces compagnies. Si elles échouent dans la protection des données, nous allons être affectés dans notre vie privée.
- Des utilisateurs de téléphones cellulaires, des imprimantes , des TV intelligentes, de réfrigérateurs intelligents, de domotique, d'ordinateurs, d'applications bancaires, de jeux, etc. chacun des éléments mentionnés est une cible de vol de données et une porte d'entrée pour compromettre ces données.

Selon le ISC2 (**International Information Systems Security Certification Consortium,** les dépenses au niveau de la sécurité de l'Information atteindraient 170 Milliards en 2022 due à l'accroissement de la cybercriminalité.

Ils estiment à 3.5 Millions le nombre de postes à combler en 2021 pour le Cybersécurité.

Il y a une demande croissante sur les profils en Cybersécurité y compris les CCA.

Isc2.org

RÉUSSIS TA CERTIFICATION CCA ET APPLIQUE LES BONNES PRATIQUES DE SÉCURITÉ À TON CHAMP D'ACTIVITÉ CAR LA SÉCURITÉ EST L'AFFAIRE DE TOUS PARTOUT EN TOUT TEMPS !

Becoming Elsewhere
Entrepreneurs

Becoming Elsewhere
Entrepreneurs