Évoluer avec l'approche *Secure by design*

Serge Drolet, MBA CISA CBCP PMP

CyberSéQurité Inc.

Octobre 2024

1

Qui suis-je ?

25 ans d'expérience en TI

- 15 ans en cybersécurité, gestion des risques et continuité des affaires
- Statistique Canada, Revenu Québec, Autorité des marchés financiers, etc.

Ancien président d'ISACA-Québec

- OBNL actif dans le développement des connaissance et compétences en TI

Conférencier dans plusieurs évènements

- les Affaires, SéQCure, Réseau Action TI, ASIQ, Crise&Résilience et maintenant l'OWASP

Suivez-moi sur LinkedIn !

2

2

Ordre du jour

1. *Secure by design* et bonnes pratiques
2. Exemple de gouvernance par les principes
3. Mise en œuvre : par où on commence ?
4. À retenir ☺

Annexe : autres référentiels et outils

3

3

1. *Secure by design* et bonnes pratiques

Attention : plusieurs courants émergents :

- Développement applicatif
  - Pour développeur (dont OWASP)
  - Pour fournisseur de services infonuagique (dont CISA)
- Conception de service (applicatif et technologique)
  - Pour équipe de livraison (dont UK Gov.Sec.)
  - Pour équipe TI et client (dont Australian Cyb.Sec)

Avec des objectifs similaires :

- Coûts : moins couteux de régler un problème en conception qu'en production
- Vélocité : livrer plus rapidement en automatisant la sécurité et la conformité
- Collaboration : travailler en équipe et rapprocher les univers Dev | Sec | Ops
- Valeur (répond aux besoins) et qualité (en amont)

4

4

Quelques référentiels intéressants à considérer*

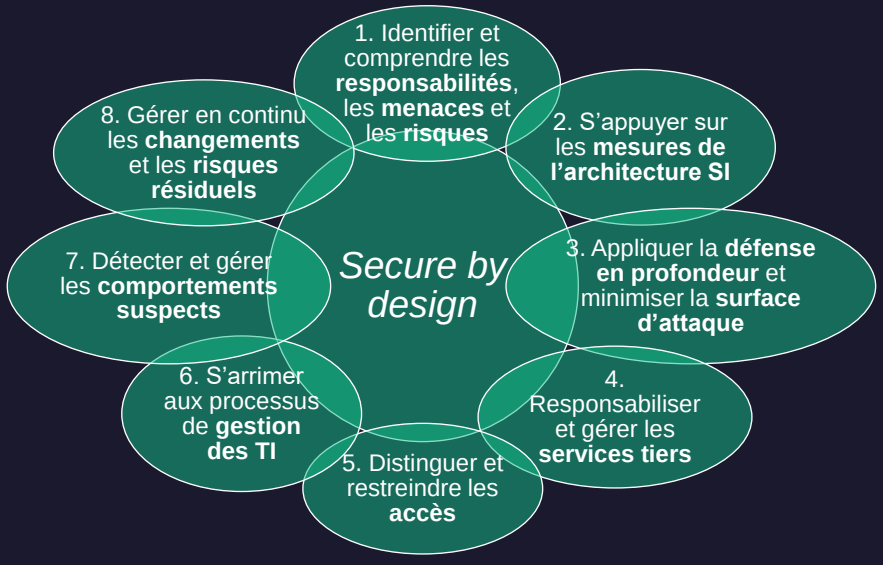
- OWASP : 4 principes du *Secure Product Design* pour développeurs
  - Moindre privilège, Défense en profondeur, Zéro trust, Security-in-the-Open
- CISA-US+ (White paper 2023) : 3 principes pour fournisseurs de service infonuagique (*CSP*)
  - Responsabilité, Transparence, Leadership
- UK Gov.Sec. (Politique et Guide Secure by design 2023) : 10 principes pour équipes de livraison
  - Responsabilités, Sources sécuritaires, Risques, Utilisabilité des contrôles, Détection/Réponse, Architecture flexible, Surface d'attaque, Défense en profondeur, Vérification, Changement
- Australian Cyb.Sec.Centre (2024) : 6 fondations pour équipes TI et clients
  - Globale, Précoce et durable, Développement produit, Tests, Assurance en continue, Désuétude

* Autres référentiels en annexe, dont ISO et NIST

5

5

2. Exemple de gouvernance par les principes



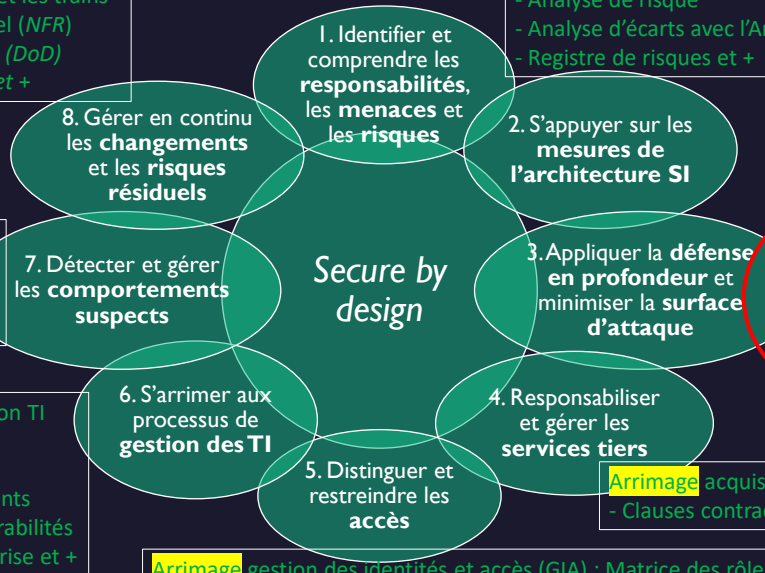
6

6

3. Mise en œuvre

Arrimage avec le SDLC et les trains
- Requis non fonctionnel (*NFR*)
- Critères d'acceptation *(DoD)*
- *Inspect&Adapt (I&A) et +*

Arrimage accompagnement de sécurité
- Analyse de risque
- Analyse d'écarts avec l'Architecture SI
- Registre de risques et +



Arrimage cyberdéfense
- Journalisation et alerte
- Tester la réponse aux incidents et +

Conception technique
- DevSecOps – *Conception*

Modélisation des menaces

Arrimage exploitation TI
- Gestion des actifs
- Gestion des accès
- Gestion des incidents
- Gestion des vulnérabilités
- Sauvegarde et reprise et +

Arrimage acquisition (si requis)
- Clauses contractuelles (et SLA) et +

Arrimage gestion des identités et accès (GIA) : Matrice des rôles et habilitations

7

7

Quelques outils

Liste de vérification de l'architecture SI de l'organisation

Listes techniques du marché :

- Listes de vérification des fournisseurs de produits et services technologiques
  Microsoft, Amazon, Java, +
- CIS Benchmark pour la configuration de plus de 25 familles de produits
  Admin. : Linux, Windows, Microsoft 365, Exchange, Intune, Azure, CISCO, VMWare, +
  Dev. : Docker, Kubernetes, Snowflake, AWS, +
- OWASP : Guide du développeur et listes de vérification associées, dont
  Application Security Verification Standard (ASVS), Secure Database Access, Validate All Inputs, Protect Data Everywhere, Implement Security Logging and Monitoring, Handle all Errors and Exceptions, +

8

8

4. À retenir

- Secure by design : un concept émergent (définition, portée et pratiques en évolution)
- Importance de développer
  - Une vision globale des principes et pratiques et de les adapter à son organisation
  - Une gouvernance forte pour communiquer clairement les attentes
  - Une gestion du changement adéquate axée sur la formation des intervenants
  - Une compréhension commune des menaces, risques et pratiques permettant de limiter les possibilités d'attaques et leurs conséquences
    - DevSecOps, dont la modélisation des menaces !
- Mesurer votre avancement (posture, maturité ou autre)

9

Annexe : autres référentiels et outils

- Autres référentiels :
  - NIST SP 800-160 (2022) : 30 principes du *Engineering Trustworthy Secure Systems*
  - NIST SP 800-218 (2022) : 20 pratiques du Secure Software Development Framework (SSDF)
  - ISO 31700 (2023) : 7 principes du *Privacy by design*
- Outils :
  - UK Gov.Sec. (2024) : Listes de vérification SbD (principes, activités et mise en œuvre)

10

10

Questions ?

Merci

Serge Drolet

CyberSéQurité Inc.

LinkedIn

11