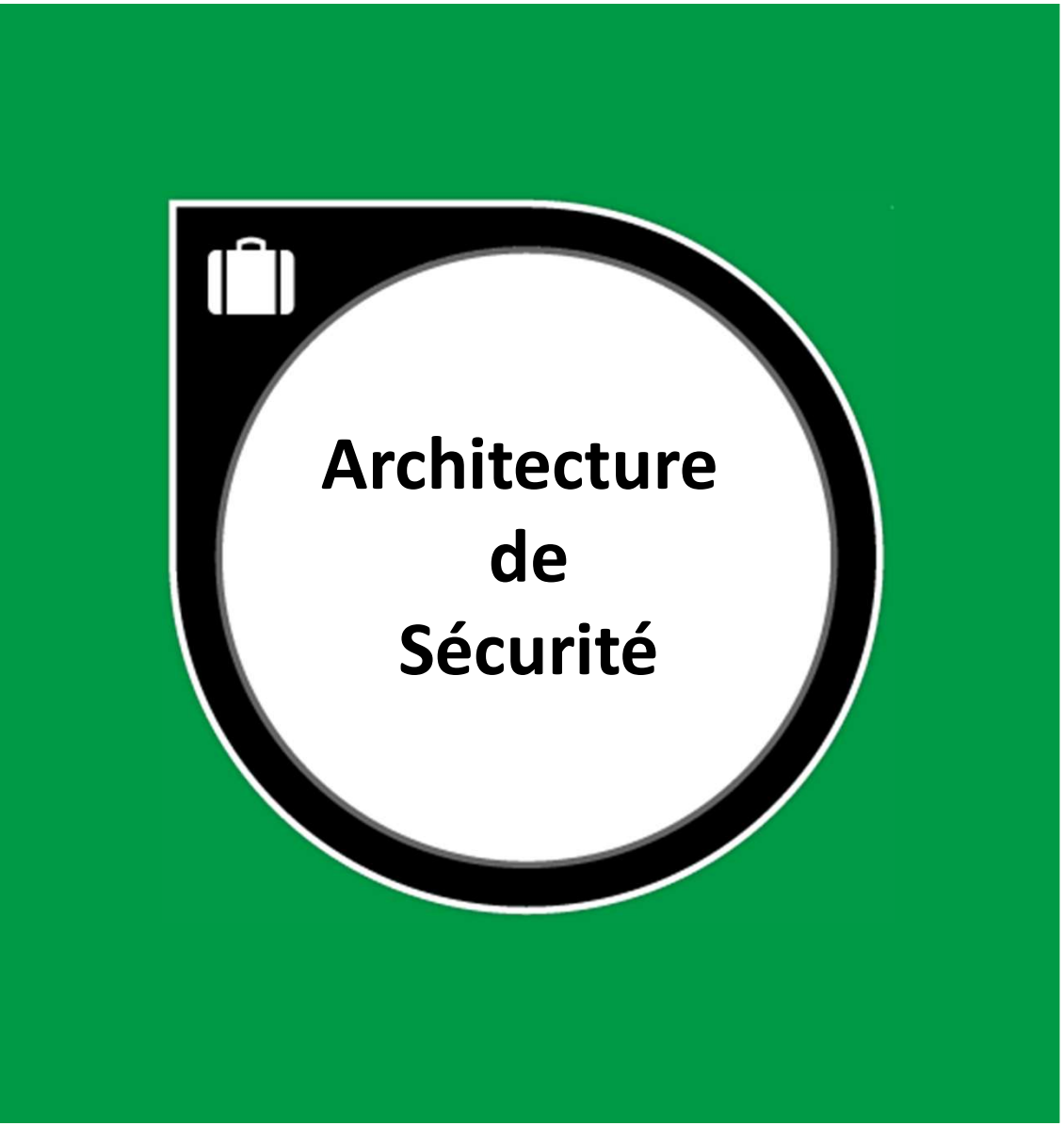


INF 809
Architecture de sécurité

Notion de base

Cours 1

Introduction et contexte de l'architecture de sécurité

UNIVERSITÉ DE SHERBROOKE

PLAN DE LA SÉANCE

- Les individus
- Présentation du cours
- Signification du concept d'architecture en contexte technologique
- Besoins du marché et les attentes de celui-ci
- Survol des modèles d'architecture d'entreprise et d'architecture de sécurité
- Principes DICAI en AS

PRÉSENTATION DE L'ENSEIGNANT

Éric Daigneault

- Études
  - B.Sc.A en Informatique et Génie Logiciel
  - M.B.A (ici, à l'UdS)
- Certification
  - CISSP-ISSAP
  - PMP
  - ++
- Expérience
  - 23 années en T.I.
  - + 20 en sécurité de l'information
  - 11 dernières années dans des rôles de leadership en architecture et modélisation (positionnement stratégique)
  - Présentement CISO à la SAQ
- Enseignement
  - INF805, INF809, INF810, INF811 depuis 4 ans approx.

PRÉSENTATION DES PARTICIPANTS

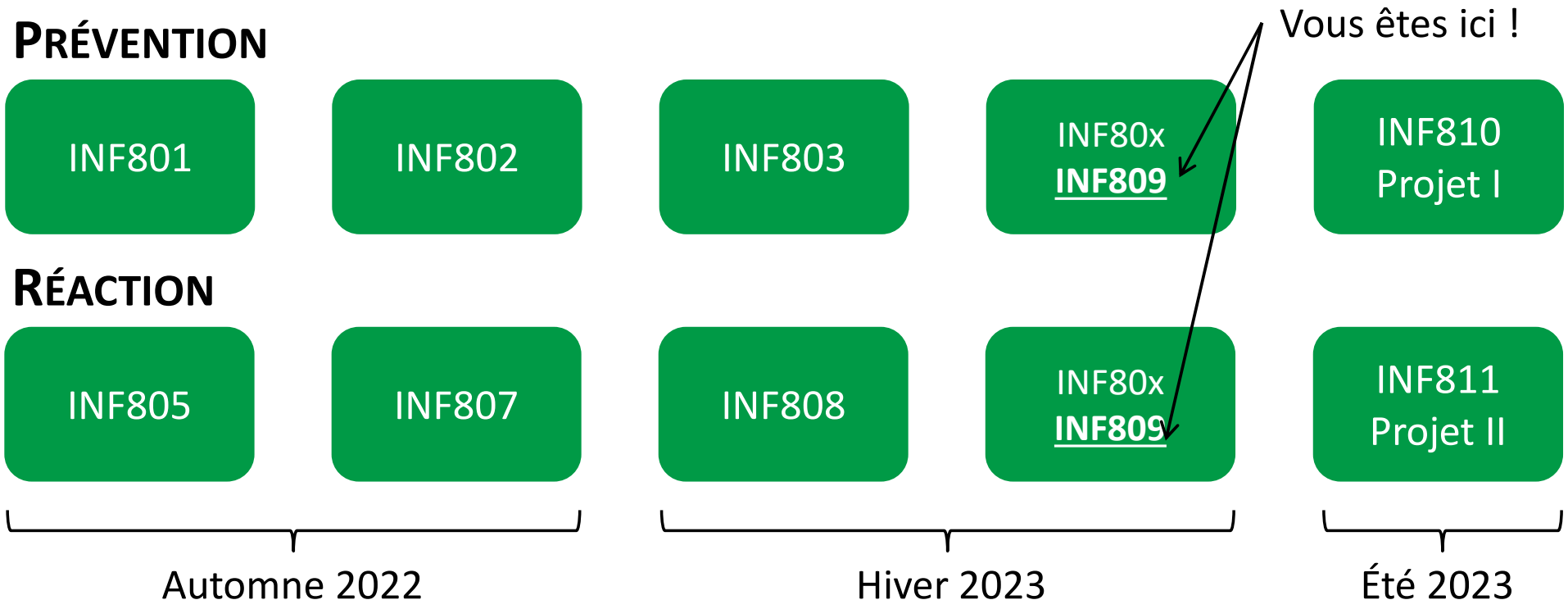
À tour de rôle

- Nom
- Poste occupé
- Expérience en informatique
- Expérience en cybersécurité
- Attentes pour le programme
- Attentes pour le cours

Le cours

UNIVERSITÉ DE SHERBROOKE

POSITIONNEMENT DANS LES MICROPROGRAMMES



LES DIFFÉRENTS TYPES D'ARCHITECTURE DE SÉCURITÉ

Deux (2) types d'architecture de sécurité

- L'architecture de sécurité au niveau de l'entreprise
  - Fait partie de l'architecture d'entreprise
  - Développement des modèles de sécurité
  - Développement des cadres de références de sécurité que l'organisation doit utiliser
- L'architecture de solution de sécurité
  - En mode projets ou programmes
  - S'occupe de gérer les besoins en sécurité de différents projets ou programmes
  - Assure une intégration des solutions d'affaire avec les modèles de sécurité
  - Tactique

LES OBJECTIFS DU COURS

Comprendre les modèles (référence) d'architecture. Appliquer les standards d'architecture dans un contexte d'entreprise. Formuler une architecture pour les besoins de sécurité d'une entreprise. Faire l'analyse et l'évaluation d'un document d'architecture de sécurité (AS).

LE CONTENU DU COURS

- Contexte : besoins, marché et tendances, définitions.
- Modèle de sécurité : place de l'AS dans l'architecture d'affaires, applicative, matérielle et de données.
- Principes d'architecture (se traduisent comment dans la pratique) : modèle zero-trust, modèle d'accès, isolation, DICAI.
- Modèle de référence : standard TOGAF et Archimate, des objets réutilisables.
- Niveaux d'architecture : AS au niveau affaires, AS au niveau applicatif, AS au niveau technologique, AS au niveau des données.
- Vues : mise en pratique; outils et/ou projet (tel que Archimatetool).

LE CONTENU DÉTAILLÉ DU COURS

Faculté des sciences
Centre de formation en technologies de l'information

UNIVERSITÉ DE SHERBROOKE

1. IDENTIFICATION ET RENSEIGNEMENTS GÉNÉRAUX

Titre officiel du cours :	**INF809 – Architecture de sécurité**
Nombre de crédits :	3 crédits – 135 heures
Programme :	Microprogramme de 2e cycle en sécurité informatique - volet prévention Microprogramme de 2e cycle en sécurité informatique - volet réaction DESS de 2e cycle en sécurité informatique
Cours préalables ou concomitants :	INF801 – Concept de base en sécurité des TI
Lieu du cours :	Moodle
Session :	Hiver 2023
Date de début :	10 janvier 2023
Date de fin :	18 avril 2023
Date limite d'abandon :	TBD
Rencontres synchrones :	Tous les mardis à partir du 10 janvier 2023 18h30 à 21h30
Personne(s)-ressource(s) :	Éric Daigneault
Courriel(s) :	eric.daigneault@usherbrooke.ca

2. MISE EN CONTEXTE

DESCRIPTION OFFICIELLE DU COURS

Cible(s) de formation :

Comprendre les modèles (référence) d'architecture. Appliquer les standards d'architecture dans un contexte d'entreprise. Formuler une architecture pour les besoins de sécurité d'une entreprise. Faire l'analyse et l'évaluation d'un document d'architecture de sécurité (AS).

Contenu :

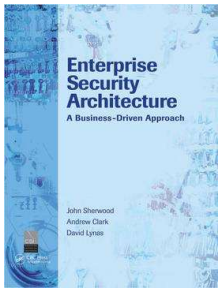
Contexte : besoins, marché et tendances, définitions. Modèle de sécurité : place de l'AS dans l'architecture d'affaires, applicative, matérielle et de données. Principes d'architecture (se traduisent comment dans la pratique) : zero-trust, modèle d'accès, isolation, DICAI. Modèle de référence : standard TOGAF et Archimate, des objets réutilisables. Niveaux d'architecture : AS au

Page 1 | 13

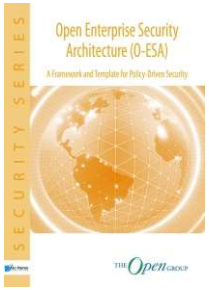
UNIVERSITÉ DE SHERBROOKE

Les Références

- **Obligatoires**
  - John Sherwood, Andrew Clark and David Lynas, Enterprise Security Architecture – A business-Driven approach, CRC Press, 2005, 608 pages.



- **Optionnelles**
  - Stefan Wabe, Open Enterprise Security Architecture (O-ESA), Van Haren Publishing, 2011, 141 pages
  - Adam Gordon, Official (ISC)2 Guide to the ISSAP CBK, CRC Press, 2014, 574 pages.



LES RÉFÉRENCES

- D’autres références seront mentionnées lors des sessions
  - Libre à vous de les consulter.

Introduction et contexte d’architecture de sécurité

L'ARCHITECTURE EN CONTEXTE TECHNOLOGIQUE

- Tire ses sources et ses origines dans l'architecture traditionnelle
  - Ensemble de règles et de convention par lesquels sont créées des œuvres complexes
  - Par sa nature, l'architecture existe pour répondre à des besoins précis
  - Est grandement influencée par les facteurs environnementaux immédiats
    - Varie grandement à travers le temps et les différents points géographiques
  - Doit respecter la capacité technique de réalisation des œuvres
- L'opéra de Sydney
  - Plusieurs élément indépendants mais en harmonie
  - Créés à partir d'une vision centrale
  - Responsabilité de l'architecte de créer cette vision
    - Devient la route à suivre

L'ARCHITECTURE EN CONTEXTE TECHNOLOGIQUE

- Gestion et organisation des éléments complexes
  - L'architecture traditionnelle permet de fournir un cadre dans lequel la complexité (en tant que concept) peut être plus facilement gérée
  - Permet d'apporter de la cohérence, une organisation et de l'harmonie à plusieurs éléments qui seraient autrement démunis de sens.
  - Le rôle de l'architecte est de transformer ce qui semble complexe en éléments simple
    - Ceci est accompli par une approche structurée transformant un design en morceaux simple à gérer qui ont une fonctionnalité précise

L'ARCHITECTURE EN CONTEXTE TECHNOLOGIQUE

- Application des concepts de base à l'architecture technologique
  - L'architecture d'entreprise (AE) a pour but d'aider à résoudre les mêmes préoccupations dans le contexte technologique que l'architecture traditionnelle dans le mode réel
  - Elle offre différents cadres pour aider à dé-complexifier la création de :
    - Ordinateurs
    - Réseaux de communication
    - Systèmes distribués
    - Etc.
  - Elle permet de :
    - Définir précisément les objectifs à atteindre
    - L'environnement dans lequel le système existera
    - Les capacités techniques des ressources à construire et opérer ce système

L'ARCHITECTURE EN CONTEXTE TECHNOLOGIQUE

L'architecture en contexte technologique se préoccupe de beaucoup plus que des simples facteurs technologiques ou des différents éléments à installer sur un réseau. Elle se préoccupe de ce que l'entreprise veut accomplir et des facteurs externes qui peuvent avoir une influence sur sa capacité à y arriver.

--> Bon nombre d'organisation on de la difficulté à bien comprendre ce rôle, ce qui rend la mission de l'architecture difficile à accomplir. Trop souvent, les facteurs technologiques et l'urgence dictent la ligne à suivre[1].

1. Réf. Gartner 2021

UN PEU D'HISTOIRE

- Les premières trace d'une méthodologie structurée présentement utilisée par TOGAF comme fondation peuvent être retracées dans un article de Marshall K. Evans et Lou R. Hague intitulé "Master Plan for Information Systems" publié en 1962 dans le "Harvard Business Review".
- Le besoin d'un alignement avec l'organisation apparait dans les années 70
- Connait un réel début dans la années 80-90
  - Coïncide avec la multiplication des langages de programmations
  - Elle suit la croissance de la popularité de la micro-informatique
  - Voient l'apparition de plusieurs cadres, standards et méthodes d'architecture adaptés au monde informatique
- Publication de PRISM en 1986*, le premier cadre d'AE
- Zachman publie « A framework for information systems architecture (ISA) » en 1987

*https://www.bcs.org/content/conWebDoc/56347

UN PEU D'HISTOIRE

- En 1990, on définie de manière formelle ce qu'est l'architecture d'entreprise*
- Zachman renomme son cadre de référence « Information System Architecture » à « Entreprise Architecture » en 1997
- TOGAF 8 réoriente ses priorités de l'architecture technologique vers les considérations **d'affaire, des données et d'application**. C'est en 2002.
- En 2011, TOGAF 9.1 précise :

  « La planification stratégique au niveau de l'organisation procure l'orientation de l'architecture d'entreprise »

  - Inclus les 4 domaines d'architecture (**affaire, données, application et technologie**)

*Richardson, G.L.; Jackson, B.M.; Dickson, G.W. (1990). "A Principles-Based Enterprise Architecture: Lessons from Texaco and Star Enterprise". MIS Quarterly. 14 (4): 385–403.

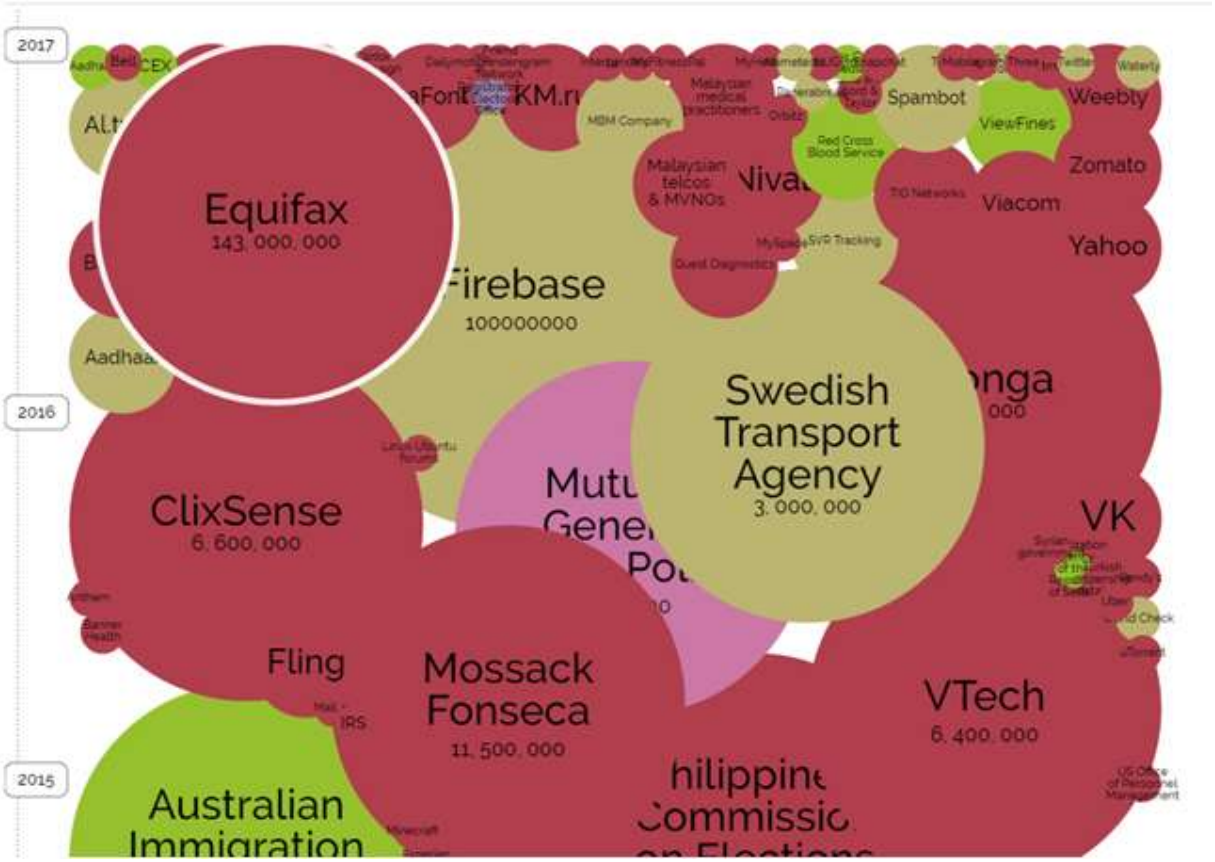
UN PEU D'HISTOIRE

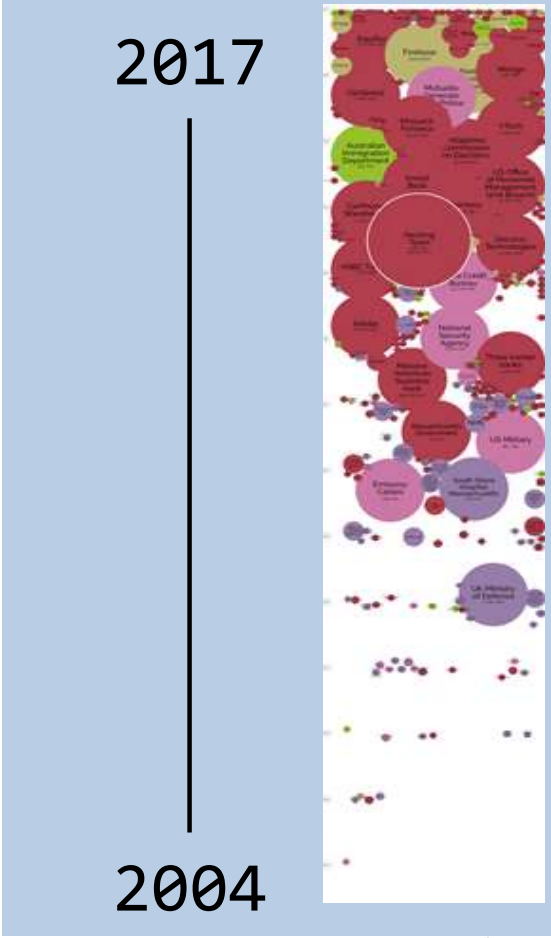
- En 1996, John Sherwood publie « SALSA: A Method of Developing the Enterprise Security Architecture and Strategy »
  - *Sherwood Associates Limited Security Architecture*
  - Son travail est grandement basé sur ISO 7498-2 (OSI security architecture)
    - ISO 7498-1 est très connu pour sa description des 7 couches du modèle OSI*. Son petit frère l'est beaucoup moins
  - SALSA sera ultérieurement renommé SABSA pour des raisons légales
- C'est en 2006 que l'architecture de sécurité au niveau entreprise est formellement définie par Gartner
  - Évoluera pour inclure tous les domaines de l'architecture (**affaire, données, application et technologie**), au même titre que l'architecture d'entreprise

*https://www.iso.org/standard/20269.html

Le marché

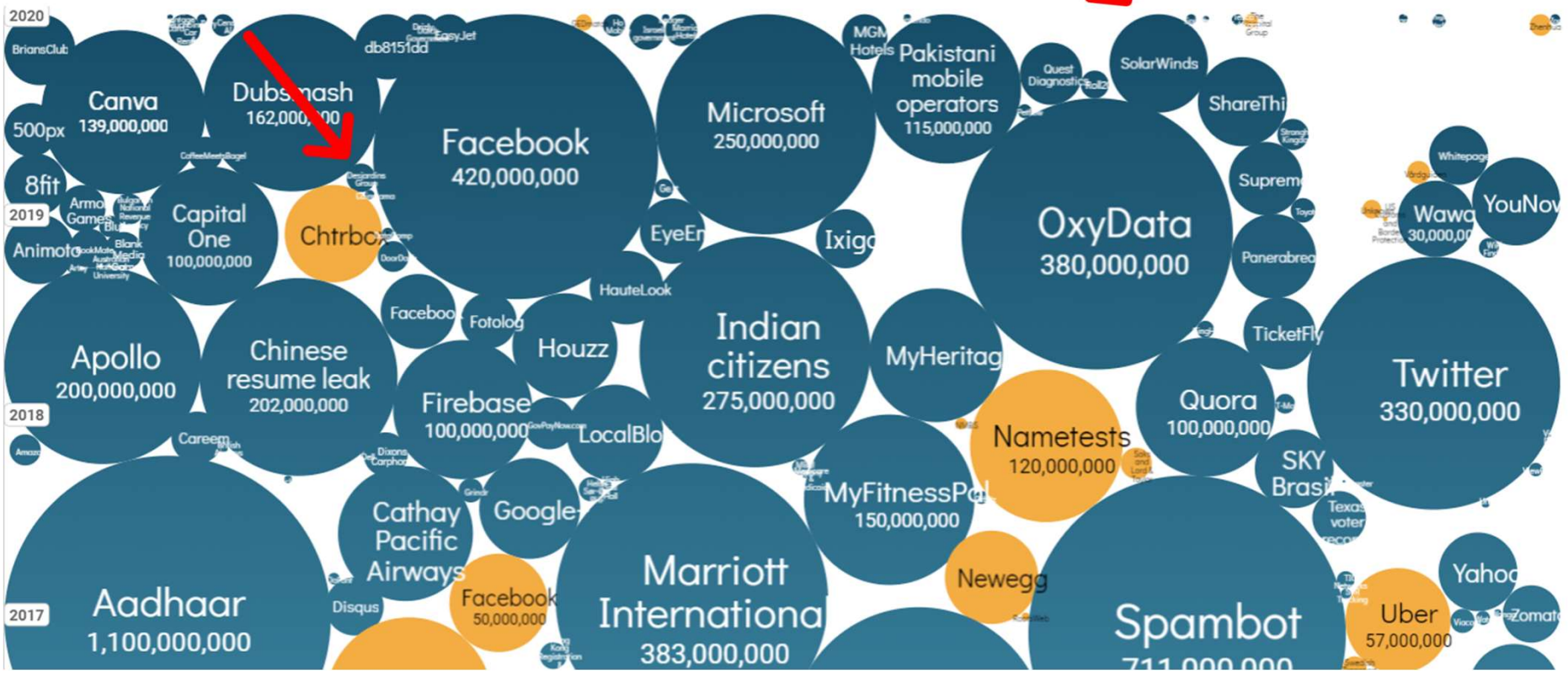
UNIVERSITÉ DE SHERBROOKE



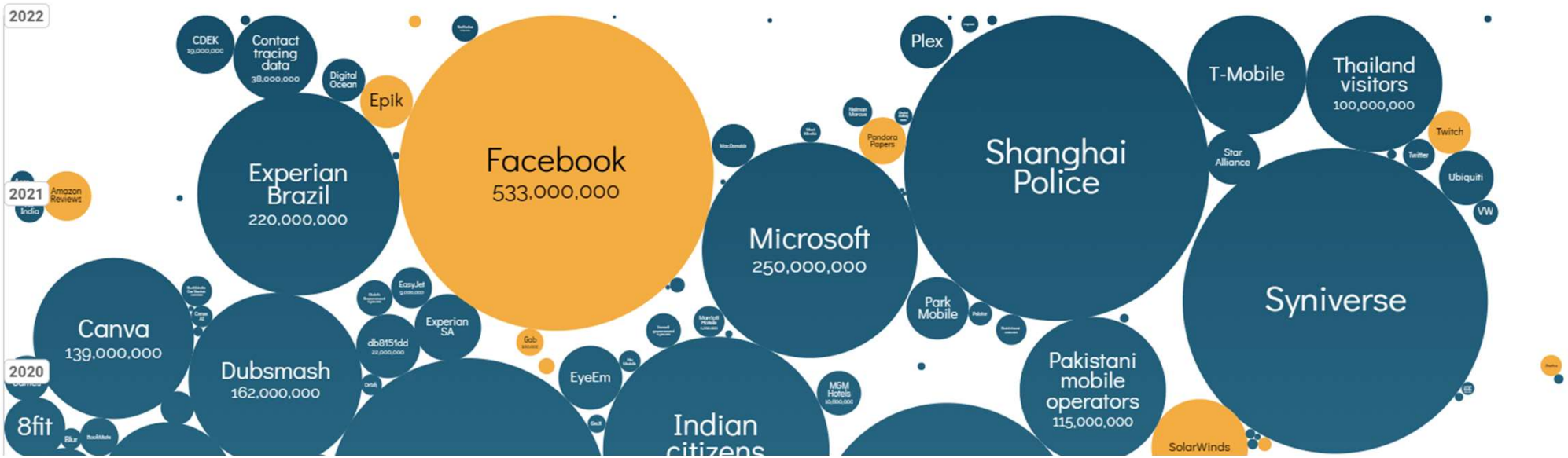


http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
En octobre 2018…. Le monde devenait fou pour : Facebook 50M de clients impactés

CeFTI



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
En Janvier 2020….



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
En Janvier 2023….

La nouvelle cible, les environnements O.T.

- Technologies industrielles
  - Chaines de production
  - Environnement de vente
  - Gestion du transport
    - Train/Avion/Bateau
- Sécurité O.T.
  - Les technologies ne respectent pas forcément les normes IT
  - Cibles facile
  - Se sont convertit vers le protocole IP
- Cible de choix pour les hackers
  - Réseau électrique
  - Centrale nucléaire
  - Panneaux routiers

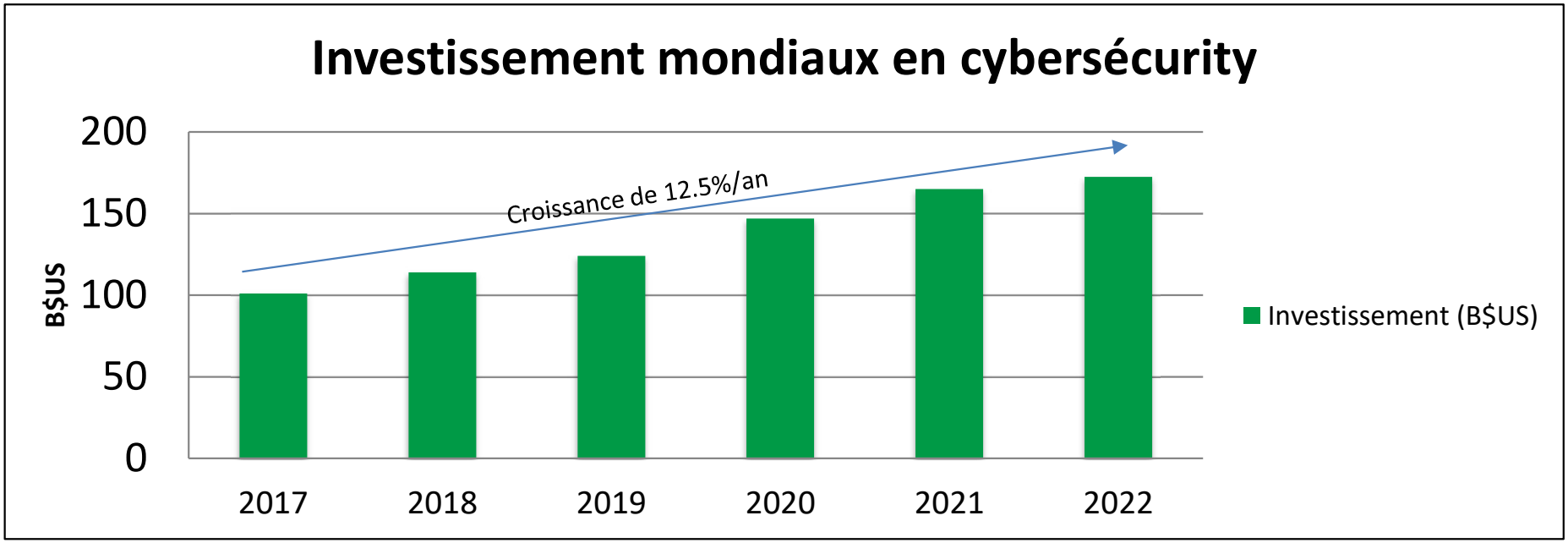
Dans la vraie vie… chez Maerks*

- Impacté massivement pas un rançongiciel (cryptoware)
  - NotPetya → Le grand frère de WannaCry
  - Cible une vulnérabilité cœur de Windows dans SMB
- Vecteur initial: mise à jour d'un logiciel de comptabilité chez un partenaire
- Technique de propagation simple mais très efficace Maersk
  - 1/5ème du trafic de conteneurs mondial
  - TI paralysés
  - Mode manuel 80% (Fax, bons manuscrits, téléphone, etc)
- 45,000PCs , 4000 serveurs et 2500 applications réinstallés **en dix jours**
- Coût: 250 à 300 millions de dollars US

*Incident survenu en Juin 2017
*https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#173939f34f9a

LES ATTENTES ENVERS L'ARCHITECTURE DE SÉCURITÉ

- En 2022, Gartner prévoit que les dépenses en cybersécurité atteindrons 172,5B$US, en fort croissance et atteignant 267.3B$US en 2026[1]



[1]www.gartner.com/en/document/4016190

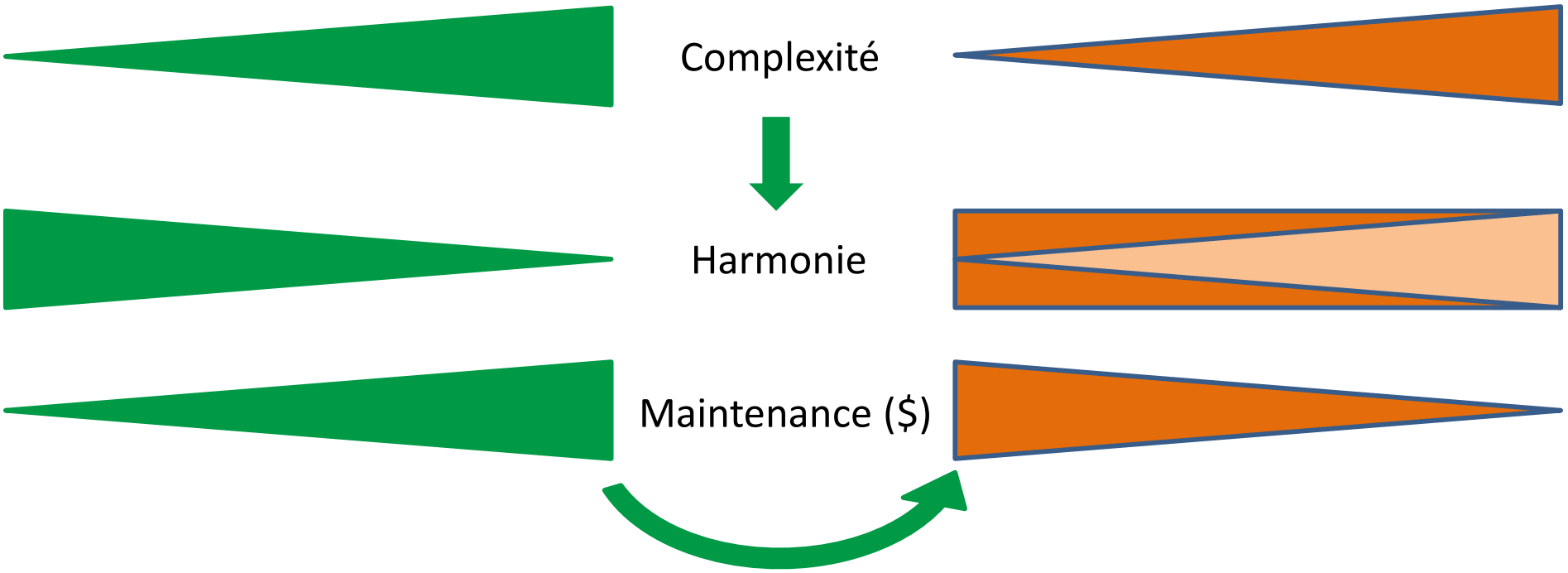
LES ATTENTES ENVERS L'ARCHITECTURE DE SÉCURITÉ

- Dans un marché en évolution
  - La surface d'attaque ne cesse de changer et de s'étendre
  - La complexité des menaces ne cesse de grandir
    - Une croissance marquée au niveau de l'organisation des groupes criminalisés
  - La complexité de la situation ne cesse d'augmenter
  - Les investissements sont en croissance

- Besoin d'alignement avec l'organisation
  - En avoir le plus possible pour son argent
  - Connaitre notre environnement, le contexte d'affaire
  - Connaitre quelles sont les menaces auxquelles l'organisation est exposée et les risques
  - Organiser sa structure de défense

LES ATTENTES ENVERS L'ARCHITECTURE DE SÉCURITÉ

- En plus du besoin d'alignement avec les besoins de l'organisation



Rôle de l'architecture de sécurité

L’Architecture d’entreprise, c’est quoi ?

L'ARCHITECTURE D'ENTREPRISE, C'EST QUOI ?

- L'architecture d'entreprise est une vision systémique de l'entreprise (les fonctions d'affaire) sous forme de composantes.
- Elle vise à standardiser les composantes de l'entreprise de manière à faciliter les assemblages complexes.
- Les méthodologies formelles d'architecture visent à mettre en place des principes ainsi qu'un cadre d'architecture dit "de référence".
- C'est une démarche visant à aligner avec la stratégie d'entreprise l'ensemble des couches technologiques de celle-ci (Affaire, données, applicative, technique, ...).

Dans le contexte du cours, l'Architecture de Sécurité est vue comme un sous-domaine de l'AE

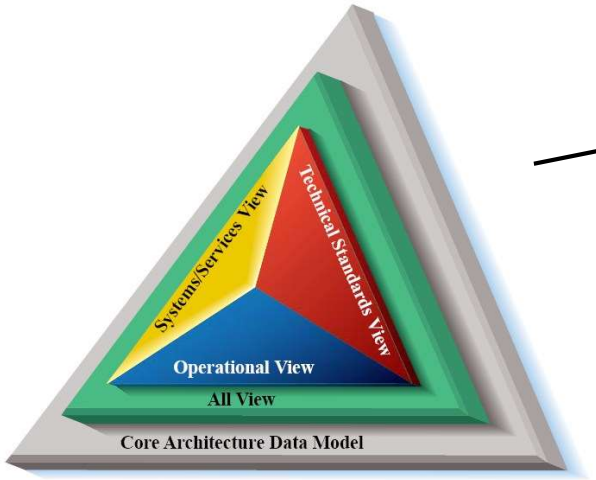
LES CADRES D'ARCHITECTURE D'ENTREPRISE ET DE SÉCURITÉ

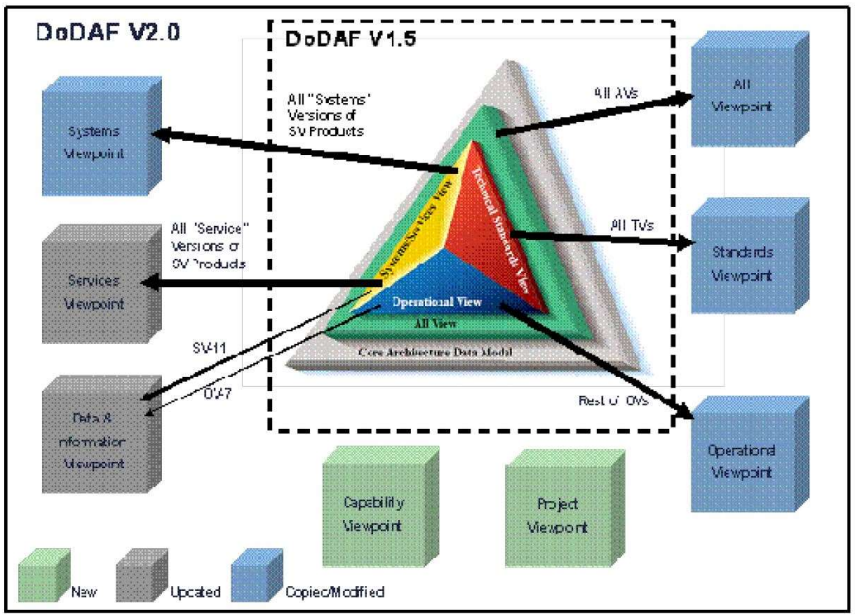
- The U.S. Department of Defense (DoD) Architecture Framework (DoDAF)
- Extended Enterprise Architecture Framework (E2AF) from the Institute For Enterprise Architecture Developments.
- Federal Enterprise Architecture of the United States Government (FEA)
- The UK Ministry of Defence (MOD) Architecture Framework (MODAF)
- Open Security Architecture (www.opensecurityarchitecture.org)
- Service-Oriented Modeling Framework (SOMF)
- SABSA framework and methodology
- The Open Group Architecture Framework (TOGAF)
- Zachman Framework

LES CADRES D'ARCHITECTURE D'ENTREPRISE ET DE SÉCURITÉ

- The U.S. Department of Defense (DoD) Architecture Framework (DoDAF)

DoDAF est un cadre d'architecture pour le DoD américain. Il procure une infrastructure de visualisation pour les parties prenantes grâces à son organisation par vue.



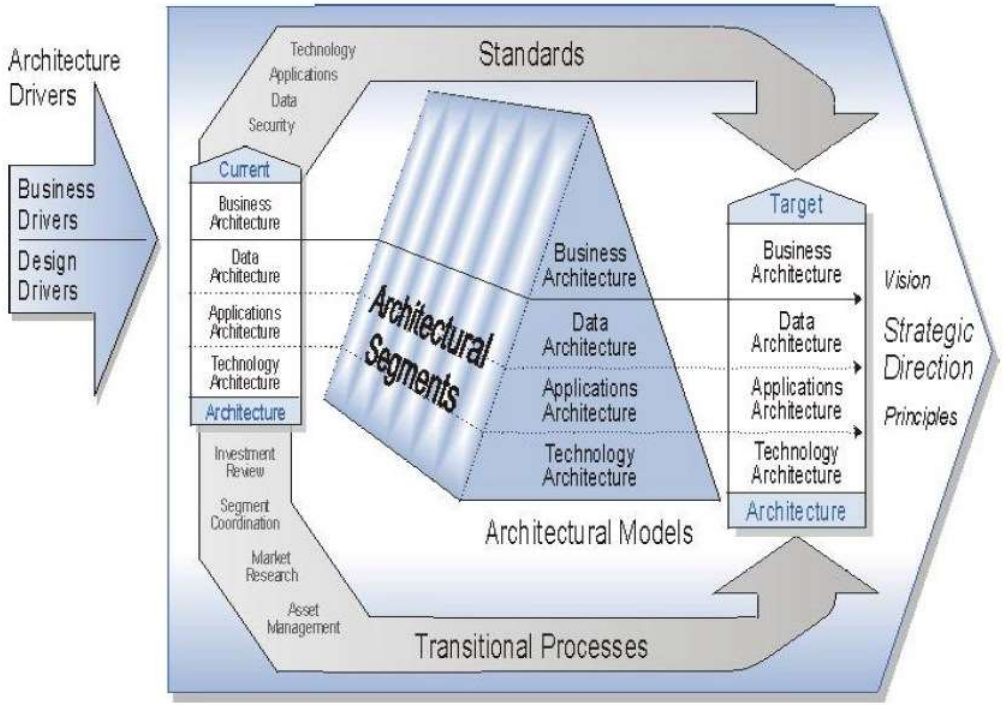


UNIVERSITÉ DE SHERBROOKE

LES CADRES D'ARCHITECTURE D'ENTREPRISE ET DE SÉCURITÉ

- Federal Enterprise Architecture of the United States Government (FEA)

Il s'agit du cadre de référence des agences américaines. Il procure une approche commune pour l'intégration des éléments de stratégie, d'affaire et technologiques en ce qui concerne le design et la gestion de la performance.



LES CADRES D'ARCHITECTURE D'ENTREPRISE ET DE SÉCURITÉ

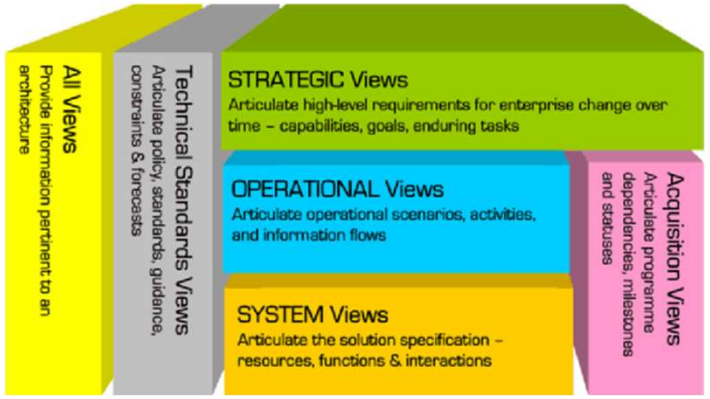
- Extended Enterprise Architecture Framework (E2AF) from the Institute For Enterprise Architecture Developments.

Le E2AF (Extended Enterprise Architecture Framework), publié pour la première fois en 2003, est basé sur la norme IEEE 1471 qui décrie l'architecture d'un système logiciel en ce qui concerne les vues et points de vue ainsi que d'autres éléments de FEAF et TOGAF. Il utilise une structure matricielle en 2 dimensions, similaire au cadre de Zachman, et définit quatre type d'éléments : métier, information, système et infrastructure. Cependant, dans l'ensemble, comparé au cadre Zachman, l'E2AF est davantage axé sur la technologie.

LES CADRES D'ARCHITECTURE D'ENTREPRISE ET DE SÉCURITÉ

- The UK Ministry of Defence (MOD) Architecture Framework (MODAF)

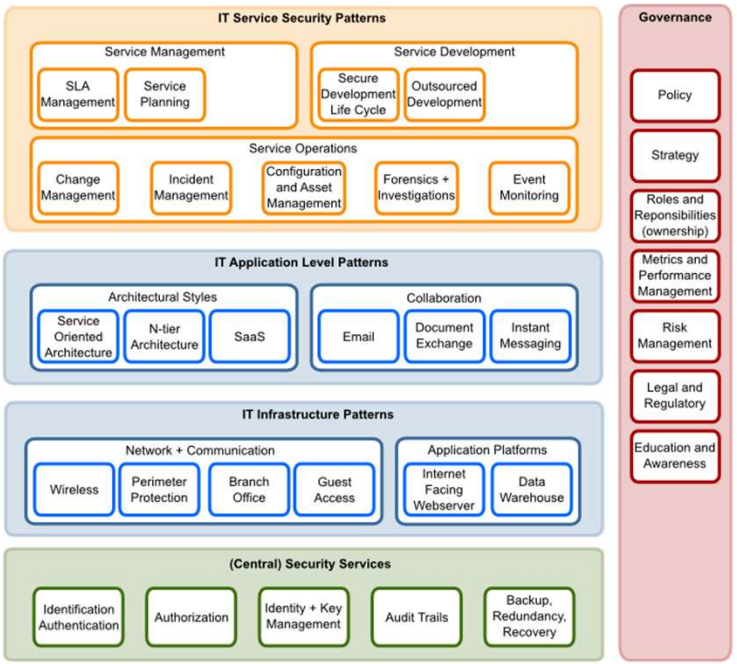
Le MODAF est un cadre d'architecture qui définie une méthode standardisée de la pratique d'architecture d'entreprise, originalement développée par le UK MOD. Son objectif original était de fournir une plus grande rigueur et une meilleure structure pour supporter la définition et l'intégration des éléments technologiques.



LES CADRES D'ARCHITECTURE D'ENTREPRISE ET DE SÉCURITÉ

- Open Security Architecture (www.opensecurityarchitecture.org)

Un ensemble d'artefact de design qui ont une pertinence dans la définition de la structure des composantes de la sécurité et de leurs interrelations.



LES CADRES D'ARCHITECTURE D'ENTREPRISE ET DE SÉCURITÉ

- Service-Oriented Modeling Framework (SOMF)

SOMF est une méthodologie orientée sur l'utilisation de modèles formels. Son approche ainsi que les pratiques qu'elle recommande sont prévues pour être utilisées dans un contexte d'architecture, de design et de développement logiciel.

SOMF offre une vue à 360 degrés pour tous types de cycles de développement logiciel, de la conceptualisation au design et incluant les activités d'architecture.

Plus particulièrement, la méthodologie vise les pratiques :

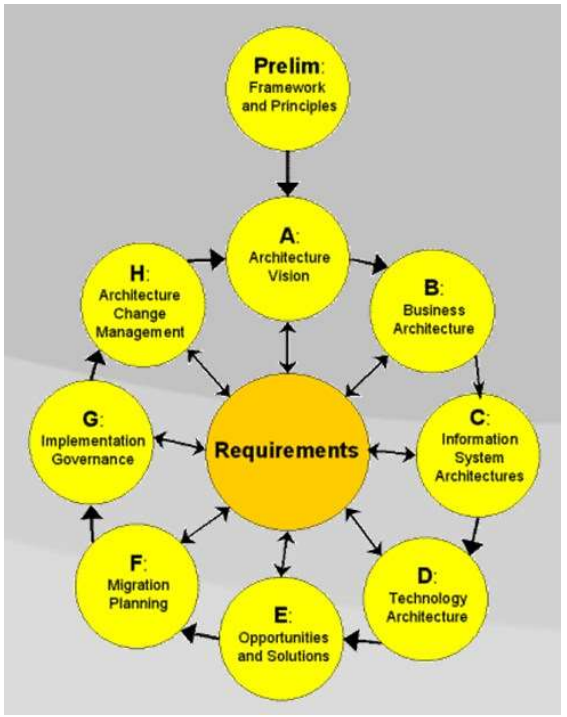
1. Service-Oriented Conceptualization Model
2. Service-Oriented Discovery and Analysis Model
3. Service-Oriented Business Integration Model
4. Service-Oriented Logical Design Model
5. Service-Oriented Software Architecture Model
6. Cloud Computing Toolbox Model

LES CADRES D'ARCHITECTURE D'ENTREPRISE ET DE SÉCURITÉ

- The Open Group Architecture Framework (TOGAF)*

TOGAF a été développé et est continuellement amélioré depuis le milieu des année 90 par différentes personnes appartenant à un certain nombre de départements informatiques d'importantes sociétés, ainsi que par des fournisseurs de conseils ou de solutions informatiques. Ce travail est effectué par l'intermédiaire du forum des architectures de l'*Open Group*

Des détails de ce forum ainsi que les plans d'évolution du standard dans l'année courante sont communiqués sur le site du forum architecture de l'Open Group**.



* Voir slide 58
**https://publications.opengroup.org/c182

LES CADRES D'ARCHITECTURE D'ENTREPRISE ET DE SÉCURITÉ

- Zachman Framework

Le cadre Zachman est un cadre d'architecture d'entreprise qui permet d'une manière formelle et hautement structurée de définir le système d'information d'une entreprise.

Il utilise un modèle de classification à deux dimensions basé sur six (6) interrogations de base : Quoi, Comment, Où, Qui, Quand, et Pourquoi (*What, How, Where, Who, When, Why*),

Ces six (6) questions croisent six types de modèles distincts qui se rapportent à des groupes de parties prenantes : Visionnaire, Propriétaire, Concepteur, Réalisateur, Sous-traitant et Exécutant (*visionary, owner, designer, builder, implementer, worker*) pour présenter une vue holistique de l'entreprise qui est modélisée.

Le modèle se représente par une matrice 6 x 6

	What? (Data)	How? (Function)	Where? (Location)	Who? (People)	When? (Time)	Why? (Motivation)
Business Concept Planner	Inventory Identification	Process Identification	Distribution Identification	Responsibility Identification	Timing Identification	Motivation Identification
Business Concept Owner	Inventory Definition	Process Definition	Distribution Definition	Responsibility Definition	Timing Definition	Motivation Definition
Business Logic Designer	Inventory Representation	Process Representation	Distribution Representation	Responsibility Representation	Timing Representation	Motivation Representation
Business Physics Builder	Inventory Specification	Process Specification	Distribution Specification	Responsibility Specification	Timing Specification	Motivation Specification
Business Component Implementer	Inventory Configuration	Process Configuration	Distribution Configuration	Responsibility Configuration	Timing Configuration	Motivation Configuration
User	Inventory Instantiations	Process Instantiations	Distribution Instantiations	Responsibility Instantiations	Timing Instantiations	Motivation Instantiations

LES CADRES D'ARCHITECTURE D'ENTREPRISE ET DE SÉCURITÉ

- Sabsa Framework

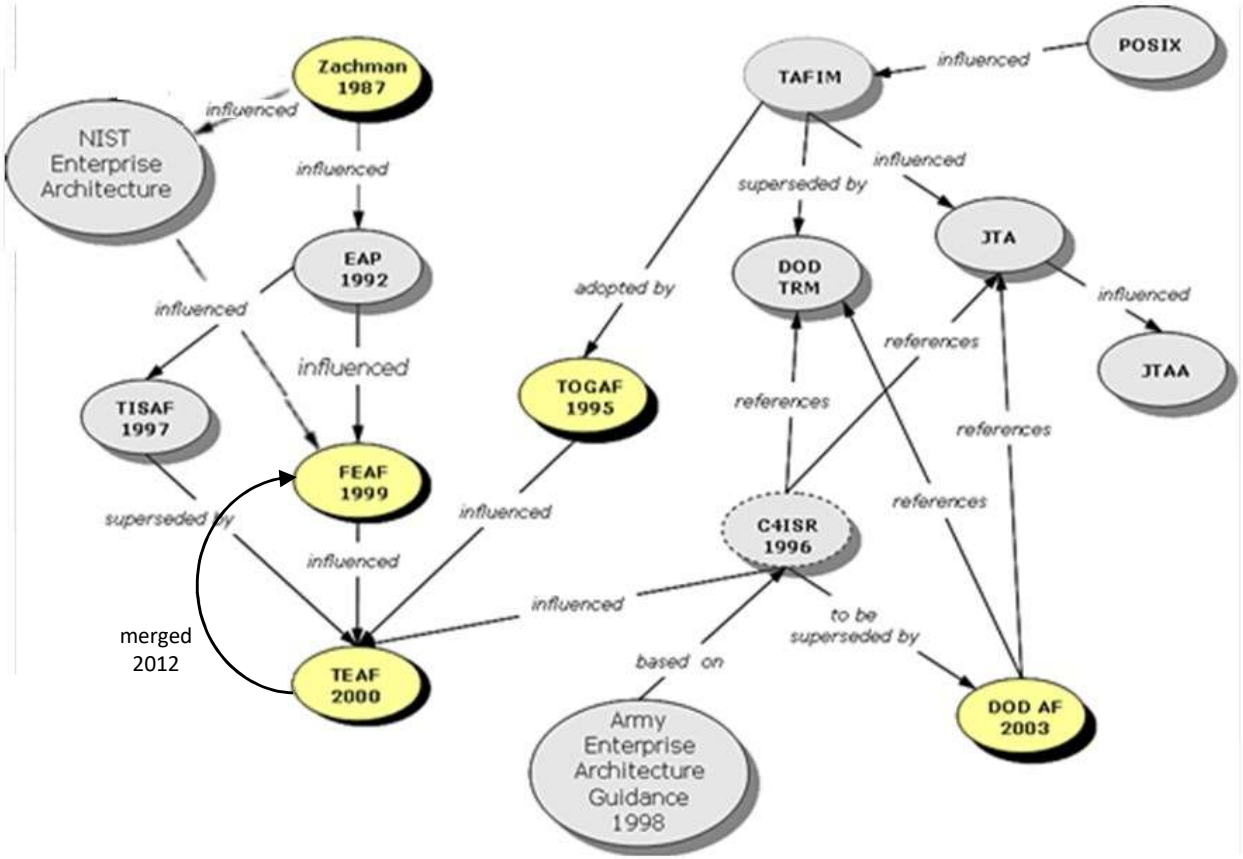
Sabsa est un cadre et une méthodologie pour l'architecture de sécurité au niveau Entreprise. Sabsa a été développée indépendamment du cadre Zachman, quoi qu'elle y utilise une structure et une approche similaire.

Sabsa est une méthodologie pour développer une architecture de sécurité basée sur les risques ainsi que pour permettre la livraison d'une infrastructure de sécurité qui supporte les initiatives et les besoins d'affaire.

Une des caractéristique principale du modèle est que TOUT doit provenir d'un besoin d'affaire.

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Management Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

L'ÉVOLUTION DES CADRES D'ARCHITECTURE



https://en.wikipedia.org/wiki/Enterprise_architecture_framework

CIA & DICAI

UNIVERSITÉ DE SHERBROOKE

Triad CIA et le modèle DICAI

- (C)onfidentialité
- (I)ntégrité
- (D)isponibilité et (A)ccessibilité

C.I.A.

Et

- (A)uthentification et identification
- (I)rrévocabilité

D.I.C.**A.I**

TRIAD CIA

• (C)ONFIDENTIALITÉ

Permet l'assurance que seules les personnes autorisées on accès aux ressources et aux données.

- Encryption des données
- Encryption des communications

• (I)NTÉGRITÉ

Utilisé pour définir l'importance d'un actif d'être altérer uniquement par des actions autorisées. Les mécanismes liés à cette fonction permettent de gérer et détecter ces modifications, qu'elles soient autorisées ou non.

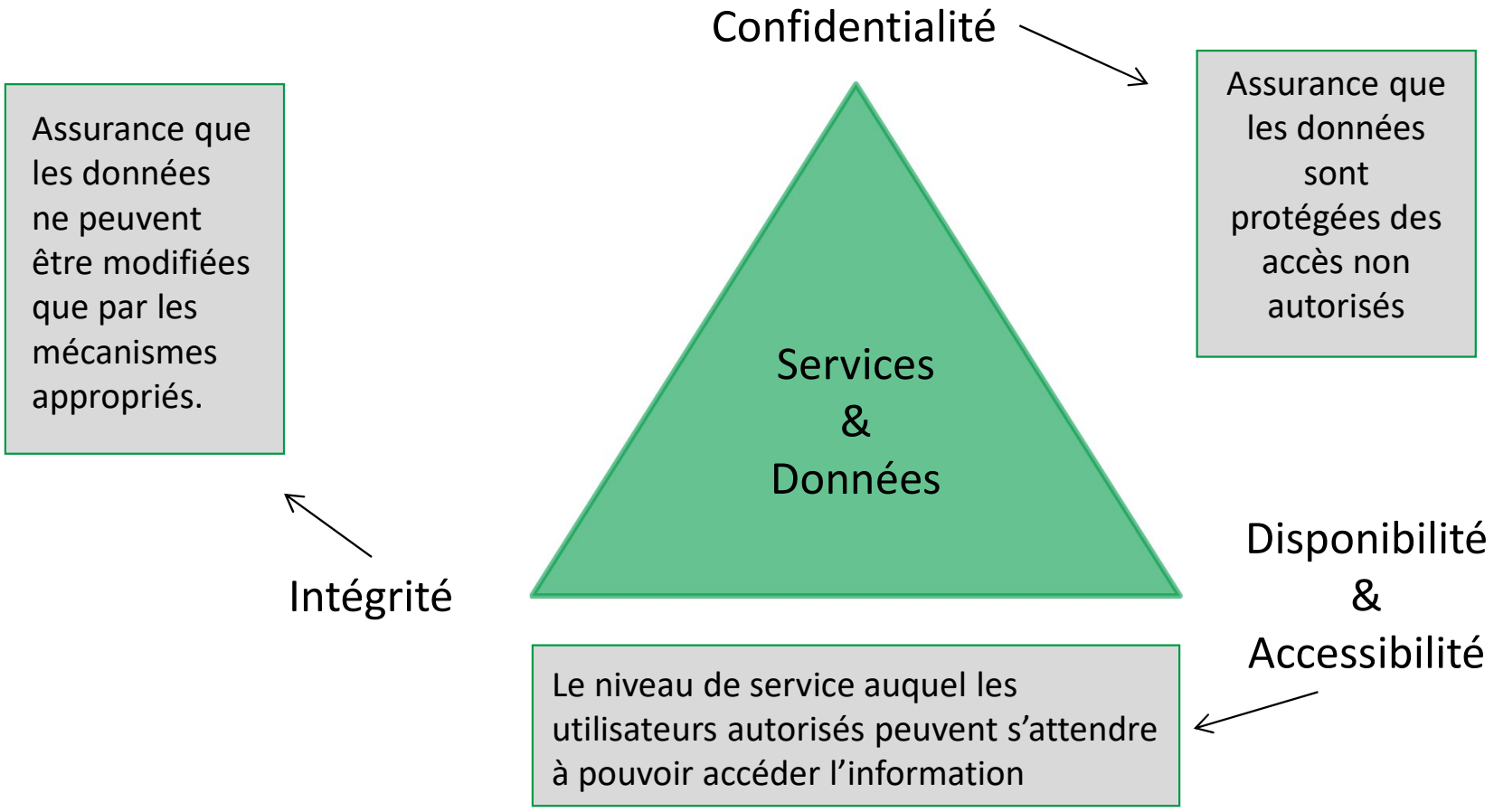
- Hashing
- Redondance
- Signature par clé

• (D)ISPONIBILITÉ ET (A)CCESSIBILITÉ

Utilisé pour définir l'importance de la présence d'un actif. Les mécanisme en place doivent avoir pour but d'assurer la disponibilité et l'accessibilité de l'actif.

- Balancement de charge
- Clustering
- Stratégie de relève
- Sauvegarde et préservation

TRIAD CIA


Confidentialité
Assurance que les données sont protégées des accès non autorisés
Assurance que les données ne peuvent être modifiées que par les mécanismes appropriés.
Services & Données
Intégrité
Disponibilité & Accessibilité
Le niveau de service auquel les utilisateurs autorisés peuvent s'attendre à pouvoir accéder l'information

MODÈLE DICAI

- **(A)UTHENTIFICATION ET IDENTIFICATION**

Assurance de l'identité du répondant

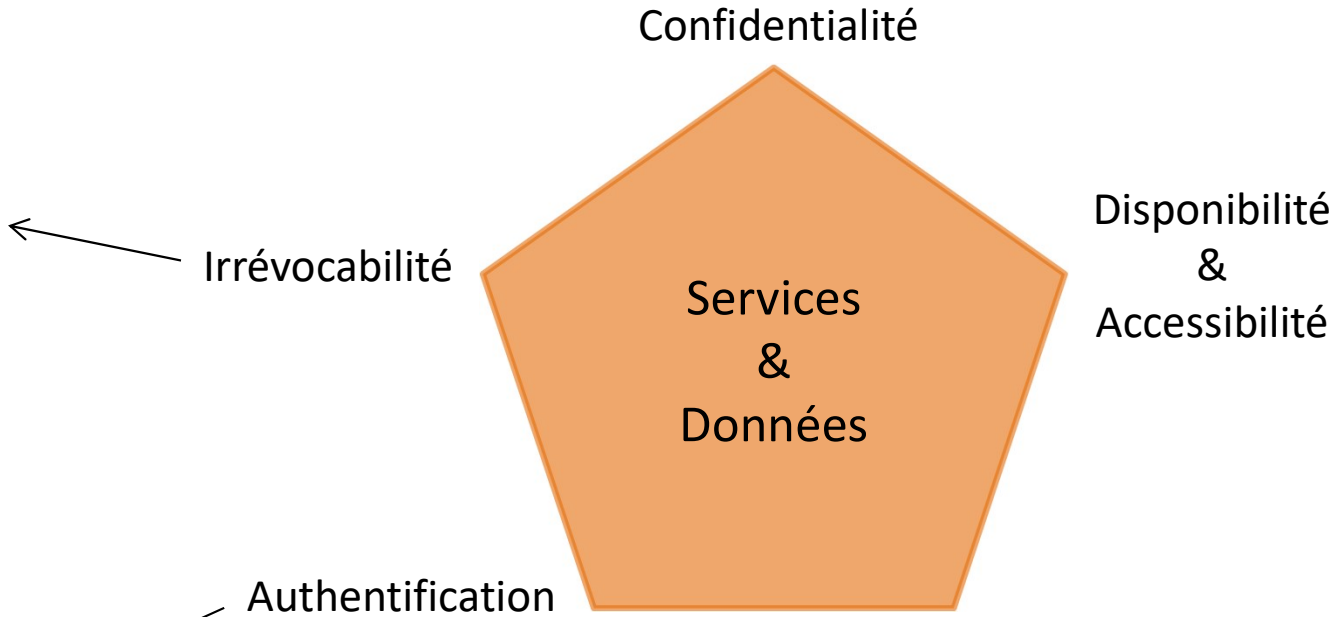
- Codes usager
- Mots de passe, jetons, cartes à puce, biométrie
- Autres facteurs d'authentification (e.g. environnemental, contextuel, comportemental, etc)

- **(I)RRÉVOCABILITÉ**

Assurance qu'il est impossible de nier qu'une opération, un transfert ou une transaction aie eu lieu et quelles étaient les acteurs impliqués

- Journalisation des transactions
- Mécanismes d'authentification

MODÈLE DICAI



L'assurance que l'émetteur et le receveur d'un message ne pourront nier la transmission de celui-ci

L'assurance que 1 ou plusieurs identités sont authentique lors d'une transaction

CIA, DICAI & L'ARCHITECTURE

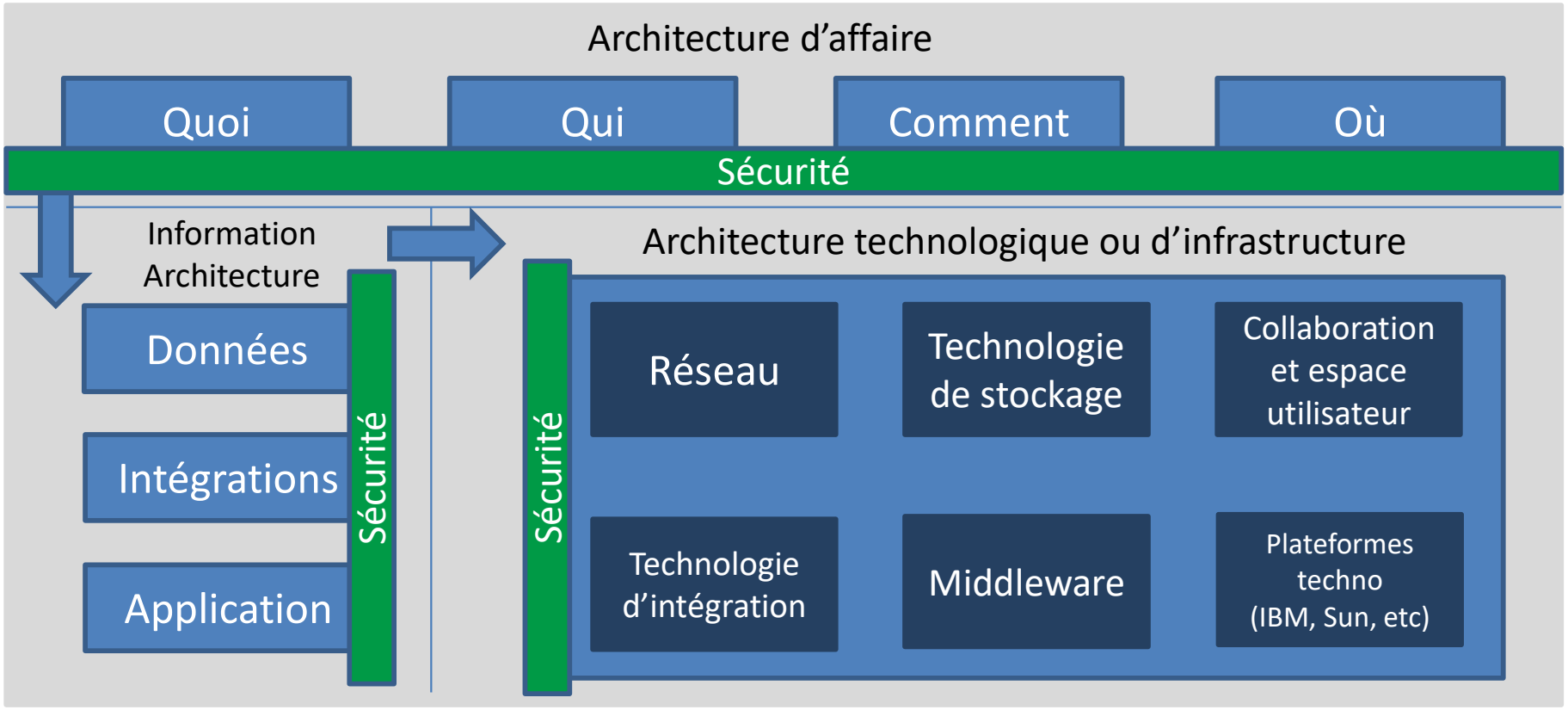


*Illustration inspirée du modèle de Huxham - https://en.m.wikipedia.org/wiki/Enterprise_information_security_architecture