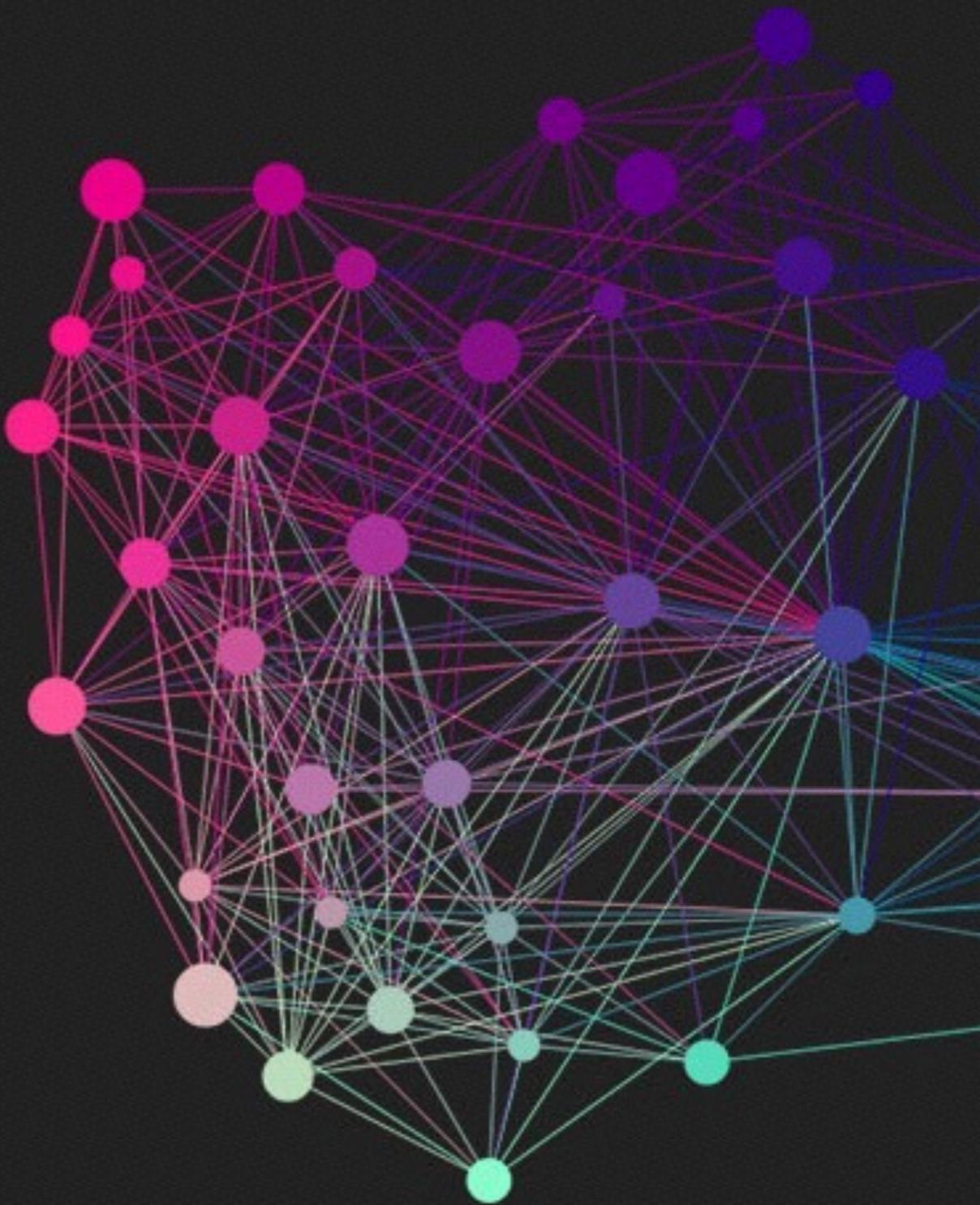


SÉCURITÉ DES

ARCHITECTURES BIGDATA-LAMBDA

SOMMAIRE

- ▶ Introduction
- ▶ Cyber : Généralité
- ▶ IT : Architecture Lambda
- ▶ Cyber : Principes de sécurité
- ▶ IT : Principes d'architecture





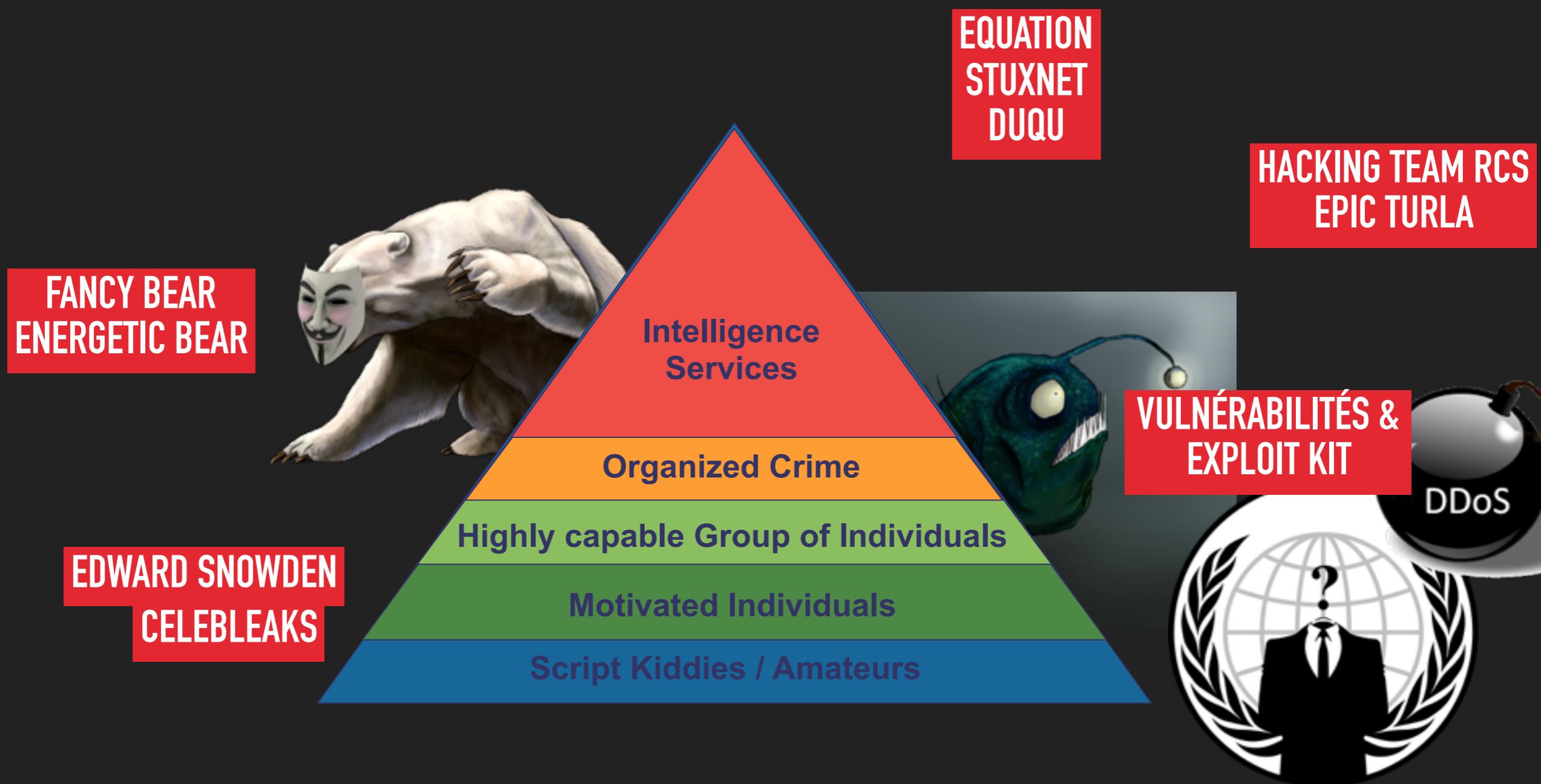
GÉNÉRALITÉ

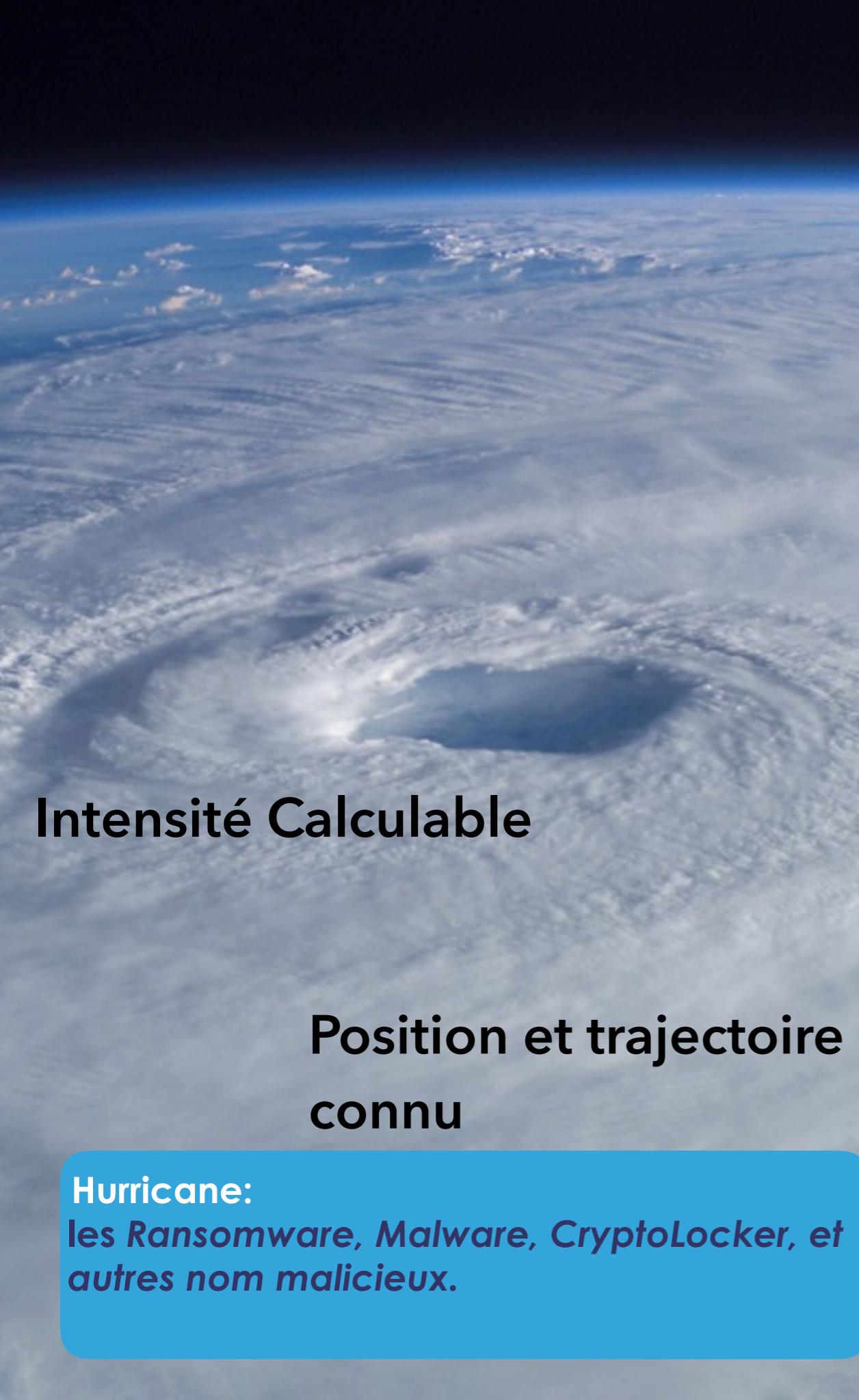
SÉCURITÉ DES ARCHITECTURES LAMBDA

QUI SONT LES ATTAQUANTS ?

QUELLES SONT LES MENACES ?

PYRAMIDE DES ATTAQUANTS





Intensité Calculable

Position et trajectoire connu

Hurricane:
les *Ransomware*, *Malware*, *CryptoLocker*, et autres nom malicieux.



Intensité imprévisible

Point d'impact imprédictible

Earthquake
APT, DDoS Ex; Mirai attack DDoS 1TB/s sur OVH en Sept. 2016, et sur des hébergeurs DNS en Oct. 2016.

RAPPEL SUR LES MENACES

Menaces Cybercrime

- ▶ DDoS, Mirai, Malware Bancaire, Botnet
- ▶ Ransomware & Cryptolocker
- ▶ Phishing

Menaces en cours d'exploitation :

- ▶ Shellshock, DirtyCow,
- ▶ ElasticSearch & MongoDB Leaks
- ▶ Moteur de recherche de failles & de leaks

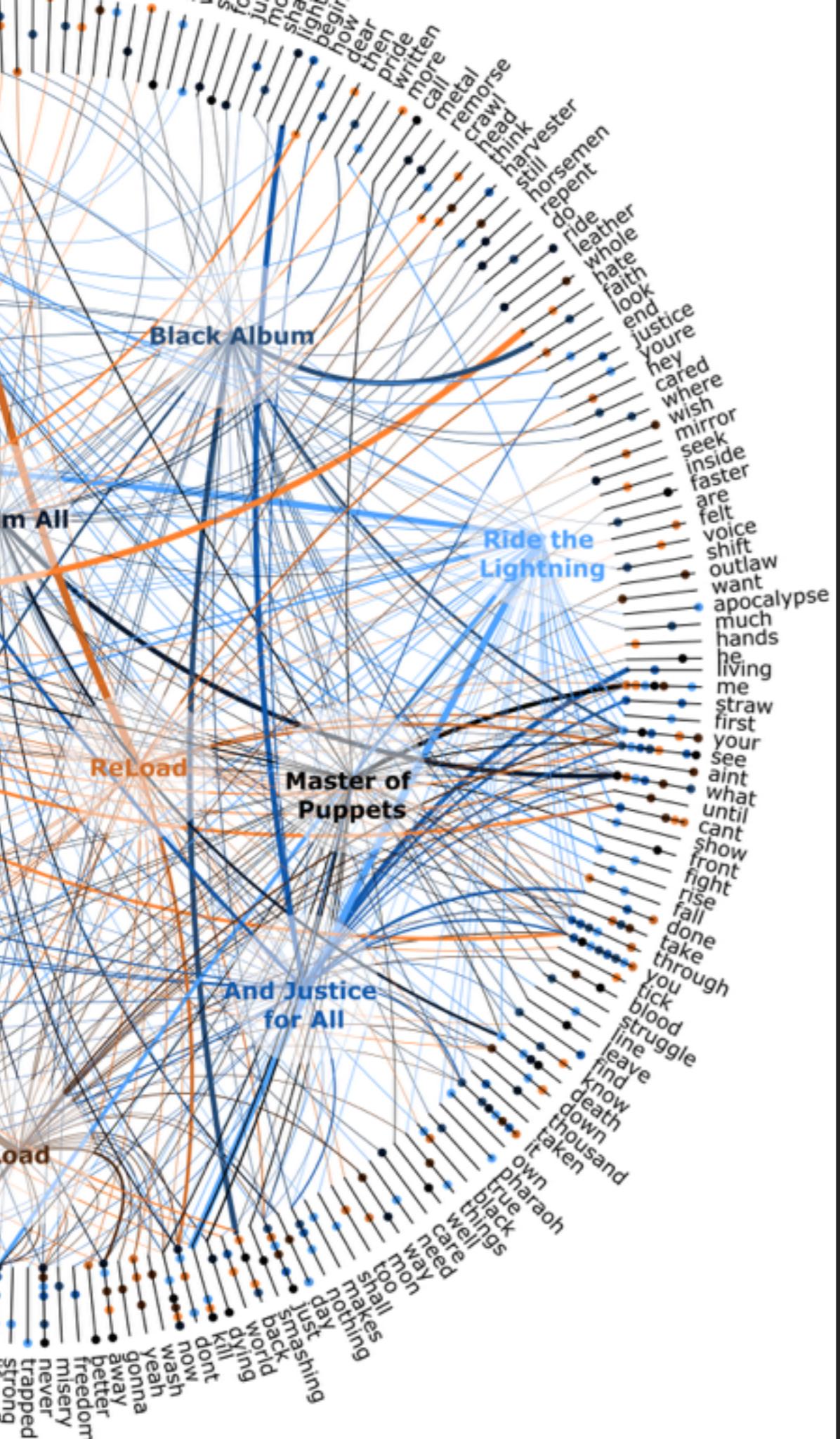
Menaces Etatique

- ▶ Les menaces proviennent des différents continents avec des motivations différentes (*économique, espionage, militaire, politique*)
- ▶ La cyber devient Doctrinale pour les pays : LPM en France, Doctrine militaire pour les Etats unis, Chine, Russie, plan NIS européen ...

CE QU'IL FAUT CONNAITRE

- ▶ Les 7 phases de l'attaque
- ▶ Les catégories de menaces
- ▶ La pyramide des attaquants
- ▶ Méthodologies & techniques :
 - ▶ pentests
 - ▶ d'analyse du risque
 - ▶ **Lutte Informatique Defensive** (Détection d'incident, DFIR, Forensics...)

POUR SAVOIR SE DÉFENDRE



ARCHITECTURE LAMBDA

SÉCURITÉ DES ARCHITECTURES LAMBDA

IT BUZZ WORDS

Bigdata:

Désignent un ensemble de données qui deviennent tellement volumineux qu'ils en deviennent difficiles à travailler avec des outils classiques de gestion de base de données ou de gestion de l'information. (src wikipedia)

NoSQL:

En informatique et en bases de données, NoSQL désigne une famille de systèmes de gestion de base de données (SGBD) qui s'écarte du paradigme classique des bases relationnelles. L'explication du terme la plus populaire de l'acronyme est Not only SQL (« pas seulement SQL » en anglais) même si cette interprétation peut être discutée. (src wikipedia)

Exemple : Cassandra, HBase, CouchDB, MongoDB, ElasticSearch

Architecture Lambda:

Architecture pour analyser des données de façon massive en utilisant les différentes méthodologies de traitement et d'exécution temps réel (stream) & temps différé (batch). (src wikipedia)

DATASCIENTIST BUZZ WORDS

Machine Learning:

L'apprentissage automatique ou apprentissage statistique (machine learning en anglais), champ d'étude de l'intelligence artificielle, concerne la conception, l'analyse, le développement et l'implémentation de méthodes permettant à une machine (au sens large) d'évoluer par un processus systématique, et ainsi de remplir des tâches difficiles ou problématiques à remplir par des moyens algorithmiques plus classiques. (*src wikipedia*)

Deep Learning:

L'apprentissage profond est un ensemble de méthodes d'apprentissage automatique tentant de modéliser avec un haut niveau d'abstraction des données grâce à des architectures articulées de différentes transformations non linéaires[réf. souhaitée]. (*src wikipedia*)

QUEL RAPPORT ENTRE LES ARCHITECTURES LAMBDA & LA CYBER ?

CYBER BUZZ WORDS

SIEM (Security Event Information Management)

Corrélation et Logs Management d'un système à surveiller

Logs provenant de : Système (Windows & Linux), Application,
Equipement de sécurité, Bureautique, BYOD

Besoin technique : **Architecture Lambda**, NoSQL,

Besoin d'infrastructure : puissance de calcul, stratégie de stockage, clustering, résilience

Volumétrie: Suivant la taille du système les analyses tournent sur des centaines de Terra pouvant aller à plusieurs Peta

CYBER BUZZ WORDS

Hunting:

Recherche de trace de compromission à posteriori sur un parc d'ordinateurs (plusieurs centaines à des milliers de machines), sur l'ensemble d'un Système d'Information.

Besoin technique : **Batch computing, NoSQL**

Besoin d'infrastructure : puissance de calcul, stratégie de stockage, clustering

Volumétrie: Suivant la taille du système les analyses tournent sur des centaines de Terra pouvant aller à plusieurs Peta

RAPPEL

A l'origine on avait des DataWare House / Puits de données
(SQL, Filesystem)

Au début était le batch *(SQL, Filesystem)*

Puis le Stream Computing *(SQL, Filesystem)*

Ensuite les architecture lambda :
batch + stream combiné
(NoSQL & Filesystem)

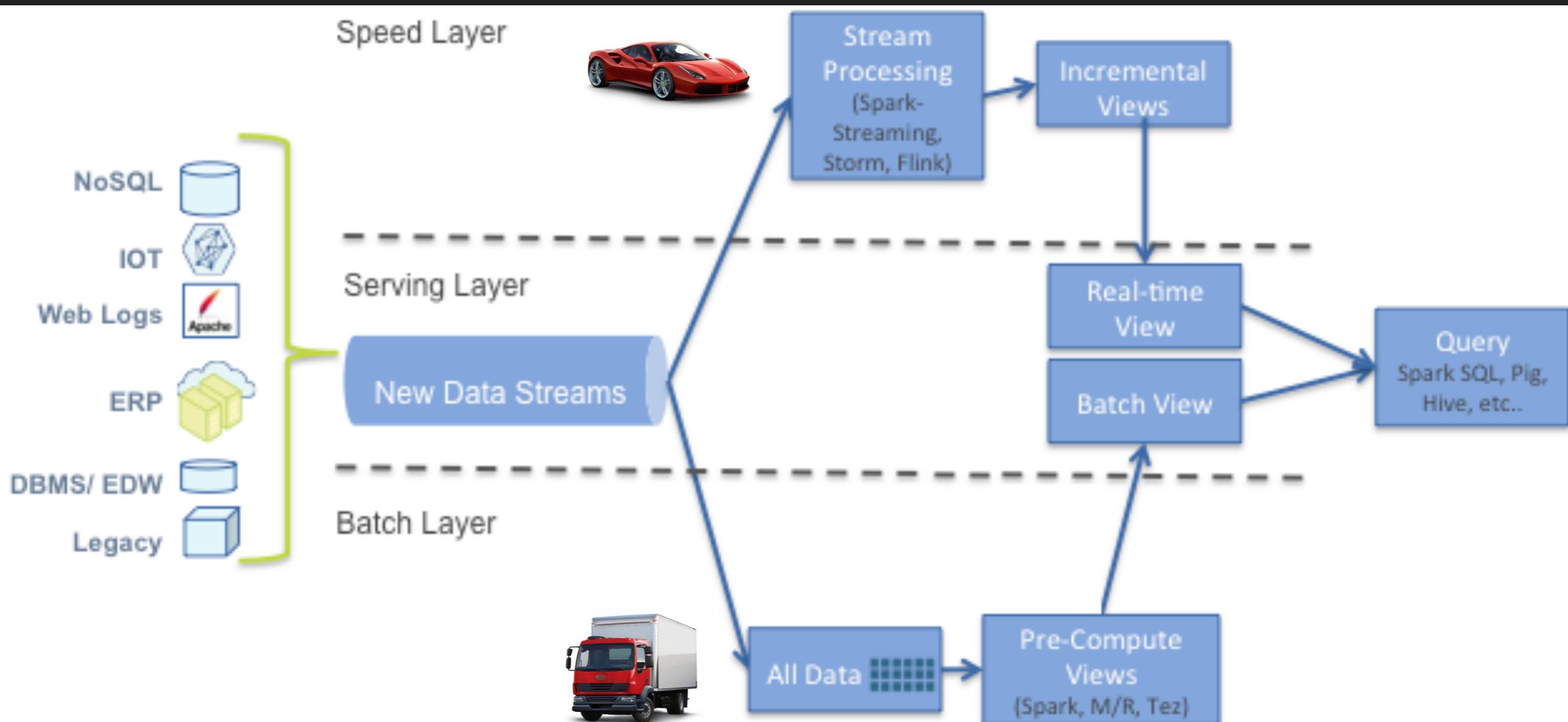


STREAMING

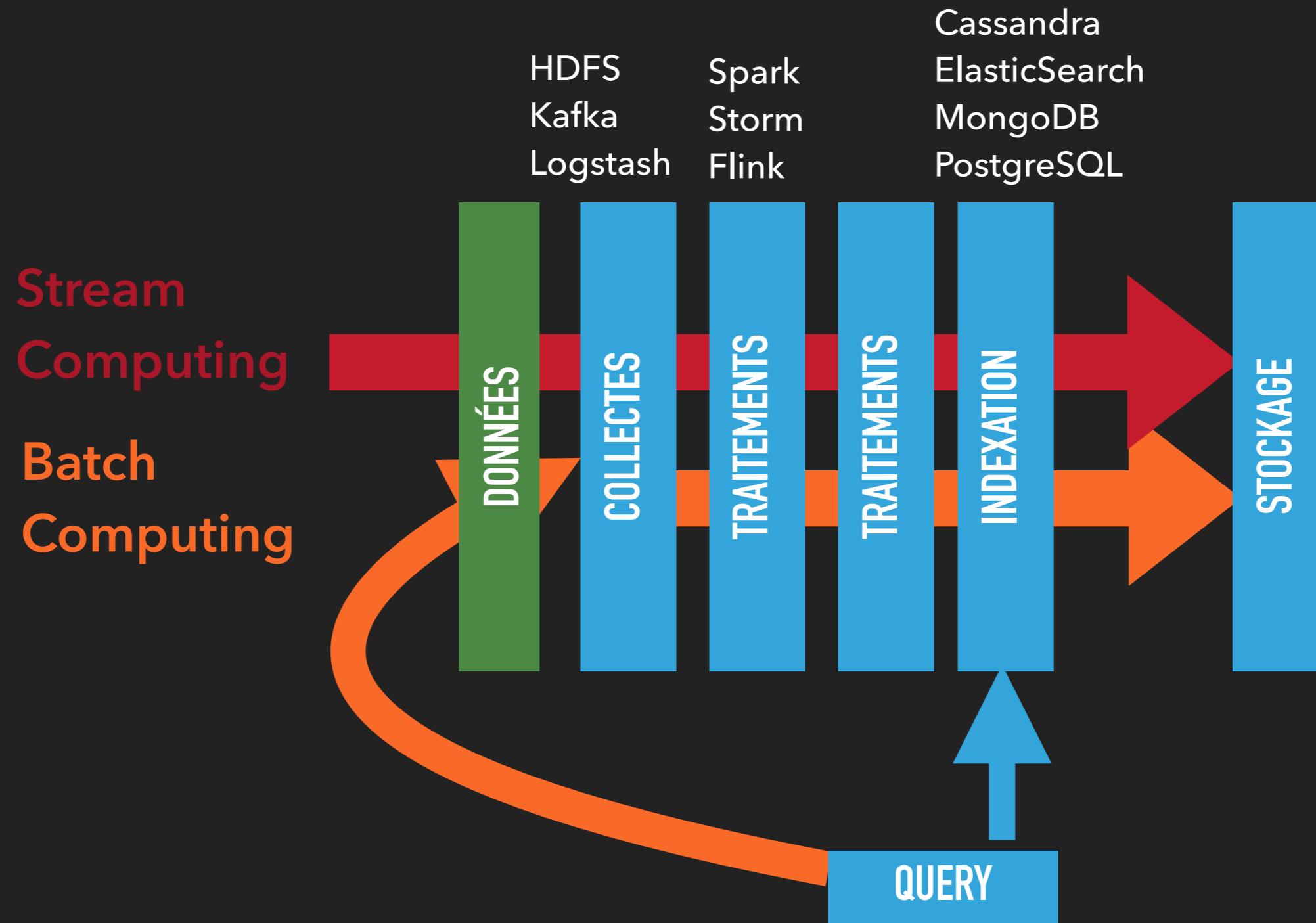


BATCH

2/ ARCHITECTURE LAMBDA



2/ ARCHITECTURE LAMBDA



TEXTE

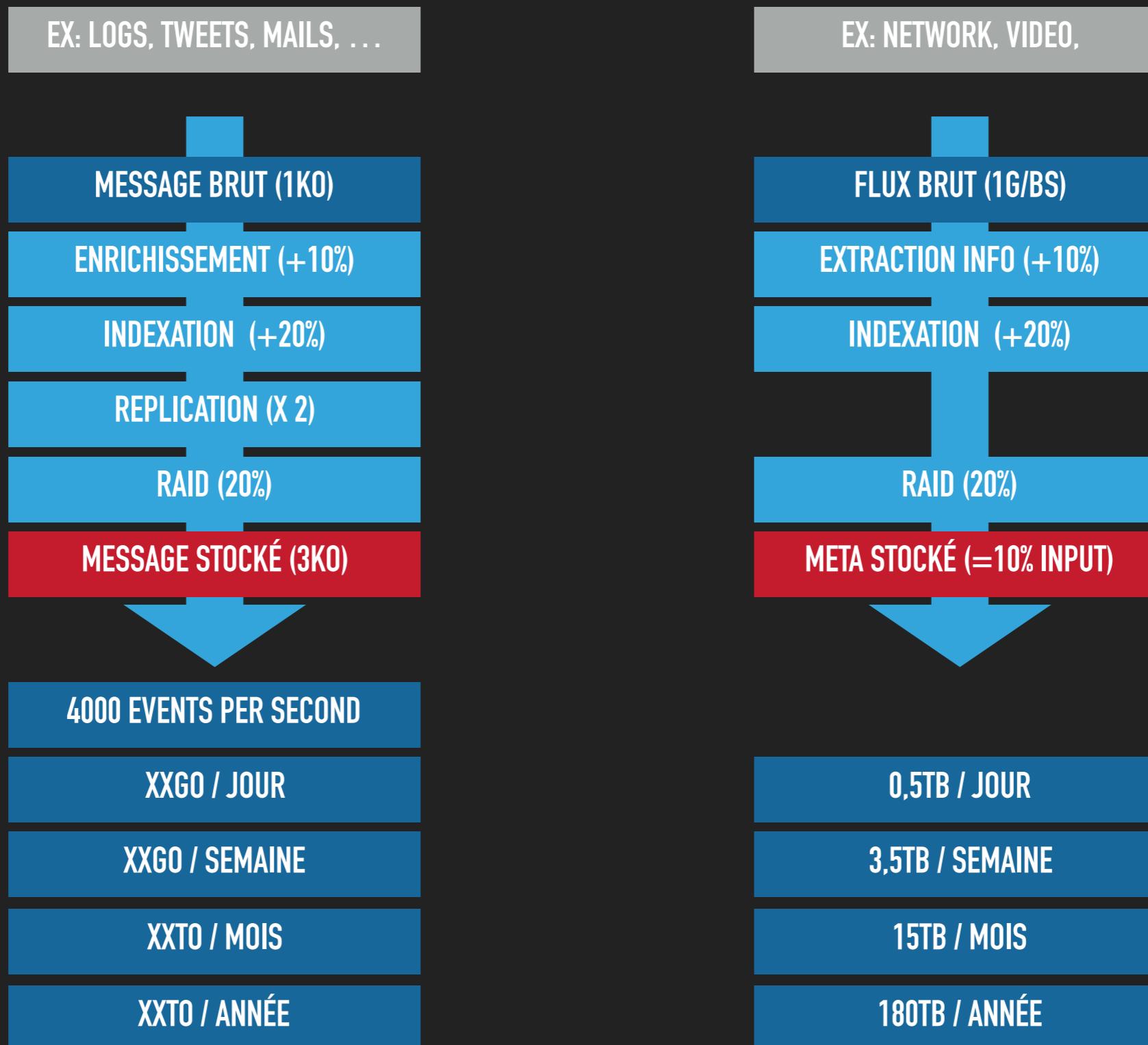
BATCH+STREAM

=

ARCHITECTURE LAMBA



CALCUL DE VOLUMETRIE



CONCEPTS

Technologies

Backend Bigdata

MongoDB, Cassandra, Elasticsearch, Splunk, PostgreSQL, ceph-fs

Computing Bigdata

Zookeeper, Storms, Sparks, Flink
Kafka, Logstash, Splunk

Visualisation

Kibana, d3.js, Splunk, HTML 5

Automatisation

ANSIBLE,
Puppet

Virtualisation

KVM, VMWare, VirtualBox, LXC, Docker, Openstack, SaaS

Machine Learning Deep Learning

algorithme, clustering de données,
SciKit framework



PRINCIPES DE SÉCURITÉ

SÉCURITÉ DES ARCHITECTURES LAMBDA

**« 10 DOLLARS EN DEFENSE CONTRE 1 DOLLAR
EN ATTAQUE »**

**« L'ATTAQUE NE DOIT TOUCHER QU'UNE FOIS, LA
DÉFENSE DOIT RÉUSSIR À TOUT LES COUPS »**

PRINCIPES DE SÉCURITÉ - FONDEMENT

Principes & Concept :

- ▶ Isolationnisme (ségrégation, AIRGAP)
- ▶ Autonomie du système

Ségrégation des réseaux et des usages :

(Technique & Organisationnelle)

- ▶ Réseau : production, d'administration, stockage, sécurité, supervision, ...
- ▶ Humains : administrateur IT, administrateur sec, développeur, utilisateur S.I

AirGAP :

Déconnexion du système d'information les réseaux internet et autres.

Isolation Physique des réseaux avec l'extérieur.

PRINCIPES DE SÉCURITÉ - FONDEMENT

Protection physique des équipements:

- ▶ Badges et contrôles d'accès physiques (Data Center, portes, baies, ...),
- ▶ Vidéo Surveillance

Autonomie :

- ▶ Retirer les adhérences avec les services IT & Réseaux externes pour maîtriser son environnement et éviter les pannes en cascades.
- ▶ Internalisation des services IT vitaux (*DNS, LDAP, NTP, AdminBastion*)

« OBJECTIF : RALENTIR LES
ATTAQUANTS »

DEFENSE DE L'ARCHITECTURE : S.I + SÉCURITÉ

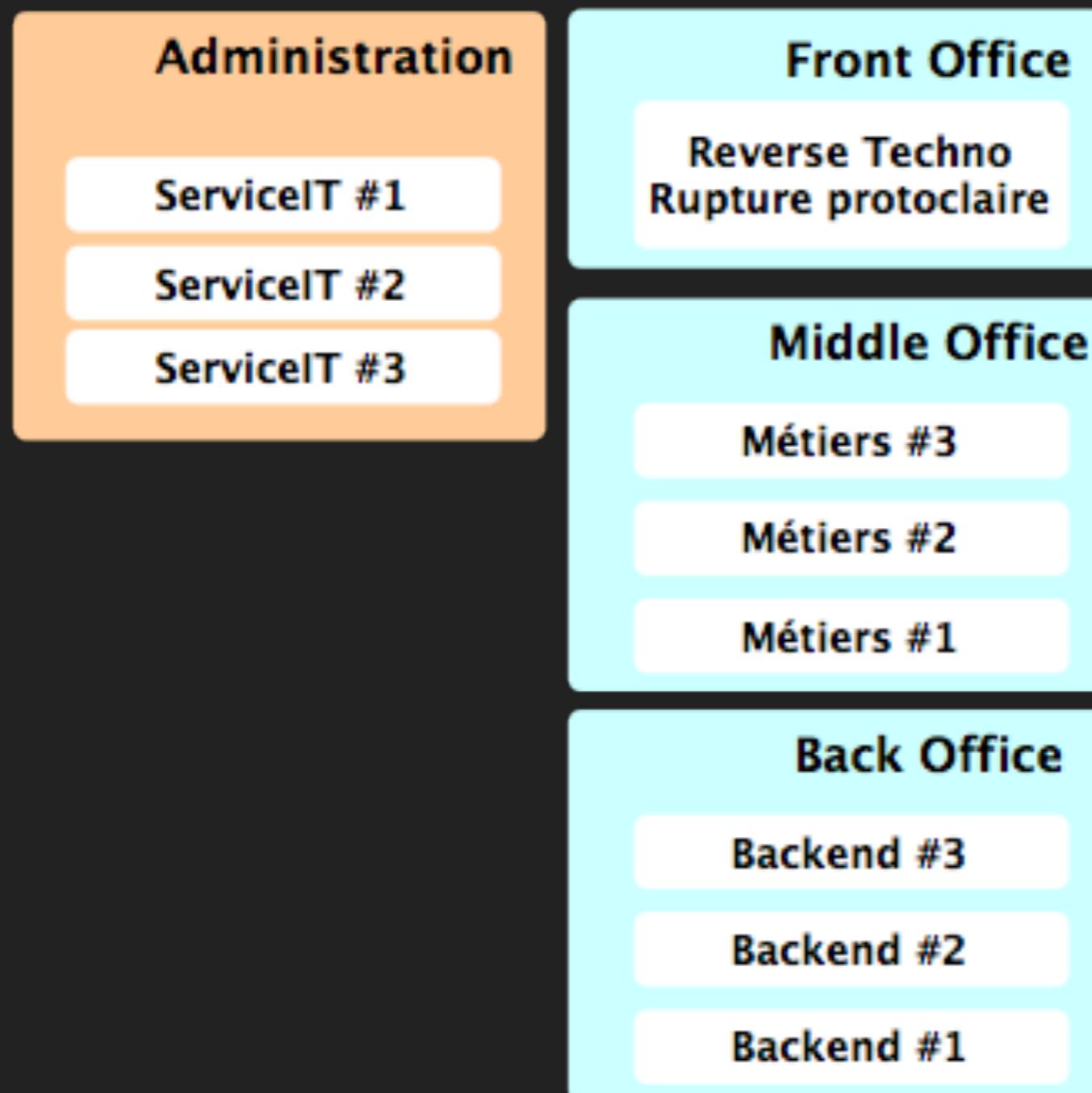
En profondeur par design:

- ▶ Définition de zones de services
(Front Office, Middle Office, Back Office, IT Services, DMZ)
- ▶ Rupture des protocoles d'accès au S.I, usages de rebonds et de reverse proxies.
- ▶ Enfouissement des biens sensibles au fond de l'architecture

Périmétrique par design:

- ▶ Différentes marques d'équipements réseaux & sécurités, déploiements des firewalls & sondes.
- ▶ Supervision de Sécurité
- ▶ autres services de sécurités : IAM, MCS, pentests

PRINCIPE DE SEGREGATION



DEFENSE DE L'ARCHITECTURE - HYGIENE

Principe de base:

- ▶ ACL des utilisateurs, Antivirus sur serveurs et postes bureautique
- ▶ Réduction de la surface d'attaque des systèmes
(retrait des services & applications de base non nécessaire ex: bluetooth, imprimante, ...)

Durcissement :

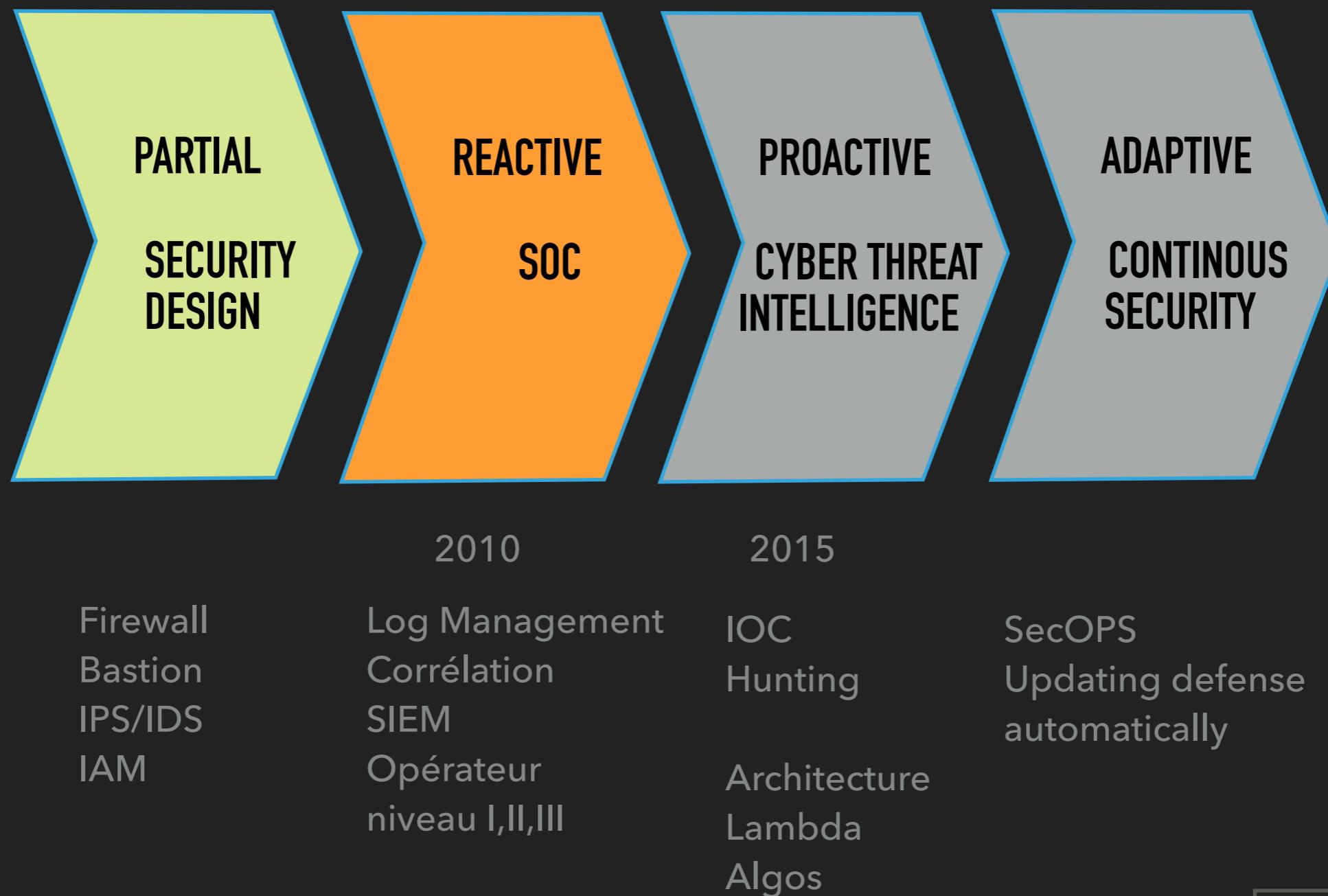
- ▶ Niveau I : Application des guide d'hygiène au niveau système
(*Linux & Windows*) et des sécurités O.S
- ▶ Niveau II : Durcissement Noyau

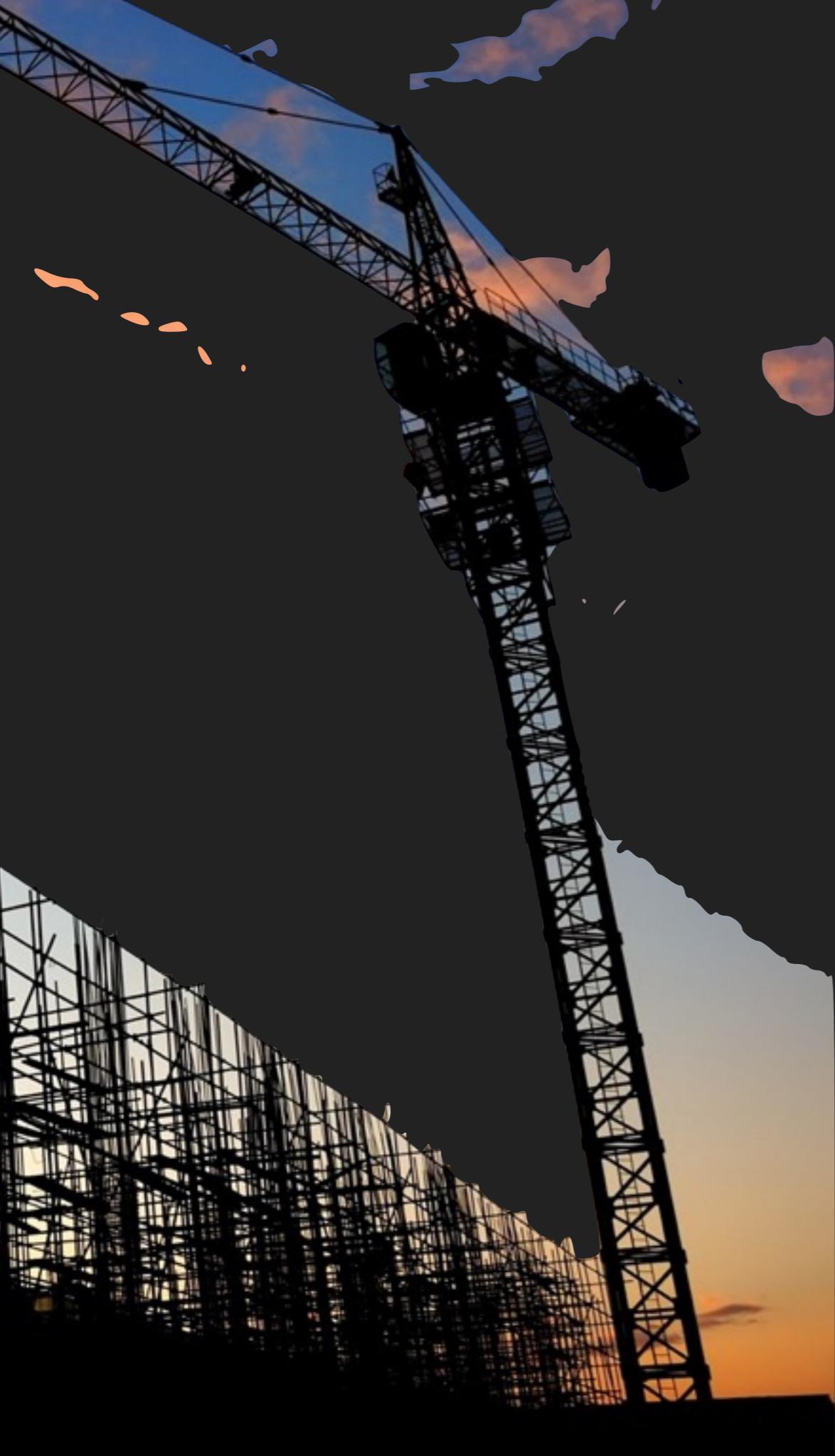
Voir guide de recommandations: [ANSSI](#), [NIST](#), [CERT-FR](#)

NIST FRAMEWORK

FUNCTION	CATEGORIES
IDENTIFY	Identification of Assets & Services
IDENTIFY	Identification of Business Env.
IDENTIFY	Identification of risks
IDENTIFY	Identification of Vulnerabilities
PROTECT	Protection against eavesdropping
PROTECT	Protection against Denial of Service
PROTECT	Protection against intrusion
PROTECT	Protection against data theft & data alteration
PROTECT	Protection against tampering
DETECT	Traceability Management
DETECT	Security Mgt
DETECT	Detection
RESPOND	Respond
RECOVER	Recover

MATURITÉ DES DÉFENSES





PRINCIPES D'ARCHITECTURE

SÉCURITÉ DES ARCHITECTURES LAMBDA

PRINCIPES D'ARCHITECTURE

Concepts :

Résilience, Urbanisation, Sécurité, Automatisation

Contraintes :

Budgets, Planning, Exigences (sécurité, technique, cliente)

Méthode :

Design to COST

RÉPONDRE AUX BESOINS MÉTIERS

CONCEPTS

Résilience:

Capacité à tolérer les pannes & dysfonctionnement.

A l'extrême :

- ▶ PRA : Plan de Reprise d'activité
- ▶ PCA : Plan de Continuité d'activité
- ▶ DR : Disaster Recovery

Moyens:

- ▶ Clusterisation des applications et des systèmes (**noeuds passif & actif**)
- ▶ Redondances des données, des réseaux et du matériels
- ▶ Sauvegarde les données
- ▶ Virtualisation & équilibrage de charge
- ▶ Réplique des disques durs, Doubles alimentation, ...

CONCEPTS

Automatisation & Déploiement Continu:

Piloter & orchestrer de façon automatique le système, permettant la construction de façon automatique.

« Plus rapide de réinstaller from scratch que de mettre à jour ou de réparer »

MCO & Supports : Maintien en Condition Opérationnel

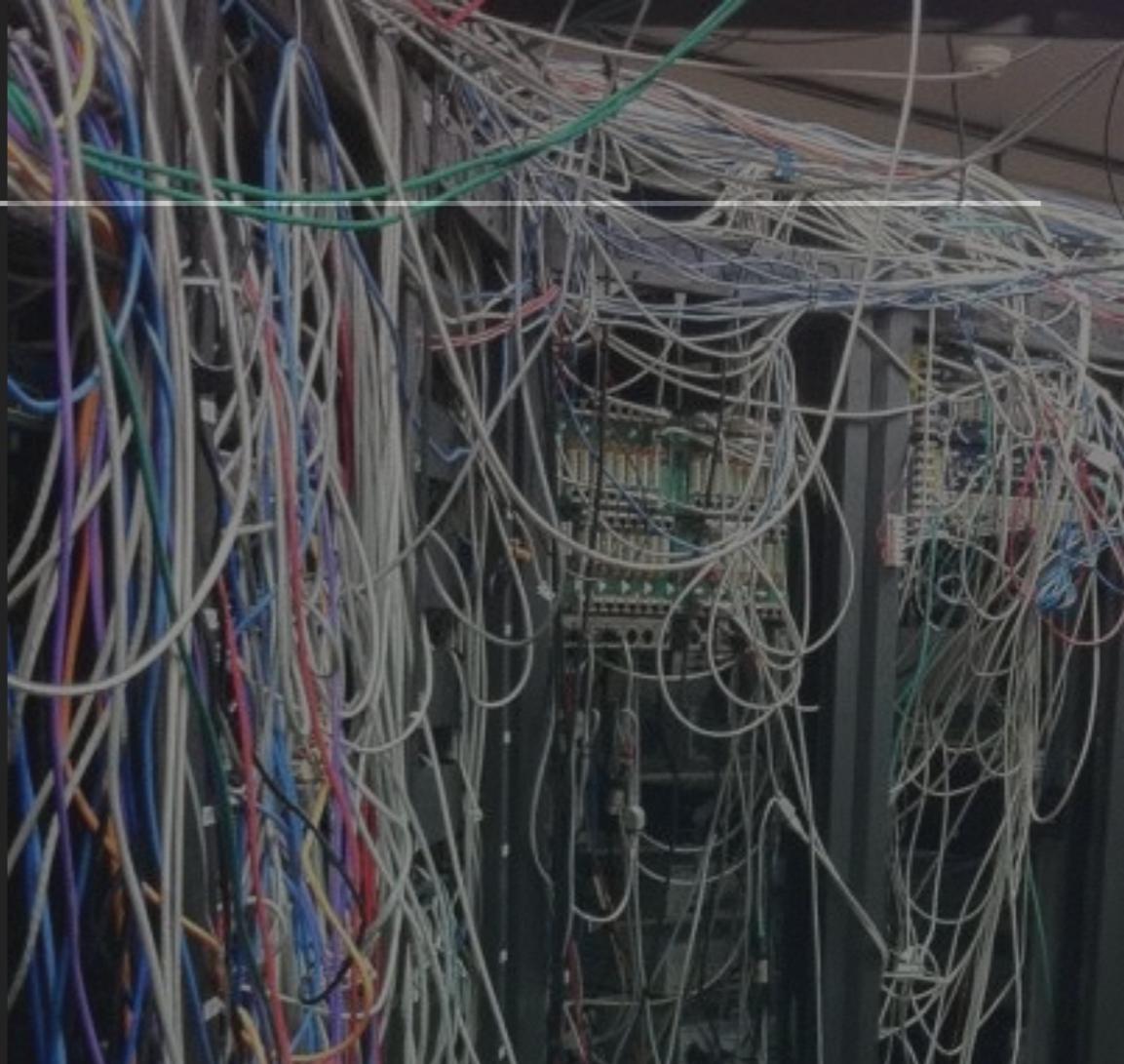
Mise à jour du système et des applications,
SLA & GTR, Cycle de vie des applicatifs, du système et du matériel

URBANISATION

Du Datacenter et des baies

Prévoir la scalabilité horizontale et verticale du système d'un point de vue :

- ▶ physique
- ▶ réseaux
- ▶ applicatifs



CONCEPTS

Technologies

Haute disponibilité

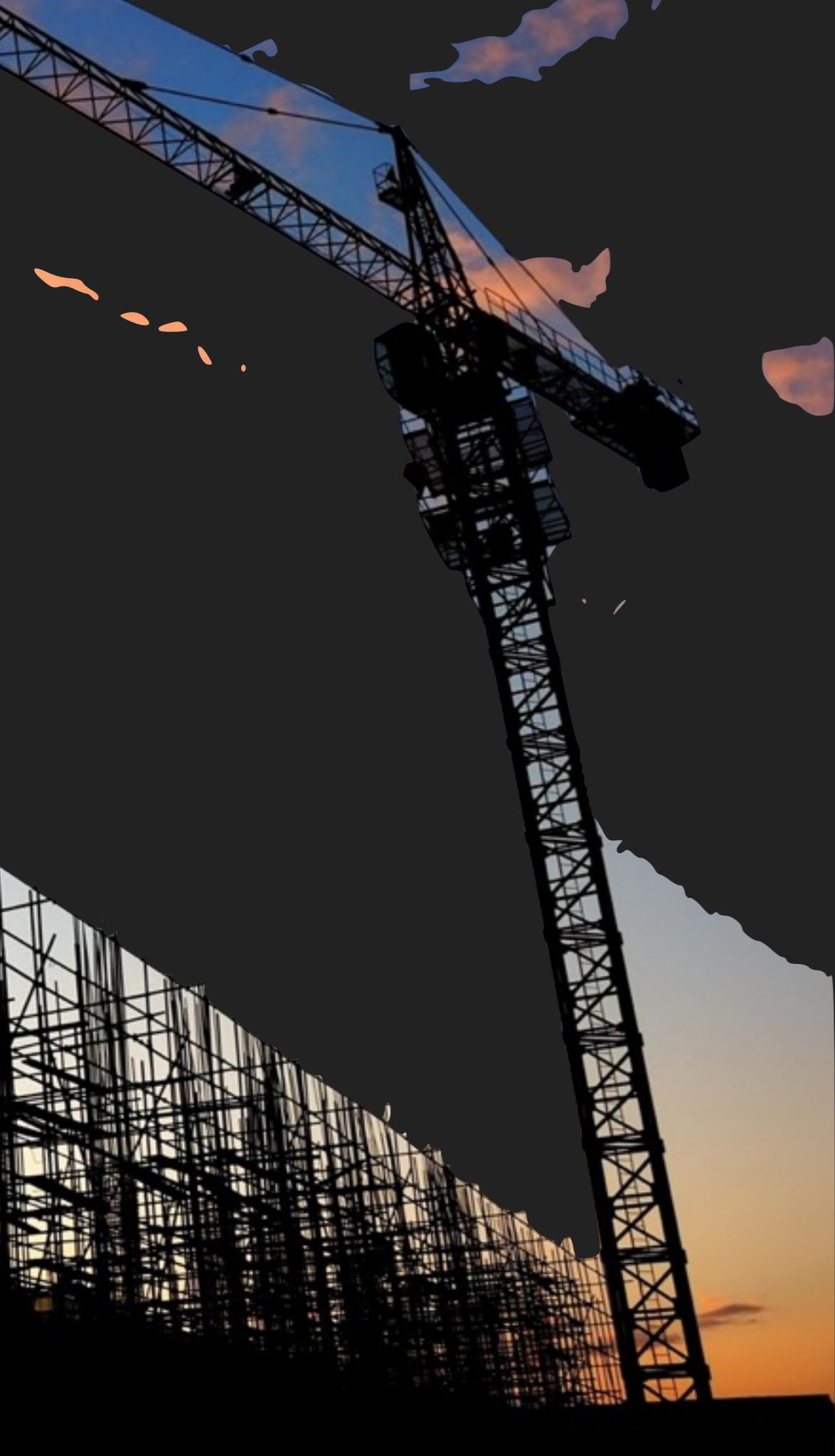
Corosync, Pacemaker, HeartBeat,
Apache load balancing, cluster
applatif, migration de machine
virtuelle, bonding des cartes
réseaux

Automatisation

ANSIBLE, Puppet

Virtualisation

KVM, VMWare, VirtualBox, LXC,
Docker, Openstack, SaaS



CONSTRUCTION D'UNE ARCHITECTURE

SÉCURITÉ DES ARCHITECTURES LAMBDA

CONSTRUCTION D'UNE ARCHITECTURE

Plan technique

- ▶ BOM : Built Of Material
- ▶ Architecture Physique
- ▶ Architecture Fonctionnelle
- ▶ Plan de Rackage & Cablage
- ▶ Matrice des flux

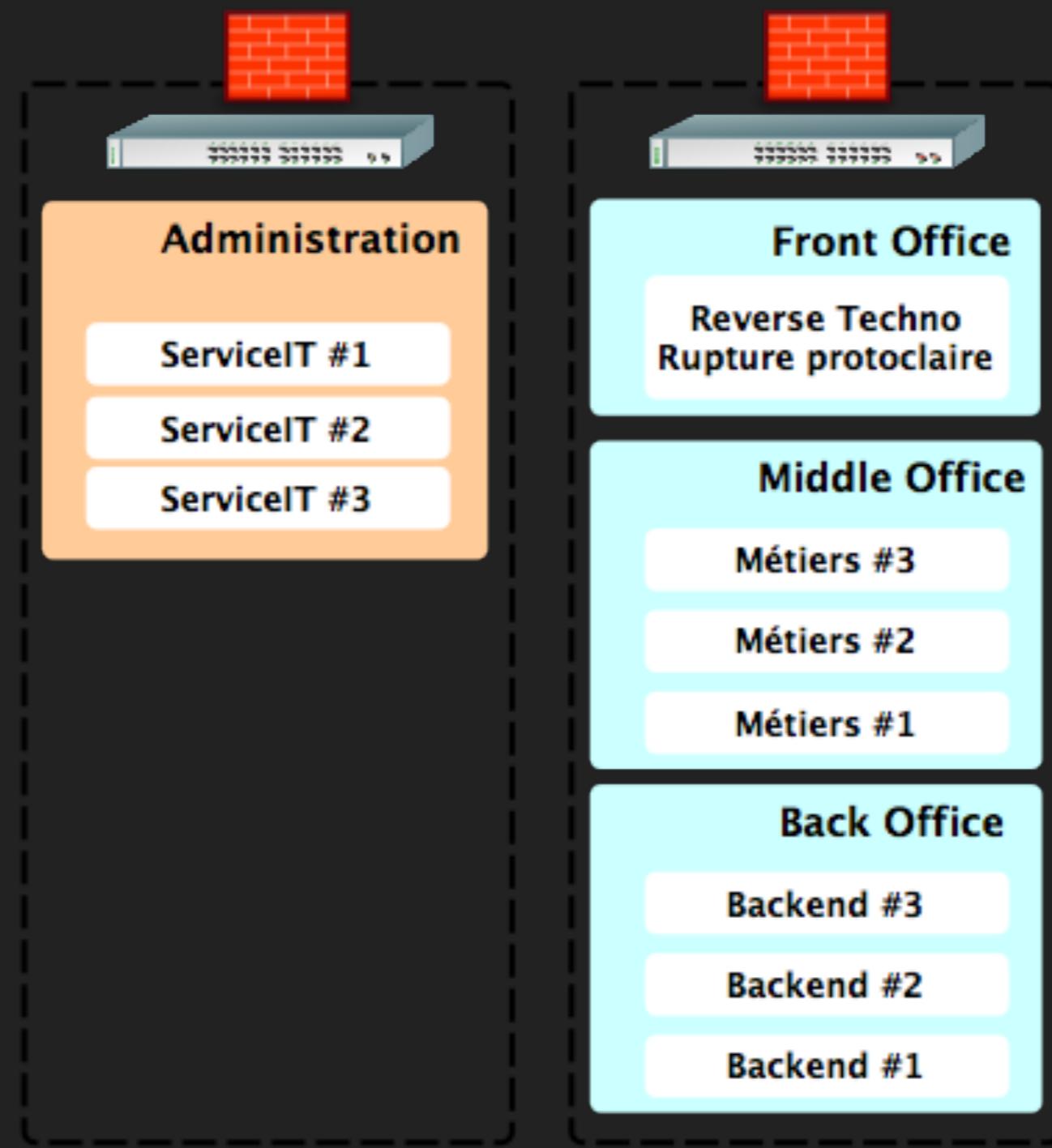
Sécurité

- ▶ Analyse de risque
- ▶ Analyse des vulnérabilités (pentest + analyses CVE)
- ▶ Stratégie de détection d'intrusion

Documentation:

- ▶ Spécifications systèmes
- ▶ Documentation utilisateurs, administrateurs
- ▶ Validation et recette

ARCHI FONCTIONNELLE + PHYSIQUE



MERCI !